COPIA DELL'ORIGINALE DI DECRETO DEL PRESIDENTE

n. 39 **del 30.12.2016**

Oggetto: Approvazione del Manuale per la Gestione Documentale adottato ai sensi del D.Lgs 82/2005, dell'art 3, comma d) del DPCM 3 dicembre 2013 (recante le regole tecniche per il protocollo informatico) e del DPCM 3 dicembre 2013 (recante le regole tecniche per la conservazione).

DOCUMENTO ISTRUTTORIO

Oggetto: Approvazione del Manuale per la Gestione Documentale adottato ai sensi del D.Lgs 82/2005, dell'art 3, comma d) del DPCM 3 dicembre 2013 (recante le regole tecniche per il protocollo informatico) e del DPCM 3 dicembre 2013 (recante le regole tecniche per la conservazione)..

IL DIRETTORE

RICHIAMATI il DPR 445/2000 (Testo unico in materia di documentazione amministrativa), il D.Lgs 82/2005 (Codice dell'amministrazione digitale) ed il DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) in base ai quali le pubbliche amministrazioni devono adottare un Manuale di gestione documentale;

ATTESO che con Decreto del Presidente n. 27 del 15/09/2016 è stata individuata un'unica area organizzativa omogenea (AOO) ed è stato istituito all'interno dell'Area Amministrativa l'Ufficio Gestione documentale responsabile della tenuta del protocollo informatico e della gestione dei flussi documentali e degli archivi e con Decreto n. 35 del 30/12/2016 è stato nominato il responsabile della Gestione documentale la figura del Responsabile della gestione documentale;

RICHIAMATA la determinazione della Direzione n. 48 del 07/04/2016 con la quale è stato acquisito un servizio archivistico di supporto alla struttura dell'ente per redigere il Manuale di gestione documentale (EBLA Soc. Coop – dott.ssa Allegra Paci);

VISTO il Manuale di gestione documentale redatto dagli uffici preposti in collaborazione con l'archivista dott.ssa Allegra Paci della EBLA Soc. Coop, comprensivo dei seguenti allegati:

- Allegato 1 Definizioni, norme e regole di riferimento
- Allegato 2 Area organizzativa omogenea, atto di istituzione del servizio gestione informatica e documentale e atto di nomina del RGD
- Allegato 3 Modello di carta intestata
- Allegato 4 Contratto Gestore Posta Elettronica Certificata
- Allegato 5 Elenco titolari di firma digitale, degli indirizzi di posta elettronica certificata e di posta elettronica dell'Ente
- Allegato 6 Timbri ed etichette in uso

- Allegato 7 Modello di Registro di emergenza
- Allegato 8 Titolario di classificazione
- Allegato 9 Incaricati al trattamento dei documenti amministrativi
- Allegato 10 Linee guida per la fascicolazione
- Allegato 11 Modello di Camicia di fascicolo cartaceo
- Allegato 12 Convenzione Regione Marche e disciplinare tecnico per il servizio di conservazione sostitutiva
- Allegato 13 Manuale dei processi per la conservazione digitale
- Allegato 14 Piano di conservazione
- Allegato 15 Piano per la sicurezza informatica

ATTESO che tale manuale detta le regole per una corretta gestione del Sistema di gestione documentale ed in particolare del protocollo informatico, della fascicolazione e successiva conservazione dei documenti amministrativi;

TUTTO CIÒ PREMESSO;

VISTI:
- il DPR 445/2000;
- il D.Lgs. 82/2005 e s.m.i.;
- il DPCM 3/12/2013" Regole tecniche protocollo informatico"
- il D.Lgs. n. 267/2000
- il D.Lgs. n. 165/2001;
- il D.Lgs. n. 150/2009,e ss.mm.ii.;
- il D.L. n. 78/2010 convertito, con modificazioni, dalla L. n. 122/2010;
- il D.L. n. 90/2014 convertito in L. n. 114/2014;
- il D.Lgs. n. 81/2015;
- il vigente Regolamento di organizzazione;
- il parere favorevole, riportato in calce, in ordine alla regolarità tecnica di cui all'art. 49, co. 1, del D.Lgs. n. 267/2000;

PROPONE

1) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2) Di approvare il Manuale di gestione documentale allegato al presente atto per farne parte integrante e sostanziale, corredato dai seguenti documenti:
   - Allegato 1 Definizioni, norme e regole di riferimento
   - Allegato 2 Area organizzativa omogenea, atto di istituzione del servizio gestione informatica e documentale e atto di nomina del RGD
   - Allegato 3 Modello di carta intestata
   - Allegato 4 Contratto Gestore Posta Elettronica Certificata
   - Allegato 5 Elenco titolari di firma digitale, degli indirizzi di posta elettronica certificata e di posta elettronica dell'Ente
   - Allegato 6 Timbri ed etichette in uso
   - Allegato 7 Modello di Registro di emergenza
   - Allegato 8 Titolario di classificazione
   - Allegato 9 Incaricati al trattamento dei documenti amministrativi

- Allegato 10 Linee guida per la fascicolazione
- Allegato 11 Modello di Camicia di fascicolo cartaceo
- Allegato 12 Convenzione Regione Marche e disciplinare tecnico per il servizio di conservazione sostitutiva
- Allegato 13 Manuale dei processi per la conservazione digitale
- Allegato 14 Piano di conservazione
- Allegato 15 Piano per la sicurezza informatica

3) Di dichiarare, riscontrata l'urgenza del caso, immediatamente eseguibile il Decreto di approvazione del presente documento istruttorio, ai sensi dell'art. 134, co. 4 del D.Lgs. 267/2000.

Jesi, 30.12.2016

La Direzione
F.to dott.ssa Elisabetta Cecchini

MANUALE
DI
GESTIONE DOCUMENTALE

(Approvato con …….. n. … del ……..)

Rev. Aggiornata al 30/12/2016

Sommario

TITOLO I - AMBITO DI APPLICAZIONE E DEFINIZIONI

Art. 1 - Ambito di applicazione del manuale

1. Il presente manuale di gestione documentale è adottato ai sensi dell'art 3, comma d) del DPCM 3 dicembre 2013, recante le regole tecniche per il protocollo informatico e del DPCM 3 dicembre 2013 recante le regole tecniche per la conservazione.
2. Il manuale descrive le attività di formazione, registrazione, classificazione, fascicolazione e conservazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi dell'Assemblea Territoriale d'Ambito ATO 2 Ancona (di seguito ATA).
3. Attraverso l'integrazione del protocollo informatico e dei repertori con le procedure di gestione dei provvedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti si è realizzato il Sistema di gestione documentale che ha lo scopo di migliorare sia il flusso informativo e documentale interno dell'Amministrazione che la trasparenza dell'azione amministrativa.
4. In estrema sintesi il presente manuale descrive il sistema di gestione, anche ai fini della conservazione, dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Disciplina altresì:
   - i livelli di esecuzione, le responsabilità ed i metodi di controllo di processi e azioni amministrative;
   - l'uso del titolario di classificazione e del Piano di conservazione;
   - le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo ed interesse in attuazione della trasparenza dell'azione amministrativa;
   - la conservazione, gestione e accesso agli archivi degli ex Consorzi di Bacino a cui è subentrata l'ATA, a far data dall'acquisizione degli stessi.

Art. 2 – Definizioni, norme e regole di riferimento

1. Per le definizioni e i riferimenti normativi si rimanda all'*Allegato 1 – Definizioni,* n*orme e regole di riferimento.*
2. Gli acronimi utilizzati nel testo sono i seguenti:

   - **ATA** – Assemblea Territoriale d'Ambito
   - **AOO** - Area Organizzativa Omogenea;
   - **RGD** – Responsabile della Gestione Documentale;
   - **RSPP** – Responsabile Servizio Prevenzione Protezione;

TITOLO II DISPOSIZIONI GENERALI

Art. 3 - Area Organizzativa Omogenea

Come modello organizzativo l'ATA ha individuato un'unica Area Organizzativa Omogenea (AOO), descritta nell'*Allegato 2 – Area Organizzativa Omogenea, atto di istituzione del servizio di gestione informatica e documentale e atto di nomina del RGD*, composta dall'insieme delle sue unità organizzative che usufruiscono in modo omogeneo e coordinato dei servizi per la gestione dei flussi documentali ed in particolar modo dell'Ufficio di gestione documentale incaricato della protocollazione dei documenti.

Art. 4 - Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

1. Nell'Area Organizzativa Omogenea è stato istituito con Decreto del Presidente il Servizio per la tenuta del protocollo informatico e della gestione dei flussi documentali e degli archivi, denominato Ufficio di Gestione Documentale, della gestione dei flussi documentali e degli archivi, cui è preposto un responsabile (RGD), *vedi Allegato 2* - al presente manuale.
2. Al Responsabile della gestione documentale (RGD) è demandata la verifica del corretto funzionamento del sistema e del suo utilizzo da parte degli utilizzatori abilitati.
   Lo stesso:
   - attribuisce il livello di autorizzazione per l'accesso alle funzioni del sistema di protocollo informatico, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
   - garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
   - garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo;
   - cura le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
   - conserva le copie dei dati di protocollo e dei documenti archiviati su supporto informatico, in luoghi sicuri e differenti;
   - garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso in base alla normativa vigente;
   - autorizza le operazioni di annullamento delle registrazioni di protocollo;
   - vigila sull'osservanza delle disposizioni del presente manuale da parte del personale autorizzato e degli incaricati.
   - provvede alla pubblicazione del manuale di gestione sul sito istituzionale dell'ATA;
   - predispone gli aggiornamenti del manuale secondo le modalità di revisione previsti all'art. 75;
   - predispone, con i necessari supporti esterni ed in collaborazione con il RSPP e il responsabile dei servizi informatici, il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla

conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato nell'allegato B del DLgs 196/2003 e successive modificazioni, con il supporto del responsabile della conservazione, del responsabile del servizioinformatico e del responsabile del trattamento dei dati personali di cui al suddetto decreto;

- provvede ad aprire e chiudere il registro di protocollazione di emergenza;
- aggiorna costantemente le procedure attuative del presente manuale;

3. Il Responsabile del Sistema di gestione documentale (RGD) è, nominato con Decreto del Presidente (*Allegato 2 - Area organizzativa omogenea, atto di istituzione del servizio gestione informatica e documentale e atto di nomina del RGS*).
4. Al Responsabile della gestione documentale sarà garantita la necessaria formazione tecnico archivistica come prescritto dalla disciplina vigente.
5. L'Ufficio Gestione documentale cura la conservazione, l'accesso, la movimentazione del materiale documentario; provvede al reinserimento dei documenti cartacei ricevuti nei rispettivi fascicoli; provvede inoltre alla redazione degli elenchi di scarto e al versamento in archivio storico della documentazione destinata a conservazione illimitata.

Art. 5 - Unicità e funzionalità del sistema di protocollo informatico

1. Nell'ambito della AOO il sistema di protocollo informatico è unico e la numerazione progressiva delle registrazioni di protocollo è unica, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

2. Con l'adozione del presente manuale si è verificata l'inesistenza di altri protocolli oltre al protocollo informatico, come previsto dal Testo unico e dalle Regole tecniche.

3. Il sistema di protocollo informatico adottato dall'ATA garantisce la "funzionalità minima" indicata dalle norme vigenti; eventuali funzionalità aggiuntive condivideranno con la funzionalità minima almeno i dati identificativi dei documenti.

4. Con l'adozione del protocollo informatico unico:

- Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.
- Non è consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.
- Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.
- Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

Art. 6- Modello operativo adottato per la gestione dei documenti

Per la gestione dei documenti è adottato un modello operativo di tipo decentrato che prevede la partecipazione attiva di più soggetti a cui sono attribuite competenze diverse

per la ricezione, registrazione, classificazione e fascicolazione, l'assegnazione dei documenti e la trasmissione (vedi *Allegato 9 Incaricati al trattamento dei documenti amministrativi*).

TITOLO III - FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Art. 7 - Flusso di lavorazione dei documenti in partenza

Le fasi della gestione dei documenti spediti sono:

- formazione (cfr. Tit. IV);
- classificazione (cfr. Tit. VIII);
- fascicolazione (cfr. Tit. X);
- assegnazione (cfr. Tit. IX);
- registrazione e segnatura di protocollo (cfr. VII);
- trasmissione (cfr. Tit. V).

Art. 8 - Flusso di lavorazione dei documenti interni

Le fasi della gestione dei documenti interni sono:

- formazione (cfr. Tit IV);
- classificazione (cfr. Tit. VIII);
- fascicolazione (cfr. Tit. X);
- assegnazione (cfr. Tit. IX);
- registrazione e segnatura di protocollo (cfr. VII);

Art. 9 - Flusso di lavorazione dei documenti in arrivo

Le fasi della gestione dei documenti ricevuti sono:

- ricezione (cfr. Tit VI);
- scansione, se si tratta di documenti su supporto cartaceo (cfr. Tit. VI art. 2);
- classificazione (cfr. Tit. VIII);
- assegnazione (cfr. Tit. IX);
- registrazione e segnatura di protocollo (cfr. VII);
- fascicolazione (cfr. Tit. X);

TITOLO IV – FORMAZIONE DEI DOCUMENTI AMMINISTRATIVI

Art. 10 - Modalità di formazione dei documenti amministrativi e contenuti minimi

1. I documenti possono essere analogici o digitali. Quando sono prodotti con sistemi informatici, devono rispettare le disposizioni dell'articolo 40 del CAD e s.m.i. e le Regole tecniche.

2. I documenti in partenza od interni sono di norma documenti digitali.

3. Le regole per la determinazione dei contenuti e della struttura dei documenti sono definite dal Responsabile del Servizio Archivio e protocollo sulla base del modello di carte intestata di cui all'*Allegato 3 – Modello di carta intestata*, che contiene logo, denominazione completa dell'ente, servizio e nominativo del responsabile indirizzo completo a cui vanno aggiunte le seguenti informazioni:

- Data completa con luogo, giorno, mese, anno;
- N. di allegati
- La classificazione: titolo/classe, numero di fascicolo;
- Oggetto del documento che risponda a criteri di sinteticità e chiarezza in merito al contenuto;
- Sigla del responsabile dell'istruttoria ed eventuale collaboratore;
- Sottoscrizione del responsabile del procedimento amministrativo e/o del Direttore.

Art. 11 - Modalità di formazione e gestione di copie dei documenti

1. Per i documenti cartacei (analogici) si considera originale quello cartaceo stampato su carta intestata o semplice, dotato di firma autografa.
2. Un documento cartaceo (analogico) può essere riprodotto in documento informatico tramite opportune procedure di scansione, come da art. 19 c. 2 del presente manuale.
3. Le copie digitali dei documenti cartacei non hanno, al momento, alcun valore legale e probatorio, non sono cioè assimilabili alle copie conformi.

Art. 12 Formato dei documenti digitali

1. I documenti digitali prodotti dall'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma digitale, sono convertiti in formati standard al fine di garantire la leggibilità per altri sistemi e la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.
2. I formati standard adottati dall'Amministrazione sono quelli previsti all'allegato 2 del DPCM 3 dicembre 2013, di cui verranno recepiti gli aggiornamenti periodici emessi con delibera dall'Agenzia per l'Italia digitale.
3. I metadati associati al documento informatico sono quelli prescritti dall'allegato 5 del DPCM 3 dicembre 2013 per il documento informatico amministrativo ai sensi degli articoli 9 e 19 delle regole tecniche per il protocollo informatico di cui al DPCM 31 ottobre 2000 e descritti nella Circolare AIPA del 7 maggio 2001, n.28;

Art. 13 Sottoscrizione dei documenti informatici

1. L'Amministrazione si avvale dei servizi di certificatori accreditati ai sensi della normativa vigente.
2. Per la formazione dei documenti informatici per i quali non è prescritta la sottoscrizione, si utilizzano i servizi di riconoscimento, autenticazione e crittografia disponibili sulla rete dell'Amministrazione.
3. Ai sensi dell'articolo 3 della Circolare n. 60 del 23 gennaio 2013 dell'Agenzia per l'Italia digitale i documenti informatici per i quali è obbligatoria l'apposizione di una firma digitale e/o qualificata sono i seguenti:

   - Deliberazioni dell'Assemblea;
   - Decreti del Presidente;
   - Contratti;
   - Provvedimenti di liquidazione e mandati di pagamento;
   - Tutti gli atti inviati tramite posta elettronica certificata. Eventuali deroghe necessarie per il funzionamento dell'ente devono risultare da apposita determinazione del direttore.

TITOLO V – TRASMISSIONE DEI DOCUMENTI

Art. 14 – Trasmissione dei documenti

1. L'Amministrazione si avvale di un servizio di "posta certificata", conforme alle regole tecniche emanate da AgID, offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche (*Allegato 4 – Contratto Gestore posta elettronica certificata*) collegato al protocollo informatico.
2. I documenti digitali, compresi di eventuali allegati, anch'essi digitali, sono inviati attraverso la procedura prevista dal protocollo informatico per mezzo della posta elettronica certificata; solo in via residuale con posta elettronica non certificata; se la dimensione del documento supera la dimensione massima dei messaggi stabilita dal sistema di posta utilizzata dall'Amministrazione si predispongono invii multipli;
3. Il documento informatico trasmesso per via telematica si intende inviato al destinatario se trasmesso all'indirizzo elettronico da questi indicato, e pervenuto dopo aver ricevuto notifica di consegna da parte del gestore di posta elettronica certificata.
4. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni correnti, sono opponibili ai terzi.
5. La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.
6. La trasmissione del documento può avvenire mediante cooperazione applicativa ai sensi del DPR 11 febbraio 2005, n. 68, artt. 16 e 17 delle Regole tecniche e della Circolare n. 60 del 23 gennaio 2013 in presenza di apposite convenzioni con altri enti pubblici.
7. La trasmissione interna di documenti protocollati avviene di norma tramite la procedura di assegnazione del protocollo informatico ovvero ove non tecnicamente possibile, tramite le caselle istituzionali di posta elettronica di cui all'art. 16 ed all'*Allegato 5 - Elenco titolari di firma digitale, degli indirizzi di posta elettronica certificata e di posta elettronica dell'Ente*.
8. Qualora si debba trasmettere un documento cartaceo, lo stesso va di norma redatto in due esemplari: la minuta che rimane all'Ufficio Gestione documentale ed inserita nel fascicolo annuale dei documenti cartacei e l'originale che viene spedito;
9. Qualora i destinatari siano più di uno, è autorizzata la spedizione di più originali dello stesso documento
10. Qualora i destinatari dei documenti in partenza siano molteplici è attribuito un unico numero di protocollo a documenti identici in partenza. In tal caso è anche possibile la spedizione di copie dell'originale.
11. L'Ufficio Gestione documentale provvede alla trasmissione del documento in partenza, cioè alla sua spedizione, di norma e compatibilmente con la mole dei documenti da inviare entro le 24 ore successive.
12. Il documento cartaceo viene comunque acquisito nel protocollo informatico dopo la sua scansione (art. 11 e art. 19 c.2).

Art. 15 - Inserimento delle ricevute di trasmissione nel fascicolo

1. L'Ufficio Gestione documentale provvede ad abbinare le ricevute digitali alla registrazione di protocollo e, se il documento protocollato è già inserito in un fascicolo, le ricevute sono automaticamente conservate insieme ad esso.
2. Analogamente nel caso di trasmissione di documenti cartacei, l'Ufficio Gestione documentale provvede ad abbinare le ricevute alla minuta del documento e quindi a conservarle all'interno del fascicolo annuale dei documenti cartacei da esso detenuto, oltre ad inserirle nel protocollo informatico dopo la relativa scansione.

Art. 16 – Caselle di posta elettronica istituzionali

L'Amministrazione ha assegnato ad ogni singolo dipendente una casella di posta elettronica istituzionale per finalità amministrative su cui si veicolano le comunicazioni interne e quelle verso l'esterno dell'AOO *(Vedi Allegato 5 – Elenco titolari di firma digitale, degli indirizzi di posta elettronica certificata e di posta elettronica dell'Ente).*

Art. 17 - Caselle di posta elettronica certificata

1. Il servizio di posta certificata è strettamente correlato all'Indice IPA, poiché in esso sono pubblicati gli indirizzi di posta certificata istituzionali associati alle AOO *(Vedi Allegato 5 – Elenco titolari di firma digitale, degli indirizzi di posta elettronica certificata e di posta elettronica dell'Ente).*

Art. 18 – Utilizzo del fax

1. L'articolo 14 della legge n. 98/2013, di conversione del Decreto Legge n. 69/2013, impone che le comunicazioni tra Pubbliche Amministrazione dovranno avvenire esclusivamente per via telematica, andando a modificare l'art. 47 del CAD, per cui l'uso del fax per inviare documenti in uscita avviene solo se non vi è altra possibilità.

TITOLO VI – RICEZIONE DEI DOCUMENTI

Art. 19 – Ricezione dei documenti su supporto cartaceo

1. I documenti su supporto cartaceo possono pervenire attraverso:
   - servizio postale tradizionale o corriere;
   - fax;
   - consegna diretta all'Ufficio Gestione documentale da parte dell'interessato o persona delegata.
2. Di tutti i documenti cartacei provenienti in formato inferiore o uguale ad A3 viene effettuata la riproduzione digitale con l'ausilio dello scanner; tale copia viene inserita nel protocollo informatico al fine di ridurre i tempi di smistamento e facilitare i procedimenti e per ridurre la riproduzione cartacea dei documenti quando non necessario (come previsto all'art. 11 comma 2).
3. Come indicato all'art. 11 c. 3 e copie digitali dei documenti cartacei non hanno, al momento, alcun valore legale e probatorio, non sono cioè assimilabili alle copie conformi.
4. Se il documento cartaceo ha una rilevante consistenza o formati diversi dai precedenti, viene acquisito in formato immagine solo se esplicitamente richiesto dal Responsabile del servizio di competenza, avvalendosi eventualmente dei servizi di una struttura esterna specializzata. In questo caso il Responsabile del Servizio, insieme al Responsabile del procedimento, se figura non coincidente, individua i documenti da sottoporre al processo di scansione e ne fissa i tempi, diversi da quelli ordinari, e le modalità esecutive.
5. Di norma gli originali sono detenuti dall'Ufficio Gestione documentale che avrà cura di inserirli nel fascicolo unico annuale cartaceo detenuto dallo stesso.
6. I documenti che non vengono scannerizzati sono trasmessi al Responsabile del procedimento lasciandone traccia nella registrazione di protocollo e nel fascicolo annuale dei documenti cartacei.
7. La copia digitale dei documenti registrati viene invece inoltrata ai destinatari mediante la procedura di assegnazione prevista dal Protocollo informatico. Sarà cura dei destinatari inserire le copie digitali nei rispettivi fascicoli digitali detenuti dagli stessi,

Art. 20 – Modalità di svolgimento del processo di scansione

1. Il processo di scansione avviene in diverse fasi:
   - acquisizione delle copie per immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico file;
   - verifica della leggibilità e qualità delle copie per immagini acquisite;
   - collegamento delle copie per immagini alle rispettive registrazioni di protocollo.

Art. 21 - Errata ricezione di documenti cartacei

1. Nel caso in cui pervengano all'Amministrazione documenti erroneamente indirizzati, se dall'indirizzo della busta si capisce a quale destinatario devono essere inoltrati, questi vengono rinviati al destinatario/mittente apponendo sulla busta la dicitura, "Corrispondenza pervenuta per errore - non di competenza di questa Amministrazione".

2. Nella circostanza in cu i venga erroneamente aperta una lettera destinata ad altri soggetti, questa viene richiusa e rispedita al destinatario, scrivendo sulla busta la dicitura "Corrispondenza pervenuta ed aperta per errore dall'Amministrazione" con timbro.

3. Nel caso in cui venga erroneamente protocollato un documento non indirizzato all'Amministrazione, l'addetto al protocollo, su autorizzazione del Responsabile del Servizio, provvede all'annullamento del protocollo, specificando che è di competenza di un'altra Amministrazione. Il documento oggetto della rettifica viene inviato al destinatario con la dicitura "protocollato per errore".

Art. 22 - Rilascio di ricevute attestanti la ricezione di documenti cartacei

1. Quando il documento cartaceo viene consegnato direttamente dal mittente o da altra persona incaricata e venga richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, solo l'Ufficio Gestione documentale è autorizzato a:

- fotocopiare la prima pagina del documento;
- apporre il timbro dell'Ente con la data di consegna e la sigla del ricevente;
- apporre gli estremi della segnatura se contestualmente alla ricezione avviene anche la protocollazione.

Art. 23 - Istanze massive di procedimenti con scadenza

1. La corrispondenza riportante l'indicazione "offerta" - "gara d'appalto" o simili, o comunque dalla cui confezione si evince la partecipazione ad una gara, non viene aperta, ma viene protocollata in arrivo con l'apposizione della data e dell' ora e dei minuti di arrivo direttamente sulla busta, plico o simili (ovvero apponendo l'etichetta) e viene conservata agli atti fino alla data di scadenza presentazione; di tutti i documenti pervenuti viene elaborato un elenco che viene consegnato, corredato dai documenti stessi, i al Responsabile del servizio competente.

2. È compito di tale Responsabile provvedere alla custodia delle buste o dei contenitori in genere protocollati, con mezzi idonei, sino all'espletamento della gara stessa.

3. Dopo l'apertura delle buste è cura del Responsabile del procedimento della gara riportare gli estremi di protocollo riportati sulla confezione esterna su tutti i documenti in esse contenuti.

4. Per motivi organizzativi i responsabili dei servizi sono tenuti ad informare preventivamente l'Ufficio Gestione documentale in relazione alle scadenze di selezioni, gare o bandi di ogni genere.

5. Alla corrispondenza consegnata con rimessa diretta dell'interessato o persona delegata può essere data ricevuta di avvenuta consegna con apposito timbro di avvenuta ricezione riportato in *Allegato 6 – Timbri ed etichette in uso*.

6. In caso di eccessivo carico, i documenti ricevuti con rimessa diretta saranno accantonati e protocollati in differita e al mittente viene rilasciata ugualmente ricevuta senza gli estremi del protocollo (timbro datario), ma parimenti valida per la finalità perseguita.

7. Nel caso in cui sia prevista la ricezione di istanze di gara anche tramite pec l'addetto dovrà protocollare senza aprire gli allegati. A tal fine sarà predisposta una procedura idonea a garantire la segretezza dell'offerta resa nota nel disciplinare di gara. Di tale procedura, approvata con la determinazione a contrarre, dovrà esserne data specifica comunicazione all'Ufficio Gestione documentale.

Art. 24 – Ricezione dei documenti digitali

1. I documenti informatici possono pervenire a mezzo:
   - posta elettronica certificata
   - posta elettronica,
   - sportello telematico,
   - fax informatico
   - rimessa diretta di supporto di memorizzazione di massa da parte dell'interessato o persona delegata all'Ufficio Gestione documentale e/o all'URP.

2. Il Responsabile del Servizio per la tenuta del Protocollo informatico provvede a rendere pubblico l'indirizzo della casella di posta utilizzando ogni possibile mezzo e all'iscrizione all'Indice delle amministrazioni pubbliche e delle aree organizzative omogenee, ai sensi dell'articolo 12, comma 2, lettera c, del DPCM 31 ottobre 2000 e s.m.i.
3. I documenti informatici che pervengono direttamente ai singoli servizi sono da questi valutati ai sensi dell'articolo 15, comma 7, del DPCM 31 ottobre 2000 e s.m.i e, se soggetti a registrazione di protocollo o ad altra forma di registrazione, immediatamente inviati all'Ufficio Gestione documentale per la registrazione.
4. Tutti i documenti digitali provenienti dall'esterno sono considerati legalmente validi e sono protocollati se soddisfano i requisiti previsti dalla normativa vigente in materia, ossia se i metadati associati al documento informatico sono quelli prescritti dall'allegato 5 del DPCM 3 dicembre 2013 per il documento informatico amministrativo ai sensi degli articoli 9 e 19 delle regole tecniche per il protocollo informatico di cui al DPCM 31 ottobre 2000 e descritti nella Circolare AIPA del 7 maggio 2001, n.28;. Nel caso in cui il documento pervenuto sia privo dei suddetti requisiti sarà cura del Responsabile del procedimento amministrativo di competenza valutarne la sua validità ed a inviarlo con la mail dedicata al Sistema di gestione documentale per la sua successiva registrazione al Protocollo.

Art. 25 - Errata ricezione di documenti digitali

1. Nel caso in cui pervengano sulla casella di posta istituzionale dell'Amministrazione (certificata o meno) o in una casella non istituzionale messaggi dal cui contenuto si rilevi che sono stati erroneamente ricevuti, l'addetto protocollatore rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore - non di competenza di questa Amministrazione". Il documento se già protocollato, viene annullato.

Art. 26 –Rilascio di ricevute attestanti la ricezione dei documenti digitali

1. Alla ricezione di un documento digitale soggetto a protocollo viene generato un messaggio di ritorno a scopo informativo, scambiato attraverso i medesimi mezzi di comunicazione previsti per i messaggi protocollati in uscita, solo su richiesta del mittente.

2. Nei casi in cui il messaggio - giunto tramite PEC - presenti anomalie, viene inviato al mittente uno dei seguenti *messaggi di notifica di eccezione:*

a) il messaggio protocollato è corrotto;
b) uno dei documenti informatici inclusi non è leggibile;
c) la segnatura informatica non è leggibile;
d) manca la corretta indicazione dei riferimenti esterni;
e) la descrizione del messaggio protocollato riportata nella segnatura informatica non corrisponde alla struttura di codifica;
f) il formato della segnatura informatica non è conforme ai formati previsti nel manuale di gestione documentale adottato dall'ATA;
g) la descrizione del destinatario contenuta nella segnatura informatica è errata;
h) il formato della segnatura di protocollo non contiene informazioni dichiarate obbligatorie previste nell'ambito di accordi di servizio;
i) la verifica di integrità di uno dei documenti informatici ha dato esito negativo.

4. Nei seguenti casi di eventi rilevanti effettuatisi successivamente alla protocollazione in ingresso, su indicazione del responsabile del procedimento, è possibile inviare un *messaggio di aggiornamento di conferma*:

a) l'avvenuta assegnazione del documento o dei documenti trasmessi;
b) l'attivazione di un procedimento;
c) la chiusura di un procedimento.

TITOLO VII – REGISTRAZIONE E SEGNATURA DEI DOCUMENTI

Art. 27 - Registrazione di protocollo dei documenti ricevuti e spediti

1. Per ogni documento ricevuto o spedito dall'Ente è effettuata una registrazione di protocollo con il sistema di gestione informatica dei documenti City Ware –on line (PAL informatica – Gruppo Apra).

2. Tale registrazione, ai sensi della normativa vigente, è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

3. Ciascuna registrazione di protocollo contiene dati obbligatori e dati opzionali.

I dati obbligatori in forma non modificabile, sono:

- numero di protocollo, generato automaticamente dal sistema;
- data di registrazione di protocollo, assegnata automaticamente dal sistema
- mittente per i documenti ricevuti o, in alternativa, destinatario o destinatari per i documenti spediti;
- oggetto del documento;
- data e numero di protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.
- tipo di supporto: cartaceo o informatico
- assegnazione;

I dati accessori, invece, sono:

- mezzo di ricezione o, in alternativa, mezzo di spedizione;
- copie per conoscenza;
- tipo di documento.

4. Alla registrazione di protocollo di documenti pervenuti tramite le caselle di posta elettronica certificata dell'Ente vengono associate le ricevute generate dal sistema di protocollo informatico e, nel caso di registrazione di messaggi di posta elettronica certificata spediti, anche i dati relativi alla consegna rilasciati dal sistema di posta certificata correlati al messaggio.

5. Nel caso di ricevimento di documenti in formato cartaceo nella registrazione, se ricorre il caso, viene inserita una delle seguenti annotazioni:

- "originale mantenuto presso l'Ufficio Gestione documentale per l'inserimento nel fascicolo annuale"
- "originale mantenuto dal RUP della procedura di gara o selezione per l'inserimento nel relativo fascicolo"
- "originale mantenuto dall'assegnatario per l'inserimento nel relativo fascicolo"
- "sono presenti degli allegati non inseriti perché non scansionabili"

Art. 28 - Registrazione di protocollo dei documenti interni

Per ogni documento prodotto dagli uffici dell'ATA, non spedito a soggetti esterni all'area organizzativa omogenea e non rientrante nelle categorie di documenti esclusi dalla registrazione ai sensi dell'articolo 30 del presente manuale, indipendentemente dal supporto sul quale è formato, è effettuata una registrazione di protocollo con le modalità indicate all'art. 27 ;

Art. 29 - Documenti soggetti a registrazione di protocollo

1. I documenti ricevuti e prodotti dagli uffici dell'ATA, indipendentemente dal supporto sul quale sono formati, ad eccezione di quelli indicati all'art. 30 – 31 e 32, sono sottoposti a registrazione di protocollo;

2. Tutti i documenti amministrativi sono soggetti a registrazione di protocollo o di repertorio.

Art. 30 - Documenti non soggetti a registrazione di protocollo

1. Sono esclusi dalla registrazione di protocollo:
   - atti e documenti interni, di preminente carattere informativo che non costituiscono fasi obbligatorie e imprescindibili dei procedimenti amministrativi;
   - i giornali, le riviste, i libri, i materiali pubblicitari;
   - gli inviti a manifestazioni che non attivino procedimenti amministrativi;
   - inviti a corsi, progetti formativi, stage;
   - lettere ed esposti anonimi qualora non vi sia specifica richiesta degli uffici,

2. Questi ultimi documenti, se contengono informazioni o dati di interesse per l'Amministrazione, sono inoltrate al Presidente ed al Direttore che valutano l'opportunità di dare seguito a queste comunicazioni ed ne individuano le eventuali procedure da sviluppare.

3. Sono inoltre esclusi dalla registrazione di protocollo perché soggetti a registrazione particolare in appositi repertori rispondenti alle vigenti regole tecniche per il protocollo informatico:
   - le deliberazioni dell'Assemblea ATA;
   - i verbali delle sedute del Comitato di coordinamento;
   - i decreti del Presidente;
   - le determinazioni dirigenziali;
   - i decreti dirigenziali di liquidazione;
   - i contratti, le convenzioni e i protocolli d'intesa.

4. La registrazione in un repertorio consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione e l'assegnazione.

5. I documenti registrati in un repertorio fanno parte del Sistema di gestione documentale e, costituiscono comunque delle serie di interesse archivistico

6. Ciascuna registrazione in un repertorio deve contenere le seguenti informazioni:
   - dati identificativi di ciascun atto (persona fisica o giuridica che adotta il documento, o che lo sottoscrive, data, oggetto);

- numero di repertorio, cioè un numero progressivo annuale;
- dati di classificazione e fascicolazione.

Art. 31 - Documenti non firmati

1. La funzione di registrazione del protocollo è quella di attestare data e provenienza certa di un documento senza interferire su di esso, pertanto l'addetto dell'Ufficio Gestione documentale attesta che un determinato documento è pervenuto così come viene registrato.

2. Spetta al Responsabile del procedimento valutare, caso per caso, ai fini della sua efficacia probatoria riguardo ad un affare o ad un determinato procedimento amministrativo, se il documento privo di firma sia da ritenersi valido.

Art. 32 - Registrazione dei messaggi di posta elettronica convenzionale (proveniente da dominio esterno all'ente)

1. Non viene protocollata la mail non contenente elementi che permettano l'identificazione del mittente a meno che i requisiti minimi di identificazione del mittente (es. carta intestata, ragione sociale, data e firma scansionata) siano contenuti in eventuali allegati

2. I documenti così ricevuti sono protocollati e sarà poi cura dell'assegnatario decidere le modalità di sviluppo dell'eventuale procedimento.

Art. 33 - Segnatura di protocollo e di repertorio

1. La segnatura di protocollo o di repertorio garantisce la corrispondenza biunivoca ed inscindibile tra una registrazione ed il relativo documento, che può essere un'entità unica, oppure costituita da un atto primario e da uno o più allegati.

2. L'operazione di segnatura va effettuata contemporaneamente all'operazione di registrazione di protocollo o repertorio.

Art. 34 - Segnatura su documenti informatici

1. I dati della segnatura di protocollo o di repertorio di un documento informatico sono attribuiti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD) reso disponibile dagli Organi competenti, *associato al documento in modo permanente ed immodificabile.*

2. La struttura ed i contenuti del file di segnatura di protocollo o repertorio di un documento informatico sono conformi alle disposizioni tecniche correnti:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- codice identificativo del registro;
- data di registrazione;
- numero progressivo di registrazione.

3. Oltre alle informazioni di cui al precedente comma 3, il file XML associato al documento deve contenere le seguenti informazioni minime:

- oggetto;
- mittente;
- destinatario o i destinatari;
- indice di classificazione;
- numero di fascicolo

Art. 35 - Segnatura su documenti cartacei

1. La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un'etichetta, sulla quale vengono riportate le seguenti informazioni della registrazione di protocollo:

- denominazione dell'Amministrazione;
- data e numero di protocollo del documento;
- classificazione e fascicolo.

2. L' etichetta autoadesiva, corredata di codice a barre, è riportata in *Allegato 6 – Timbri ed etichette in uso.*

3. L'operazione di segnatura dei documenti in partenza viene effettuata dagli uffici competenti che redigono il documento.

4. Nel caso di documenti soggetti a registrazione di repertorio, la segnatura come sopra rappresentata è apposta dall'Ufficio Gestione documentale direttamente sul documento.

Art. 36 - Annullamento delle registrazioni di protocollo

1. Le registrazioni di protocollo possono essere annullate su autorizzazione del responsabile del servizio per la tenuta del protocollo informatico.
2. *Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema con un simbolo o una dicitura.* . In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.
3. Solo il Responsabile del Servizio è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.
4. L'annullamento della registrazione di protocollo viene richiesto con specifica mail adeguatamente motivata, indirizzata all'Ufficio Gestione documentale.
5. Le richieste di annullamento e le motivazioni vengono tracciate.
6. L'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immodificabile determina l'automatico e contestuale annullamento della intera registrazione di Protocollo.
7. Non costituisce modifica sostanziale tale da generare l'annullamento della intera registrazione di Protocollo, il completamento delle registrazioni di pec di altri enti pubblici avvenute in automatico con segnatura informatica (XLM);

8. L'annullamento anche di un solo campo delle altre informazioni registrate in forma immodificabile, necessario per correggere errori intercorsi in sede di immissione di dati delle altre informazioni, comporta la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, all'ora e all'autore della modifica. La disposizione di cui al primo periodo si applica per lo stesso campo, od ogni altro, risultato successivamente errato.
9. Nel caso di annullamento di documenti informatici si invia obbligatoriamente al mittente un *messaggio di annullamento protocollazione* in cui deve essere riportato il motivo dell'annullamento della protocollazione del messaggio.

Art. 37 - Registro giornaliero di protocollo

1. Il responsabile del servizio per la tenuta del protocollo informatico provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

2. Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione della Regione Marche.

3. Il Responsabile della Gestione documentale provvede alla memorizzazione dei dati contenuti nel registro di protocollo sul server dedicato e un sistema di backup garantisce il salvataggio quotidiano di tali registrazioni riversandole su apposito supporto.

4. Tali operazioni vengono espletate con il supporto del Responsabile del Servizio informatico (Amministratore di sistema).

Art. 38 - Differimento dei termini di registrazione

1. Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e comunque non oltre le quarantotto ore dal ricevimento degli atti.

2. Eccezionalmente, il responsabile della tenuta del protocollo informatico può autorizzare la registrazione in tempi successivi, fissando comunque un limite di tempo e conferendo valore, nel caso di scadenze predeterminate, al timbro datario d'arrivo.

Art. 39 - Registro di emergenza

10. Il responsabile del Servizio per la tenuta del protocollo informatico, autorizza lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su registri di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema.
11. Per le modalità di registrazione dei documenti sul registro di emergenza e di recupero delle stesse nel sistema di protocollo informatico, si applica quanto previsto all'articolo 63 del Testo unico, commi 1-5.
12. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati o, in caso di registrazioni su supporti analogici, tramite inserimento manuale degli stessi, nella prima giornata lavorativa successiva al ripristino delle funzionalità del sistema.

Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

13. Il registro di emergenza analogico è depositato presso l'Ufficio Gestione documentale.
14. Qualora non fosse possibile fruire del Servizio di Protocollo informatico per interruzione accidentale o programmata, l'Amministrazione è tenuta ad effettuare le registrazioni di protocollo sul Registro di Emergenza che si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.
15. Le registrazioni di protocollo sono identiche a quelle eseguite sul registro di protocollo generale.
16. Il registro di emergenza viene sostanzialmente a configurarsi come un repertorio del protocollo unico.
17. Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo effettivo, seguendo senza soluzioni di continuità la numerazione del protocollo unico raggiunta al momento dell'interruzione del servizio, fatte salve le protocollazioni automatiche di pec di altri enti pubblici con segnatura informatica (XLM) che dovessero intervenire dal momento della riattivazione del sistema al momento del trasferimento dei dati dal registro emergenza a sistema informatico.
18. A tale registrazione viene associato anche il numero di protocollo e la data di registrazione del relativo protocollo di emergenza.
19. I documenti annotati nel registro di emergenza e trasferiti nel protocollo unico recano, pertanto, due numeri: uno del protocollo di emergenza e uno del protocollo unico.
20. L'efficacia della registrazione è dunque garantita dal numero attribuito dal registro di emergenza a cui viene fatto riferimento per l'avvio dei termini del procedimento amministrativo.
21. L'efficienza, invece, viene garantita dall'unicità della catena documentale e dalla normalizzazione dei dati gestionali, comprese la classificazione e la fascicolazione archivistica.

Art. 40 - Modalità di apertura del registro di emergenza

1. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile della gestione documentale autorizza l'uso del registro di emergenza per effettuare manualmente le operazioni di protocollazione.
2. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione.
3. Per semplificare e normalizzare la procedura di apertura del registro di emergenza nell'*Allegato 7 – Modello di Registro di emergenza* è riportato il modulo (cartaceo o digitale) da utilizzare.
4. Il Responsabile del Servizio dà comunicazione alla struttura organizzativa dell'Amministrazione dell'apertura del registro.

Art. 41 - Modalità di utilizzo del registro di emergenza

1. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente.
2. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.
3. Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono quelli stessi previsti dal protocollo informatico.

Art. 42 - Modalità di chiusura e recupero del registro di emergenza

1. E' compito del Responsabile del sistema di gestione documentale, con l'eventuale collaborazione dell'Amministratore di sistema, verificare la chiusura del Registro di emergenza e attivarsi per riportare dal Registro di emergenza al sistema informatizzato le protocollazioni relative ai documenti protocollati manualmente.
2. Al fine di ridurre la probabilità di commettere errori in fase di trascrizione dei dati riportati dal registro di emergenza a quello del protocollo informatico e di evitare la duplicazione di attività di inserimento, le informazioni relative ai documenti protocollati in emergenza su una o più postazioni di lavoro dedicate della AOO, possono essere inserite nel sistema informatico di protocollo, utilizzando un'apposita funzione di recupero dei dati.
3. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.
4. Una volta ripristinata la piena funzionalità del sistema, il Responsabile del Servizio revoca l'autorizzazione allo svolgimento delle operazioni su l registro di emergenza e ne dà comunicazione alla struttura organizzativa dell'Amministrazione.

TITOLO VIII - CLASSIFICAZIONE DEI DOCUMENTI

Art. 43 - Classificazione

1. La classificazione dei documenti è l'operazione finalizzata a realizzare una corretta organizzazione dei documenti nell'archivio, secondo un ordinamento logico, in relazione alle funzioni e alle competenze dell'Amministrazione, al quale viene ricondotta la molteplicità dei documenti prodotti.

2. Tutti i documenti ricevuti e prodotti dagli Uffici dell'Amministrazione, indipendentemente dal supporto sul quale vengono formati, sono quindi classificati in base al titolario di classificazione riportato nell'*Allegato 8 – Titolario di classificazione*.

3. Mediante la classificazione si assegna al documento il Titolo e la Classe.

4. I Titoli e le Classi sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto.

5. Tutti gli uffici sono abilitati all'operazione di classificazione dei documenti.

Art. 44 - Modifiche e aggiornamenti al titolario

1. Le modifiche e gli aggiornamenti del titolario di classificazione competono esclusivamente al Responsabile del Servizio per la tenuta del Protocollo informatico, e sono assicurati, quando se ne presenta la necessità, nel pieno rispetto delle disposizioni contenute nella normativa vigente in materia di formazione e conservazione degli archivi.

2. Di ogni variazione introdotta deve essere garantita la storicizzazione e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del piano di fascicolazione vigente al momento della produzione degli stessi.

3. Per ogni modifica deve essere riportata la data di introduzione e la data di variazione ma di norma le variazioni vengono introdotte a partire dal 1 gennaio.

4. Ad ogni modifica del piano di classificazione il Responsabile provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo.

5. Il titolario non è retroattivo.

TITOLO IX - ASSEGNAZIONE DEI DOCUMENTI

Art. 45 - Assegnazione dei documenti protocollati o repertoriati

1. Per assegnazione si intende di norma l'azione di conferimento:
   - della responsabilità del procedimento amministrativo ad una scrivania virtuale condivisa;
   - del materiale documentario da lavorare.

2. L'assegnazione, ai responsabili dei servizi o agli uffici di competenza, dei documenti ricevuti è effettuata dal Responsabile della Gestione documentale o dalle altre unità abilitate alla ricezione dei documenti, come previsto al Titoli VI del presente manuale.

4. L'assegnatario del documento:
- esegue una verifica di congruità con le proprie competenze;
- in caso di errore restituisce il documento all'Ufficio Gestione documentale;
- in caso di verifica positiva, esegue l'operazione di presa in carico anche smistandolo all'interno del proprio servizio.

5. Lo smistamento può essere effettuato per competenza o per conoscenza. Il Responsabile del servizio o Ufficio competente è incaricato della gestione del procedimento cui il documento è relativo e prende in carico il documento. I termini per la definizione del procedimento amministrativo che prende avvio dal documento, decorrono comunque dalla data di protocollazione. Il sistema di gestione informatica dei documenti tiene traccia di tutti i passaggi, memorizzando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione. La tracciatura risultante definisce, ai fini regolamentari e normativi, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

6. Con la presa in carico del documento da parte del Responsabile del procedimento ha termine il processo di assegnazione.

Art. 46 - Modifica delle assegnazioni

1. Nel caso di un'assegnazione errata, l'ufficio utente che riceve il documento è tenuto a restituirlo nel minor tempo possibile all'unità che ha effettuato l'assegnazione, la quale, provvederà a correggere le informazioni inserite nel sistema informatico e ad inviare il documento all'ufficio utente di competenza.

2. Il sistema di gestione informatica dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora di esecuzione.

TITOLO X - FASCICOLAZIONE DEI DOCUMENTI

Art. 47 – Fascicolazione dei documenti nell'archivio corrente

Nell'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le attività di fascicolazione del documento secondo le procedure stabilite dall'Amministrazione e dettagliate all'*Allegato 10 - Linee Guida per la fascicolazione*.

Art. 48 - Identificazione dei fascicoli

1. Il fascicolo è l'insieme ordinato di documenti, relativi a uno stesso affare/procedimento/processo amministrativo, a una stessa materia, a una stessa tipologia, che si forma sempre nel corso delle attività amministrative dell'ente, allo scopo di riunire, a fini decisionali o informativi, tutti i documenti utili allo svolgimento di tali attività.
2. Nel fascicolo sono generalmente inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se non è infrequente la creazione di fascicoli formati da insiemi di documenti della stessa tipologia e forma raggruppati in base a criteri di natura di versa (cronologici, geografici, ecc.). I fascicoli costituiscono la componente più diffusa degli archivi contemporanei e sono costituiti, in base alle esigenze di servizio, secondo criteri diversi che sono, tuttavia, stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento.
3. Tutti i documenti, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli.
4. I fascicoli possono essere articolati in sottofascicoli.
5. I documenti sono archiviati all'interno di ciascun fascicolo, sottofascicolo o inserto, secondo l'ordine cronologico di registrazione.

Art. 49 - Processo di formazione e gestione dei fascicoli

1. I fascicoli dell'Amministrazione si dividono in due grandi classi:
a. fascicoli relativi ad affari o procedimenti amministrativi;
b. fascicoli di persona fisica o giuridica.
2. Ogni UO agisce autonomamente nell'apertura e nella chiusura dei fascicoli, siano essi digitali, analogici o ibridi.
3. Per il fascicolo cartaceo si utilizza il modello di camicia in *Allegato 11 – Modello di camicia di fascicolo*.
4. I documenti i cui originali sono pervenuti in modo cartaceo sono trattenuti presso l'Ufficio Gestione documentale e vanno a costituire un fascicolo unico annuale secondo l'ordine di registrazione.

Art. 50 - Processo di formazione dei fascicoli

1. Al momento della ricezione di un documento cartaceo o digitale, il Responsabile del servizio archivio e protocollo in collaborazione con il Responsabile del servizio competente stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se esso si colloca nell'ambito di un affare o procedimento in corso, oppure se ne avvia uno nuovo.

2. In presenza di un documento che si colloca nell'ambito di un affare o procedimento in corso:

- seleziona il relativo fascicolo;
- collega la registrazione di protocollo del documento al fascicolo selezionato;
- invia il documento digitale o scansione del documento cartaceo al servizio competente cui è assegnato il fascicolo, il quale ne assicura l'inserimento nel relativo fascicolo informatico;
- colloca il documento cartaceo nel relativo fascicolo annuale di cui all'articolo precedente;

3. In presenza di un documento che dà avvio ad un nuovo fascicolo si procede all'apertura dello stesso, registrando nel sistema informatico le seguenti informazioni:

- codice di classificazione nell'ambito dei quali il fascicolo si colloca;
- numero del fascicolo, progressivo all'interno del medesimo codice di classificazione, generato automaticamente dal sistema informatico;
- oggetto del fascicolo;
- anno di apertura;
- presenza e numero di eventuali sottofascicoli.

Art. 51 – Camicie dei fascicoli

1. Ogni fascicolo cartaceo è costituito da uno o più documenti racchiusi in una camicia.
2. Sulla camicia deve essere riportato:
   a) Logo dell'ATA (se cartaceo);
   b) Area, servizio ;
   c) Anno di apertura e di chiusura
   d) Titolo e classe di appartenenza
   e) Numero fascicolo
   f) Oggetto

Art. 52 – Metadati dei fascicoli informatici

1. Ai sensi della normativa vigente i metadati minimi relativi al fascicolo informatico sono i seguenti:

- identificativo;
- amministrazione titolare;
- amministrazioni partecipanti;
- responsabile del procedimento;
- oggetto;
- documento.

2. La classificazione e il numero di fascicolo sono una delle componenti obbligatorie dei metadati relativi al fascicolo informatico.

Art. 53 – Chiusura dei fascicoli SE VANIA DA OK CIOè POSSO MANTENERE APERTO IL FASCICOLO E NELLA RICERCA DEL 2017 MI DA ANCHE QUELLO APERTO NEL 2016 NON ANCORA CHIUSO

1. Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare a cui si riferisce;

2. I fascicoli relativi a persone fisiche o giuridiche vengono chiusi al momento della cessazione del rapporto con l'Amministrazione;

3. La data di chiusura si riferisce alla data dell'ultimo documento prodotto**;**

4. Il fascicolo va archiviato rispettando l'ordine del repertorio, quindi in base all'anno di apertura;

5. Nel caso di un procedimento che non si esaurisce nell'anno solare, qualora lo si ritenga necessario, è possibile aprire nell'anno successivo un nuovo fascicolo con il medesimo oggetto in cui verrà trasportato l'intero contenuto del fascicolo e, nel caso di fascicolo cartaceo, la camicia originale;

6. Dei fascicoli trasportati nell'anno successivo occorre darne notizia nel repertorio dei fascicoli di origine e di destinazione.

7. I fascicoli informatici chiusi sono trattati come da convenzione DigiP integrata dal Disciplinare Tecnico per il servizio di conservazione sostitutiva, riportata in Allegato 12 - *Convenzione con la Regione Marche e disciplinare tecnico per il servizio di conservazione sostitutiva* e nel rispetto del Piano di conservazione di cui all'Allegato 13 - *Manuale dei processi per la conservazione digitale;*

Art. 54 – Modifica delle assegnazioni dei fascicoli

1. Nel caso di un'assegnazione errata di un fascicolo o di una sua successiva riassegnazione, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'ufficio utente di competenza.

2. Il sistema di gestione informatica dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora di esecuzione.

Art. 55 – Tenuta dei fascicoli dell'archivio corrente

1. I fascicoli cartacei dell'archivio corrente, formati a cura del Responsabili del protocollo, sono conservati, fino al versamento nell'archivio di deposito, presso l'ufficio archivio e protocollo

Art. 56 – Repertorio dei fascicoli

1. Il Repertorio dei fascicoli è il registro informatico in cui sono riportati tutti i fascicoli istruiti all'interno del piano di classificazione nell'anno di riferimento.
2. Il Repertorio dei fascicoli è un registro annuale, inizia il 1 gennaio e termina il 31 dicembre.
3. Il Repertorio è generato recuperando le informazioni dal sistema di protocollo informatico. Per ciascun fascicolo è riportato
    a) anno di apertura;
    b) classificazione;
    c) numero di fascicolo;
    d) anno di chiusura;
    e) oggetto del fascicolo;
    f) presenza e descrizione dei sottofascicoli;
    g) annotazione del passaggio dall'archivio corrente all'archivio di deposito;
    h) annotazione dell'eventuale trasposto all'anno successivo

4. Il Repertorio dei fascicoli è sottoposto alle stesse disposizioni e allo stesso regime conservativo del protocollo informatico.

TITOLO XI - GESTIONE DEI FLUSSI DOCUMENTALI

Art. 57 – Sistema di gestione dei flussi documentali

1. L'ATA è dotata di un sistema predisposto per la gestione informatica dei documenti che memorizza tutti i passaggi conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.
2. Le modalità di inoltro e ricezione dei documenti sono specificati nei relativi punti del presente manuale.

Art. 58 – Scambio di documenti e fascicoli tra uffici interni

1. Per scambio di documenti tra uffici interni s'intende lo scambio di documenti rilevanti ai fini dell'azione amministrativa.
2. I documenti interni di cui al comma 1 sono gestiti con un'apposita funzione del sistema di protocollo informatico in cui sono registrate secondo le modalità indicate all'articolo 14 comma 7 del presente manuale.
3. Nel caso di trasmissioni di intere pratiche l'ufficio mittente produce una lettera di trasmissione che assegna al Responsabile del servizio/Ufficio destinatario con indicazione del fascicolo informatico e/o cartaceo in cui sono conservati i relativi documenti.
   Il destinatario:
   a) riceve la lettera di trasmissione e verifica la completezza dei documenti e la corretta attribuzione al fascicolo indicato.

   Il sistema di gestione informatica dei documenti:
   a) archivia la lettera di trasmissione collegandola ai fascicoli specificati dai due uffici, mittente e destinatario;
   b) registra automaticamente la data e l'ora d'invio e di ricezione della comunicazione;
   c) gestisce l'assegnazione da parte del mittente e la presa in carico da parte del destinatario

Art. 59 – Comunicazioni informali tra servizi ed uffici

1. Per comunicazione informale tra i vari servizi ed uffici si intende uno scambio di informazioni, con o senza documenti allegati, del quale non si ritiene necessario tenere traccia in archivio.

2. Questo genere di comunicazioni sono normalmente ricevute e trasmesse per posta elettronica e non incidono sul sistema di protocollo informatico.

TITOLO XII – ARCHIVIAZIONE E CONSERVAZIONE DEI DOCUMENTI

Art. 60 – Piano di conservazione dell'Archivio

Il piano di conservazione adottato dall'ATA, "integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti", ai sensi dell'articolo 68 del Testo unico, è quello riportato in *Allegato 14 – Piano di conservazione*.

Art. 61 – Selezione e scarto archivistico

1. In base al piano di conservazione adottato, inserito nel sistema di gestione informatica dei documenti, sarà cura del Responsabile produrre annualmente l'elenco dei documenti e dei fascicoli sui quali, trascorso il periodo obbligatorio di conservazione, è possibile operare lo scarto.

2. L'elenco di scarto è redatto secondo il modulo predisposto dalla Soprintendenza archivistica dell'Umbria e delle Marche e a questa inviato per la necessaria autorizzazione, ai sensi dell'articolo 21, comma 5 del D. lgs 490/1999.

Art. 62 – Memorizzazione dei documenti informatici e delle rappresentazioni digitali dei documenti cartacei

1. I documenti informatici e le loro aggregazioni documentali con i metadati a essi associati sono conservati in modo da garantire il mantenimento nel tempo delle caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, accessibilità, riproducibilità e intelligibilità all'interno del contesto proprio di produzione e archiviazione e preservando il vincolo originario per mantenere l'archivio nella sua organicità.

2. Le rappresentazioni digitali dei documenti su supporto cartaceo, acquisite con l'ausilio dello scanner, sono memorizzate nel sistema al termine del processo di scansione secondo gli stessi principi di cui al comma 1 del presente articolo.

Art. 63 – Conferimento all'archivio storico dei fascicoli cartacei

1. I documenti selezionati per la conservazione permanente relativi ad affari esauriti da oltre quarant'anni sono trasferiti a cura del Responsabile, contestualmente agli strumenti che ne garantiscono la consultazione nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di archivi storici di enti pubblici ed in particolare ai sensi dell'articolo 30, comma 4 del D. lgs 22 gennaio 2004, n. 42.

2. Nella sezione separata verranno garantiti i requisiti minimi volti a garantire la conservazione dei documenti cartacei.

3. Contestualmente al trasferimento dei documenti nella sezione separata verrà aggiornato l'Elenco topografico del locale in cui è conservata tutta la documentazione cartacea e l'Inventario analitico dell'archivio storico.

4. La consultazione dei documenti a fini storici sarà garantita a norma di legge secondo le disposizioni che saranno inserite nell'apposito Regolamento per la consultazione dell'archivio storico.

Art. 64 – Archiviazione e conservazione digitale dei documenti informatici

Per la conservazione dei documenti informatici l'ATA ha individuato il Polo di conservazione regionale DiGiP (Digital preservation) della Regione Marche.

3. Con la convenzione in corso di sottoscrizione, la Regione Marche si impegna alla conservazione dei documenti trasferiti, garantendo il rispetto dei requisiti previsti dalle norme vigenti e sulla base del disciplinare tecnico, versione 1.0, *Allegato 12 – Convenzione con la Regione Marche e disciplinare tecnico per il servizio di conservazione sostitutiva;*

4. L'ATA mantiene la titolarità e la proprietà dei documenti depositati.

5. Il responsabile della conservazione è individuato nella figura del responsabile della conservazione del Polo Regione Marche.

TITOLO XIII – GESTIONE DEI PROCEDIMENTI

Art. 65 – Catalogo delle attività e dei prodotti

La gestione delle attività e dei procedimenti amministrativi, il loro iter, l'individuazione del responsabile e i relativi termini, sono definiti così come stabilito dal Regolamento del procedimento e dell'amministrazione digitale, protempore vigente.

TITOLO XIV – ACCESSIBILITÀ AL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Art. 66 – Accessibilità da parte degli utenti interni

1. La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili e password, od altre tecniche e dispositivi di autenticazione sicura.
2. L'operatore che effettua la registrazione di protocollo inserisce il livello di riservatezza richiesto per il documento in esame, se diverso da quello standard applicato automaticamente dal sistema.
3. In modo analogo, l'ufficio che effettua l'operazione di apertura di un nuovo fascicolo ne determina anche il livello di riservatezza.
4. Il livello di riservatezza applicato ad un fascicolo è ereditato automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti che hanno invece un livello di riservatezza superiore lo mantengono.
5. Per quanto concerne i documenti sottratti all'accesso, si rinvia allo specifico Regolamento.
6. I livelli di riservatezza gestiti dal sistema, il livello standard applicato automaticamente e le relative abilitazioni all'accesso interno alle informazioni documentali sono riportati nell'*Allegato 9 – Incaricati al trattamento dei documenti amministrativi.*

Art. 67 – Accesso esterno

1. L'accesso al sistema di gestione informatica dei documenti da parte di utenti esterni è realizzato mediante l'impiego di sistemi di riconoscimento ed autenticazione sicura basati sulla carta d'identità elettronica o Spid, sulla firma digitale, ecc. fatta eccezione per l'apposita sezione *Amministrazione Trasparente* del sito istituzionale www.atarifiuti.an.it.
2. Sono rese disponibili tutte le informazioni necessarie e sufficienti all'esercizio del diritto di accesso ai documenti amministrativi.

Art. 68 – Accesso da parte di altre pubbliche amministrazioni

L'accesso al sistema di gestione informatica dei documenti da parte di altre pubbliche amministrazioni, è realizzato su apposita convenzione applicando le norme ed i criteri tecnici emanati per la realizzazione della rete unitaria delle pubbliche amministrazioni ed in particolare avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui agli articoli 72 e ss del D.lgs 7 marzo 2005 n. 82.

TITOLO XV – FUNZIONALITÀ DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Art. 69 – Il sistema di gestione informatica dei documenti

1. La procedura informatica funzionale e tecnica del sistema di gestione informatica dei documenti utilizzato dall'Amministrazione è definita nel piano per la sicurezza informatica, di cui al Titolo XVI del presente manuale e all'*Allegato 15 – Piano per la sicurezza informatica.*
2. Essa assicura le seguenti funzionalità:
   - misure di sicurezza di cui all'articolo 7, commi 2, 3 e 4, del DPCM 31 ottobre 2000;
   - misure tecniche ed organizzative atte a garantire la non modificabilità delle registrazioni di protocollo, nonché del registro giornaliero di protocollo e dei repertori;
   - misure tecniche ed organizzative che assicurano la contemporaneità delle operazioni di registrazione e segnatura di protocollo;
   - modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di registrazione;
   - funzione di recupero dei dati registrati sul protocollo di emergenza;
   - modalità di trasmissione e registrazione di documenti informatici;
   - calcolo dell'impronta dei documenti informatici;
   - segnatura di protocollo dei documenti di cui agli articoli 9, 18 e 19 del DPCM 31 ottobre 2000;
   - sistema operativo utilizzato per la gestione informatica dei documenti di cui all'articolo 7, comma 1 e 6, del DPCM 31 ottobre 2000;
   - funzionalità per lo scambio di documenti informatici tra uffici utente;
   - modalità di utilizzo delle funzioni del sistema.

TITOLO XVI – SICUREZZA E SISTEMA INFORMATICO

Art. 70 – Piano di sicurezza informatica

Ai sensi dell'articolo 4 del DPCM 3 dicembre 2013, l'ATA ha predisposto un piano per la sicurezza informatica, riportato nell'*Allegato 15 - Piano per la sicurezza informatica,* al presente manuale. Tale Piano sarà oggetto di verifica ed integrazione avendo riguardo alle prescrizioni del presente Titolo e corredato dal Piano per la continuità operativa in corso di redazione.

Art. 71 – Predisposizione del piano per la sicurezza informatica

Il responsabile della gestione documentale d'intesa con il responsabile della conservazione e il responsabile del servizio informatico, predispone il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del D.lgs 196/2003 e s.m.i..

Art. 72 – Obiettivi del piano di sicurezza informatica

1. Il piano per la sicurezza prevede le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici.
2. Il piano per la sicurezza si basa sull'analisi dei rischi e definisce le politiche di sicurezza, le modalità di accesso al servizio di gestione documentale, gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, i piani di formazione degli addetti e le modalità con le quali deve essere effettuato il monitoraggio periodico delle misure di sicurezza.

Art. 73 – Controllo del rischio

L'azione di controllo del rischio si esprime con la messa in esercizio di una serie di misure classificate e dettagliate come segue:

1. Misure di sicurezza organizzative:
   - analisi dei rischi;
   - regolamento per l'accesso;
   - assegnazione degli incarichi;
   - linee guida per la sicurezza;
   - altre istruzioni interne;
   - formazione;
   - verifiche periodiche sui dati;
   - distruzione controllata dei supporti.
2. Misure di sicurezza logiche:
   - identificazione e autenticazione utente;

- controllo degli accessi ai dati e programmi;
- politica antivirus;
- firma digitale, crittografia;
- monitoraggio sessioni di lavoro;
- disponibilità del software e dell'hardware.

Art. 74 – Codice identificativo per l'utilizzo degli elaboratori

A ciascun utente o incaricato del trattamento è attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore. Lo stesso codice non è, neppure in tempi diversi, assegnabile a persone diverse.

TITOLO XVII - NORME TRANSITORIE E FINALI

Art. 75 - Modalità di approvazione e aggiornamento del manuale

1. Il Manuale di Gestione e le successive modifiche dello stesso sono approvate con Decreto del Presidente su proposta Responsabile del Servizio di gestione informatica e documentale.

2. Le disposizioni del presente manuale si intendono modificate per effetto di:

- sopravvenute norme o regolamenti vincolanti per l'Amministrazione;
- introduzione di miglioramenti in termini di efficacia ed efficienza dell'azione amministrativa, di trasparenza e di ottimizzazione generale del sistema di gestione documentale;
- inadeguatezze rilevate in corso d'opera con l'esercizio delle attività correnti.

3. All'occorrenza, il Responsabile del servizio gestione informatica e documentale si avvale della consulenza di esperti esterni oppure della Soprintendenza archivistica.

Art. 76 - Norme abrogate

Con l'entrata in vigore del presente manuale sono abrogate tutte le norme regolamentari interne all'Amministrazione con esso contrastanti.

Art. 77 - Norme transitorie

Essendo l'ATA un Ente di nuova istituzione l'Archivio Storico sarà istituito solo quando saranno maturati i tempi di versamento previsti della normativa vigente e dal presente manuale.

Art. 78 - Entrata in vigore del presente manuale

Il presente regolamento entra in vigore il primo gennaio 2017.

ALLEGATI

Allegato 1 *Definizioni, norme e regole di riferimento*

Allegato 2 *Area organizzativa omogenea, atto di istituzione del servizio gestione informatica e documentale e atto di nomina del RGD*

Allegato 3 *Modello di carta intestata*

Allegato 4 *Contratto Gestore Posta Elettronica Certificata*

Allegato 5 *Elenco titolari di firma digitale, degli indirizzi di posta elettronica certificata e di posta elettronica dell'Ente*

Allegato 6 *Timbri ed etichette in uso*

Allegato 7 *Modello di Registro di emergenza*

Allegato 8 *Titolario di classificazione*

Allegato 9 *Incaricati al trattamento dei documenti amministrativi*

Allegato 10 *Linee guida per la fascicolazione*

Allegato 11 *Modello di Camicia di fascicolo cartaceo*

Allegato 12 *Convenzione Regione Marche e disciplinare tecnico per il servizio di conservazione sostitutiva*

Allegato 13 *Manuale dei processi per la conservazione digitale*

Allegato 14 *Piano di conservazione*

Allegato 15 *Piano per la sicurezza informatica*

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 1

DEFINIZIONI, NORME E REGOLE DI RIFERIMENTO

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

DEFINIZIONI

1. Ai fini del presente manuale s'intende:

a) per accesso, l'operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici;
b) per affidabilità, la caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico;
c) per allegato, un documento unito stabilmente ad altro documento per prova, chiarimento o memoria, con cui condivide la stessa segnatura di protocollo;
d) per amministrazione, l'Assemblea Territoriale d'ambito ATO 2 - Ancona;
e) f) per archivio corrente, la parte di documentazione relativa ad affari e procedimenti in corso di trattazione, o comunque verso i quali sussiste un interesse corrente;
f) per archivio di deposito, la parte di documentazione relativa ad affari esauriti, non più occorrenti quindi alla trattazione degli affari in corso, ma non ancora destinata istituzionalmente alla conservazione permanente ed alla consultazione a fini storici;
g) per archivio storico, il complesso dei documenti relativi ad affari e procedimenti amministrativi conclusi da più di quarant'anni, selezionati e destinati a conservazione permanente;
h) per area organizzativa omogenea (AOO), un insieme di funzioni e di strutture, individuate dalla Amministrazione che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del DPR 28 dicembre 2000, n. 445;
i) per assegnazione, l'operazione d'individuazione dell'ufficio utente competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
j) per autenticità, la caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico;
k) per base di dati, una collezione di dati registrati e correlati tra loro;
l) per CAD, il Codice dell'Amministrazione digitale di cui al Decreto legislativo 7 marzo 2005 n. 82 modificato con Decreto Legge del 21 giugno 2013 n.69;
m) per casella di posta elettronica istituzionale, la casella di posta elettronica attraverso la quale vengono inviati e ricevuti i messaggi protocollati. Le caselle di posta elettronica istituzionale, definite da ciascuna Amministrazione, sono pubblicate sull'IPA (Indice delle Pubbliche Amministrazioni) e sul sito istituzionale dell'ente;
n) per classificazione, l'operazione che consente di organizzare i documenti in relazione alle funzioni ed alle modalità operative dell'Amministrazione, in base al piano di classificazione adottato le cui voci, in ambiente digitale, sono individuate attraverso specifici metadati;
o) per conservazione, l'insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione;
p) per destinatario, il soggetto/sistema al quale il documento informatico è indirizzato;
q) per documento amministrativo, ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa;
r) per documento informatico, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
s) per fascicolazione, l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari, attività o persone, ovverosia l'operazione di riconduzione logica e fisica di un documento all'interno dell'unità

archivistica che ne raccoglie i precedenti, garantendo il mantenimento del vincolo archivistico;

t) per fascicolo, l'unità archivistica indivisibile di base che raccoglie i documenti relativi ad un procedimento amministrativo, a un soggetto o ad un affare;

u) per fascicolo informatico, l'aggregazione strutturata ed univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice;

v) per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

w) per formato, la modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file;

x) per funzionalità aggiuntive, le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti, nonché alla accessibilità delle informazioni;

y) per gestione dei documenti, l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dall'Amministrazione, nell'ambito del piano di classificazione adottato;

z) per impronta di un documento informatico, una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione di una opportuna funzione di hash, che garantisce l'associazione biunivoca tra l'impronta stessa e il documento di origine;

aa) per integrità, l'insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato;

bb) per *interoperabilità*, la capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi;

cc) per leggibilità, l'insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti;

dd) per manuale di conservazione, lo strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione;

ee) gg) per memorizzazione, il processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici;

ff) per metadati, l'insieme dei dati associati ad un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione;

gg) per piano di classificazione, un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle competenze dell'Amministrazione, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la sedimentazione secondo un ordine logico che rispecchi storicamente lo sviluppo dell'attività svolta;

hh) per piano di conservazione degli archivi, il piano, integrato con il piano di classificazione, contenente i criteri di organizzazione dell'archivio, di selezione periodica e conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;

ii) per polo di conservazione, il Polo Archivistico della Regione Marche (DiGiP);

jj) per registro di protocollo, registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
kk) per Regole tecniche, si intendono le regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis , 41, 47, 57-bis e 71, del CAD di cui al decreto legislativo n. 82 del 2005, DPCM 3 dicembre 2013;
ll) per repertorio dei fascicoli, il registro annuale ordinato e aggiornato dei fascicoli istruiti all'interno di ciascuna classe e riportante tutti i dati del fascicolo;
mm) per repertorio informatico, registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica;
nn) per responsabile del protocollo o della gestione documentale, il dirigente o funzionario in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi;
oo) per responsabile del trattamento dei dati personali, la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali;
pp) per scarto, l'operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti privi di valore amministrativo e di interesse storico culturale;
qq) per segnatura di protocollo, l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso;
rr) per sistema di gestione informatica dei documenti, l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dall'Amministrazione per la gestione dei documenti;
ss) per supporto di memorizzazione, il mezzo fisico atto a registrare permanentemente informazioni rappresentate in modo digitale, su cui l'operazione di scrittura comporti una modifica permanente ed irreversibile delle caratteristiche del supporto stesso;
tt) per Testo unico, il Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, pubblicato con DPR 28 dicembre 2000, n. 445;
uu) per ufficio utente, un ufficio dell'area organizzativa omogenea che utilizza i servizi messi a disposizione dal sistema di gestione informatica dei documenti;
vv) per utente, la persona, l'ente o il sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

*****

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 2

AREA ORGANIZZATIVA OMOGENEA,

ATTO DI ISTITUZIONE DEL SERVIZIO GESTIONE INFORMATICA E DOCUMENTALE,

ATTO DI NOMINA DEL RGD

(Rev. 0 – dicembre 2016)

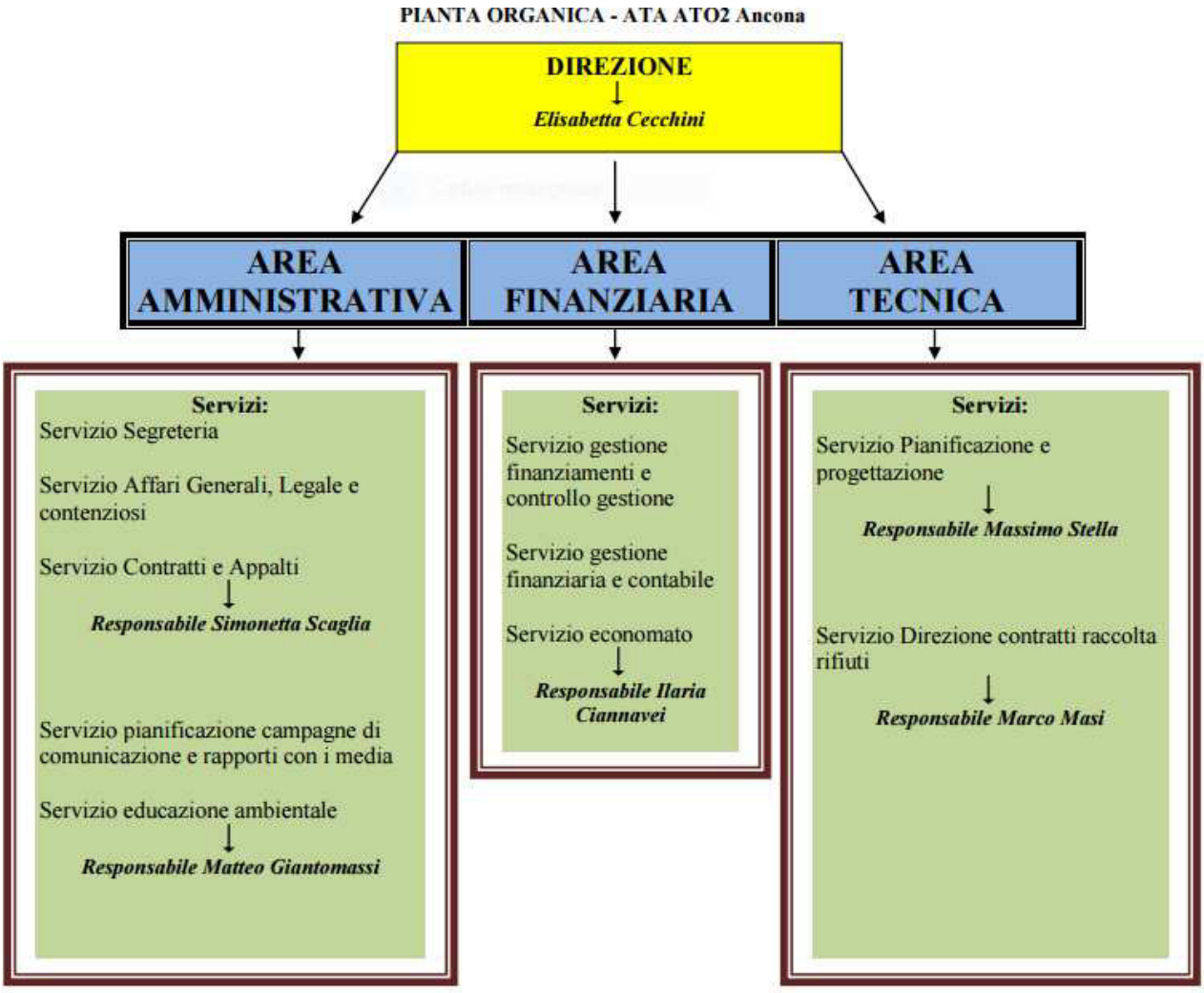
Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

Descrizione dell'Amministrazione, organizzazione e funzioni istituzionali

L'organizzazione viene rappresentata come segue (fonte Organigramma come da sito istituzionale ASSEMBLEA TERRITORIALE D'AMBITO ATO 2):



.

Di seguito è rappresentata l'articolazione dei servizi e degli uffici, come risulta dal portale istituzionale, area Amministrazione Trasparente, sezione Organizzazione > Articolazione degli uffici:

GLI UFFICI

Direzione

dott.ssa **Elisabetta Cecchini**
E-mail: cecchini@atarifiuti.an.it

Area Amministrativa

Servizio segreteria - Servizio affari generali, legale e contenziosi - Servizio contratti e appalti
Responsabile
dott.ssa Simonetta Scaglia
E-mail: scaglia@atarifiuti.an.it

Servizio pianificazione campagne di comunicazione e rapporti con i media - Servizio educazione ambientale
Responsabile
dott. Matteo Giantomassi
E-mail: giantomassi@atarifiuti.an.it

Area Finanziaria

Servizio gestione finanziamenti e controllo gestione - Servizio gestione finanziaria e contabile - Servizio economato
Responsabile
dott.ssa Ilaria Ciannavei
E-mail: ciannavei@atarifiuti.an.it

Area Tecnica

Servizio pianificazione e progettazione
Responsabile
ing. Massimo Stella
E-mail: stella@atarifiuti.an.it

Servizio direzione contratti raccolta rifiuti
Responsabile
Marco Masi
E-mail: masi@atarifiuti.an.it

SEDE LEGALE

Assemblea Territoriale d'Ambito
ATO2 - Ancona (ATA)
strada di Passo Varano, 19/A -
60131 Ancona - c/o Provincia di Ancona
C.F.: 93135970429

Sito web: www.atarifiuti.an.it
Pec: atarifiutiancona@pec.it
E-mail: segreteria@atarifiuti.an.it

SEDE OPERATIVA

E-mail: segreteria@atarifiuti.an.it

Viale dell'Industria, 5
60035 Jesi (AN)
Tel: 0731/200969
Fax: 0731/221630

Si allegano i seguenti Decreti del Presidente riguardanti:

- Individuazione dell'area organizzativa omogenea (AOO) e degli uffici di riferimento: decreto n. 27/2016;
- Nomina del Responsabile della gestione documentale (RGD):decreto n. 35/2016.

COPIA DELL'ORIGINALE DI DECRETO DEL PRESIDENTE

n. 27 **del 15.09.2016**

Oggetto: Individuazione dell'area organizzativa omogenea (AOO) e degli uffici di riferimento ai sensi degli artt. 50 e 61 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e dell'art. 3 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico).

DOCUMENTO ISTRUTTORIO

Oggetto: Individuazione dell'area organizzativa omogenea (AOO) e degli uffici di riferimento ai sensi dell'art. 50 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e dell'art. 3 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico).

IL DIRETTORE

RICHIAMATI l'art. 50 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e l'art. 3 comma 1 lettera a) del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) in base ai quali le pubbliche amministrazioni, di cui all'articolo 1, comma 2, del D.lgs n. 165/2001, nell'ambito del loro ordinamento debbono provvedere ad individuare le aree organizzative omogenee e i relativi uffici di riferimento;

VALUTATO che la struttura dell'Ente necessiti di un'unica area organizzativa omogenea (AOO) in quanto la sua struttura suddivisa nelle seguenti aree presenta esigenze di gestione della documentazione in modo unitario e coordinato:

AREA Amministrativa
AREA Finanziaria
AREA Tecnica

RITENUTO che, avendo individuato un'unica AOO, gli uffici di riferimento previsti dalle norme succitate siano i servizi identificati nel vigente Regolamento di Organizzazione dell'Ente;

ATTESO che per la fatturazione elettronica all'interno dell'Area Finanziaria è stato individuato l'Ufficio Fatturazione Elettronica già inserito sull'IPA (indice delle Pubbliche amministrazioni) a cui è dedicato l'indirizzo pec areafinanziaria.atarifiutiancona@pec.it;

ATTESO inoltre che ai sensi dell'art. 61 del DPR 445/2000 all'interno della AOO va individuato il Servizio responsabile della tenuta del protocollo informatico e della gestione dei flussi documentali e degli archivi;

RITENUTO che tale servizio possa essere collocato all'interno dell'Area Amministrativa e venga denominato Ufficio Gestione documentale a cui è dedicato l'indirizzo pec atarifiutiancona@pec.it;

PRESO ATTO che l'art. 61 del DPR 445/2000 e l'art. 3 del DPCM 3/12/2013 prevedono l'individuazione del Responsabile della gestione documentale a cui sono attribuite le competenze previste dagli artt. 61 DPR 445/2000 e 4 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) che saranno poi meglio dettagliate nel Manuale per la Gestione documentale in corso di redazione;

PRECISATO che si provvederà con separato atto alla nomina del Responsabile della gestione documentale e un suo vicario per casi di vacanza, assenza o impedimento del primo;

VISTI:
- il DPR 445/2000;
- il D.Lgs. 82/2005;
- il DPCM 3/12/2013" Regole tecniche protocollo informatico"
- il D.Lgs. n. 267/2000
- il D.Lgs. n. 165/2001;
- il D.Lgs. n. 150/2009, come modificato ed integrato dal D.Lgs. n. 141/2011;
- il D.L. n. 78/2010 convertito, con modificazioni, dalla L. n. 122/2010;
- il D.L. n. 90/2014 convertito in L. n. 114/2014;
- il D.Lgs. n. 81/2015;
- la Deliberazione dell'Assemblea n. 1 del 23.02.2016 di approvazione del bilancio di previsione 2016-2018 e le Deliberazioni dell'Assemblea n. 5 e n. 6 del 27.04.2016, nonché n. 10 del 27.07.2016, di variazione dello stesso;
- il vigente Regolamento di organizzazione;

PROPONE

1) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2) Di individuare nell'Ente, ai sensi dell'art. 50 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e dell'art. 3 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) un'unica area organizzativa omogenea (AOO) denominata "Assemblea Territoriale d'Ambito – ATO 2 Ancona";
3) Di dare atto che, avendo individuato al precedente punto 2 un'unica AOO, gli uffici di riferimento previsti dalle norme succitate coincidano di fatto con i servizi identificati nel vigente Regolamento di Organizzazione dell'Ente;
4) Di dare atto inoltre che all'interno dell'Area Finanziaria è istituito, per le finalità della fatturazione elettronica, l'Ufficio Fatturazione Elettronica già inserito sull'IPA (indice delle Pubbliche amministrazioni) a cui è dedicato l'indirizzo pec areafinanziaria.atarifiutiancona@pec.it;
5) Di istituire all'interno dell'Area Amministrativa ai sensi dell'art. 61 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) un nuovo servizio responsabile della tenuta del protocollo informatico e della gestione dei flussi documentali e degli archivi denominato Ufficio Gestione documentale a cui è dedicato l'indirizzo pec atarifiutiancona@pec.it;

6) Di istituire altresì la figura del Responsabile della gestione documentale, preposto al servizio di cui al precedente punto 5, a cui sono demandati i compiti previsti dagli artt. 61 DPR 445/2000 e 4 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) che saranno poi meglio dettagliate nel Manuale per la Gestione documentale in corso di redazione;

7) Di provvedere con separato atto alla nomina del Responsabile della gestione documentale e di un vicario per casi di vacanza, assenza o impedimento del primo;

8) Di dichiarare, riscontrata l'urgenza del caso, immediatamente eseguibile il Decreto di approvazione del presente documento istruttorio, ai sensi dell'art. 134, co. 4 del D.Lgs. 267/2000.

Jesi, 15.09.2016

La Direzione
f.to dott.ssa Elisabetta Cecchini

PARERE DI REGOLARITÀ TECNICA

Ai sensi dell'art. 49, co. 1, del D.Lgs. n. 267/2000, si esprime **parere favorevole** in ordine alla regolarità tecnica del presente atto.

Jesi, lì 15.09.2016

Il Direttore
f.to dott.ssa Elisabetta Cecchini

PARERE DI REGOLARITÀ CONTABILE

Ai sensi dell'art. 49, co. 1, del D.Lgs. n. 267/2000, si esprime **parere favorevole** in ordine alla regolarità contabile del presente atto.

Jesi, lì 15.09.2016

Il Direttore
f.to dott.ssa Elisabetta Cecchini

IL PRESIDENTE

VISTO il documento istruttorio redatto dal Direttore in data 15.09.2016, sopra riportato a formare parte integrante e sostanziale del presente atto, contenente la proposta di individuazione di un'unica area organizzativa omogenea (AOO) denominata "Assemblea Territoriale d'Ambito – ATO 2 Ancona" e dell'istituzione Ufficio Gestione documentale ai fini del protocollo informatico e della gestione documentale e archivi;

RITENUTO di condividere la proposta di cui sopra per le motivazioni addotte, che si intendono qui integralmente riportate;

VISTO che il documento istruttorio di cui sopra riporta i prescritti pareri di regolarità tecnica e contabile;

DECRETA

1) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2) Di individuare nell'Ente, ai sensi dell'artt. 50 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e dell'art. 3 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) un'unica area organizzativa omogenea (AOO) denominata "Assemblea Territoriale d'Ambito – ATO 2 Ancona";
3) Di dare atto che, avendo individuato al precedente punto 2 un'unica AOO, gli uffici di riferimento previsti dalle norme succitate coincidano di fatto con i servizi identificati nel vigente Regolamento di Organizzazione dell'Ente;
4) Di dare atto inoltre che all'interno dell'Area Finanziaria è istituito, per le finalità della fatturazione elettronica, l'Ufficio Fatturazione Elettronica già inserito sull'IPA (indice delle Pubbliche amministrazioni) a cui è dedicato l'indirizzo pec areafinanziaria.atarifiutiancona@pec.it;
5) Di istituire all'interno dell'Area Amministrativa ai sensi dell'art. 61 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) un nuovo servizio responsabile della tenuta del protocollo informatico e della gestione dei flussi documentali e degli archivi denominato Ufficio Gestione documentale a cui è dedicato l'indirizzo pec atarifiutiancona@pec.it;
6) Di istituire altresì la figura del Responsabile della gestione documentale, preposto al servizio di cui al precedente punto 5, a cui sono demandati i compiti previsti dagli artt. 61 DPR 445/2000 e 4 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) che saranno poi meglio dettagliate nel Manuale per la Gestione documentale in corso di redazione;
7) Di provvedere con separato atto alla nomina del Responsabile della gestione documentale e di un vicario per casi di vacanza, assenza o impedimento del primo;
8) Di dichiarare, riscontrata l'urgenza del caso, immediatamente eseguibile il Decreto di approvazione del presente documento istruttorio, ai sensi dell'art. 134, co. 4 del D.Lgs. 267/2000.

Jesi, 15.09.2016

Il Presidente
f.to dott.ssa Liana Serrani

CERTIFICATO DI PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che della copia del presente atto è stata disposta la pubblicazione all'Albo pretorio on line in data odierna per 15 giorni interi e consecutivi.

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

CERTIFICATO DI ESEGUITA PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che copia del presente atto è stata affissa all'Albo pretorio on line per 15 giorni interi e consecutivi dal _____ al _____

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

Il presente decreto è divenuto esecutivo il 15.09.2016

☐ Per decorrenza dei termini di cui all'art. 134 del D.Lgs. n. 267/2000.

X Perché dichiarata immediatamente eseguibile ai sensi dell'art. 134, co. 4, del D.Lgs. n. 267/2000.

Jesi, lì 15.09.2016

Il Direttore
f.to dott.ssa Elisabetta Cecchini

CERTIFICATO DI CONFORMITÀ ALL'ORIGINALE

La presente copia, composta di n. 6 pagine, è conforme all'originale conservato in atti.

Jesi, lì 15.09.2016

Il Direttore
f.to dott.ssa Elisabetta Cecchini

COPIA DELL'ORIGINALE DI DECRETO DEL PRESIDENTE

n. 35 **del 30.12.2016**

Oggetto: Nomina del Responsabile della gestione documentale (RGD) ai sensi degli artt. 61 comma 2 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e dell'art. 3 comma1 lettera b) del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico).

DOCUMENTO ISTRUTTORIO

Oggetto: Nomina del Responsabile della gestione documentale (RGD) ai sensi degli artt. 61 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e dell'art. 3 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico).

IL DIRETTORE

RICHIAMATI l'art. 61 commi 1 e 2 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e l'art. 3 comma 1 lettera b) del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) in base ai quali le pubbliche amministrazioni dopo aver individuato il servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi nell'area organizzativa omogenea (AOO) devono nominare un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente, quale Responsabile della gestione documentale (RGD);

ATTESO che con Decreto del Presidente n. 27 del 15/09/2016 è stata individuata un'unica area organizzativa omogenea (AOO) ed è stato istituito all'interno dell'Area Amministrativa l'Ufficio Gestione documentale responsabile della tenuta del protocollo informatico e della gestione dei flussi documentali e degli archivi e la figura del Responsabile della gestione documentale;

PRESO ATTO che al Responsabile della gestione documentale è demandata la verifica del corretto funzionamento del sistema e del suo utilizzo da parte degli utilizzatori abilitati e sono attribuite le competenze previste dagli artt. 61 DPR 445/2000 e 4 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) che saranno poi riportate nel Manuale per la Gestione documentale in corso di redazione, ed in particolare il RGD:

- attribuisce il livello di autorizzazione per l'accesso alle funzioni del sistema di protocollo informatico, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
- garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo;

- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- conserva le copie dei dati di protocollo e dei documenti archiviati su supporto informatico, in luoghi sicuri e differenti;
- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso in base alla normativa vigente;
- autorizza le operazioni di annullamento delle registrazioni di protocollo;
- vigila sull'osservanza delle disposizioni del presente manuale da parte del personale autorizzato e degli incaricati.
- provvede alla pubblicazione del manuale di gestione sul sito istituzionale dell'ATA;
- predispone gli aggiornamenti del manuale secondo le modalità di revisione previste dal manuale di gestione documentale;
- predispone, con i necessari supporti esterni ed in collaborazione con il RSPP, il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato nell'allegato B del DLgs 196/2003 e successive modificazioni, con il supporto del responsabile della conservazione, del responsabile dei sistemi informativi e del responsabile del trattamento dei dati personali di cui al suddetto decreto;
- provvede ad aprire e chiudere il registro di protocollazione di emergenza;
- aggiorna costantemente le procedure attuative del manuale di gestione documentale.

PRESO ATTO che l'attuale struttura dell'Ente prevede un unico Dirigente coincidente con il Direttore responsabile delle tre Aree individuate dal Regolamento di Organizzazione approvato con deliberazione dell'Assemblea n. 4 del 09/09/2013 e sono stati individuati i Responsabili dei servizi con determinazione della Direzione n. 19 del 31/12/2013;

DATO ATTO che l'Ufficio Gestione documentale responsabile della tenuta del protocollo informatico e della gestione dei flussi documentali e degli archivi è stato inserito nell'Area Amministrativa nell'ambito dei servizi che fanno capo alla dott.ssa Simonetta Scaglia;

ATTESO che la dott.ssa Simonetta Scaglia ha iniziato una specifica formazione in materia partecipando a corsi di formazione promossi dalla Regione ed ANAI Marche e ad altre specifiche giornate di studio e che pertanto la stessa possa essere individuata Responsabile della gestione documentale dell'Ente, possedendo i requisiti minimi previsti dalla normativa vigente;

RILEVATO che operativamente il Responsabile della gestione documentale si avvale della sig.ra Loredana Marinelli a cui è già affidata la protocollazione in arrivo della posta e la repertoriazione dei contratti dell'Ente;

ATTESO che il Responsabile della gestione documentale deve operare in stretta collaborazione con il Responsabile della sicurezza informatica dott. Matteo Giantomassi e che lo stesso possa essere quindi individuato quale sostituto del Responsabile della gestione documentale in caso di sua assenza o impedimento, con l'opportuno e necessario affiancamento della sig.ra Loredana Marinelli;

TUTTO CIÒ PREMESSO;

VISTI:
- il DPR 445/2000;
- il D.Lgs. 82/2005 e s.m.i.;
- il DPCM 3/12/2013" Regole tecniche protocollo informatico"
- il D.Lgs. n. 267/2000
- il D.Lgs. n. 165/2001;
- il D.Lgs. n. 150/2009,e ss.mm.ii.;
- il D.L. n. 78/2010 convertito, con modificazioni, dalla L. n. 122/2010;
- il D.L. n. 90/2014 convertito in L. n. 114/2014;
- il D.Lgs. n. 81/2015;
- il vigente Regolamento di organizzazione;

PROPONE

1) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2) Di nominare ai sensi dell'artt. 61 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e dell'art. 3 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) la dott.ssa Simonetta Scaglia, già Responsabile del Servizio Segreteria, Responsabile della gestione documentale dell'Ente (tenuta del protocollo informatico e gestione dei flussi documentali, e archivi) e suo sostituto in caso di assenza o impedimento il dott. Matteo Giantomassi, entrambi coadiuvati dalla dipendente sig.ra Loredana Marinelli;
3) Di dichiarare, riscontrata l'urgenza del caso, immediatamente eseguibile il Decreto di approvazione del presente documento istruttorio, ai sensi dell'art. 134, co. 4 del D.Lgs. 267/2000.

Jesi, 30.12.2016

La Direzione
F.to dott.ssa Elisabetta Cecchini

PARERE DI REGOLARITÀ TECNICA

Ai sensi dell'art. 49, co. 1, del D.Lgs. n. 267/2000, si esprime **parere favorevole** in ordine alla regolarità tecnica del presente atto.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

IL PRESIDENTE

VISTO il documento istruttorio redatto dal Direttore in data 30.12.2016, sopra riportato a formare parte integrante e sostanziale del presente atto, contenente la proposta di nomina della dott.ssa Simonetta Scaglia quale Responsabile della gestione documentale dell'Ente e del dott. Matteo Giantomassi suo sostituto in caso di assenza o impedimento;

RITENUTO di condividere la proposta di cui sopra per le motivazioni addotte, che si intendono qui integralmente riportate;

VISTO che il documento istruttorio di cui sopra riporta il prescritto parere di regolarità tecnica;

DECRETA

1) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2) Di nominare ai sensi dell'artt. 61 del DPR 445/2000 (Testo unico in materia di documentazione amministrativa) e dell'art. 3 del DPCM 3/12/2013 (Regole tecniche per il protocollo informatico) la dott.ssa Simonetta Scaglia, già Responsabile del Servizio Segreteria, Responsabile della gestione documentale dell'Ente (tenuta del protocollo informatico e gestione dei flussi documentali, e archivi) e suo sostituto in caso di assenza o impedimento il dott. Matteo Giantomassi, entrambi coadiuvati dalla dipendente sig.ra Loredana Marinelli;
3) Di dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'articolo 134, co. 4, del D.Lgs. n. 267/2000.

Il Presidente
F.to dott.ssa Liana Serrani

CERTIFICATO DI PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che della copia del presente atto è stata disposta la pubblicazione all'Albo pretorio on line in data odierna per 15 giorni interi e consecutivi.

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

CERTIFICATO DI ESEGUITA PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che copia del presente atto è stata affissa all'Albo pretorio on line per 15 giorni interi e consecutivi dal _____ al _____

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

Il presente decreto è divenuto esecutivo il 30.12.2016

☐ Per decorrenza dei termini di cui all'art. 134 del D.Lgs. n. 267/2000.

X Perché dichiarata immediatamente eseguibile ai sensi dell'art. 134, co. 4, del D.Lgs. n. 267/2000.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

CERTIFICATO DI CONFORMITÀ ALL'ORIGINALE

La presente copia, composta di n. 6 pagine, è conforme all'originale conservato in atti e consta altresì di n. 3 allegati.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 3

MODELLO DI CARTA INTESTATA

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

La carta intestata è identificata dal logo dell'ATA e dal servizio proponente come segue:

RIFIUTI
ATO2 - ANCONA

Direzione

Elisabetta Cecchini
e-mail: cecchini@atarifiuti.an.it

RIFIUTI
ATO2 - ANCONA

Presidenza

Liana Serrani
e-mail: segreteria@atarifiuti.an.it

RIFIUTI
ATO2 - ANCONA

Servizio segreteria
Servizio affari generali, legale e contenziosi
Servizio contratti e appalti

Responsabile
Simonetta Scaglia
e-mail: scaglia@atarifiuti.an.it

RIFIUTI
ATO2 - ANCONA

Servizio pianificazione campagne di comunicazione
e rapporti con i media

Servizio educazione ambientale

Responsabile
Matteo Giantomassi
e-mail: giantomassi@atarifiuti.an.it

RIFIUTI
ATO2 - ANCONA

Servizio gestione finanziamenti e controllo gestione
Servizio gestione finanziaria e contabile
Servizio economato

Responsabile
Ilaria Ciannavei
e-mail: ciannavei@atarifiuti.an.it

RIFIUTI
ATO2 - ANCONA

Servizio pianificazione e progettazione

Responsabile
Massimo Stella
e-mail: stella@atarifiuti.an.it

RIFIUTI
ATO2 - ANCONA

Servizio direzione contratti raccolta rifiuti

Responsabile
Marco Masi
e-mail: masi@atarifiuti.an.it

E a piè di pagina dall'indirizzo e i dati dell'ente:

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

A titolo di esempio si allega la carta intestata della Direzione.

ATA RIFIUTI
ATO2 - ANCONA

Direzione

Elisabetta Cecchini
e-mail: cecchini@atarifiuti.an.it

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 4

CONTRATTO GESTORE
POSTA ELETTRONICA CERTIFICATA

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

Condizioni di Fornitura dei Servizi E-Security

Disposizioni di carattere generale

Le presenti Condizioni di fornitura, unitamente ai documenti indicati al successivo Art. 2, disciplinano, il rapporto contrattuale che si perfeziona tra Aruba S.p.a., con sede in Bibbiena Stazione (AR), Loc. Palazzetto 4, P.I. 01573850516, Aruba Pec S.p.A., con sede in Arezzo, Via Sergio Ramelli n. 8, P.I. 01879020517 (anche "Fornitori") ed il Cliente per la fornitura dei servizi E-Security come di seguito descritti.

Indice degli articoli

SEZIONE I - CONDIZIONI GENERALI

1. Definizioni

Ove nominati nel Contratto i termini sotto riportati sono da intendersi con il seguente significato:

24/7/365: acronimo utilizzato nel Contratto per indicare la continuità dei Servizi 24 ore su 24, 7 giorni alla settimana, 365 giorni all'anno.

Aruba PEC S.p.A.: società facente parte del Gruppo Aruba, iscritta negli elenchi pubblici dei Gestori di Posta Elettronica Certificata, dei Certificatori e dei Conservatori accreditati, predisposti, tenuti ed aggiornati dall'Agenzia per l'Italia Digitale (già DigitPA), che gestisce ed eroga il Servizio di Posta Elettronica Certificata, emette Certificati di Firma Digitale aventi valore legale a norma del combinato disposto del D.P.R. 10 novembre 1997, n. 513 e del D.P.C.M. 13 gennaio 2004 e successive modifiche ed integrazioni, eroga i servizi di Conservazione dei documenti informatici ed è Prestatore di servizi fiduciari qualificato per la fornitura del Servizio di Validazione Temporale Elettronica qualificata.

Aruba S.p.A.: società holding del Gruppo Aruba che, in forza di autonomo contratto, è Partner di Aruba Pec S.p.A. nella commercializzazione dei Servizi di Certificazione ed è competente ad emettere fattura nei confronti del Cliente per i Servizi ordinati.

Cliente: la persona fisica o giuridica individuata nel Modulo d'ordine.

Conferma di attivazione: la comunicazione con la quale si conferma l'avvenuta attivazione del Servizio ordinato.

Conferma d'Ordine: la comunicazione con la quale si conferma la ricezione dell'ordine, sulla quale è riportata una sintetica indicazione delle principali caratteristiche dei Servizi scelti, gli eventuali documenti che il Cliente dovrà inviare ai Fornitori ai fini dell'attivazione dei Servizi ed allegate le presenti Condizioni di fornitura.

Condizioni: le presenti Condizioni di fornitura dei servizi E-Security.

Contratto: il complesso dei documenti indicati all'art. 2.

Codice convenzione/i: il codice fornito al Cliente dal soggetto terzo (a titolo esemplificativo e non esaustivo, Ordine professionale e/o Ente di appartenenza) che abbia stipulato con i Fornitori specifico e separato accordo, utilizzando il quale il Cliente può accedere all'apposita area presente alla pagina

https://www.pec.it/Convenzioni.aspx per acquistare uno o più Servizi ai prezzi, nelle opzioni, con le caratteristiche e limitazioni ivi indicati.

Credenziali: codici di accesso ai Servizi inviati dai Fornitori al Cliente a seguito del perfezionamento del Contratto.

Fornitori: Aruba S.p.A. e Aruba Pec S.p.A. i quali, ai fini del Contratto, potranno agire anche disgiuntamente tra di loro.

Informazioni confidenziali: (i) le informazioni relative ai Fornitori e dai medesimi ritenute o classificate come riservate e/o confidenziali di cui il Cliente abbia avuto conoscenza per qualsivoglia ragione legata all'applicazione del contratto e/o (ii) le informazioni relative ai Fornitori che, per loro natura, contenuto o circostanza in cui vengono rivelate, normalmente verrebbero considerate tali. Al riguardo, a titolo esemplificativo e non esaustivo, informazioni confidenziali dei Fornitori sono tutte le prestazioni, le caratteristiche, le configurazioni e le informazioni tecniche dei Servizi, i preventivi, le relazioni di audit o di sicurezza, i piani di sviluppo del prodotto.

Listino prezzi: il documento pubblicato sul sito www.pec.it, nella sezione dedicata a ciascun Servizio, nel quale sono riportate tutte le caratteristiche economiche del Servizio o in alternativa, se del caso, il documento contenente tali caratteristiche inviato dai Fornitori al Cliente in caso di separato, specifico e diverso accordo tra le Parti.

Manuale: il documento pubblicato e pubblico a norma di legge contenente l'indicazione delle procedure di rilascio, delle modalità operative e le istruzioni per l'uso dei servizi E-Security disponibile, per ciascun Servizio, al link http://www.pec.it/DocumentazioneFirmaDigitale.aspx (ove previsto nell'ambito di ciascun Servizio, quello di riferimento per il Cliente che sia munito Codice convenzione).

Modulo d'ordine: modulo elettronico disponibile sul sito www.pec.it che, interamente compilato on-line dal Cliente e dal medesimo inviato ai Fornitori, costituendo proposta contrattuale, formalizza la richiesta di attivazione del Servizio.

Pannello : l'area per la gestione dei Servizi alla quale il Cliente accede con le proprie Credenziali dalla pagina http://www.pec.it/.

Parti: I Fornitori ed il Cliente.

Policy di utilizzo dei servizi Aruba: il documento redatto dai Fornitori e pubblicato alla pagina link http://www.pec.it/termini-condizioni.aspx nel quale vengono indicate le norme comportamentali e i limiti di utilizzo dei Servizi, cui sono soggetti tutti i Clienti.

Servizio o Servizi: i servizi di E - Security, costituiti dal servizio di Firma Digitale con o senza CNS e/o Validazione Temporale Elettronica qualificata e/o Posta Elettronica Certificata e/o DocFly Fatturazione PA.

Specifiche tecniche: le informazioni pubblicate sui siti web www.pec.it e http://guide.pec.it/home.aspx, nella sezione dedicata a ciascun Servizio, ovvero nei documenti indicati nella sezione stessa, contenenti le caratteristiche tecniche del medesimo.

Le definizioni qui non specificatamente richiamate mantengono il significato indicato nelle Condizioni Particolari e nel Manuale di riferimento di ciascun Servizio.

2. Struttura del Contratto

2.1 Il Contratto è costituito dai documenti appresso indicati:

1) Le Condizioni di fornitura: condizioni generali e condizioni particolari del Servizio fornito;
2) Il Modulo d'ordine;
3) Le Specifiche tecniche del Servizio fornito;
4) La conferma di attivazione;
5) La Policy di utilizzo dei servizi Aruba;
6) I Manuali del Servizio fornito;
7) Il Listino prezzi del Servizio fornito.

2.2 Altresì, quando acquistati dal Cliente i Servizi DocFly di cui alla Sez. V delle Condizioni, costituiscono parte integrante del Contratto dal momento e per effetto della loro sottoscrizione e/o trasmissione ad Aruba in modalità telematica anche se posteriori al perfezionamento del Contratto stesso, i seguenti documenti:

8) Scheda di conservazione
9) Elenco Persone

3. Oggetto del Contratto

Oggetto del Contratto è la fornitura al Cliente dei Servizi con le caratteristiche tecniche ed economiche, nella tipologia e con le modalità riportate nel Modulo d'ordine, nelle Specifiche tecniche dei Servizi stessi e, quando in possesso del Cliente il Codice convenzione, alla pagina https://www.pec.it/Convenzioni.aspx.

Qualsiasi prestazione ulteriore rispetto a quelle oggetto del Contratto potrà essere fornita, previo esame di fattibilità, su richiesta specifica del Cliente a condizioni, termini e corrispettivi da concordare.

4. Perfezionamento del Contratto

4.1 Il Contratto si perfeziona alla data del corretto e puntuale ricevimento da parte dei Fornitori del Modulo d'ordine, compilato ed accettato dal Cliente in ogni sua parte unitamente all'avvenuto pagamento del corrispettivo per il Servizio. L'invio del Modulo d'ordine comporta l'integrale accettazione da parte del Cliente delle presenti Condizioni e di tutti gli altri documenti menzionati al precedente art. 2. All'attivazione dei Servizi seguirà invio della relativa Conferma di attivazione. Resta inteso, in ogni caso, che l'utilizzo dei Servizi da parte del Cliente attesta l'accettazione di tutte le condizioni contrattuali.

4.2 Il Cliente è responsabile della veridicità delle informazioni fornite e riconosce ai Fornitori il diritto di assumere eventuali

ulteriori informazioni ai fini dell'attivazione dei Servizi, nel rispetto della normativa vigente.

4.4 Il Cliente, inviando il Modulo d'ordine, prende atto ed accetta che conclude un contratto la cui sola versione valida ed efficace è quella in lingua italiana, mentre le altre versioni fornite dai Fornitori in una qualsiasi altra lingua straniera sono messe a sua disposizione esclusivamente a titolo di cortesia.

4.5 Resta inteso che il mancato pagamento del corrispettivo entro tre mesi dalla data di ricevimento del Modulo d'ordine, comporta l'annullamento/cancellazione dell'ordine stesso senza alcun preavviso o comunicazione.

5. Attivazione ed erogazione del Servizio

5.1 I Servizi sono attivati nel rispetto dell'ordine cronologico delle richieste pervenute, purché assistite dalla conferma dell'avvenuto pagamento del corrispettivo dovuto, e dei tempi resi necessari dalla disponibilità delle risorse hardware e, comunque, nel più breve tempo possibile. Resta inteso che i termini eventualmente prospettati per l'attivazione del Servizio devono considerarsi meramente indicativi. Il Cliente è tenuto ad eseguire le eventuali prestazioni poste a suo carico dal Contratto ai fini dell'attivazione di ciascun Servizio (a titolo esemplificativo e non esaustivo, invio di copia di un documento d'identità); eventuali ritardi dovuti all'inerzia del Cliente non saranno imputabili ai Fornitori. In ogni caso, il Cliente sarà informato di eventuali ritardi nell'attivazione del Servizio.

5.2 Salve le eventuali limitazioni per il Cliente che abbia acquistato il Servizio mediante il Codice convenzione, di cui al successivo art. 9.8, i Servizi vengono erogati fino alla data di loro scadenza, come individuata nella relative Condizioni Particolari. All'approssimarsi della predetta data, i Fornitori a mero titolo di cortesia e quindi senza con ciò assumere alcuna obbligazione nei confronti del Cliente, si riservano di inviare al medesimo a mezzo e-mail avviso di prossima scadenza dei Servizi.

5.3. Resta espressamente inteso che i Fornitori non sono soggetti ad alcun obbligo generale di sorveglianza, essi pertanto non controllano né sorvegliano i comportamenti o gli atti posti in essere dal Cliente mediante il Servizio ovvero non controllano né sorvegliano le informazioni e/o i dati e/o i contenuti ad ogni modo trattati dal Cliente o da suoi incaricati e/o collaboratori con i Servizi stessi; i Fornitori sono e restano estranei alle attività che il Cliente effettua in piena autonomia accedendo al Servizio, da remoto via internet. In ogni caso il Cliente una volta avuto accesso al Servizio è l'unico titolare, ai sensi del d.lgs. 196/03, del trattamento degli eventuali dati immessi e/o trattati in fase di ordine del Servizio o comunque mediante il Servizio medesimo, per tutta la durata del Contratto e per i 30 (trenta) giorni successivi alla sua scadenza.

6. Durata del Contratto e rinnovo

6.1 Il Contratto disciplina la fornitura dei Servizi al Cliente con decorrenza dalla data del suo perfezionamento. Salve le eventuali limitazioni per il Cliente che abbia acquistato il Servizio mediante il Codice convenzione, di cui al successivo art. 9.8, il Contratto è a tempo indeterminato ed ha la durata selezionata dal Cliente nel Modulo d'ordine. Con il rinnovo del/i Servizio/i come disciplinato ai successivi paragrafi 2 o 3 si rinnova il Contratto.

6.2.In caso di pagamento con modalità diversa dalla carta di credito o da PayPal ovvero negli altri casi espressamente previsti dai Fornitori, il/i Servizio/i dovrà/dovranno essere rinnovato/i dal Cliente prima della sua/loro scadenza - preferibilmente almeno 15 (quindici) giorni prima di tale termine – mediante inoltro della relativa richiesta ed il pagamento, con le modalità ed i tempi di cui all'Art. 7, dell'importo previsto dal Listino prezzi in vigore al momento del rinnovo. Completata la procedura di rinnovo come sopra descritta, il/i Servizio/i si rinnova/no per il periodo di tempo richiesto con decorrenza dal giorno della sua/loro scadenza anche nel caso in cui il rinnovo si perfezioni dopo la scadenza del/i Servizio/i.

6.3 Con riferimento ai Servizi di Posta Elettronica Certificata e/o DocFly – DocFly Fatturazione PA, qualora il Cliente abbia scelto la modalità di pagamento con carta di credito o PayPal, il/i Servizio/i si rinnova/no automaticamente alla sua/loro scadenza per un periodo di tempo uguale a quello indicato inizialmente dal Cliente stesso nel Modulo d'ordine, salvo disdetta inviata da una parte all'altra con modalità idonee ad attestare l'avvenuta sua ricezione e con preavviso di almeno 15 (quindici) giorni sul termine di scadenza. Al momento del rinnovo automatico si applicheranno il Listino prezzi e le altre condizioni contrattuali vigenti. Al fine di garantire la continuità dell'erogazione del/i Servizio/i Aruba chiederà al proprio Istituto bancario, con 7 (sette) giorni di anticipo rispetto alla scadenza effettiva del/i Servizio/i, di eseguire il pagamento in suo favore dell'importo previsto per il rinnovo del/i Servizio/i; in caso di mancato accredito dell'importo previsto per uno o più dei Servizi da rinnovare, i Fornitori, fermo restando quanto previsto al successivo par. 6.4, a mero titolo di cortesia e quindi senza con ciò assumere alcuna obbligazione nei confronti del Cliente, si riservano di effettuare nuovamente detta operazione nei successivi giorni precedenti la scadenza del Servizio. Fatto salvo quanto previsto nelle Condizioni particolari di ciascun Servizio, equivale a tempestiva disdetta del/i Servizio/i da parte del Cliente il mancato accredito a favore di Aruba dell'importo dovuto per il suo/loro rinnovo almeno 2 (due) giorni prima della scadenza.
Il Cliente prende atto ed accetta che i dati della sua carta di credito, se utilizzata per effettuare il pagamento del/i Servizio/i, saranno memorizzati dall'Istituto bancario dei Fornitori per consentirgli di effettuare con lo stesso mezzo il pagamento di qualsiasi altro servizio erogato da Aruba.

6.3.1 Il Cliente prende atto ed accetta, ora per allora, che potrà disabilitare il rinnovo automatico in qualsiasi momento dallo specifico campo dell'Area clienti e comunque : i) cancellando e/o rimuovendo, sempre dall'Area clienti, il codice identificativo univoco di una o più sue Carte di credito e/o uno o più account PayPal e/o ii) per il pagamento c.d. "PayPal", disabilitando autonomamente dal proprio account PayPal, l'opzione che consente di effettuare pagamenti automatici . Una volta disabilitato il rinnovo automatico, il/i Servizio/i potrà/potranno essere rinnovati solo con la procedura

ordinaria prevista al precedente par. 6.2; si applica inoltre la disciplina di cui al successivo par. 6.3. Il Cliente prende atto ed accetta, ora per allora, che nel caso sub ii) del presente comma, l'operazione avverrà in modalità asincrona.

6.4 Fatto salvo quanto previsto dagli altri documenti che costituiscono il Contratto e qualora non diversamente previsto dalle Condizioni particolari di ciascun Servizio, il Cliente prende atto ed accetta che alla data di scadenza dell'ultimo Servizio fornito e comunque, al termine del Contratto a qualsiasi causa dovuto, le Parti saranno automaticamente libere dalle rispettive obbligazioni; il Cliente prende atto ed accetta che costituisce suo esclusivo onere procurarsi e mantenere una copia dei dati e/o informazioni e/o contenuti trattati mediante il/i Servizio/i, restando inteso che una volta terminato il Contratto o scaduto il Servizio tali dati e/o informazioni e/o contenuti potranno essere non più recuperabili. In ogni caso il Cliente solleva, ora per allora, Aruba da ogni e qualsiasi responsabilità per l'eventuale perdita o il danneggiamento totale o parziale di dati e/o informazioni e/o contenuti immessi e/o trattati dal Cliente stesso mediante il/i Servizio/i. Resta ad esclusivo carico del Cliente, l'eventuale ripristino dei dati e/o informazioni e/o contenuti dal medesimo immessi e/o trattati, previa riattivazione del Servizio di cui si tratta, se necessario concludendo un nuovo Contratto.

7. Corrispettivi, modalità e termini di pagamento, garanzie

7.1 Salvo specifico, separato e diverso accordo tra le Parti, e fermo quanto indicato al successivo art. 9.8, il pagamento dei corrispettivi dovuti per i Servizi come indicati nel Listino prezzi dovrà essere effettuato dal Cliente contestualmente all'invio del Modulo d'ordine e comunque anticipatamente rispetto all'attivazione dei medesimi.

7.2 Ogni pagamento effettuato dal Cliente riporterà un proprio numero identificativo e per esso i Fornitori, in persona di Aruba S.p.A., emetteranno la relativa fattura entro il mese di competenza. A tutti gli importi fatturati sarà applicata l'Iva dovuta che, assieme a qualunque altro onere fiscale derivante dall'esecuzione del Contratto, sarà a carico del Cliente. In ogni caso, il Cliente solleva ora per allora i Fornitori da ogni e qualsiasi responsabilità derivante da transazioni o pagamenti effettuati.

7.3 Il Cliente prende atto ed accetta che:

a) il pagamento del prezzo di ciascun Servizio deve essere effettuato con una delle modalità pubblicate alla pagina http://guide.pec.it/pagamento-e-fatturazione/gestione-pagamenti/modalita-di-pagamento-e-tempistiche-di-accredito.aspx ; e

b) ai fini della determinazione dei tempi di attivazione, costituisce suo espresso ed esclusivo onere provvedere alla scelta della modalità di pagamento tenendo conto dei tempi medi di lavorazione dei pagamenti indicati alla pagina http://guide.pec.it/pagamento-e-fatturazione/gestione-pagamenti/modalita-di-pagamento-e-tempistiche-di-accredito.aspx ; e per l'effetto,

c) costituisce suo espresso ed esclusivo onere provvedere al pagamento del prezzo per il rinnovo dei Servizi in tempo utile al fine di poterne garantire la continuità e, comunque, prima che i medesimi siano disattivati per scadenza, tenendo a tal fine in considerazione anche i tempi di lavorazione dei pagamenti indicati alla lett. b) del presente articolo. Fermo quanto precede, il Cliente prende atto ed accetta, ora per allora, che, al fine di evitare la disattivazione di ciascun Servizio, il pagamento dovrà risultare correttamente accreditato e registrato da Aruba entro e non oltre il termine concesso dai Fornitori per il rinnovo del Servizio medesimo.

7.4 Il Cliente prende atto ed accetta espressamente che la fattura possa essergli trasmessa e/o messa a disposizione in formato elettronico.

7.5 Il Cliente potrà utilizzare eventuali suoi residui crediti che per qualsiasi ragione non sono stati imputati ad alcun Servizio per acquistare o rinnovare qualsiasi altro dei servizi erogati da Aruba S.p.A. Tale facoltà potrà essere esercitata dal cliente entro e non oltre 12 (dodici) mesi dalla data del versamento di tali crediti con le modalità indicate al link http://guide.pec.it/pagamento-e-fatturazione/gestione-pagamenti/utilizzo-di-un-eventuale-credito-residuo.aspx. Trascorso inutilmente il periodo di tempo sopra indicato, senza che il Cliente abbia utilizzato il predetto credito, questo si intenderà definitivamente acquisito ed incamerato dai Fornitori ed il Cliente non potrà pretenderne la restituzione o la sua utilizzazione.

7.6 In caso di ordine di un Servizio in promozione gratuita, non troveranno applicazione le disposizioni delle presenti Condizioni relative al pagamento del corrispettivo. Il predetto Servizio potrà essere rinnovato con le modalità indicate al precedente art. 6.

8. Ritardato o mancato pagamento

8.1 Il Cliente non potrà sollevare contestazioni di alcun tipo se prima non avrà provveduto ad eseguire correttamente i pagamenti previsti dal Contratto ed a fornire la relativa documentazione ai Fornitori.

8.2 Nel caso in cui, per qualsiasi motivo, il pagamento del prezzo non risulti valido o venga revocato o annullato dal Cliente, oppure non sia eseguito, confermato o accreditato a beneficio dei Fornitori, gli stessi si riservano la facoltà di sospendere e/o interrompere con effetto immediato l'attivazione e/o la fornitura del relativo Servizio se già attivato. Durante la sospensione del Servizio il Cliente non potrà avere accesso a dati e/o informazioni e/o contenuti dal medesimo immessi, trasmessi e/o comunque trattati mediante il Servizio di cui si tratta.

9. Obblighi e limitazioni di responsabilità dei Fornitori

9.1 I Fornitori garantiscono al Cliente la fornitura e l'utilizzo di ciascun Servizio 24/7/365 in conformità a quanto previsto dalle Specifiche tecniche e nel Contratto. I Fornitori assumono obbligazioni di mezzi e non di risultato e non garantiscono che

il Servizio ordinato dal Cliente si adatti perfettamente a scopi particolari o comunque alle esigenze del medesimo.

9.2 Salvo quanto espressamente previsto nelle singole condizioni particolari contenute nella sezione relativa al Servizio fornito, gli obblighi e le responsabilità dei Fornitori verso il Cliente sono esclusivamente quelli definiti dal Contratto pertanto in qualsiasi caso di violazione o inadempimento imputabile ai Fornitori, gli stessi non rispondono per un importo superiore al corrispettivo versato dal Cliente per il singolo Servizio, ordinato o rinnovato, interessato dall'evento dannoso. Resta espressamente escluso, ora per allora, qualsiasi altro indennizzo o risarcimento al Cliente per danni diretti o indiretti di qualsiasi natura e specie.

9.3 I Fornitori non effettuano nessun backup specifico dei dati e/o informazioni e/o contenuti trattati dal Cliente mediante i Servizi. Il Cliente è pertanto tenuto ad effettuare, a propria cura e spese, il backup completo dei dati e/o informazioni e/o contenuti da egli immessi e/o trattati mediante il Servizio ed a prendere tutte le necessarie misure di sicurezza per la salvaguardia dei medesimi. I Fornitori in ogni caso non offrono alcuna garanzia relativamente all'utilizzo del Servizio per quanto riguarda la tutela e la conservazione dei suddetti dati e/o informazioni e/o contenuti.

9.4 I Fornitori non saranno considerati in nessun caso responsabili per l'uso fatto del Servizio in relazione a situazioni critiche che comportino, a titolo esemplificativo, rischi specifici per l'incolumità delle persone, danni ambientali, rischi specifici in relazione a servizi di trasporto di massa, alla gestione di impianti nucleari e chimici e di dispositivi medici; in tali casi, i Fornitori si rendono disponibili a valutare e negoziare con il Cliente uno specifico accordo "mission critical" con i rispettivi "SLA".

9.5 I Fornitori non prestano alcuna garanzia sulla validità ed efficacia, anche probatoria, del Servizio o di qualsiasi dato, informazione, messaggio, atto o documento ad esso associato o comunque immesso, comunicato, trasmesso, conservato o in ogni modo trattato mediante il Servizio medesimo:

a) quando il Cliente intende utilizzarli o farli valere in Stati ovvero ordinamenti diversi da quello Italiano, fatta eccezione, per quanto riguarda gli Stati facenti parte dell'Unione Europea, per il Servizio di Validazione temporale elettronica qualificata, di cui alla Sez. III delle Condizioni.

b) per la loro segretezza e/o integrità (nel senso che eventuali violazioni di queste ultime sono, di norma, rilevabili dall'Utente o dal destinatario attraverso l'apposita procedura di verifica).

9.6 I Fornitori non assumono, in nessun caso, alcuna responsabilità per le informazioni, i dati, i contenuti immessi o trasmessi e, comunque, trattati dal Cliente mediante il Servizio ed in genere per l'uso fatto dal medesimo del predetto Servizio e si riservano di adottare qualsiasi iniziativa ed azione, a tutela dei propri diritti ed interessi, ivi compresa la comunicazione ai soggetti coinvolti dei dati utili a consentire l'identificazione del Cliente.

9.7 Nell'ipotesi in cui il Cliente sia una Pubblica Amministrazione, i Fornitori assumono tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3 della Legge 13 agosto 2010 n. 136 e successive modifiche ed integrazioni.

9.8 Fermo quanto sopra, l'erogazione dei Servizi acquistati dal Cliente utilizzando il/i Codice/i Convenzione/i ed accedendo alla pagina https://www.pec.it/Convenzioni.aspx avviene in forza di specifici e separati accordi tra il soggetto terzo che fornisce detto Codice al Cliente medesimo (a titolo esemplificativo e non esaustivo, Ordine professionale e/o Ente di appartenenza) ed i Fornitori; pertanto, il Cliente, ora per allora, prende atto ed accetta che i Servizi acquistati utilizzando detto Codice possano essere erogati con particolari limitazioni e/o specifiche (a titolo esemplificativo e non esaustivo: limitazioni alla configurazione del Servizio prescelto e/o alla sua durata, possibilità di cessazione e/o disattivazione anticipata del Servizio, limitazioni d'uso, limitazioni alla possibilità di rinnovo, caratteristiche economiche) disciplinate dai suddetti accordi, cui si fa espresso rinvio, e solleva i Fornitori da ogni responsabilità per gli eventuali danni, diretti o indiretti, di qualsiasi natura e specie, patiti e patiendi per o a causa delle suddette limitazioni e/o specifiche e per o a causa di tutte le operazioni eseguite dai Fornitori stessi riguardo ai Servizi in ottemperanza ai suddetti accordi.

10. Obblighi e diritti del Cliente

10.1 Il Cliente ha diritto di utilizzare il Servizio 24/7/365 secondo le Specifiche tecniche e quanto indicato nel Contratto e prende atto che, in qualsiasi caso di violazione o inadempimento imputabile ai Fornitori o, comunque, per mancato e/o parziale e/o difettoso funzionamento del Servizio, gli stessi non rispondono per un importo superiore all'importo versato dal Cliente per il singolo Servizio, ordinato o rinnovato, interessato dall'evento dannoso. Resta espressamente escluso, ora per allora, qualsiasi altro indennizzo o risarcimento al Cliente per danni diretti o indiretti di qualsiasi natura e specie.

10.2 Il Cliente garantisce che i dati e le informazioni trasmessi ai Fornitori ai fini della conclusione del Contratto sono veritieri, corretti e tali da consentire la sua identificazione, e si impegna a comunicare ai Fornitori ogni variazione dei medesimi, compreso l'indirizzo e-mail indicato nella Modulo d'ordine. I Fornitori si riservano la facoltà di verificare tali dati e/o informazioni richiedendo anche documenti integrativi che il Cliente si impegna, ora per allora, a trasmettere. Qualora il Cliente, al momento dell'identificazione abbia, anche mediante l'utilizzo di documenti personali non veri, celato la propria reale identità o dichiarato falsamente di essere altro soggetto, o comunque, agito in modo tale da compromettere il processo di identificazione Egli prende atto ed accetta che sarà ritenuto penalmente responsabile per le dichiarazioni mendaci e/o l'utilizzo di falsa documentazione e sarà altresì considerato esclusivamente responsabile di tutti i danni subiti e subendi dai Fornitori e/o da terzi dall'inesattezza e/o falsità delle informazioni comunicate, assumendo sin da ora l'obbligo di manlevare e mantenere indenne i Fornitori da ogni eventuale pretesa, azione e/o richiesta di indennizzo o

risarcimento danni che dovesse essere avanzata da chiunque nei loro confronti.

10.3 Il Cliente riconosce che la rete internet non è controllata dai Fornitori e che per la peculiare struttura della rete medesima non se ne possa garantire le prestazioni e la funzionalità né controllare i contenuti delle informazioni che sono trasmesse mediante la medesima. Per questo motivo nessuna responsabilità potrà essere imputata ai Fornitori per la trasmissione o la ricezione di informazioni illegali di qualsiasi natura e specie.

10.4 Il Cliente dichiara di possedere l'insieme delle conoscenze tecniche necessarie ad assicurare la corretta utilizzazione, amministrazione e gestione del Servizio ed in ogni caso riconosce e prende atto che il trattamento di dati e/o informazioni e/o contenuti da egli posto in essere mediante il suddetto Servizio e la conseguente loro diffusione nella rete internet attraverso il Servizio stesso sono eseguiti esclusivamente a suo rischio e sotto la sua responsabilità.

10.5 Il Cliente dichiara, altresì, di essere l'unico ed esclusivo amministratore del Servizio e come tale dichiara di essere l'unico responsabile (i) a proprio rischio, della gestione di dati e/o informazioni e/o contenuti da egli trattati mediante il Servizio, della loro sicurezza e del loro salvataggio e del compimento di ogni altra attività ritenuta utile o necessaria a garantirne l'integrità, impegnandosi, per l'effetto, a fare applicazione, a sua cura e spese, di misure di sicurezza idonee ed adeguate; (ii) del contenuto delle informazioni, dei suoni, dei testi, delle immagini, degli elementi di forma e dei dati accessibili e/o resi disponibili mediante ciascun Servizio e comunque, a qualsiasi titolo, trasmessi, diffusi o messi online dal Cliente; (iii) dei malfunzionamenti di ciascun Servizio per qualsiasi utilizzo non conforme alla Policy di utilizzo dei Servizi Aruba; (iv) dello smarrimento o della divulgazione dei codici di utilizzo del Servizio o degli ulteriori codici ad Egli assegnati dai Fornitori.

10.6 Fermo restando quanto previsto in riferimento al trattamento dei dati di cui al precedente art. 5.3 il Cliente garantisce, in riferimento ai dati di terzi da Egli trattati in fase di ordine e/o di utilizzo del Servizio, di aver preventivamente fornito ad essi le informazioni di cui all'art. 13 D.lgs. 196/2003 e di aver acquisito il loro consenso al trattamento. Resta comunque inteso che il Cliente si pone, rispetto a tali dati, quale Titolare autonomo del trattamento e si assume tutti gli obblighi e le responsabilità ad esso connesse a manlevando i Fornitori, ai sensi del successivo art. 10.9, da ogni contestazione, pretesa o altro che dovesse provenire da terzi soggetti in riferimento a tali ipotesi di trattamento.

10.7 Il Cliente si impegna a comunicare ai Fornitori, aprendo apposito ticket dalla pagina http://assistenza.aruba.it/, ogni variazione dei propri dati anagrafici e dei propri recapiti compreso l'indirizzo e mail indicato in fase d'ordine.

10.8 Il Cliente prende atto ed accetta che qualsiasi operazione effettuata tramite il Servizio del Cliente si presume effettuata dal Cliente stesso e che la conoscenza da parte di terzi dei codici di utilizzo del Servizio o degli ulteriori codici ad Egli assegnati dai Fornitori, potrebbe consentire a questi ultimi l'indebito utilizzo del Servizio nonché l'accesso alle informazioni, contenuti, dati di trattati mediante esso; Egli, pertanto, si impegna a conservare ed utilizzare tali codici con la massima riservatezza e diligenza e ad informare tempestivamente i Fornitori di qualsiasi loro uso non autorizzato o di qualsiasi altra riscontrata violazione alla sicurezza.

10.9 Il Cliente si impegna, ora per allora, a mantenere indenne e manlevare i Fornitori da ogni e qualsiasi richiesta o pretesa di terzi per i danni agli stessi arrecati dal o mediante l'utilizzo dei Servizi. Il Cliente dovrà sostenere tutti i costi, risarcimento di danni ed oneri, incluse le eventuali spese legali, che dovessero scaturire da tali azioni di responsabilità e si impegna ad informare i Fornitori qualora tale azione dovesse essere intentata nei propri confronti.

10.10 Per quanto concerne l'attestazione di tutte le operazioni effettuate (a titolo esemplificativo e non esaustivo, assegnazioni, attivazioni, disattivazioni, storico delle operazioni) il Cliente prende atto ed accetta che faranno fede esclusivamente i LOG dei Fornitori conservati a norma di legge.

10.11 Il Cliente si impegna, ora per allora, a compiere ogni ragionevole sforzo per riscontrare tempestivamente quanto i Fornitori abbiano ad esso formalmente comunicato in relazione al verificarsi delle seguenti circostanze:

a) vi siano fondate ragioni per ritenere che ciascun Servizio vengano utilizzata da Terzi non autorizzati; ovvero

b) il Cliente si trovi coinvolto, a qualsiasi titolo, in una controversia giudiziale o stragiudiziale di natura civile, penale o amministrativa nel caso in cui detta controversia abbia ad oggetto atti e comportamenti posti in essere attraverso il Servizio; ovvero

c) il comportamento del Cliente sia tale da ingenerare il fondato e ragionevole timore che egli si renda inadempiente al Contratto o responsabile di una o più violazioni alle sue disposizioni; ovvero

d) il Cliente utilizzi apparecchiature difettose o non omologate, o che presentano delle disfunzioni che possano danneggiare l'integrità della rete e/o disturbare il Servizio e/o creare rischi per l'incolumità fisica delle persone e delle cose.

10.12 Il Cliente è tenuto al rispetto degli ulteriori obblighi indicati nelle Condizioni particolari di ciascun Servizio nonché di tutte le procedure indicate nei Manuali di riferimento di ciascun Servizio pubblicati al link http://www.pec.it/termini-condizioni.aspx.

11. Assistenza e manutenzione

11.1 L'assistenza tecnica è resa esclusivamente nei tempi e secondo le modalità indicate sul sito http://assistenza.aruba.it/. Il Cliente è tenuto in ogni caso a comunicare tempestivamente ai Fornitori eventuali irregolarità o disfunzioni dal medesimo rilevate per ciascun Servizio. I Fornitori faranno ogni ragionevole sforzo per

prendere in carico quanto prima i problemi comunicati dal Cliente.

11.2 Eventuali richieste di intervento "personalizzato" e, in ogni caso, di intervento che richieda la comunicazione ai Fornitori dei codici di utilizzo del Servizio o degli altri codici ad Egli assegnati da parte del Cliente, o di accesso ai propri documenti, dovranno essere inoltrate agli stessi a mezzo ticket dal sito http://assistenza.aruba.it/. In tali ipotesi, con la mera apertura del ticket, il Cliente autorizza i Fornitori e/o le aziende eventualmente dagli stessi incaricate ad effettuare l'intervento hardware/software richiesto e/o necessario; il Cliente prende atto ed accetta che detto intervento avvenga con tempistiche variabili in ragione dei seguenti criteri: a) tipo di intervento richiesto; b) ordine di arrivo della richiesta di intervento; c) carattere di priorità della richiesta di intervento. Al fine di consentire la corretta e celere esecuzione dell'intervento richiesto il Cliente si impegna a fornire tutte le specifiche e le informazioni richieste dai Fornitori. Con l'invio della richiesta di intervento di cui al presente comma il Cliente:

a) dichiara di essere consapevole che tale intervento può avere un alto grado di rischio per il funzionamento del relativo Servizio o per l'integrità di dati e/o informazioni e/o contenuti dallo stesso immessi e/o trattati mediante il Servizio; e

b) accetta, ora per allora, di farsi carico di tutti i rischi connessi; e

c) si impegna, ora per allora, a procurarsi, prima dell'esecuzione dell'intervento, una copia di backup completa dei dati e/o informazioni e/o contenuti dal medesimo immessi e/o trattati attraverso il Servizio.

Fermo quanto sopra, in ogni caso il Cliente, ora per allora, solleva da ogni responsabilità i Fornitori e/o le Aziende facenti parte del Gruppo Aruba ed il loro personale, nonché le Aziende esterne incaricate dell'intervento ed il loro personale, per gli eventuali danni, diretti o indiretti, di qualsiasi natura e specie, patiti e patiendi per o a causa dell'intervento di cui al presente comma quali, in via meramente esemplificativa, perdita o danneggiamento totale o parziale di dati e/o informazioni e/o contenuti dal Cliente stesso immessi e/o trattati attraverso il Servizio, interruzione totale o parziale del Servizio stesso.

11.3 I Fornitori si riservano la facoltà di interrompere l'erogazione dei Servizi per procedere ad interventi tecnici di manutenzione. In tal caso sarà data comunicazione al Cliente a mezzo e-mail con un preavviso di 7 (sette) giorni; detta comunicazione indicherà altresì le tempistiche del ripristino.

12. Sospensione dei Servizi

12.1 Fatta salva l'applicazione del successivo articolo 14, i Fornitori, a loro discrezione e senza che l'esercizio di tale facoltà possa essergli contestata come inadempimento o violazione del Contratto, si riservano la facoltà di sospendere ciascun Servizio, anche senza alcun preavviso nel caso in cui:

a) il Cliente si renda inadempiente o violi anche una soltanto delle disposizioni contenute nel Contratto, ivi comprese quelle contenute nella Policy di utilizzo dei servizi Aruba;

b) il Cliente ometta di riscontrare, in tutto o in parte, le richieste dei Fornitori e comunque il suo comportamento sia tale da ingenerare il fondato e ragionevole timore che egli si renda inadempiente al Contratto o responsabile di una o più violazioni alle sue disposizioni;

c) vi siano fondate ragioni per ritenere che il Servizio venga utilizzato da Terzi non autorizzati;

d) si verifichino casi di forza maggiore o circostanze che, ad insindacabile giudizio dei Fornitori, impongano di eseguire interventi di emergenza o relativi alla risoluzione di problemi di sicurezza, pericolo per l'intera rete e/o per persone o cose; in tal caso, il Servizio sarà ripristinato quando i Fornitori, a loro discrezione, abbiano valutato che siano state effettivamente rimosse o eliminate le cause che avevano determinato la sua sospensione/interruzione;

e) il Cliente si trovi coinvolto, a qualsiasi titolo, in una qualsiasi controversia giudiziale o anche stragiudiziale di natura civile, penale o amministrativa e comunque nel caso in cui detta controversia abbia ad oggetto atti e comportamenti posti in essere attraverso i Servizio o relativi ad esso;

f) sia richiesta dall'Autorità Giudiziaria.

g) ricorrano motivate ragioni di sicurezza e/o garanzia di riservatezza;

h) il Cliente utilizzi apparecchiature difettose o non omologate, o che presentano delle disfunzioni che possano danneggiare l'integrità della rete e/o disturbare il Servizio e/o creare rischi per l'incolumità fisica delle persone e delle cose.

12.2 In qualsiasi caso di sospensione del Servizio imputabile al Cliente resta impregiudicata l'eventuale azione dei Fornitori per il risarcimento del danno.

12.3 Durante la sospensione del Servizio, a qualsiasi causa dovuta, il Cliente non potrà avere accesso a dati e/o informazioni e/o contenuti dal medesimo immessi e/o trattati mediante il Servizio stesso.

13. Recesso

13.1 Il Cliente qualificabile come "consumatore" ai sensi dell'art. 3 del D.lgs. 206/2005 (cd. "Codice del Consumo"), può esercitare il diritto di recesso nelle forme e modalità previste dagli artt. 52 e seguenti del Codice del Consumo entro il termine di 14 (quattordici) giorni dalla data di perfezionamento del Contratto senza alcuna penalità e senza indicarne le ragioni. Nello specifico, il Cliente dovrà manifestare espressamente la volontà di recesso, utilizzando il modulo presente al link http://www.pec.it, o una qualsiasi altra dichiarazione esplicita della sua volontà di recedere dal Contratto, inviando la comunicazione di recesso esclusivamente a mezzo raccomandata A/R o posta elettronica certificata (PEC) ai recapiti indicati al successivo art. 13.2.

In caso di esercizio del diritto di recesso per la prestazione dei Servizi, i Fornitori rimborseranno al Cliente, senza indebito ritardo e comunque entro 14 giorni dal giorno in cui in cui è

stata comunicata l'intenzione di recedere dal presente contratto, tutti i pagamenti ricevuti, mediante lo stesso mezzo di pagamento utilizzato dal Cliente per il pagamento, ovvero con modalità concordate con il Cliente per le quali questi non dovrà sostenere alcun costo quale conseguenza del rimborso.

In caso di esercizio del diritto di recesso per la fornitura di Prodotti parzialmente personalizzati quali i Dispositivi di firma digitale costituiti dal Lettore con smart card o SIM card ovvero dalla "Aruba Key" o dalla "Aruba Token" (salvo se altri espressamente indicati), i Fornitori rimborseranno al consumatore tutti i pagamenti ricevuti a esclusione dei costi sostenuti dai Fornitori strettamente connessi alla personalizzazione dei Prodotti quali *certificato di firma e/o di autenticazione, riconoscimento de visu al momento della consegna*. Resta inteso che i Fornitori potranno sospendere il rimborso fino al ricevimento dei Prodotti oppure finché il Cliente non abbia dimostrato di averli correttamente spediti, a seconda di quale situazione si verifichi per prima. I Prodotti dovranno essere restituiti ai Fornitori integri, nel loro imballo originale, unitamente alla documentazione di corredo con essi spedita, nella condizione di Prodotti nuovi e mai usati.

Il Cliente è responsabile della diminuzione del valore dei Prodotti risultante da una loro manipolazione diversa da quella necessaria a stabilire la natura, le caratteristiche e il funzionamento degli stessi. In tal caso sarà addebitato al Cliente il costo dei Prodotti interessati da detta diminuzione di valore.

Il Cliente prende atto ed accetta che il Dispositivo di firma digitale costituito dalla sola smart card o dalla sola SIM card è un prodotto interamente personalizzato. Pertanto la sua vendita rientra nella previsione di cui all'art. 59.1, lett. c) del D. Lgs. 206/2005 e non si applicherà la disciplina sul recesso di cui al presente articolo. Il Cliente potrà chiedere la disattivazione di detto Dispositivo in data antecedente alla sua scadenza, ma non avrà diritto di ottenere il rimborso, totale o parziale, del corrispettivo versato. L'ordine può essere bloccato ed eventualmente disdetto qualora la produzione ad esso relativa non sia stata ancora in alcun modo avviata; in tal caso il Cliente avrà diritto ad ottenere esclusivamente la restituzione del corrispettivo versato, con esclusione dei costi già sostenuti dai Fornitori.

13.2 Il Cliente sia egli qualificato o meno come "consumatore" ai sensi dell'art. 3 del D.lgs. 206/2005 (cd. "Codice del Consumo"), avrà sempre facoltà di recedere dal Contratto ovvero da ciascun Servizio, se non diversamente previsto dalle Condizioni Particolari di riferimento del Servizio, senza pregiudizio per validità ed efficacia del Contratto, in qualsiasi momento, senza alcuna penalità e senza indicarne le ragioni, con comunicazione scritta inviata a mezzo raccomandata A/R ad Aruba S.p.A., Loc. Palazzetto n° 4, 52011 Bibbiena Stazione (Arezzo) oppure a mezzo di posta elettronica certificata (PEC) all'indirizzo recessi@aruba.pec.it. Il recesso avrà efficacia entro 30 (trenta) giorni dalla data di ricevimento da parte di Aruba S.p.A. della predetta comunicazione legittimando i Fornitori, se non diversamente previsto dalle Condizioni Particolari di riferimento a disattivare ciascun Servizio in caso di recesso dal Contratto, ovvero, il solo Servizio per il quale è stata esercitata la facoltà di recesso e ad effettuare l'eventuale rimborso del rateo del corrispettivo pagato per i Servizi interessati dal recesso, corrispondente al numero di giorni non utilizzati fino alla successiva scadenza naturale del Contratto o del Servizio per il quale è stato esercitato il recesso, detratti i costi sostenuti e/o da sostenere, conformemente a quanto stabilito dall'art. 1 comma 3 della L. 40/2007.

13.3 I Fornitori si riservano la facoltà di recedere dal Contratto o da ciascun Servizio in qualsiasi momento e senza obbligo di motivazione, dandone comunicazione scritta al Cliente, con un preavviso di almeno 15 (quindici) giorni, fatto salvo il caso in cui:

(i) sopraggiungano eventi determinati da cause di forza maggiore;

(ii) il Cliente risulti iscritto nell'elenco dei protesti, sia stato dichiarato insolvente, sia stato ammesso o sottoposto ad una procedura concorsuale;

In tali ipotesi i Fornitori si riservano il diritto di recedere dal Contratto o da ciascun Servizio con effetto immediato.

Resta inteso tra le Parti che dalla data di efficacia del recesso, in qualsiasi momento e senza ulteriore avviso, ciascun Servizio o il Servizio per il quale è stato esercitato il recesso, se non diversamente previsto dalle Condizioni Particolari di riferimento del Servizio, saranno disattivati ed i Fornitori rimborseranno al Cliente il rateo dell'importo pagato corrispondente al numero di giorni non utilizzati, fino alla successiva scadenza naturale del Contratto o del Servizio interessato, detratti i costi sostenuti e/o da sostenere. In ogni caso, resta espressamente esclusa ogni altra responsabilità dei Fornitori per l'esercizio del diritto di recesso e/o per il mancato utilizzo di ciascun Servizio da parte del Cliente ovvero il conseguente diritto di questi a pretendere ogni altro rimborso o indennizzo o risarcimento di qualsiasi tipo e genere.

13.3 La predetta disciplina si applica compatibilmente con le Condizioni Particolari di riferimento di ciascun Servizio.

14. Clausola risolutiva espressa – risoluzione per inadempimento – condizioni risolutive

14.1 Senza pregiudizio per quanto previsto in altre clausole del Contratto, il medesimo sarà da considerarsi risolto con effetto immediato, ai sensi e per gli effetti di cui all'Art. 1456 Codice Civile, qualora il Cliente:

a) violi gli obblighi previsti negli Articoli 10, 16 e 17 delle Condizioni così come le disposizioni previste in documenti cui esse facciano rinvio; ovvero,

b) violi la Policy di utilizzo dei servizi Aruba; ovvero,

c) compia, utilizzando i Servizi, qualsiasi attività illecita; ovvero,

d) ceda tutto o parte del contratto a terzi, senza il preventivo consenso scritto dei Fornitori.

14.2 Inoltre, in caso di inadempimento agli obblighi previsti dal Contratto, i Fornitori si riservano di inviare al Cliente, in qualsiasi momento, ai sensi e per gli effetti di cui all'art. 1454 cod. civ. diffida ad adempiere entro 15 (quindici) giorni dalla ricezione della relativa raccomandata A.R.

14.3 A far data dalla risoluzione del Contratto verificatasi nei casi previsti dal presente articolo ciascun Servizio, conformemente a quanto previsto dalle Condizioni Particolari di riferimento, sarà disattivato senza alcun preavviso. In tali ipotesi, il Cliente prende atto ed accetta che le somme pagate dal medesimo saranno trattenute dai Fornitori a titolo di penale i quali avranno facoltà di addebitare al Cliente ogni eventuale ulteriore onere che gli stessi abbiano dovuto sopportare, restando in ogni caso salvo il diritto dei medesimi al risarcimento degli eventuali danni subiti.

15. Modifiche al Contratto, alle Policy Aruba e/o ai Manuali

15.1 Il Cliente prende atto ed accetta che ciascun Servizio oggetto del Contratto è caratterizzato da tecnologia in continua evoluzione, per questi motivi i Fornitori si riservano il diritto di modificare in meglio le caratteristiche tecniche ed economiche dello stesso e degli strumenti ad esso correlati in qualsiasi momento, senza che ciò faccia scaturire obblighi di alcun genere per il Cliente. I costi delle licenze software pagati, per il tramite dei Fornitori, ai rispettivi licenziatari saranno adeguati automaticamente in caso di variazione dei prezzi da parte del licenziatario stesso.

15.2 Qualora i Fornitori apportino modifiche tecnico-economiche che risultino peggiorative o di aggravio in termini prestazionali e/o economici o modifichino le condizioni contrattuali in qualsiasi parte, dette modifiche saranno comunicate al Cliente tramite e-mail o pubblicazione sul sito http://www.pec.it. Le predette modifiche avranno effetto decorsi 30 (trenta) giorni dalla data della loro comunicazione. Salvo quanto previsto nelle Condizioni Particolari relative a ciascun Servizio, qualora il Cliente non intenda accettare le suddette modifiche comprese quelle riguardanti il corrispettivo, potrà esercitare nel suddetto termine la facoltà di recedere dal Contratto ovvero dal singolo Servizio con comunicazione scritta da inviarsi tramite raccomandata A.R. ad Aruba S.p.A., Loc. Palazzetto n. 4, 52011 Bibbiena Stazione (Arezzo) od a mezzo posta elettronica certificata (PEC) all'indirizzo recessi@aruba.pec.it . In mancanza di esercizio della facoltà di recesso da parte del Cliente, nei termini e nei modi sopra indicati, le variazioni si intenderanno da questi definitivamente conosciute ed accettate.

15.3 Fermo quanto sopra, i Fornitori potranno variare le caratteristiche tecniche, i sistemi, le risorse in conseguenza della normale evoluzione tecnologica delle componenti hardware e software garantendo al Cliente le medesime funzionalità.

15.4 I Fornitori si riservano altresì la facoltà di modificare in qualsiasi momento la Policy di utilizzo dei servizi Aruba in ragione di esigenze di cui al precedente comma 2 od in ottemperanza a disposizioni di legge; anche in tal caso il Cliente potrà esercitare i diritti previsti al precedente comma 2.

15.5 Aruba Pec S.p.A. si riserva il diritto di effettuare modifiche alle previsioni dei Manuali relativi a ciascun Servizio per sopravvenute esigenze tecniche, legislative e gestionali, che saranno efficaci nei confronti del Cliente decorsi 30 (trenta) giorni dalla comunicazione mediante la loro pubblicazione sul sito istituzionale; anche in tal caso il Cliente potrà esercitare i diritti previsti al precedente comma 2.

16. Copyright e licenze

16.1. Il Cliente è tenuto ad utilizzare ciascun Servizio nel rispetto dei diritti di proprietà intellettuale e/o industriale dei Fornitori secondo quanto indicato in merito nella Policy di utilizzo dei servizi Aruba. I software come qualsiasi altro diritto di autore o altro diritto di proprietà intellettuale sono di proprietà esclusiva dei Fornitori e/o dei loro danti causa, pertanto Il Cliente non acquista nessun diritto o titolo al riguardo ed è tenuto all'utilizzo degli stessi soltanto nel periodo di vigenza contrattuale.

16.2. Nel caso di licenze fornite da terzi fornitori per il tramite dei Fornitori, il Cliente dà atto di aver preso visione dei termini e si impegna ad utilizzare i software secondo le modalità indicate sui rispettivi siti esclusivamente per proprio uso personale. Il Cliente si impegna ad accettare e rispettare i termini delle suddette licenze. Il Cliente dichiara di essere a conoscenza del fatto che le Licenze intercorrono fra il Cliente ed il titolare dei diritti di copyright sulle stesse con esclusione di qualsiasi responsabilità dei Fornitori.

17. Sicurezza delle informazioni

Il Cliente, preso atto che i Fornitori si sono dotati della certificazione ISO 27001:2005 e degli altri mezzi e/o strumenti ritenuti idonei a tutelare nella maniera più efficace la sicurezza delle informazioni (fisica, logica, informatica ed organizzativa), si impegna, ora per allora, a non divulgare ovvero rendere in alcun modo disponibili a terzi le informazioni confidenziali conosciute o gestite in relazione alla esecuzione e/o applicazione del Contratto in assenza di specifico consenso scritto dei Fornitori.

18. Disposizioni finali

18.1. Il Contratto annulla e sostituisce ogni altra precedente intesa eventualmente intervenuta tra i Fornitori e il Cliente in ordine allo stesso oggetto, e costituisce la manifestazione ultima ed integrale degli accordi conclusi tra le Parti su tale oggetto. Nessuna modifica, postilla o clausola comunque aggiunta al Contratto sarà valida ed efficace tra le Parti, se non specificatamente ed espressamente approvata per iscritto da entrambe. In caso di accordi particolari con il Cliente questi dovranno essere formulati per iscritto e costituiranno addendum al Contratto.

18.2. In nessun caso eventuali inadempimenti e/o comportamenti del Cliente difformi rispetto al Contratto, potranno essere considerati quali deroghe al medesimo o tacita accettazione degli stessi, anche se non contestati dai Fornitori. L'eventuale inerzia dei Fornitori nell'esercitare o far valere un qualsiasi diritto o clausola del Contratto, non costituisce rinuncia a tali diritti o clausole.

18.3. A meno di espressa diversa indicazione nel Contratto, tutte le comunicazioni al Cliente relative al presente rapporto contrattuale potranno essere effettuate dai Fornitori indistintamente a mano, tramite posta elettronica, certificata e non, a mezzo di lettera raccomandata A.R., posta ordinaria oppure a mezzo telefax agli indirizzi e/o recapiti indicati dal Cliente nel Modulo d'ordine e, in conseguenza, le medesime si considereranno da questi conosciute. Eventuali variazioni degli indirizzi e dei recapiti del Cliente compreso l'indirizzo e-mail indicato nel Modulo d'ordine non comunicate ai Fornitori con le modalità previste dal Contratto non saranno ad essa opponibili.

18.4. Fatta eccezione per i casi specificatamente previsti in Contratto, tutte le comunicazioni che il Cliente intenda inviare ai Fornitori relativamente al Contratto, ivi comprese le richieste di assistenza, dovranno essere inviate ai recapiti indicati sul sito http://www.pec.it/Contacts.aspx.

18.5. L'eventuale inefficacia e/o invalidità, totale o parziale, di una o più clausole del Contratto non comporterà l'invalidità delle altre, le quali dovranno ritenersi pienamente valide ed efficaci.

18.6. Il Cliente prende atto ed accetta che i Fornitori potranno comunicare a soggetti terzi e/o divulgare in qualsiasi forma i dati relativi al Contratto (a titolo esemplificativo ma non esaustivo: l'oggetto, la durata, la denominazione del Cliente) come referenza commerciale per la promozione di propri prodotti o servizi.

18.7 I rapporti tra i Fornitori ed il Cliente stabiliti nel Contratto non possono essere intesi come rapporti di mandato, rappresentanza, collaborazione o associazione o altre forme contrattuali simili o equivalenti.

18.9 Il Cliente si impegna a non cedere il Contratto a terzi senza previa autorizzazione scritta da parte dei Fornitori.

19. Gestione dispute e reclami

Eventuali dispute e/o reclami in merito alla fornitura del Servizio possono essere comunicati a:

Aruba S.p.A.
Loc. Palazzetto n. 4
52011 Bibbiena Stazione (Arezzo)

Tramite lettera raccomandata A.R., o inoltrati tramite ticket dal servizio di assistenza, entro e non oltre 7 (sette) gg. dal momento in cui si verifichi il fatto oggetto di disputa e/o reclamo. I Fornitori esamineranno la comunicazione e forniranno risposta scritta entro 30 (trenta) giorni dal ricevimento del medesimo. Nel caso di dispute e/o reclami per fatti di particolare complessità, che non consentano una risposta esauriente nei termini di cui sopra, i Fornitori informeranno il Cliente entro i predetti termini sullo stato di avanzamento della pratica.

20. Ultrattività

La presente clausola, le altre clausole delle Condizioni qui di seguito indicate così come le disposizioni previste in documenti cui tali clausole facciano rinvio continueranno ad essere valide ed efficaci tra le Parti anche dopo la cessazione ovvero la risoluzione a qualsiasi causa dovute o a qualsiasi parte imputabile:

1. Definizioni
5. Attivazione ed erogazione del Servizio
9. Obblighi e limitazioni di responsabilità dei Fornitori
10. Obblighi e diritti ed Cliente
13. Recesso
14. Clausola risolutiva espressa - risoluzione per inadempimento – condizioni risolutive
16. Copyright e licenze
17. Sicurezza delle informazioni
22. Legge applicabile e foro competente
23. Rinvio ai Manuali

21. Trattamento dei dati personali

Il trattamento dei dati personali del Cliente e da Egli comunicati ai Fornitori ai fini dell'esecuzione del presente Contratto e della successiva erogazione del Servizio, avverrà in conformità al D.lgs. 196/2003, all'informativa privacy rilasciata dai Fornitori in fase di iscrizione anagrafica ed in forza del consenso al trattamento dei dati manifestato in tale sede dal Cliente.

22. Legge applicabile e foro competente

22.1 Il Contratto è regolato esclusivamente dalla legge italiana. Le presenti Condizioni sono state redatte e predisposte in osservanza ed in conformità alle disposizioni contenute nel D.lgs. 206/2005 (Codice del Consumo), nella L. 40/2007 (Misure urgenti per la tutela dei consumatori, la promozione della concorrenza, lo sviluppo di attività economiche e la nascita di nuove imprese) e nel D.lgs. 70/2003 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno); esse si intendono automaticamente modificate e/o adeguate a quanto previsto in materia da successive disposizioni di legge e/o regolamenti.

22.2. Per ogni e qualsiasi controversia relativa all'interpretazione, esecuzione e risoluzione del presente contratto sarà esclusivamente competente il Foro di Arezzo, salvo il caso in cui il Cliente abbia agito e concluso il presente contratto in qualità di Consumatore per scopi estranei all'attività imprenditoriale o professionale svolta; in tal caso sarà esclusivamente competente il Foro del luogo dove il Cliente ha la propria residenza o domicilio, se ubicati sul territorio dello stato italiano.

23. Rinvio ai Manuali

Per quanto non espressamente indicato nelle presenti Condizioni si rinvia a quanto stabilito nei Manuali di ciascun Servizio, pubblicati al link http://www.pec.it/termini-condizioni.aspx.

SEZIONE II - CONDIZIONI PARTICOLARI DI FORNITURA DEL SERVIZIO DI FIRMA DIGITALE CON O SENZA CNS

1. Definizioni

Ove nominati nel Contratto i termini sotto riportati sono da intendersi con il seguente significato:

CAD: il D.Lgs. 7 marzo 2005, n. 82 e s.m.i.;

Certificato/i: la definizione utilizzata nel Contratto per indicare indifferentemente il Certificato di firma e/o il Certificato di autenticazione quando non è necessario specificare di quale certificato si tratti;

Certificato di autenticazione: Il Certificato consistente nell'attestato elettronico che assicura l'autenticità delle informazioni necessarie per l'identificazione in rete del titolare della CNS rilasciato da Aruba Pec su delega dell'Ente Emettitore come previsto nel D.P.R. 2 marzo 2004, n. 117, e nel Manuale Operativo CNS e che permette l'accesso ai sistemi informatici detenuti dalle Pubbliche Amministrazioni;

Certificato di firma: Il Certificato che collega i dati utilizzati per verificare la Firma digitale al titolare e confermare la sua identità, emesso dal Certificatore ARUBA PEC S.p.A. come previsto nel CAD, nelle regole tecniche da esso richiamate e nel Manuale Operativo "Servizio di certificazione digitale";

Chiave privata: la componente della coppia di chiavi asimmetriche nota esclusivamente al soggetto che ne è Titolare, mediante la quale detto titolare appone la Firma digitale su un documento informatico oppure decifra il documento informatico in precedenza cifrato mediante la corrispondente Chiave pubblica.

Chiave pubblica: la componente della coppia di chiavi asimmetriche destinata ad essere resa pubblica, mediante la quale si verifica la Firma digitale apposta sul documento informatico del Titolare della Chiave privata o si cifrano i documenti informatici da trasmettere al Titolare della predetta chiave.

CNS: acronimo di Carta Nazionale dei Servizi come definita nel CAD e cioè lo strumento per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica;

Dispositivo di firma digitale: la soluzione di Firma digitale descritta in dettaglio nel Manuale e distribuita dai Fornitori al Cliente, come dal medesimo indicata nel Modulo d'ordine.

Ente Emettitore: L'Ente Pubblico – Università della Calabria con sede in Arcavacata di Rende (CS), 87036, via Pietro Bucci, che in quanto legittimato all'emissione del Certificato di autenticazione ai fini dell'esecuzione del Contratto delega Aruba Pec alla sua emissione e gestione per via telematica;

Firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Cliente tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

Firma digitale CNS: tipologia di Firma digitale contenente anche il Certificato di autenticazione;

Firma digitale remota: particolare tipo di firma digitale, generata su HSM sotto il pieno controllo di Aruba Pec, che garantisce al Cliente un controllo esclusivo sulle chiavi private; su richiesta del Cliente tale firma può essere fornita anche con l'opzione "Modalità verificata" giusto quanto previsto dall'art. 19 DPCM 22 febbraio 2013.

HSM: insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche.

Manuale Operativo "Servizi di certificazione": il manuale pubblicato e pubblico a norma di legge contenente l'indicazione delle procedure di rilascio del Certificato di firma (quando insieme al Manuale Operativo "Carta Nazionale dei Servizi – CNS" Manuale o anche "Manuali") disponibile per il download al link http://www.pec.it/DocumentazioneFirmaDigitale.aspx;

Manuale Operativo "Carta Nazionale dei Servizi – CNS": il manuale pubblicato e pubblico a norma di legge contenente l'indicazione delle procedure di rilascio del Certificato di autenticazione (quando insieme al Manuale Operativo "Servizi di Certificazione", Manuale o anche "Manuali") disponibile per il download al link http://www.pec.it/DocumentazioneFirmaDigitale.aspx;

Modalità verificata: La modalità che subordina l'utilizzo della Firma Remota alla verifica della sua validità da parte di Aruba Pec e cioè che il corrispondente certificato non è scaduto, né sospeso, né revocato al momento della generazione della firma.

Modulo di Richiesta: il modulo con il quale il Cliente richiede il Dispositivo di firma indicato nel Modulo d'ordine, contenente tutti i dati necessari ad identificarlo, dal medesimo redatto e sottoscritto ed inviato ai Fornitori unitamente ai documenti ivi richiamati.

Riconoscimento de visu: procedura mediante la quale il Certificatore, con le modalità indicate nel Manuale, effettua l'identificazione certa del Cliente ai sensi dell'art. 32, comma 3, lett. a, del D.lgs. 82/2005, necessaria ai fini dell'emissione dei Certificati.

Titolare: il Cliente a nome del quale viene/vengono emesso/i il/i Certificato/i sulla base del Modulo di Richiesta inviata ai Fornitori.

2. Richiesta del Cliente

2.1 Il Cliente potrà richiedere ai Fornitori il Dispositivo di firma digitale, nelle opzioni rese disponibili sul sito web www.pec.it, seguendo l'apposita procedura telematica.

2.2 Ai fini di quanto previsto al precedente parag. 2.1. Il Cliente dovrà comunicare ai Fornitori:

a) dati, documenti, informazioni corrette e veritiere, specificando tra le informazioni fornite quelle che intende escludere dal certificato;

b) l'esistenza di eventuali limitazioni nell'uso della coppia delle chiavi di certificazione (a titolo esemplificativo, poteri di rappresentanza, limitazioni di poteri, ecc.), comprovate da idonea documentazione;

c) l'esistenza di eventuali divieti, anche normativi, nella richiesta del servizio;

d) tempestivamente ogni eventuale modifica delle informazioni o dei dati forniti.

2.3 Il Dispositivo di firma digitale, con o senza il Certificato di autenticazione secondo quanto richiesto dal Cliente, sarà rilasciato solo in caso di esito positivo delle verifiche a tal fine necessarie; in caso di mancata emissione del/i Certificato/i, i Fornitori indicheranno al Cliente le ragioni che ne hanno determinato il mancato rilascio restituendo al medesimo il 50% (cinquanta %) dell'importo versato a titolo di canone annuale per la Firma Digitale; resta inteso, e di ciò il Cliente prende atto ed accetta, che il residuo 50% (cinquanta %) sarà trattenuto dai Fornitori a titolo di indennità per le spese relative all'istruttoria di rilascio del Certificato.

2.4 Il Dispositivo di Firma digitale richiesto dal Cliente viene emesso e consegnato al medesimo nel rispetto dei tempi resi necessari dalla disponibilità delle risorse hardware e, comunque, nel più breve tempo possibile. In ogni caso, il Cliente sarà informato di eventuali ritardi nella fornitura del Dispositivo di Firma digitale.

2.5 La consegna del Dispositivo di firma digitale sarà eseguita dai Fornitori al Cliente:

a) nella modalità indicata sul modulo d'ordine tra quelle messe a sua disposizione;

b) previo suo Riconoscimento de visu da eseguirsi sempre nella modalità indicata sul modulo d'ordine, selezionata tra quelle previste nel Manuale ed indicate sul sito www.pec.it.

2.6 Affinché la consegna del Dispositivo di firma digitale vada a buon fine il Cliente dovrà seguire le indicazioni che gli saranno di volta in volta indicate dai Fornitori nonché quelle ulteriori che gli saranno indicate dai terzi da essi incaricati di eseguire il Riconoscimento de visu e la consegna del Dispositivo di firma digitale. Il Cliente, anche in forza di quanto previsto all'art. 5.1 delle Condizioni generali, prende atto che non potrà avanzare nei confronti dei Fornitori alcuna richiesta di indennizzo e/o risarcimento del danno e/o pretesa di alcun genere, in caso di mancata o ritardata consegna del Dispositivo di firma digitale per motivi non riconducibili a dolo o colpa grave dei Fornitori stessi.

2.7 Nell'ipotesi in cui il Cliente abbia scelto la modalità di Riconoscimento de visu a domicilio, è consapevole che in qualsiasi caso di mancata consegna del Dispositivo di firma digitale lo stesso sarà restituito ai Fornitori.

Il Cliente, entro il termine di giacenza indicato nel presente articolo, potrà richiedere ai Fornitori, con le modalità indicate sul sito web http://guide.pec.it/soluzioni-firma-digitale/firma-digitale/acquisto-e-rinnovo-firma-digitale/de-visu-domicilio-firma-digitale.aspx#a_1461065571302, di effettuare un nuovo tentativo di consegna del Dispositivo di firma digitale da eseguirsi previo pagamento dell'importo da essi a tal fine indicato.

In caso di sua mancata consegna, il Dispositivo di firma digitale resterà in giacenza presso i Fornitori per 6 (sei) mesi dalla data in cui gli stessi hanno dato conferma al Cliente dell'avvenuto pagamento del corrispettivo dovuto per detto Dispositivo. Il Cliente prende atto ed accetta che, fatti salvi i casi di recesso esercitati con le modalità e nei termini previsti dalle presenti Condizioni particolari, la mancata richiesta ai Fornitori di effettuare un nuovo tentativo di consegna del Dispositivo di firma digitale entro il periodo di giacenza, comporta la sua rinuncia ad ogni diritto sul Dispositivo stesso e sul relativo corrispettivo a suo tempo versato il quale, per l'effetto, sarà automaticamente trattenuto e imputato dai Fornitori quale rimborso forfetario delle spese amministrative e di giacenza sostenute dai Fornitori stessi a causa della mancata consegna del Dispositivo di firma digitale. A tal proposito resta inteso che i Fornitori non potranno essere ritenuti responsabili del Dispositivo di firma digitale in questione ovvero della sua mancata consegna ed avranno la facoltà di procedere al suo smaltimento ovvero alla soluzione ritenuta più opportuna, previa revoca ai sensi di legge del o dei Certificati nello stesso contenuti. Il Cliente manleva ora per allora i Fornitori da qualsiasi responsabilità in merito al predetto Dispositivo di firma digitale, al o ai Certificati di Firma in esso presenti, autorizzandoli al tempo stesso, rinunciata e rimossa ora per allora ogni eccezione, a trattenere ed imputare il corrispettivo versato per il suo acquisto a rimborso forfetario delle spese amministrative e di giacenza sopra menzionate.

2.8 E' onere del Cliente generare la coppia di chiavi di sottoscrizione in sicurezza, nel rispetto delle procedure indicate nel Manuale.

2.9 Il servizio di Firma digitale si considera attivato al termine della procedura a tal fine prevista nel Manuale. Resta inteso che l'attivazione del Certificato, ad eccezione di quello di Firma digitale remota, dovrà essere effettuata direttamente dal Cliente mediante l'apposita procedura entro 12 (dodici) mesi dalla sua emissione; in difetto, trascorso detto termine, il Certificato non sarà più utilizzabile. In tale ipotesi il Cliente, se del caso, dovrà acquistare un nuovo Dispositivo di firma digitale senza poter avanzare alcuna pretesa nei confronti dei Fornitori, anche a titolo di rimborso, per il Certificato divenuto non più utilizzabile.

2.10 Anche in deroga a quanto previsto all'art. 4.1 delle Condizioni generali, nel caso in cui il primo Servizio attivato al Cliente sia quello di Firma Digitale, il Contratto si perfeziona ed entra in vigore con l'emissione del Certificato da parte dei Fornitori.

3. Durata e rinnovo dei Certificati

3.1 La durata del Certificato è pari alla durata indicata sul medesimo nella sezione "validità (validity)", salvo revoca, in conformità a quanto previsto nei Manuali.

3.2 Secondo quanto previsto nei Manuali, il Cliente può chiedere il rinnovo del Certificato di firma prima della sua scadenza e, qualora mantenga lo stesso supporto hardware (Dispositivo di firma digitale) su cui detto Certificato è contenuto, secondo le modalità indicate nei Manuali stessi nonché in quelle pubblicate sul sito www.pec.it. Il Cliente prende atto ed accetta che con l'attivazione del Certificato di firma rinnovato, il precedente Certificato di firma non sarà più valido ed utilizzabile. Un Certificato di firma scaduto o revocato non può essere rinnovato.

4. Obblighi del Cliente

4.1 Il Cliente, consapevole che:

a) il Certificato di firma consente di sottoscrivere atti e documenti rilevanti a tutti gli effetti della legge italiana e riconducibili unicamente alla sua persona;

b) il Certificato di autenticazione è uno strumento di identificazione in rete che consente la fruizione dei servizi delle amministrazioni pubbliche,

Si obbliga ad osservare la massima diligenza nell'utilizzo, conservazione e protezione della chiave privata, del Dispositivo di firma digitale con o senza CNS e del codice di attivazione ad esso associato (PIN), nonché degli ulteriori codici ad egli trasmessi dai Fornitori per l'uso del Servizio.

4.2 In particolare, il Cliente è obbligato, ai sensi dell'art. 29 bis del T.U., ad adottare tutte le misure idonee ad evitare che dall'utilizzo della Firma digitale derivi danno a terzi. Il Cliente è tenuto, altresì, a proteggere la segretezza della Chiave privata non comunicando o divulgando a terzi il codice personale identificativo (PIN) di attivazione della stessa, provvedendo a digitarlo con modalità tali da impedire ad altri soggetti di prenderne conoscenza e conservandolo in un luogo sicuro e diverso da quello in cui è custodito il dispositivo contenente la chiave. Il Cliente prende atto che la Chiave privata è strettamente personale e non può essere per alcuna ragione ceduta o data in uso a terzi; Egli pertanto è il responsabile esclusivo della sua protezione da danni, perdite, divulgazioni, modifiche o usi non autorizzati.

4.3 Il Cliente è altresì responsabile dei danni derivanti ai Fornitori e/o a terzi nel caso di ritardo di attivazione da parte sua delle procedure previste dal Manuale per la revoca e/o la sospensione del Certificato.

4.4 In caso di violazione anche di uno soltanto dei suddetti obblighi/impegni, i Fornitori avranno facoltà di intervenire nelle forme e nei modi ritenuti opportuni per eliminare, ove possibile, la violazione ed i suoi effetti, e di sospendere/revocare immediatamente e senza alcun preavviso i certificati, riservandosi inoltre il diritto di risolvere il contratto ai sensi del precedente art. 14 delle Condizioni generali – Sezione I.

5. Obblighi e limitazioni di responsabilità dei Fornitori

In nessun caso i Fornitori potranno essere ritenuti responsabili per i danni diretti o indiretti da chiunque subiti, ivi compreso il Cliente causati da revoche e/o sospensioni deli Certificato/i effettuate in conformità a quanto previsto nel relativo Manuale qualunque sia la motivazione posta a fondamento della stessa.

6. Revoca e sospensione del Certificato

La revoca o la sospensione del/i Certificato può essere eseguita nel rispetto dei presupposti, delle procedure e delle tempistiche indicate nel Manuale cui integralmente si rinvia.

7. Disattivazione del Servizio prima della scadenza

7.1 Ferme le disposizioni di cui all'art. 13 delle Condizioni generali – I Sezione, in ogni caso di disattivazione del Servizio in data antecedente la scadenza il Cliente è obbligato a non farne più alcun utilizzo.

7.2 In caso di esercizio della facoltà di recesso dal Contratto o dal Servizio da parte del Cliente o dei Fornitori, trascorso il termine di preavviso ivi indicato, il certificato di Firma Digitale Remota sarà disattivato/disabilitato in qualsiasi momento.

7.4 L'esercizio della facoltà di recesso da parte dei Fornitori, ai sensi del precedente art. 13 della Sezione I: Condizioni generali, cosi come la risoluzione del contratto ai sensi dell'art. 14 della Sezione I: Condizioni generali, non pregiudica il funzionamento del Dispositivo di firma digitale con o senza CNS già attivo alla data di efficacia del recesso fino alla sua naturale scadenza, salvo i casi di revoca del certificato o dei certificati in esso contenuti.

8. Modifiche dei Servizi e variazioni alle condizioni dell'offerta

In caso di modifiche al Servizio di Firma Digitale con o senza CNS, ai sensi dell'art. 15 delle Condizioni generali – Sezione I, i Servizi attivati o rinnovati precedentemente la data della variazione saranno mantenuti, fino alla loro prima scadenza, alle condizioni pattuite.

9. Hardware e software per il funzionamento del certificato

Qualora richiesto dal Cliente, il Certificatore consegnerà a questi, previa corresponsione del relativo costo, un dispositivo (hardware-Smart Card e/o lettore) di firma in grado di conservare e leggere la Chiave privata dello stesso e generare al proprio interno le firme digitali, nonché dispositivi software a valore aggiunto.

SEZIONE III - CONDIZIONI PARTICOLARI DI FORNITURA DEL SERVIZIO DI VALIDAZIONE TEMPORALE ELETTRONICA QUALIFICATA

1. Definizioni

Ove nominati nella presente Sezione i termini sotto riportati sono da intendersi con il seguente significato:

ETSI: acronimo di "European Telecommunications Standards Institute", l'organismo internazionale, indipendente e senza fini di lucro ufficialmente responsabile della definizione e dell'emissione di standard nel campo delle telecomunicazioni nell'UE.

Manuale: il Manuale Operativo del Servizio, presente al link https://www.pec.it/DocumentazioneMarcheTemporali.aspx, il quale riporta la politica e la descrizione del Servizio, le sue caratteristiche, i livelli di servizio, le eventuali limitazioni d'uso del medesimo e le prescrizioni per coloro che accedano alla verifica delle validazioni temporali elettroniche.

Organismo di valutazione della conformità: l'organismo accreditato ai sensi del Regolamento competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati.

Prestatore di servizi fiduciari qualificato: una persona fisica o giuridica che presta uno o più servizi fiduciari come prestatore di servizi fiduciari qualificato cui l'organismo di valutazione della conformità abbia assegnato tale qualifica.

Regolamento: il Regolamento UE n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, in materia di "identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno".

Servizio fiduciario qualificato: il servizio elettronico consistente negli elementi indicati dal Regolamento e che ne rispetta i relativi requisiti.

Servizio: il Servizio di validazione temporale elettronica qualificata, Servizio fiduciario qualificato erogato da Aruba PEC, che soddisfa i requisiti di cui all'art. 42 del Regolamento e delle Norme ETSI EN 319 401, 421 e 422, che consente di apporre una validazione temporale certa, opponibile a terzi, ad un documento informatico mediante un sistema valutato conforme alla politica riportata nel Manuale, reso disponibile mediante l'attivazione di un account di accesso al Servizio nelle modalità, con le caratteristiche e nei termini previsti dal Manuale stesso.

2. Descrizione, durata e rinnovo del Servizio

2.1 Il Servizio di cui alla presente Sezione consiste nell'erogazione al Cliente da parte di Aruba PEC, Prestatore di servizi fiduciari qualificato, del Servizio di validazione temporale elettronica qualificata, dal medesimo ordinato ed indicato nel Modulo d'ordine, che soddisfa i requisiti di cui all'art. 42 del Regolamento e delle Norme ETSI EN 319 401, 421 e 422, che consente di apporre una validazione temporale certa, opponibile a terzi, ad un documento informatico mediante un sistema valutato conforme alla politica riportata nel Manuale, reso disponibile mediante l'attivazione di un account di accesso al Servizio stesso nelle modalità, con le caratteristiche e nei termini previsti dal Manuale.
2.2 Il Cliente potrà usufruire del Servizio fino all'esaurimento del lotto acquistato, terminato il quale il Servizio sarà disattivato.
2.2 Esaurito il lotto, ed in mancanza di nuovi acquisti, l'account del Cliente rimarrà attivo per 6 mesi, successivamente ai quali sarà disattivato ed il Cliente per poter procedere ad un nuovo acquisto sarà tenuto a creare un nuovo account.

3. Utilizzo, revoca e sospensione, disattivazione del Servizio

3.1 Il Servizio sarà utilizzabile secondo le modalità, nei termini, con le caratteristiche e le limitazioni previste nel Manuale e nel Contratto.

3.2 I Fornitori garantiscono la fornitura e l'utilizzo del Servizio 24/7/365, secondo quanto previsto nel Manuale; altresì, garantiscono che le politiche utilizzate per la fornitura del Servizio rendono il medesimo accessibile paritariamente a tutti gli utenti senza alcuna forma di discriminazione.

3.3 I registri elettronici delle validazioni temporali emesse sono mantenuti nei termini riportati nel Manuale.

3.4 I Fornitori provvederanno alla revoca ovvero alla sospensione dell'account qualora si verifichi una delle seguenti circostanze:

a) richiesta esplicita formulata dal titolare dell'account per iscritto;

b) riscontro di una avvenuta violazione degli obblighi incombenti sul richiedente e/o sul titolare dell'account;

c) abusi e falsificazioni;

d) richiesta proveniente dall'Autorità Giudiziaria.

3.5 Il Cliente potrà richiedere ai Fornitori la revoca/sospensione/disattivazione dell'account con apposita comunicazione sottoscritta, contenente gli elementi utili ai fini dell'identificazione del medesimo e del relativo account nonché l'indicazione delle ragioni per le quali si richiede la revoca/sospensione. Il Cliente prende atto ed accetta che il Servizio, prevedendo la fornitura di un prodotto personalizzato, rientra nella previsione di cui all'art. 13.1, ultimo capoverso, della Sez. 1 delle Condizioni. L'ordine può essere bloccato ed eventualmente disdetto qualora la

produzione ad esso relativa non sia stata ancora in alcun modo avviata; in tal caso il Cliente avrà diritto ad ottenere esclusivamente la restituzione del corrispettivo versato, con esclusione dei costi già sostenuti dai Fornitori.

3.6 In caso di revoca dell'account, per qualsiasi motivo, nessuno escluso e/o eccettuato, il Cliente non avrà diritto alla restituzione del corrispettivo versato.

3.7 La revoca o la sospensione determinano rispettivamente la disattivazione o la sospensione del relativo Servizio.

4. Disposizioni finali

4.1 I Fornitori potranno delegare, in tutto o in parte, a terzi soggetti, anche esterni alla propria organizzazione, singole funzioni o fasi del Servizio, mantenendo nei confronti del Cliente l'integrale responsabilità dell'esecuzione e della fornitura del Servizio stesso, rispondendo in proprio di tutte le attività del delegato come se fossero state poste in essere dalla medesima. I Fornitori garantiscono che tali soggetti, quando delegati, sono vincolati ad adottare tutte le misure di sicurezza dalla medesima indicate e tutte le prescrizioni imposte dalla normativa vigente.
4.2 Il Cliente prende atto ed accetta di essere tenuto ad informare coloro che accedano alla verifica delle validazioni temporali elettroniche delle prescrizioni indicate al riguardo nel Manuale.
4.3 Gli obblighi e le limitazioni di responsabilità dei Fornitori sono quelli riportati nel Manuale e nel Contratto. In deroga a quanto previsto dall'art. 2 della Sez. I delle Condizioni, per quanto riguarda il Servizio di cui alla presente Sezione, in caso di contrasto le disposizioni del Manuale prevarranno su quelle delle Condizioni.

SEZIONE IV - CONDIZIONI PARTICOLARI DI FORNITURA DEL SERVIZIO DI POSTA ELETTRONICA CERTIFICATA

1. Definizioni

Ove nominati nel Contratto i termini sotto riportati sono da intendersi con il seguente significato:

Casella PEC: casella di Posta Elettronica Certificata definita all'interno di un dominio PEC alla quale è associato un sistema di "trasporto" di documenti informatici che presenta delle forti similitudini con il servizio di posta elettronica "tradizionale", cui però sono state aggiunte delle caratteristiche tali da fornire agli utenti la certezza, con valore legale, dell'invio e della consegna (o meno) dei messaggi e-mail al destinatario;

Dominio Pec: dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata.

Rinnovo automatico: l'opzione che consente il rinnovo automatico del Servizio Posta Elettronica Certificata – Pec alla relativa scadenza, secondo quanto previsto all'art. 6 della Sez. I delle Condizioni;

Servizio Posta Elettronica Certificata - Pec: la casella o le caselle di Posta Elettronica Certificata (PEC), e altri servizi aggiuntivi, definita/e all'interno di un dominio certificato che è/sono concessa/e in uso al Cliente.

Utilizzatore: persona fisica alla quale il Cliente concede l'utilizzo della singola casella di posta elettronica attivata con il servizio Pec, alla quale però non sono attribuiti diritti e/o obblighi derivanti dal presente Contratto.

2. Requisiti

Il Cliente, per poter ordinare ed usufruire del Servizio di Posta Elettronica Certificata è tenuto a dotarsi autonomamente delle risorse hardware e software necessarie alla sua fruizione, assumendosi al riguardo ogni responsabilità per la loro funzionalità e compatibilità con il predetto Servizio e per la loro corretta configurazione. Il Cliente manleva fin da ora i Fornitori da qualsiasi responsabilità circa eventuali problemi di configurazione, funzionalità o compatibilità delle risorse hardware o software rispetto a detto servizio.

3. Durata e rinnovo del Servizio di Posta Elettronica Certificata

3.1 Fermo quanto previsto all'art. 6 della Sez. I delle Condizioni, il servizio di Posta Elettronica Certificata ha durata annuale ed alla scadenza fissata cesserà la sua efficacia salvo rinnovo, da effettuarsi prima della data di scadenza mediante l'inoltro dell'apposito ordine di rinnovo ed il pagamento del corrispettivo richiesto. Il Cliente prende atto ed accetta che, in caso la procedura di rinnovo sopra descritta sia completata in data antecedente a quella di scadenza, i servizi oggetto dell'ordine di rinnovo saranno erogati in favore del Cliente dalla data del loro rinnovo, mentre i servizi non rinnovati saranno disattivati alla data di completamento della procedura di rinnovo, anche se antecedente a quella di loro scadenza.
3.1.1 Nel caso in cui alla data di scadenza, il Cliente non abbia rinnovato il Servizio di PEC, o, avendo attivato l'opzione di "Rinnovo automatico", il pagamento non sia stato validamente accreditato ai Fornitori nei termini per qualsivoglia motivo o causale caselle PEC saranno sospese ed il Cliente non potrà accedere o utilizzare il Servizio; Il Cliente avrà la possibilità di rinnovare il Servizio per altri 90 (novanta) giorni decorrenti dalla data di scadenza, trascorsi inutilmente i quali le caselle PEC saranno disattivate, restando esplicitamente esclusa, ora per allora, ogni e qualsiasi responsabilità da parte dei Fornitori. il Cliente, pertanto, è tenuto ad effettuare il backup e/o copia del contenuto delle caselle pec prima della data di scadenza, in quanto i Fornitori, a seguito del mancato rinnovo, non garantiscono il recupero dei messaggi.

4. Accesso al Servizio

Il Cliente dichiara di essere l'unico ed esclusivo amministratore del Servizio e come tale di essere l'unico soggetto in possesso delle password di accesso ad esso. Fermo restando quanto previsto al precedente art. 10.7 delle Condizioni Generali – Sezione I, il Cliente mantiene la facoltà di decidere, a proprio ed esclusivo rischio, se e con quali modalità abilitare ad altri l'accesso al Servizio; in tali casi, anche qualora l'accesso ad altri

sia consentito per il tramite dei servizi erogati dai Fornitori, il Cliente dichiara di: (i) essere l'unico ed esclusivo responsabile di tali accessi, rispondendo di essi e delle attività a loro conseguenti come se fossero state da Egli eseguite, e (ii) di impegnarsi ora per allora a mantenere indenni e manlevare i Fornitori da ogni e qualsiasi richiesta o pretesa di chiunque per i danni agli stessi arrecati dal o mediante l'utilizzo del Servizio. Il Cliente dovrà sostenere tutti i costi, risarcimento di danni ed oneri, incluse le eventuali spese legali, che dovessero scaturire da tali azioni di responsabilità e si impegna ad informare i Fornitori qualora tale azione dovesse essere intentata nei propri confronti.

5. Capienza casella di posta elettronica certificata

Il Cliente prende atto ed accetta che la/e casella/e di posta elettronica ha/hanno la capienza indicata nella singola offerta scelta dal Cliente e che, pertanto, nell'ipotesi in cui si raggiunga la quota ivi indicata non sarà più possibile ricevere messaggi. Il Cliente prende atto ed accetta che è suo esclusivo onere provvedere in modo autonomo alla cancellazione dei messaggi per poter liberare spazio. Il Cliente manleva fin da ora i Fornitori da qualsiasi responsabilità per la mancata ricezione dei messaggi di posta.

6. Servizi aggiuntivi

Il Cliente, assegnatario di una casella di posta elettronica certificata, ha facoltà di acquistare, mediante apposito ordine online e pagamento del relativo corrispettivo, uno o più dei Servizi Aggiuntivi indicati sul sito www.pec.it. Il Cliente prende atto ed accetta che i Servizi Aggiuntivi sono forniti con le modalità, i termini e le caratteristiche tecniche ed economiche indicate sul sito istituzionale e su quello di assistenza, nelle apposite sezioni ad essi dedicate, di cui il Cliente dichiara di aver preso visione e di accettare ed a cui si rinvia integralmente. Resta inteso che i Servizi Aggiuntivi, indipendentemente dal momento della loro attivazione, assumono la medesima data di scadenza della casella di Posta Elettronica Certificata cui sono associati e non potranno essere acquistati nei 3 (tre) mesi antecedenti la predetta scadenza. L'attivazione e la fornitura dei Servizi Aggiuntivi sono disciplinate dalle presenti Condizioni di fornitura.

7. Documentazione

7. Documentazione Il Cliente prende atto che, come previsto dalla vigente normativa in materia di PEC, art. 11 D.P.R. n. 68/2005, durante le fasi di trasmissione del messaggio di posta elettronica certificata, il Gestore mantiene traccia delle operazioni svolte su un apposito log dei messaggi. I dati contenuti nel suddetto registro sono conservati dal gestore di posta elettronica certificata per trenta mesi. Pertanto, entro il predetto termine il Cliente potrà richiedere ai Fornitori un estratto del file di log relativo ad un messaggio afferente la propria casella di posta elettronica certificata, specificando nella richiesta la data di invio o di ricezione, gli indirizzi di PEC del mittente e del/i destinatario/i e facoltativamente l'oggetto del messaggio. Per quanto riguarda gli eventuali altri log generati e conservati dai Fornitori saranno esibiti in conformità alle vigenti disposizioni di legge e costituiranno piena ed incontrovertibile prova dei fatti e degli atti compiuti dal Cliente medesimo in relazione ai Fornitori.

8. Limitazioni di responsabilità dei Fornitori

8.1 In nessun caso i Fornitori potranno essere ritenuti responsabili per i danni diretti o indiretti:

a) causati ai Clienti o a terzi per uso improprio del sistema o per mancato rispetto delle regole e degli obblighi descritti nelle presenti condizioni contrattuali, nel/nei Manuale/i e nel sito www.pec.it;

b) derivanti da cause di forza maggiore, caso fortuito, eventi catastrofici (a titolo esemplificativo ma non esaustivo: incendi, esplosioni ecc.);

c) provocati dalla mancata conservazione dei messaggi inviati e/o ricevuti e/o trasmessi e/o conservati attraverso il Servizio PEC, restando inteso che tale responsabilità è assunta unicamente dal Cliente;

d) cagionati dal contenuto dei messaggi inviati e ricevuti mediante il Servizio PEC restando inteso che la responsabilità civile e penale dei contenuti inviati tramite PEC sono e restano a carico del Cliente;

e) di qualsiasi tipo, da chiunque patiti derivanti da uno scorretto utilizzo della password di accesso, il Cliente è tenuto, pertanto, a conservare e a far conservare, ove trasmessi, ai propri dipendenti e/o collaboratori la password di accesso con la massima diligenza e riservatezza obbligandosi a non cederla o consentirne l'uso a terzi;

f) di qualsiasi natura ed entità patiti dal Cliente e/o da terzi causati da manomissioni o interventi sul servizio o sulle apparecchiature effettuati dal Cliente e/o da parte di terzi non autorizzati dai Fornitori;

g) di qualsiasi natura da chiunque patiti derivanti dal mancato invio o dalla mancata consegna dei messaggi.

Restano ferme in tali casi le limitazioni di cui agli art. 9.2 e 9.5 delle Condizioni Generali – Sezione I.

8.2 Fermo quanto sopra, qualora il Servizio Posta Elettronica Certificata – Pec sia definito all'interno di un dominio certificato non assegnato ai Fornitori e pertanto non sotto il loro controllo e/o gestione, il Cliente, ora per allora, prende atto ed accetta che il Servizio acquistato possa essere erogato con particolari limitazioni (a titolo esemplificativo e non esaustivo: limitazioni alla sua durata, possibilità di cessazione e/o disattivazione anticipata del Servizio, limitazioni alla possibilità di rinnovo), così sollevando i Fornitori da ogni responsabilità per gli eventuali danni, diretti o indiretti, di qualsiasi natura e specie, patiti e patiendi per o a causa delle suddette limitazioni e/o derivanti da qualsiasi operazione eseguita dall'assegnatario/titolare del dominio certificato sul quale è definita la casella Pec oggetto del Servizio Posta Elettronica Certificata – Pec.

9. Disattivazione del Servizio prima della scadenza

9.1 Il Cliente prende atto ed accetta che potrà chiedere la disattivazione di una o di più caselle di posta elettronica certificata attivate con il Servizio di Posta Elettronica Certificata, in data antecedente la loro scadenza, con le modalità indicate all'art. 13 delle Condizioni generali – I Sezione. In ogni caso di disattivazione delle caselle di posta elettronica certificata in data antecedente la scadenza, il Cliente è obbligato a non farne più alcun utilizzo.

9.2 In caso di esercizio della facoltà di recesso dal Contratto o dal Servizio da parte del Cliente o dei Fornitori, trascorso il termine di preavviso ivi indicato, la/e casella/e di posta elettronica certificata sarà/saranno disattivata/e e disabilitata/e in qualsiasi momento. In tale ipotesi i Fornitori restituiranno al Cliente il rateo del prezzo del Servizio come indicato all'art. 13 delle Condizioni generali – Sezione I.

SEZIONE V - CONDIZIONI PARTICOLARI DI FORNITURA DEI SERVIZI DOCFLY E DOCFLY FATTURAZIONE PA

1. Definizioni

Ove nominati nella presente Sezione V, e negli altri documenti da essa richiamati, i termini sotto riportati sono da intendersi con il seguente significato:

Agente di alterazione: qualsiasi codice contenuto in un documento informatico potenzialmente idoneo a modificare la rappresentazione dell'informazione senza alterarne il contenuto binario (in via meramente esemplificativa e non esaustiva: macro, codici eseguibili nascosti, formule di foglio di lavoro occulte in tutto o in parte, sequenze di caratteri occultate all'interno dei documenti informatici);

Delega Fattura PA: atto contenuto all'art. 11 della presente Sez. V con il quale il Cliente, predisposta la/e Fattura/e PA con i dati e le informazioni in suo possesso, delega espressamente Aruba Pec ad emetterla e ad apporvi la sua firma digitale;

Elenco Persone: Elenco delle persone designate dal Cliente ad operare in suo nome, conto e interesse con i Fornitori per l'esecuzione del contratto;

Fattura/e PA: il documento informatico, privo di codice non eseguibile e/o di macroistruzioni, da trasmettere allo Sdi in formato Xml, contenente i dati della/e fattura/e elettronica/che emessa/e dal Cliente, ovvero da Aruba Pec se delegata, ai sensi dell'articolo 21, comma 1, del DPR 633/72 per l'attuazione di quanto previsto dalla legge n. 244/2007 e dal Decreto del Ministero dell'Economia e delle Finanze n. 55 del 3 Aprile 2013 e loro ss.mm.ii;

Manuale: il Manuale del Sistema di conservazione digitale dei documenti informatici predisposto da Aruba Pec, accettato e fatto proprio in ogni sua parte dal Cliente, disponibile per il download al link http://www.agid.gov.it/sites/default/files/documentazione/manuale_di_conservazione_aruba_ver_1.2.pdf;

Manuale utente Fatturazione PA: il documento contenente le Specifiche Tecniche disponibile al link http://kb.aruba.it/KB/a5839/manuale-fatturazione-pubblica-amministrazione.aspx;

Pannello : l'area che Aruba mette a disposizione del Cliente per la gestione dei Servizi attraverso una applicazione sicura raggiungibile via web utilizzando le proprie Credenziali di accesso;

Produttore: è il Cliente che in proprio o attraverso persone fisiche dallo stesso incaricate di cui all'Elenco persone produce il Pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione;

Responsabile della conservazione: il Cliente, od il soggetto dal medesimo nominato di cui all'Elenco persone, il quale ha facoltà di affidare a terzi, in tutto o in parte, l'esecuzione delle attività previste a suo carico dalla vigente normativa;

Responsabile del servizio di conservazione: Aruba Pec a seguito della delega del Responsabile della conservazione anche per tramite del Cliente secondo quanto previsto all'art. 6.1.1, alla esecuzione delle attività indicate nell'Atto di delega all'art. 10 della presente Sezione V;

Rinnovo automatico: l'opzione che consente il rinnovo automatico del Servizio alla relativa scadenza , secondo quanto previsto all'art. 6 della Sez. I delle Condizioni;

Scheda di conservazione: Elenco dei documenti informatici che il Cliente sottopone a conservazione con il Contratto;

SLA: i livelli di servizio indicati nel Manuale utente e/o nelle Specifiche tecniche;

Servizio/i: il Servizio DocFly di conservazione digitale a norma dei documenti informatici e/o il Servizio DocFly - Fatturazione PA, secondo quanto prescelto dal Cliente nel Modulo d'ordine, il tutto come meglio descritto nelle Specifiche Tecniche e nel Manuale;

Sistema di interscambio (in breve **"Sdi**"): sistema informatico attraverso il quale avviene la trasmissione della FatturaPA, le cui modalità di funzionamento sono stabilite dal D.M. 3 aprile 2013, numero 55.

Xml: acronimo di "eXtensible Markup Language"cioè l'insieme di regole per strutturare in formato testo i dati oggetto di elaborazione ai fini della trasmissione della Fattura PA allo Sdi;

2. Requisiti

2.1 Il Servizio DocFly risponde all'esigenza di conservare - per il periodo stabilito nel Contratto - i documenti informatici di cui il Cliente è Titolare ovvero, quando consentito dalle Specifiche tecniche del Servizio, dei documenti informatici di cui sono Titolari terzi soggetti, prodotti, sottoscritti digitalmente e versati in conservazione dal Cliente in virtù di specifica delega a tal fine rilasciatagli dai suddetti terzi e, garantendone l'integrità e la validità legale nel tempo nonché la loro Esibizione, ed è reso disponibile al Cliente tramite il Pannello.

2.2.1 Con specifico riguardo al Servizio DocFly Fatturazione PA il Cliente riconosce e prende atto che esso:
a) gli consente di emettere e trasmettere, la/le sua/e fattura/e PA alla Pubblica Amministrazione interessata attraverso il Sdi;
b) non è acquistabile né rinnovabile disgiuntamente dal servizio DocFly di conservazione digitale a norma dei documenti informatici oggetto del Servizio DocFly Fatturazione PA stesso;
c) è resa disponibile al Cliente tramite il Pannello;
d) prevede l'aggregazione dei dati trasmessi dal Cliente mediante il Pannello in formato Xml.

2.2.2 La Fattura PA sarà trasmessa alla Pubblica Amministrazione interessata attraverso il Sistema di interscambio solo dopo che il Cliente avrà confermato la correttezza e completezza dei dati e delle informazioni ivi riportate e autorizzato detta trasmissione. Resta inteso che oltre all'erogazione del Servizio DocFly Fatturazione PA le altre attività poste a carico dei Fornitori sono esclusivamente quelle indicate nella Delega Fattura PA, contenuta Contratto rilasciata dal Cliente e nei limiti ivi stabiliti;

3. Attivazione del Servizio

3.1 Salvo diverso accordo tra le Parti, il Servizio è attivato ed erogato nel rispetto dei tempi resi necessari dalla disponibilità delle risorse hardware e software. Resta altresì inteso che l'attivazione potrà avvenire solo dopo che il Cliente avrà correttamente eseguito le attività previste a suo carico per l'attivazione del Servizio come previste nel Manuale.

3.2 Il Cliente prende atto ed accetta che con l'avvenuta attivazione del Servizio di cui al precedente comma saranno da intendersi accettate da parte di Aruba Pec le nomine e/o le deleghe di cui ai successivi articoli 10 e 11.

3.3. Fatte salve le altre disposizioni in materia contenute nel Contratto il Cliente prende atto ed accetta che nessun diritto o pretesa potrà far valere nei confronti dei Fornitori per la omessa o ritardata attivazione e/o erogazione del Servizio ed in ogni caso si impegna a a manlevare e/o tenere indenne i Fornitori da ogni richiesta di risarcimento da chiunque avanzata.

4. Durata del Servizio e cessazione

4.1 Fermo quanto previsto all'art. 6 della Sez. I delle Condizioni, il Servizio ha la durata indicata nel Modulo d'ordine fatti salvi: i) gli eventuali giorni di proroga riconosciuti ai sensi dello SLA o, ii) i casi di sua cessazione come dallo stesso Contratto previsti; alla scadenza fissata cesserà la sua efficacia salvo rinnovo, da effettuarsi prima della data di scadenza mediante l'inoltro dell'apposito ordine di rinnovo ed il pagamento del corrispettivo richiesto. Il Cliente prende atto ed accetta che, in caso la procedura di rinnovo sopra descritta sia completata in data antecedente a quella di scadenza, i servizi oggetto dell'ordine di rinnovo saranno erogati in favore del Cliente dalla data del loro rinnovo, mentre i servizi non rinnovati saranno disattivati alla data di completamento della procedura di rinnovo, anche se antecedente a quella di loro scadenza.

4.1.1 Nel caso in cui alla data di scadenza il Cliente non abbia rinnovato il Servizio, o, avendo attivato l'opzione di "Rinnovo automatico", il pagamento non sia stato validamente accreditato ai Fornitori nei termini per qualsivoglia motivo o causa, il Servizio sarà cessato, restando esplicitamente esclusa, ora per allora, ogni e qualsiasi responsabilità da parte dei Fornitori. Il Cliente avrà comunque la possibilità di rinnovare il Servizio per altri 60 (sessanta) giorni decorrenti dalla data di cessazione, fermo quanto previsto all'art. 7.3 della Sezione I delle Condizioni.

4.4 Il Cliente, consapevole degli obblighi previsti esclusivamente a suo carico dalla vigente normativa in ordine al periodo minimo di conservazione e accesso al documento informatico di volta in volta interessato, prende atto ed accetta che la cessazione, per qualsiasi causa, del Contratto comporta l'automatica cessazione del Servizio. In tale ipotesi al Cliente sarà:

i) inibito il versamento di nuovi documenti nel Sistema di conservazione ; e
ii) consentito il prelievo dei documenti informatici presenti nel Sistema di conservazione secondo le modalità e nei termini stabiliti nel Manuale e nel Contratto, fermo quanto previsto al successivo comma 4.5.

4.5 In tutti i casi di cessazione del Contratto e/o del Servizio i Fornitori consentiranno al Cliente di recuperare i propri documenti, entro e non oltre 60 (sessanta) giorni dalla data di detta cessazione. I documenti informatici dovranno essere prelevati dal Cliente– quindi non incombe sui Fornitori alcun obbligo di provvedere alla materiale restituzione dei documenti informatici conservati – secondo le modalità stabilite nel Manuale e dal Contratto. Decorso il suddetto termine, il Cliente autorizza sin da ora i Fornitori a cancellare i documenti informatici e gli annessi metadati versati in conservazione (e tutte le relative copie di salvataggio). Fermo quanto sopra, i documenti informatici originariamente versati

dal Cliente nel Sistema di conservazione saranno a quest'ultimo restituiti nel loro formato originale, fatto salvo il caso che i suddetti documenti abbiano subito una conversione di formato per sopperire all'obsolescenza del formato originario; in quest'ultimo caso saranno restituiti nel formato convertito. Contestualmente, saranno restituiti anche i metadati associati ai documenti informatici originariamente forniti dal Cliente.

4.6. Fatte salve le altre disposizioni in materia contenute nel Contratto il Cliente solleva ora per allora i Fornitori da ogni e qualsiasi responsabilità per il mancato rinnovo del Servizio e si impegna a manlevare e/o tenere indenne i Fornitori stessi da ogni richiesta di risarcimento da chiunque avanzata.

5. Obblighi e limitazioni di responsabilità dei Fornitori

5.1 Per tutta la durata del Contratto, i Fornitori si impegnano a rendere disponibile al Cliente un Sistema di conservazione funzionante ed a norma di legge raggiungibile via web che operi secondo modelli organizzativi che garantiscano la sua distinzione logica e fisica dal sistema di gestione documentale del Cliente;

5.2.1 Relativamente al programma software utilizzato per l'erogazione del Servizio, i Fornitori garantiscono:

a) il ripristino delle funzionalità in caso di malfunzionamenti del software di sistema e/o d'ambiente, anche secondo quanto indicato nel Manuale;
b) l'arricchimento delle funzioni degli applicativi software determinato da nuove release innovative del software di sistema e/o d'ambiente;
c) l'adeguamento del software all'evoluzione della vigente normativa in materia.

5.3 Il Cliente riconosce che la rete internet non è controllata dai Fornitori e che per la peculiare struttura della rete medesima non se ne possa garantire le prestazioni e la funzionalità né controllare i contenuti delle informazioni che sono trasmesse mediante la medesima. Per questo motivo nessuna responsabilità potrà essere imputata ai Fornitori per eventuali illeciti commessi da terzi in danno del Cliente durante l'utilizzo del Servizio tramite la connessione internet.

5.4 Fatte salve le ipotesi inderogabilmente previste dalla legge, in nessun altro caso, per nessun titolo e/o ragione, i Fornitori potranno essere ritenuti responsabili nei confronti del Cliente, ovvero verso altri soggetti, direttamente o indirettamente, connessi o collegati al Cliente, per danni, diretti o indiretti, perdite di dati, alterazione del contenuto semantico dei documenti, violazione di diritti di terzi, ritardi, malfunzionamenti, interruzioni, totali o parziali, che si dovessero verificare a fronte dell'erogazione del Servizio, ove connessi, direttamente o indirettamente, o derivanti:

a) dal non corretto utilizzo del Servizio da parte del personale e/o incaricati del Cliente;
b) da qualsiasi abuso relativo alla veridicità dei dati personali comunicati in occasione della richiesta di attivazione del Servizio e di ogni altra variazione che dovesse intervenire relativamente ai dati comunicati in occasione della richiesta;
c) dal malfunzionamento dei macchinari, hardware e software, utilizzati dal Cliente e/o per il non regolare funzionamento di internet, delle linee elettriche, telefoniche nazionali e/o internazionali;
d) dalla mancata attivazione o dal mancato accesso al Servizio dovuta al mancato adeguamento dei sistemi informativi ed applicativi del Cliente stesso;
e) da ritardi, malfunzionamenti e interruzioni del Servizio causati da insufficiente adeguamento dei sistemi informatici ed applicativi del Cliente, da comunicazione errata, incompleta o non veritiera da parte del Cliente dei dati necessari per l'esecuzione del Servizio;
f) dalla presenza di virus, errori o, più in generale, dalla presenza di qualsiasi Agente di alterazione nei documenti informatici, dati e/o files consegnati dal Cliente a i Fornitori per l'esecuzione del Servizio;
g) dal mancato rispetto da parte del Cliente degli obblighi e termini di formazione, trasmissione, di spedizione, di consegna, di versamento, di controllo e di verifica dei documenti informatici e/o dei dati, inerenti lo svolgimento delle proprie attività stabilite nel Contratto compreso il Manuale;
h) dalla fallita integrità della rappresentazione (a video o in stampa) di dati o fatti contenuti nei documenti informatici o dalla loro non leggibilità, qualora il Cliente non si sia attenuto alla formazione/produzione/emissione dei documenti informatici nei formati previsti dal Contratto e/odal Manuale;
i) dai dati, fatti e/o informazioni contenute nei documenti informatici, che saranno determinati solo ed esclusivamente dal soggetto passivo d'imposta ovvero dal Cliente con esonero da ogni responsabilità verso i terzi compresa l'Amministrazione finanziaria;
j) dall'inosservanza e/o dal mancato adempimento e/o dalle violazioni degli obblighi di legge imputabili al Cliente, (quali, a titolo esemplificativo ma non esaustivo: Codice della Privacy, norme in materia di lavoro, sicurezza, ecc.);
k) dall'utilizzo da parte del Cliente, per la sottoscrizione dei documenti informatici versati in conservazione, di certificati di sottoscrizione non validi, scaduti o non rinnovati entro il termine previsto per la Chiusura dei pacchetti di archiviazione;

5.5 In ogni caso resta inteso che ai fini della classificazione dei documenti versati in conservazione, i Fornitori si attengono ai requisiti di classificazione specificati dal Cliente nei metadati associati ai rispettivi documenti informatici. Nel caso in cui non sia fornita dal Cliente alcuna indicazione sulla classificazione dei documenti informatici in ingresso, i Fornitori sono fin da

ora autorizzati a rifiutare i singoli documenti privi dei metadati di classificazione o l'intero pacchetto di versamento contenente uno o più documenti privi dei metadati di classificazione.

5.6. In caso di erogazione del Servizio DocFly - Fatturazione PA resta inteso tra le parti che:

a) i Fornitori sono tenuti a rendere disponibili le necessarie funzioni offerte con i Servizi solo all'esito positivo della procedura di autenticazione del Cliente tramite il Pannello ;

b) il Cliente riconosce e prende atto che i Fornitori non hanno alcun potere, dovere e/o compito in relazione:

i. alla forma ed ai contenuti dei documenti informatici rilevanti ai fini delle disposizioni tributarie versati in conservazione;

ii. ai metadati associati ai documenti rilevanti ai fini delle disposizioni tributarie forniti dal Cliente e dallo stesso versati in conservazione;

iii. ai dati contenuti nelle fatture, alla determinazione della natura, qualità e quantità dei beni e dei servizi formanti l'oggetto dell'operazione;

iv. ai dati contenuti nelle Fatture PA, alla determinazione della natura, qualità e quantità dei beni e dei servizi formanti l'oggetto dell'operazione;

v. al contenuto ed alla semantica dei documenti conservati la cui sottoscrizione nei relativi pacchetti di archiviazione è effettuata al solo fine di dare atto che il processo di conservazione è stato eseguito correttamente, nel rispetto della vigente normativa;

vi. alla determinazione dei corrispettivi, della base imponibile e delle aliquote riportati nelle Fatture PA;

vii. alla determinazione dei dati richiesti dall'art. 21 del DPR 633/72 e s.m.i. e da eventuali altre disposizioni riportati nelle Fatture PA;

viii. alla verifica della corretta sequenzialità cronologica e continuità numerica delle Fatture PA e più in generale di qualsiasi documento a queste collegato;

ix. alla verifica della presenza di tutti i dati ed informazioni necessari ad attivare le funzionalità di ricerca logica delle fatture e/o dei documenti rilevanti ai fini delle disposizioni tributarie;

c) in ragione di quanto sopra, i Fornitori non potranno altresì in alcun modo essere ritenuti direttamente o indirettamente responsabili di alcuna conseguenza pregiudizievole, di carattere fiscale, tributario, civile o penale in cui dovesse incorrere il Cliente per le suddette cause nei confronti delle Pubbliche Amministrazioni e dei terzi per tutte le operazioni connesse e derivanti dall'emissione e sottoscrizione con firma digitale delle Fatture PA, anche quando delegata dal Cliente alla stessa Aruba Pec.

5.7 i Fornitori non potranno in alcun modo essere ritenuti responsabili di alcuna conseguenza pregiudizievole, di carattere fiscale, tributario, civile o penale in cui dovesse incorrere il Cliente in ragione delle suddette cause.

5.8 Fermo quanto sopra resta inteso che gli obblighi e le responsabilità dei Fornitori verso il Cliente sono esclusivamente quelli definiti dal Contratto, pertanto in caso di violazione o inadempimento esclusivamente imputabile ai Fornitori, la stessa risponderà nei limiti previsti dallo SLA come meglio indicati al successivo art. 17 restando espressamente escluso, ora per allora, qualsiasi altro indennizzo o risarcimento al Cliente per danni diretti o indiretti di qualsiasi natura e specie. Quando non trova applicazione lo SLA il Cliente prende atto ed accetta, ora per allora, che i Fornitori non saranno tenuti a versargli alcun indennizzo o risarcimento e non risponderà di alcun danno, diretto o indiretto, di qualsiasi natura e specie. In ogni caso, anche in tale ipotesi, la somma massima che i Fornitori potranno essere chiamati a versare al Cliente non dovrà essere superiore ad € 1,00 (euro uno/00) per ogni Gb di documenti conservati.

6. Obblighi e diritti del Cliente

6.1.1 Il Cliente, assumendosi ogni rischio e responsabilità al riguardo, dichiara:

a) di possedere l'insieme delle conoscenze tecniche necessarie per la corretta utilizzazione del Servizio, compreso il trattamento e/o la sicurezza di dati e/o informazioni e/o contenuti da egli stesso immessi nel Sistema di conservazione o comunque forniti ai Fornitori. Il Cliente è in ogni caso tenuto a conoscere le disposizioni relative alla vigente normativa ed a controllare l'esattezza dei risultati ottenuti con l'utilizzo del Servizio. Costituisce onere del Cliente procurarsi, a sua cura e spese, la connessione per collegare le sua sede ovvero le sue postazioni di lavoro al Data Center attraverso il quale i Fornitori erogano il Servizio; e

b) qualora abbia incaricato un proprio Responsabile della Conservazione, di aver ricevuto da questi apposita delega in corso di validità ad effettuare le nomine e le deleghe di cui ai successivi artt. 10 e 11.

c) che i soggetti dallo stesso designati mediante l'Elenco persone sono stati dallo stesso valutati come persone esperte ed affidabili ed in grado di interagire autonomamente con i Fornitori ed il sistema di conservazione dalla stessa fornito, e d inoltre di aver impegnato per iscritto i suddetti soggetti a rispettare quanto previsto dal Contratto inclusi i relativi allegati, e che i medesimi a loro volta hanno dichiarato per

iscritto di essere informati circa il contenuto dei richiamati documenti e di conoscere quanto previsto dalla normativa vigente regolante la conservazione di documenti informatici ivi inclusa quella relativa alla privacy. Il cliente si assume ogni responsabilità in ordine all'operato dei suddetti soggetti impegnandosi a manlevare e/o tenere indenni i Fornitori da ogni e qualsiasi responsabilità per eventuali richieste danni, diretti o indiretti, da chiunque avanzate per fatti imputabili a detti soggetti. Il Cliente si obbliga a tenere aggiornato l'elenco dei suddetti incaricati nonché a comunicare tempestivamente ai Fornitori ogni variazione rispetto ai dati sopra riportati.

6.2 I documenti informatici oggetto del Servizio saranno versati in conservazione dal Cliente, completi dei metadati ad essi associati, affinché siano conservati in modo elettronico per il periodo di durata stabilito in Contratto. Le funzioni di versamento in conservazione e di esibizione dei documenti informatici saranno svolte attraverso il Pannello Gestione che rende disponibili al Cliente l'insieme delle componenti funzionali a supporto del processo di conservazione, nelle modalità e nei termini stabiliti dal Manuale. Salvo diverso e specifico accordo i documenti informatici saranno posti in conservazione nel medesimo formato che avevano al momento in cui sono stati versati in conservazione dal Cliente.

6.3 Nei casi in cui sia richiesto l'intervento del Pubblico Ufficiale, il Cliente è tenuto a garantire ai Fornitori l'assistenza e le risorse, anche economiche, necessarie per l'espletamento delle attività che i Fornitori attribuiranno al medesimo. In ogni caso il Cliente è e resta l'unico ed esclusivo titolare dei documenti informatici e dei dati da egli stesso versati in conservazione assumendosi espressamente ogni più ampia responsabilità in ordine al loro contenuto; per l'effetto il Cliente solleva, ora per allora, e comunque si impegna a manlevare e/o tenere indenne i Fornitori da ogni obbligo e/o onere di accertamento e/o di controllo diretto e indiretto al riguardo.

6.4 Il Cliente prende atto ed accetta che:

a) per tutta la durata del Contratto ed in qualsiasi momento il Sistema di conservazione è in grado di esibire tutti i documenti informatici in esso conservati;

b) fermo quanto precede, la ricezione e l'esibizione dei documenti informatici potrà avvenire solo per via telematica e solo dietro specifica istanza presentata dai soggetti autorizzati;

c) solo il Cliente e l'Utente, e per essi i loro incaricati, qualora specificatamente autorizzati, potranno richiedere al Sistema di conservazione l'accesso e l'esibizione dei documenti informatici conservati per acquisire le informazioni di loro interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal Sistema di conservazione secondo le modalità previste dal Manuale;

d) l'Esibizione del documento informatico ottenuto tramite interrogazione del Sistema di conservazione o tramite la consultazione su supporto ottico rappresentano un'esibizione completa e legalmente valida.

6.5.1 Con specifico riguardo alle Credenziali di accesso il Cliente si impegna a custodirle con la massima diligenza e a non consentirne l'utilizzo da parte di terzi non espressamente autorizzati e del cui comportamento in ogni caso il Cliente si assume ogni più ampia responsabilità.

6.5.2 Il Cliente è obbligato ad osservare le procedure di generazione, rilascio, sospensione e rigenerazione delle Credenziali di accesso, e/o di altre eventuali credenziali di autenticazione, necessarie ad accedere al Servizio. Il Cliente, successivamente al ricevimento della password, è tenuto a modificarla ed a mantenerla segreta e s'impegna a non trasferirla a terzi, sollevando comunque i Fornitori da ogni responsabilità per qualsiasi atto illegittimo compiuto con detta password. Il Cliente assume altresì l'onere di provvedere alla variazione periodica della password di accesso nel rispetto degli standard di sicurezza e della normativa in tema di protezione dei dati personali di cui al D.Lgs. 196/2003 e s.m.i.

6.5.3. In caso di smarrimento, furto o perdita delle Credenziali di attivazione e accesso, il Cliente è tenuto a comunicare tempestivamente la circostanza ai Fornitori e ad attivare prontamente la procedura di rilascio di nuove credenziali di autenticazione e accesso.

6.6 Il Cliente prende altresì atto ed accetta che:

a) i Fornitori non controllano né sorvegliano come il Cliente utilizza il Servizio ovvero i documenti informatici dal medesimo versati in conservazione; in ogni caso i Fornitori sono e restano estranei alle attività che il Cliente effettua in piena autonomia accedendo da remoto via internet tramite le Credenziali di accesso al Servizio; e

b) Per tutta la durata del Contratto e per i 60 (sessanta) giorni successivi alla sua scadenza, giusto quanto previsto al precedente Art. 6 comma 4, il Cliente è l'unico titolare, ai sensi del d.lgs. 196/03, del trattamento degli eventuali dati immessi e/o trattati e/o presenti sul Sistema di conservazione.

6.7.1 Qualora il Cliente utilizzi il Servizio per la conservazione di documenti di cui sono titolari terzi soggetti è fatto espresso divieto al Cliente di consentire, in qualsiasi modo e forma, direttamente o indirettamente, a detti soggetti il versamento dei documenti e comunque l'accesso al Servizio che resta in via esclusiva riservato al solo Cliente.

6.7.2 Il Cliente si impegna a fare quanto necessario per rendere edotti detti terzi di quanto previsto nel presente paragrafo.

6.7.3 La violazione, sia diretta che indiretta, anche attraverso altri soggetti, dei suddetti obblighi, legittima ed autorizza i Fornitori a risolvere, con effetto immediato, il Contratto.

6.8 Fermo quanto previsto al precedente paragrafo e fatti salvi gli altri obblighi previsti a suo carico in Contratto, nel Manuale e dalla vigente normativa in materia, il Cliente si obbliga:

a) a versare in conservazione esclusivamente dati e documenti informatici di cui detiene legittima e completa disponibilità;
b) a non versare in conservazione, né a trasmettere, spedire

o divulgare tramite il Servizio, documenti informatici o dati riportanti materiale e/o notizie diffamatorie, illegali o comunque lesive di diritti di terzi, obbligandosi a vigilare sul corretto utilizzo del Servizio da parte dei soggetti autorizzati ad accedervi, con totale esonero dei Fornitori da ogni responsabilità e da ogni obbligo di verifica in proposito;

c) a formare i documenti che versa in conservazione in formato statico e non modificabile, ovvero che non contengano:

i) macroistruzioni corrispondenti in comandi interni che, al verificarsi di determinati eventi, possono generare automaticamente modifiche o variazioni dei dati contenuti nel documento; o

ii) codici eseguibili corrispondenti in istruzioni, non sempre visibili all'utente, che consentono all'elaboratore di modificare il contenuto del documento informatico;

d) ad utilizzare il Servizio in conformità a quanto indicato in Contratto compreso il Manuale nel rispetto della normativa vigente, della morale e dell'ordine pubblico;

e) ad individuare e comunicare ai i Fornitori le tipologie/classi di documenti informatici da versare in conservazione attraverso la compilazione della Scheda di conservazione, nonché a quale Titolare detti documenti sono riferiti;

f) a versare in conservazione documenti informatici nei formati conformi a quelli descritti nella Scheda di conservazione;

g) a garantire che i documenti informatici versati in conservazione siano privi di Agenti di alterazione;

h) a garantire che i documenti informatici versati in conservazione siano muniti di tutti i metadati previsti dal Manuale, dalla Scheda di conservazione, nonché dalle regole tecniche in materia di conservazione digitale dei documenti informatici, compresi quelli previsti per i documenti informatici rilevanti ai fini delle disposizioni tributarie;

i) a garantire che i certificati delle firme digitali utilizzate non siano stati revocati o sospesi;

j) a versare in conservazione i documenti informatici non oltre i termini previsti dalla Scheda di conservazione;

k) a gestire i processi di formazione dei documenti informatici, creare e sottoscrivere con firma digitale i pacchetti di versamento contenenti i documenti informatici da versare in conservazione nel rispetto di quanto stabilito in Contratto compreso il Manuale e nella Scheda di conservazione;

l) ad inviare ai Fornitori i pacchetti di versamento ed i relativi documenti informatici nei tempi e nei modi e secondo gli standard, le specifiche tecniche e i formati utilizzabili quali riferimento per il Sistema di conservazione previsti nel Manuale e nella Scheda di conservazione;

m) a comunicare tempestivamente ai Fornitori eventuali variazioni del periodo di imposta (come definito dal DPR 22/12/1986, n. 917 e s.m.i.) dei soggetti titolari dei documenti informatici versati in conservazione; tale comunicazione dovrà essere effettuata almeno entro 3 (tre) mesi dalla scadenza del nuovo periodo di imposta al fine di poter consentire a i Fornitori di procedere alla corretta "chiusura" dei processi di conservazione in atto;

n) ad inviare tutte le eventuali comunicazioni da presentare all'Agenzia delle Entrate ovvero ad ogni altro competente Autorità e/o Ufficio;

o) ad eseguire ogni ulteriore e/o eventuale adempimento presso le competenti Autorità che fosse richiesto in conseguenza della conservazione digitale dei documenti informatici di cui al Contratto.

6.9 Il Cliente dovrà dotarsi, a sua cura e spese, di un proprio manuale del sistema di conservazione costituito dalla descrizione di componenti, processi ed organizzazione propri, integrato e completato, se ritenuto opportuno, dal Manuale.

6.10 Resta altresì inteso che il Cliente assume a proprio carico le responsabilità in sede civile, penale ed amministrativa in relazione al contenuto dei documenti informatici versati in conservazione, impegnandosi a manlevare e tenere indenni i Fornitori da qualsiasi pretesa di terzi o conseguenza pregiudizievole che possa comunque derivare a tal proposito.

6.11 Quando non presente, al documento informatico immodificabile il Cliente dovrà associare una Validazione temporale.

6.11.1 Al documento informatico immodificabile il Cliente dovrà associare, in relazione ad ogni classe/tipologia documentale, i metadati previsti dalla legge (anche tributaria) e dalle regole tecniche di cui all'art. 71 del CAD e, più in generale, dalla vigente normativa in materia o gli eventuali ulteriori metadati riportati nella Scheda Conservazione; i suddetti metadati dovranno essere generati dal Cliente durante la fase di produzione/formazione/emissione dei documenti informatici.

6.12 I documenti informatici formati mediante copia per immagine su supporto informatico di documenti originali (anche unici) formati in origine su supporto analogico, dovranno essere prodotti dal Cliente mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto.

6.13 Nel caso in cui il Cliente intenda conservare documenti informatici ottenuti mediante copia per immagine di documenti formati in origine su supporto analogico dovrà attenersi alle regole tecniche stabilite dal CAD.

6.14 L'obbligo di rispettare, sia nella fase di formazione/produzione/emissione che in quella successiva di versamento in conservazione, l'ordine cronologico e la non soluzione di continuità per periodo di imposta dei documenti informatici destinati alla conservazione, è posto ad esclusivo carico e responsabilità del Cliente e rispecchia il requisito di ordinata tenuta della contabilità richiesto dall'articolo 2214 del Codice Civile.

6.15.1 Il versamento dei documenti informatici nel Sistema di conservazione avviene in modalità telematica a cura, spese e

sotto l'esclusiva responsabilità del Cliente, il quale dovrà generare uno o più pacchetti di versamento per ogni Titolare e in relazione ad ogni classe/tipologia documentale, nelle modalità, nei termini e con il formato previsti dal Manuale.

6.15.2 Il buon esito dell'operazione di versamento è verificato tramite il rapporto di versamento prodotto dal Responsabile della conservazione ovvero dal Responsabile del Servizio di conservazione, in conformità a quanto previsto dal Manuale.

6.16 In corso di validità del Contratto il Cliente, sotto la sua esclusiva responsabilità e comunque nei soli casi previsti dalla legge, può procedere allo scarto dei documenti informatici conservati.

6.17. In caso di erogazione del Servizio DocFly - Fatturazione PA resta inteso tra le parti che:

a) anche in caso di rilascio della Delega Fattura PA ad Aruba Pec, il Cliente è tenuto a predisporre la/e Fattura/e PA con i dati e le informazioni necessari allo scopo;
b) il Cliente prende atto ed accetta, ora per allora, che rimangono comunque a suo carico, in via esclusiva, tutte le responsabilità relative ai contenuti, alla veridicità, correttezza e completezza dei dati trasmessi ai Fornitori ai fini dell'erogazione del Servizio DocFly - Fatturazione PA. In ogni caso il Cliente è tenuto a fornire ai Fornitori tutte le relative istruzioni con congruo anticipo.
c) Il Cliente, solleva, ora per allora, i Fornitori da ogni responsabilità, per qualsiasi conseguenza pregiudizievole, di carattere fiscale, tributario, civile o penale in cui dovesse incorrere in ragione delle suddette cause ovvero nei confronti delle Pubbliche Amministrazioni e dei terzi per tutte le operazioni connesse e derivanti dall'emissione e sottoscrizione con firma digitale delle Fatture PA, anche quando delegata dal Cliente ai Fornitori.
d) fermo quanto previsto al precedente paragrafo e fatti salvi gli altri obblighi previsti a suo carico in Contratto, il Cliente si obbliga:
   1) ad utilizzare il Servizio DocFly - Fatturazione PA in conformità a quanto indicato in Contratto nel rispetto della normativa vigente, della morale e dell'ordine pubblico;
   2) a garantire che le firme digitali utilizzate per la sottoscrizione delle Fatture PA abbiano e mantengano piena validità;
   3) al pagamento dell'imposta di bollo eventualmente dovuta sulle Fatture PA. Il versamento dell'imposta di bollo dovuta dovrà pertanto avvenire ad esclusiva cura e carico del Cliente nei termini e con le modalità previsti dalla legge.
e) resta altresì inteso che il Cliente assume a proprio carico le responsabilità in sede civile, penale ed amministrativa in relazione al contenuto delle Fatture PA emesse e trasmesse alla Pubblica Amministrazione interessata attraverso il Sistema di interscambio, impegnandosi a manlevare e tenere indenne i Fornitori da qualsiasi pretesa di terzi o conseguenza pregiudizievole che possa comunque derivare a tal proposito.

6.18 In caso di violazione anche di uno soltanto dei suddetti obblighi/impegni, il Cliente si obbliga a manlevare e tenere indenne i Fornitori da ogni danno, responsabilità e/o onere, diretti o indiretti comprese le spese legali, che i Fornitori dovessero subire o sopportare in conseguenza degli inadempimenti contestati, ancorché derivanti da richieste di risarcimento di terzi. In tale ipotesi i Fornitori avranno facoltà di intervenire nelle forme e nei modi ritenuti opportuni per eliminare, ove possibile, la violazione ed i suoi effetti, ovvero di sospendere o interrompere il Servizio, riservandosi altresì il diritto di risolvere il Contratto ai sensi del successivo art. 11.

6.19 Il Cliente dichiara di aver preso attenta visione del Contratto compresi tutti i documenti che lo formano e di aver compreso appieno il loro contenuto e di essere edotto della validità e degli effetti giuridici della conservazione digitale dei documenti informatici.

7. Servizio: modalità di utilizzo, configurazione assistenza e manutenzione

7.1 Ai fini del Servizio si individuano i seguenti ruoli:

a) Produttore;
b) Responsabile della conservazione;
c) Responsabile del servizio di conservazione;
d) Utente.

7.2 Le classi documentali per le quali è attivato il Servizio sono quelle indicate nella Scheda di conservazione. Resta inteso che se il Cliente vorrà sottoporre a conservazione documenti informatici appartenenti a tipi/classi documentali diverse e/o ulteriori rispetto a quelle indicate nella Scheda Conservazione, dovrà formulare apposita istanza scritta ai Fornitori, allegando ad essa una nuova Scheda Conservazione predisposta dagli stessi, ferme le modalità e le limitazioni previste dal Manuale e dal Contratto. In ogni caso il Cliente prende atto ed accetta di essere l'unico responsabile degli eventuali documenti non aventi formato e/o caratteristiche conformi a quanto indicato nel Manuale e/o non idonei per la conservazione ai sensi della vigente normativa in materia da egli stesso versati in conservazione ed accettati dai Fornitori a qualsiasi titolo; il Cliente, prende altresì atto ed accetta, ora per allora, che i Fornitori non garantiscono in alcun modo la validità e/o l'autenticità e/o la leggibilità e/o l'integrità a norma di legge dei documenti versati in conservazione non aventi formato e/o caratteristiche conformi a quanto indicato nel Manuale e/o non idonei per la conservazione ai sensi della vigente normativa in materia e per l'effetto, con l'invio della richiesta di versamento in conservazione di tali documenti, solleva ora per allora i Fornitori da ogni e qualsiasi responsabilità al riguardo, diretta e/o indiretta, e rinuncia a far valere nei confronti degli stessi Fornitori qualsiasi diritto e/o pretesa propria e/o di terzi.

7.3 Fermo quanto precede, il Servizio viene configurato in base a quanto richiesto dal Cliente tenendo altresì conto, per ogni tipologia/classe documentale, dei parametri specifici risultanti dal Contratto e dalla Scheda di conservazione.

7.4 Salvo specifico, diverso e separato accordo tra le Parti, e fermo quanto indicato al riguardo nella Sez. I delle Condizioni, l'assistenza tecnica è resa esclusivamente nei tempi e secondo le modalità indicate nel Contratto e nelle Specifiche tecniche. Il Cliente è tenuto in ogni caso a comunicare tempestivamente ai Fornitori eventuali irregolarità o disfunzioni dal medesimo rilevate nel Servizio.

7.5 I Fornitori si riservano la facoltà di interrompere l'erogazione del Servizio per procedere ad interventi tecnici di manutenzione. In tal caso sarà data comunicazione al Cliente a mezzo e-mail con un preavviso di 48 ore; detta comunicazione indicherà altresì le tempistiche del ripristino.

8. Sospensione del Servizio

8.1 Fermo quanto previsto all'art. 12 sez. I delle Condizioni **e f**atta salva l'applicazione del successivo art. 9, i Fornitori, a loro discrezione e senza che l'esercizio di tale facoltà possa essergli contestata come inadempimento o violazione del Contratto, si riservano la facoltà di sospendere il Servizio, anche senza alcun preavviso, nel caso in cui il Cliente abbia esaurito lo spazio messo a sua disposizione;

8.2 In caso di erogazione del Servizio DocFly - Fatturazione PA, i Fornitori si riservano a loro discrezione e senza che l'esercizio di tale facoltà possa esser loro contestata come inadempimento o violazione del Contratto la facoltà di sospendere l'erogazione del Servizio, anche senza alcun preavviso, nel caso in cui il Cliente abbia esaurito le risorse hardware o il numero di fatture da emettere e trasmettere rese disponibili dai Fornitori.

8.3. Il Cliente solleva i Fornitori da ogni e qualsiasi responsabilità o pretesa di terzi per l'eventuale cessazione, sospensione o interruzione del Servizio verificatasi perché prevista dal Contratto.

9. SLA e indennizzi

9.1 Lo SLA entra in vigore per ciascun Cliente a decorrere dall'attivazione del Servizio e termina con la sua cessazione. I Fornitori si riservano la facoltà di modificarlo o sostituirlo più volte nel corso del Contratto ed in qualsiasi momento. Le modifiche apportate allo SLA ovvero il nuovo SLA - sostitutivo di quello precedente - entrano in vigore dalla data della loro pubblicazione sul Pannello Gestione e così le successive modifiche o sostituzioni.

9.2 Il tempo di manutenzione programmata non viene conteggiato ai fini del calcolo dell'Uptime. La manutenzione programmata riguarda le attività svolte regolarmente dai Fornitori per mantenere la funzionalità delle risorse del Data Center attraverso il quale viene erogato il Servizio; essa è ordinaria e straordinaria.

9.3 ai fini del riconoscimento degli indennizzi di cui al successivo comma 4 saranno presi in considerazione soltanto i disservizi confermati dal sistema di monitoraggio dei Fornitori.

9.3.1 Il monitoraggio da parte dei Fornitori viene effettuato tramite software specifici che rilevano ed indicano eventuali guasti o anomalie dandone comunicazione in tempo reale al servizio assistenza operativo 24/7/365;

9.4 Per ogni ora completa di violazione dello SLA i Fornitori riconoscono al Cliente, a titolo di indennizzo, 1 (uno) giorno di proroga della durata del Contratto fino ad un massimo di 30 (trenta) giorni.

9.5 Fermo quanto sopra resta inteso in ogni caso che al Cliente non spetta l'indennizzo previsto al precedente comma 3 verificandosi una delle seguenti circostanze:

a) cause di forza maggiore e cioè eventi che, oggettivamente, impediscano al personale de i Fornitori di intervenire per eseguire le attività poste dal Contratto a carico degli stessi i Fornitori (in via meramente esemplificativa e non esaustiva: scioperi e manifestazioni con blocco delle vie di comunicazione; incidenti stradali; guerre e atti di terrorismo; catastrofi naturali quali alluvioni, tempeste, uragani etc);

b) interventi straordinari da effettuarsi con urgenza ad insindacabile giudizio dei Fornitori per evitare pericoli alla sicurezza e/o stabilità e/o riservatezza e/o integrità del Servizio e/o dei dati e/o informazioni in essi contenuti. L'eventuale esecuzione di tali interventi sarà comunque comunicata al Cliente a mezzo e mail inviata all'indirizzo di posta elettronica indicato in fase d'ordine con preavviso anche inferiore alle 48 ore oppure contestualmente all'avvio delle operazioni in questione o comunque non appena possibile;

c) indisponibilità o blocchi del Servizio imputabili al Cliente ovvero ad anomalie e malfunzionamenti dei software applicativi/gestionali forniti al Cliente da terze parti;

d) anomalia o malfunzionamento del Servizio, ovvero loro mancata o ritardata rimozione o eliminazione imputabili ad inadempimento o violazione del Contratto da parte del Cliente ovvero ad un cattivo uso del Servizio da parte del medesimo;

e) cause che determinano l'inaccessibilità, totale o parziale, del Servizio imputabili a guasti nella rete internet esterna al perimetro dei Fornitori e comunque fuori dal suo controllo (in via meramente esemplificativa guasti o problemi).

f) sospensione o interruzione del Servizio per inadempimento o violazione del Contratto imputabile al Cliente;

10. Nomina di Aruba PEC a Responsabile del servizio di conservazione

10.1.1 Con l'accettazione delle Condizioni, ed in relazione ai Servizi di cui alla presente Sez. V delle medesime, ad ARUBA PEC vengono formalmente affidate dal Cliente, previa separata e specifica delega al riguardo da parte del Responsabile della Conservazione, lo svolgimento delle seguenti attività:

a) definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente, inclusa la gestione delle convenzioni, la definizione degli aspetti tecnico-operativi nonché le modalità di trasferimento da parte del Cliente dei documenti informatici versati in conservazione;
b) gestire il processo di conservazione garantendo nel tempo la conformità alla normativa vigente;
c) generare il rapporto di versamento, secondo le modalità previste dal Manuale;
d) generare e sottoscrivere il pacchetto di distribuzione con Firma digitale nei casi previsti dal Manuale;
e) effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
f) assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del D.P.C.M.;
j) richiedere la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite; ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovranno essere garantite e sostenute interamente dal Cliente; pertanto, qualora il Cliente non se ne sia fatto carico direttamente, ARUBA PEC è sin da ora autorizzata ad addebitare al Cliente tutti i costi e le spese, compresi gli onorari inerenti le attività prestate dal Pubblico Ufficiale, qualora la normativa ne richieda obbligatoriamente la presenza;
k) assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti, curare l'aggiornamento periodico del manuale del sistema di conservazione di cui all'art. 8 del D.P.C.M..

10.1.2 Aruba Pec, alla luce di quanto previsto dall'art. 44 del CAD, dovrà verificare che il sistema di conservazione dei documenti informatici garantisca:

- il mantenimento dell'identificazione certa del soggetto che ha formato il documento informatico;
- l'integrità dei documenti informatici depositati in conservazione;
- la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari, nei modi e nei termini stabiliti nel Manuale;
- il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B, e loro successive modificazioni ed integrazioni.

10.1.3 Aruba Pec dovrà altresì :

- terminare il processo di conservazione dei documenti informatici, entro e non oltre i termini convenuti nell'Elenco dei documenti informatici sottoposti a conservazione allegato al Contratto;
- provvedere, entro i suddetti termini, alla "chiusura" del processo di conservazione, apponendo oltre alla Firma digitale dell'incaricato preposto a tale adempimento, una Validazione temporale rilasciata da una Certification Authority iscritta nell'elenco ufficiale dei certificatori tenuto dall'Agenzia per l'Italia Digitale sull'insieme dei documenti ovvero su un'evidenza informatica contenente l'impronta o le impronte dei documenti conservati;
- provvedere, qualora richiesto dal Cliente o dalle Autorità competenti, all'esibizione dei documenti informatici conservati e delle relative evidenze informatiche che comprovano la corretta conservazione degli stessi, fornendo gli elementi necessari per valutare la loro autenticità e validità giuridica.

10.1.4 Resta inteso che:

a) Aruba PEC non sarà responsabile per la mancata o non corretta esecuzione degli obblighi su di essa incombenti, quale Responsabile del servizio di conservazione in tutti i casi in cui il mancato o non corretto adempimento sia dovuto a cause ad essa non imputabili, quali, a titolo meramente esemplificativo: forza maggiore, calamità naturali, eventi bellici, interventi dell'Autorità;
b) a carico di Aruba PEC non è posto alcun obbligo/dovere di elaborare i documenti informatici versati in conservazione al fine di estrarre i relativi metadati che, pertanto, dovranno essere forniti e associati ai rispettivi documenti esclusivamente a cura e carico del Cliente.

10.2.1. Aruba Pec, quale Responsabile del servizio di conservazione, potrà operare anche attraverso uno o più persone fisiche dalla stessa incaricate all'esecuzione delle attività finalizzate alla conservazione dei documenti informatici nell'ambito della fornitura del Servizio.

10.2.2. Aruba Pec potrà delegare, in tutto o in parte, a terzi soggetti persone fisiche o giuridiche, anche esterne alla propria organizzazione, singole funzioni o fasi del processo di conservazione.

10.3. Il corrispettivo relativo alla presente nomina è quello regolato e stabilito dal Contratto.

10.4. La presente nomina di Responsabile del servizio di conservazione avrà la stessa durata del Contratto.

11. Delega Fattura PA

Ai fini dell'erogazione dei Servizi DocFly avvalendosi delle facoltà previste dal Contratto, con l'accettazione delle Condizioni ed in relazione al Servizio DocFly Fatturazione PA di cui alla presente Sez. V delle medesime, il Cliente in relazione al Servizio DocFly Fatturazione PA, delega Aruba Pec all'emissione della fattura PA ed all'apposizione della firma digitale sulla medesima, secondo quanto previsto dal Contratto; a tal proposito il Cliente prende atto e dichiara che rimangono a suo carico, in via esclusiva, tutte le responsabilità in sede civile, penale ed amministrativa in relazione al contenuto delle Fatture PA emesse e trasmesse alla Pubblica Amministrazione interessata attraverso il Sistema di interscambio e per l'effetto, si impegna, ora per allora, a manlevare e tenere indenne Aruba Pec da qualsiasi pretesa di terzi o conseguenza pregiudizievole che possa comunque alla stessa derivare dal compimento delle attività delegate .

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 5

ELENCO TITOLARI DI FIRMA DIGITALE, DEGLI INDIRIZZI DI POSTA ELETTRONICA CERTIFICATA E DI POSTA ELETTRONICA DELL'ENTE

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

Elenco titolari di firma digitale:

il Presidente Liana Serrani

il Direttore Elisabetta Cecchini

il Funzionario Marco Masi

il Funzionario Simonetta Scaglia

il Funzionario Massimo Stella

l'Istruttore direttivo Ilaria Ciannavei

l'Istruttore direttivo Matteo Giantomassi

Elenco indirizzi istituzionali di posta elettronica certificata:

- atarifiutiancona@pec.it
- areafinanziaria.atarifiutiancona@pec.it

Elenco indirizzi istituzionali di posta elettronica:

quelle con la x sono le correzioni e/o integrazioni:

- segreteria@atarifiuti.an.it

x ato2@atarifiuti.an.it - ata2@atarifiuti.an.it

x educazione@atarifiuti.an.it

x serviziorifiuti@atarifiuti.an.it

x protmail@atarifiuti.an.it

x anticorruzione@atarifiuti.an.it

- amici@atarifiuti.an.it

- cecchini@atarifiuti.an.it

- ciannavei@atarifiuti.an.it

- finelli@atarifiuti.an.it

- giantomassi@atarifiuti.an.it

- marinelli@atarifiuti.an.it

- martarelli@atarifiuti.an.it

x martini@atarifiuti.an.it

- masi@atarifiuti.an.it

- pieralisi@atarifiuti.an.it

x ponziano@atarifiuti.an.it

- scaglia@atarifiuti.an.it

- stella@atarifiuti.an.it

- newsletter@atarifiuti.an.it

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 6

TIMBRI ED ETICHETTE IN USO

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

TIMBRO ISTITUZIONALE:

ETICHETTA PROTOCOLLO:

Assemblea territoriale d'Ambito ATO 2

Prot. nr. 5519 del 21/12/2016 (A)
Titolo e classe 6.1 pr.7990

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 7

MODELLO DI REGISTRO DI EMERGENZA

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

numero di protocollo	data	mittente / destinatario	oggetto del documento	data e numero di protocollo del documento ricevuto	tipo di supporto	mezzo di ricezione	tipo di documento	assegnazione	classificazione	fascicolo

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 8

TITOLARIO DI CLASSIFICAZIONE

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

TITOLARIO - in vigore dal 18/07/2016

(approvato con Decreto del Presidente n. 21 del 14/07/2016)

codice	*descrizione*
1	***AMMINISTRAZIONE GENERALE***
1.1	LEGISLAZIONE E CIRCOLARI ESPLICATIVE
1.2	ATTI ISTITUTIVI E REGOLAMENTARI
1.3	ARCHIVIO GENERALE
1.4	SISTEMA INFORMATIVO
1.5	INFORMAZIONI E COMUNICAZIONI AD ENTI E CITTADINI
1.6	POLITICA DEL PERSONALE, ORDINAMENTO DEGLI UFFICI E DEI SERVIZI
1.7	RELAZIONI CON LE ORGANIZZAZIONI SINDACALI E DI RAPPRESENTANZA DEL PERSONALE
1.8	CONTROLLI INTERNI ED ESTERNI
1.9	EDITORIA ED ATTIVITA' INFORMATIVO-PROMOZIONALE INTERNA ED ESTERNA
1.10	CERIMONIALE, ATTIVITA' DI RAPPRESENTANZA, RICONOSCIMENTI
1.11	RAPPORTI ISTITUZIONALI
1.12	FORME ASSOCIATIVE PER ESERCIZIO DI FUNZIONI E SERVIZI E ADESIONE AD ASSOCIAZIONI
2	***ORGANI DI GOVERNO, GESTIONE, CONTROLLO, CONSULENZA E GARANZIA***
2.1	PRESIDENTE
2.2	ASSEMBLEA DEGLI ENTI CONVENZIONATI
2.3	COMITATO DI COORDINAMENTO
2.4	COMMISSARIO STRAORDINARIO
2.5	DIRETTORE E DIRIGENZA
2.6	REVISORI DEI CONTI
2.7	COMMISSARIO 'ad acta'
2.8	ORGANI DI CONTROLLO INTERNI
2.9	ORGANI CONSULTIVI
3	***RISORSE UMANE***
3.0	FASCICOLI DEL PERSONALE
3.1	CONCORSI, SELEZIONI, COLLOQUI
3.2	ASSUNZIONI E CESSAZIONI
3.3	COMANDI, DISTACCHI, MOBILITA'
3.4	ATTRIBUZIONE DI FUNZIONI, ORDINI DI SERVIZIO E MISSIONI
3.5	INQUADRAMENTI ED APPLICAZIONE CONTRATTI COLLETTIVI DI LAVORO

3.6	RETRIBUZIONI E COMPENSI
3.7	TRATTAMENTO FISCALE, CONTRIBUTIVO ED ASSICURATIVO
3.8	TUTELA DELLA SALUTE E SICUREZZA SUL LUOGO DI LAVORO
3.9	DICHIARAZIONI DI INFERMITA' ED EQUO INDENNIZZO
3.10	INDENNITA' PREMIO DI SERVIZIO E TRATTAMENTO DI FINE RAPPORTO, QUIESCIENZA
3.11	SERVIZI AL PERSONALE SU RICHIESTA
3.12	ORARIO DI LAVORO, PRESENZA ED ASSENZE
3.13	GIUDIZI, RESPONSABILITA' E PROVVEDIMENTI DISCIPLINARI
3.14	FORMAZIONE ED AGGIORNAMENTO PROFESSIONALE
3.15	COLLABORATORI ESTERNI
4	***RISORSE FINANZIARIE E PATRIMONIO***
4.1	BILANCIO PREVENTIVO E PIANO ESECUTIVO DI GESTIONE (PEG)
4.2	GESTIONE DEL BILANCIO E DEL PEG (CON EVENTUALI VARIAZIONI)
4.3	GESTIONE DELLE ENTRATE: ACCERTAMENTO, RISCOSSIONE, VERSAMENTO
4.4	GESTIONE DELLA SPESA: IMPEGNO, LIQUIDAZIONE, ORDINAZIONE E PAGAMENTO
4.5	PARTECIPAZIONI FINANZIARIE
4.6	RENDICONTO DELLA GESTIONE; ADEMPIMENTI E VERIFICHE CONTABILI
4.7	ADEMPIMENTI FISCALI, CONTRIBUTIVI E ASSICURATIVI
4.8	BENI IMMOBILI
4.9	BENI MOBILI
4.10	ECONOMATO
4.11	TESORERIA
5	***AFFARI LEGALI***
5.1	CONTENZIOSO
5.2	RESPONSABILITA' CIVILE E PATRIMONIALE VERSO TERZI; ASSICURAZIONI
5.3	PARERI E CONSULENZE
6	***GESTIONE INTEGRATA DEI RIFIUTI URBANI E ASSIMILATI***
6.1	PIANIFICAZIONE E STUDI
6.2	GESTIONE SERVIZIO RIFIUTI, TRATTAMENTO, SMALTIMENTO
6.3	PROGETTI DI SENSIBILIZZAZIONE AMBIENTALE
6.4	REALIZZAZIONE OPERE E IMPIANTI
7	***OGGETTI DIVERSI***

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 9

INCARICATI AL TRATTAMENTO

DEI DOCUMENTI AMMINISTRATIVI

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

Ad ogni Responsabile di servizio vengono assegnati per competenza i documenti amministrativi relativi ai propri servizi.

Sarà cura dello stesso responsabile decidere o meno la riassegnazione degli stessi ai suoi collaboratori.

Ogni dipendente avrà quindi la visibilità limitata ai documenti amministrativi ad esso assegnati.

E' fatta eccezione per il Direttore e per i componenti dell'Ufficio gestione documentale che per le loro proprie funzioni debbono avere la visibilità dell'intero registro di protocollo anche ai fini archivistici.

Alla data di stesura del presente documento i Responsabili dei servizi sono quelli individuati con Determinazione del Direttore n. 19/2013, mentre il Responsabile delle tre Aree in cui è suddivisa l'organizzazione dell'ATA è il Direttore dott.ssa Elisabetta Cecchini.

ATA
Assemblea Territoriale d'Ambito ATO 2 - Ancona

DETERMINAZIONE DELLA DIREZIONE

N. 19 DEL 31 DICEMBRE 2013

Oggetto: Assegnazione del personale dipendente alle Aree ed ai Servizi e individuazione dei Responsabili ai sensi degli art. 6 e 7 del Regolamento di Organizzazione.

Il presente atto, non comportando impegno di spesa, non necessita di visto di regolarità contabile attestante la copertura finanziaria.

LA DIREZIONE

PREMESSO che

- ai sensi del comma 2, lettera d), dell'art. 7 della L.R. Marche n. 24/2009 e s.m.i. e del comma 3, dell'art. 6 della L.R. Marche n. 18/2011 e s.m.i., il personale dell'ATA è prioritariamente costituito dal personale dei Consorzi obbligatori ex L.R. Marche n. 28/1999, quali Consorzio Intercomunale Conero Ambiente e Consorzio Intercomunale Vallesina - Misa;
- che entrambi i Consorzi di cui sopra sono in liquidazione rispettivamente a decorrere dal 01/01/2014 (deliberazione Assemblea del Consorzio Intercomunale Conero Ambiente n. 5 del 09/12/2013) e dal 21/12/2013 (deliberazione Assemblea del Consorzio Intercomunale Vallesina-Misa n. 16 del 05/11/2013);
- l'ATA si è dotata di un documento programmatico (deliberazione dell'Assemblea n. 1 del 24/04/2013) che esprime gli indirizzi in merito al trasferimento del personale dei due Consorzi;
- l'ATA si è dotata di un Regolamento di Organizzazione (deliberazione dell'Assemblea n. 4 del 09/09/2013);
- tale Regolamento prevede, all'art. 21, che "*il trasferimento del personale dai Consorzi all'ATA sarà effettuato nel rispetto dell'art. 31 del D.Lgs. 165/2001 e dell'art. 2112 del C.C. garantendo ai dipendenti il mantenimento del trattamento giuridico-economico in godimento; specifico accordo sindacale dovrà prevedere l'equiparazione delle qualifiche possedute dai dipendenti del Consorzio Conero Ambiente con il CCNL Federambiente a quelle del CCNL del comparto Regioni ed enti locali adottato dall'ATA*";
- in data 12/12/2013 è stato sottoscritto il prescritto verbale di concertazione tra l'ATA, i Consorzi e le OO.SS. che prevede il nuovo inquadramento giuridico-economico del personale del Consorzio Intercomunale Conero Ambiente nell'ATA, con indicazione dell'effettivo trasferimento dell'intero personale dei Consorzi con decorrenza al 01/01/2014;
- con prot. n. 189 e n. 192 del 31/12/2013 è stato comunicato a tutti i dipendenti dei predetti Consorzi il suddetto trasferimento con decorrenza 01/01/2014;

DATO ATTO che il sopra citato Regolamento dispone che:

- ai sensi dell'art. 6, co. 1, l'organizzazione degli uffici e dei servizi, così come la gestione del personale in servizio presso l'ATA, compete al Direttore;
- ai sensi del predetto art. 6, co. 2, la struttura organizzativa dell'ATA si articola in una Direzione e tre Aree articolate in servizi, come di seguito specificato:
  - DIREZIONE;
  - AREA AMMINISTRATIVA:
    - x Servizio Segreteria;
    - x Servizio Affari Generali, Legale e contenziosi;
    - x Servizio Contratti e Appalti;
    - x Servizio pianificazione campagne di comunicazione e rapporti con i media;
    - x Servizio educazione ambientale;
  - AREA FINANZIARIA:
    - x Servizio gestione finanziamenti e controllo gestione;
    - x Servizio gestione finanziaria e contabile;
    - x Servizio Economato;
  - AREA TECNICA:
    - x Servizio Pianificazione e progettazione;
    - x Servizio Direzione contratti raccolta rifiuti;

- ai sensi dell'art. 7, il personale dipendente è assegnato alle Aree con determinazione del Direttore e che, con la stessa determinazione, vengono individuati i Responsabili delle varie Aree e/o Servizi e assegnati i compiti specifici di attività attinenti all'inquadramento professionale posseduto;

RICHIAMATA la deliberazione n. 2 del 19/07/2013 con la quale l'Assemblea ha nominato, nelle more della selezione pubblica relativa all'individuazione del Direttore, la dott.ssa Simonetta Scaglia ed il dott. Raffaello Tomasetti, Direttori congiunti dell'ATA;

DATO ATTO che, ai sensi dell'art. 4 del predetto Regolamento di Organizzazione, alla Direzione risulta attribuita la responsabilità gestionale dell'Ente e, ferma la responsabilità dell'istruttoria e di ogni altro adempimento inerente il singolo procedimento in capo ai responsabili dei servizi, la responsabilità dell'adozione del provvedimento finale, con la connessa competenza ad apporre i necessari visti di regolarità tecnica e contabile ai sensi del D.Lgs. n. 267/2000 e s.m.i.;

VALUTATO di attribuire la responsabilità delle Aree alla Direzione, in considerazione di quanto disposto dal predetto art. 4 del Regolamento di Organizzazione;

CONSIDERATO che, ai sensi dell'art. 8 del Regolamento di Organizzazione, la Direzione, nell'esercizio del suo potere di gestione del rapporto di lavoro, può adibire, con atto motivato il personale dipendente o comandato a svolgere, in via temporanea, compiti specifici, non prevalenti, della qualifica superiore, compiti immediatamente inferiori, compiti complementari e strumentali al perseguimento degli obiettivi di lavoro, al fine di assicurare la funzionalità nonché il regolare ed efficace funzionamento degli uffici;

VISTO l'allegato "A" del Regolamento di Organizzazione nel quale per ciascuna Area sono riportati i singoli servizi e le attività connesse;

VISTA, altresì, la dotazione organica dell'ATA, di cui alla deliberazione dell'Assemblea n. 12 del 19.12.2013 di approvazione del Bilancio annuale di previsione 2014 e allegati;

DATO ATTO che, a decorrere dal 01.01.2014, la dott.ssa Simonetta Scaglia risulta in aspettativa non retribuita dal ruolo di Funzionario Amministrativo dell'ente al fine di assumere l'incarico dirigenziale presso l'ATA, come da Decreto del Presidente n. 2 del 31.12.2013;

VISTI:
- il D.Lgs. n. 267/2000 e s.m.i.;
- il D.Lgs. n. 165/2001 e s.m.i., con particolare riferimento all'art. 5, co. 2;
- la L. n. 241/1990;
- il Regolamento di Organizzazione dell'ATA, approvato con deliberazione dell'Assemblea n. 4 del 09/09/2013;

DETERMINA

1. Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2. Di stabilire che i singoli incaricati della Direzione congiunta possono operare disgiuntamente in base alla seguente suddivisione operata tra gli stessi della responsabilità dei procedimenti, ferma restando la responsabilità congiunta della gestione dell'Ente: Area Amministrativa dott.ssa Simonetta Scaglia, Area finanziaria dott. Raffaello Tomasetti, Area Tecnica, responsabilità congiunta ad eccezione delle procedure relative agli appalti dovei gli stessi sono già individuati quali RUP;
3. Di dare atto che, ai sensi dell'art. 4 del Regolamento di Organizzazione, alla Direzione risulta attribuita la responsabilità gestionale dell'Ente e, ferma la responsabilità dell'istruttoria e di ogni altro adempimento inerente il singolo procedimento in capo ai responsabili dei servizi, la responsabilità dell'adozione del provvedimento finale, con la connessa competenza ad apporre i necessari visti di regolarità tecnica e contabile (responsabile dei procedimenti Area finanziaria) ai sensi del D.Lgs. n. 267/2000 e s.m.i.;
4. Di attribuire la responsabilità delle Aree alla Direzione, in considerazione di quanto disposto dal predetto art. 4 del Regolamento di Organizzazione;
5. Di assegnare il personale dipendente alle Aree come di seguito riportato:

Dipendente	**Area Amministrativa**	**Area Finanziaria**	**Area Tecnica**
Ciannavei Ilaria		x	
Filonzi Laura (in aspettativa)		x	
Finelli Matteo			x
Giantomassi Matteo	x		
Marinelli Loredana	x		
Masi Marco			x
Pieralisi Silvia			x
Scaglia Simonetta (in aspettativa)	x		
Stella Massimo			x

6. Di individuare i Responsabili dei servizi come segue:

Area Amministrativa	Responsabile del Servizio
Servizio segreteria (compresa la gestione degli archivi organizzati in collaborazione con il *Servizio pianificazione campagne di comunicazione e rapporti con i media)*	Scaglia Simonetta
Servizio affari generali, legale e contenziosi (compresa la predisposizione e tempestiva comunicazione degli atti da pubblicare nel sito internet al *Servizio pianificazione campagne di comunicazione e rapporti con i media*)	Scaglia Simonetta
Servizio contratti e appalti	Scaglia Simonetta
Servizio pianificazione campagne di comunicazione e rapporti con i media (nella gestione del sito internet è ricompresa la cura della pubblicazione dei documenti per le sedute delle Assemblee, degli atti nell'albo Pretorio on-line, e quant'altro previsto dalle norme vigenti in collaborazione con il *Servizio affari generali, legale e contenziosi*)	Giantomassi Matteo
Servizio educazione ambientale	Giantomassi Matteo

Area Finanziaria	Responsabile del Servizio
Servizio gestione finanziamenti e controllo gestione	Ciannavei Ilaria
Servizio gestione finanziaria e contabile	Ciannavei Ilaria
Servizio economato	Ciannavei Ilaria

Area Tecnica	Responsabile del Servizio
Servizio pianificazione e progettazione	Stella Massimo
Servizio direzione contratti raccolta rifiuti	Masi Marco

7. Di stabilire che.
   - per le attività riguardanti il funzionamento generale dell'ATA il Servizio segreteria si avvale della collaborazione del responsabile del Servizio Economato, dott.ssa Ilaria Ciannavei;
   - per le trasmissioni connesse al versamento delle ritenute previdenziali, fiscali e assistenziali il Servizio segreteria si avvale della collaborazione del responsabile del Servizio gestione finanziaria e contabile, dott.ssa Ilaria Ciannavei;
   - il Servizio contratti e appalti si avvale del responsabile del Servizio Pianificazione e progettazione ing. Massimo Stella.
8. Di dare atto che in caso di assenza o impedimento dei singoli responsabili dei servizi, la responsabilità viene prevista in capo alla Direzione;
9. Di stabilire che la dott.ssa Scaglia, collocata in aspettativa non retribuita per lo svolgimento dell'incarico di Direzione congiunta dell'ATA, con diritto alla conservazione del posto, assuma ad interim le responsabilità dei servizi dell'Area Amministrativa;
10. Di valutare l'eventuale attribuzione ai dipendenti di cui sopra delle indennità per specifiche responsabilità previste dall'art. 17, co. 2, lett. f) del CCNL 01/04/1999, secondo i criteri generali, le modalità e le quantità economiche che saranno definite in sede di contrattazione decentrata integrativa per l'anno 2014;
11. Di dare atto che gli effetti del presente atto decorrono dal 01/01/2014.

Ancona, 31 dicembre 2013

La Direzione
dott.ssa Simonetta Scaglia dott. Raffaello Tomasetti

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 10

LINEE GUIDA PER LA FASCICOLAZIONE

(Rev. 0 – dicembre 2016)

Premessa

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

Linee guida per l'organizzazione dei fascicoli e delle serie

Partendo dalle linee guida prodotte nell'ottobre 2005 dal "*Gruppo di lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni*", l'ATA ha predisposto con il supporto specialistico della dott.ssa Allegra Paci le seguenti linee guida operative per la gestione degli archivi.

Titolo I. Amministrazione generale

I.1 Legislazione e circolari esplicative

- Pareri chiesti dall'ATA su leggi specifiche: fasc. annuale per attività, eventualmente articolato in sottofascicoli
- Circolari pervenute all'ATA: repertorio annuale
- Circolari emanate dall'ATA: repertorio annuale

I.2 Atti istitutivi e regolamentari

- Redazione, modifiche, interpretazioni della convenzione o dello statuto: fasc. per affare
- Regolamenti emessi dall'ATA: repertorio annuale
- Redazione dei regolamenti: un fasc. per ciascun affare

I.3 Archivio generale

- Registro di protocollo
- Repertorio dei fascicoli
- Organizzazione del servizio e dell'attività ordinaria (aggiornamento del manuale di gestione con titolario e piano di conservazione, selezione periodica, riordino, inventariazione, spostamenti e versamenti di materiale, depositi e comodati): fasc. annuale per attività
- Versamenti: fasc. annuale per attività
- Scarti: fasc. annuale per attività
- Interventi straordinari sull'Archivio: un fasc. per ciascun affare
- Richieste di accesso per fini amministrativi: fasc. annuale per attività
- Richieste di informazioni archivistiche e richieste per motivi di studio: fasc. annuale per attività
- Adempimenti per la tutela della privacy: fasc. annuale per attività
- Richieste di pubblicazione all'albo pretorio: fasc. annuale per attività
- Registro Albo pretorio
- Repertori

I.4 Sistema informativo

- Organizzazione del sistema: fasc. annuale per attività
- Statistiche promosse dall'ATA: un fasc. per ciascun affare
- Statistiche richieste dall'ISTAT o altro ente: un fasc. per ciascun affare
- Richie dati da parte enti convenzionati per adempimenti di legge: un fascicolo per ogni adempimento

I.5 Informazioni e comunicazioni ad enti e cittadini

- Iniziative dell'URP: un fasc. per ciascun affare
- Reclami dei cittadini: repertorio annuale
- Bandi e avvisi a stampa: repertorio annuale
- Gestione del sito Web: fasc. annuale per attività

I.6 Politica del personale, ordinamento degli uffici e dei servizi

- Attribuzione di competenze agli uffici: fasc. annuale per attività
- Organigramma: un fasc. per ciascuna definizione dell'organigramma (fasc. per affare)
- Organizzazione degli uffici: un fasc. per ciascun affare
- Orari di apertura al pubblico degli uffici: fasc. annuale per attività
- Materiale preparatorio per le deliberazioni in materia di politica del personale: fasc. per affare

I.7 Relazioni con le organizzazioni sindacali e di rappresentanza del personale

- Rapporti di carattere generale: un fasc. per ciascun affare
- Costituzione e modifica delle rappresentanze del personale: un fasc. per ciascun affare
- Verbali della Delegazione trattante per la contrattazione integrativa decentrata: repertorio annuale

I.8 Controlli interni ed esterni
- Controllo degli enti preposti: un fasc. per ciascun controllo

I.9 Editoria e attività informativo promozionale interna ed esterna
- Pubblicazioni istituzionali dell'ATA (libri, riviste, inserzioni o altro): raccolta bibliografica
- Pubblicazioni istituzionali dell'ATA (materiali preparatori): un fasc. per ciascun numero
- Comunicati stampa: un fasc. per ciascun periodo (fasc. per attività)
- Materiali televisivi e altre forme di promozione

I.10 Cerimoniale, attività di rappresentanza, riconoscimenti
- Iniziative specifiche: un fasc. per ciascun affare
- Concessione dell'uso del logo e/o patrocinio: fasc. per attività

I.11 Rapporti istituzionali
- Iniziative specifiche: un fasc. per ciascun affare
- Gemellaggi: un fasc. per ciascun affare

I.12 Forme associative per esercizio di funzioni e servizi e adesione ad Associazioni
- Costituzione di enti controllati dall'ATA: fasc. per persona giuridica
- Partecipazione dell'ATA a enti e associazioni: fasc. per persona giuridica
- Nomina dei rappresentanti dell'ATA in Enti: fasc. per persona giuridica

Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia

II.1 Presidente
- fascicolo personale (da chiudere al termine del mandato)

II.2 Assemblea degli enti convenzionati
- convocazione dell'Assemblea e ordine del girono: fasc. annuale per attività
- interrogazioni e mozioni (materiale preparatorio e connesso): fasc. per attività

II.3 Comitato di Coordinamento
- convocazioni
- verbali delle sedute

II.4 Commissario Straordinaio
- fascicolo personale (da chiudere al termine del mandato)

II.5 Direttore e dirigenza
- fascicolo personale (da chiudere al termine del mandato)

II.6 Revisori dei conti
- Revisori dei conti: fascicoli personali
- verbali e relazioni: repertorio annuale

II.7 Commissario *ad acta*
- fascicolo personale (da chiudere al termine del mandato)

II.8 Organi di controllo interni
- Nomina, revoca degli organi di controllo: un fasc. per ogni organo
- Relazioni degli organi di controllo: repertorio annuale

II.9 Organi consultivi
- Nomina, revoca degli organi consultivi: un fasc. per ogni organo
- relazioni degli organi consultivi: repertorio annuale

Titolo III. Risorse umane

III.0 Fascicoli del personale
- un fascicolo per ogni dipendente o assimilato

III.1 Concorsi, selezioni, colloqui
- Criteri generali e normativa per il reclutamento del personale: fasc. per affare
- Procedimenti concorsuali (bandi, domande, verbali, prove d'esame): fasc. per affare
- Curricula inviati per richieste di assunzione: serie organizzata cronologicamente
- Domande di assunzione pervenute senza indizione di concorso o selezione: serie organizzata cronologicamente

III.2 Assunzioni e cessazioni
- Criteri generali e normativa per le assunzioni e cessazioni: fasc. per affare
- Atti di nomina, licenziamenti, dimissioni, promessa solenne, giuramento, nomina in prova: fasc. per affare e fasc. personale

III.3 Comandi e distacchi; mobilità
- Criteri generali e normativa per comandi, distacchi, mobilità: fasc. per affare
- Atti di comandi, distacchi, mobilità: fasc. per affare e fasc. personale

III.4 Attribuzione di funzioni, ordini di servizio e missioni
- Criteri generali e normativa per le attribuzioni di funzioni, ordini di servizio e missioni: fasc. per affare
- Attribuzione di funzioni: fasc per affare e fasc. personale
- Ordini di servizio: fasc. per attività e fasc. personale
- Missioni dei dipendenti: fasc. per attività e fasc. personale
- Autorizzazioni allo svolgimento di attività esterne: fasc. per affare e fasc. personale

III.5 Inquadramenti e applicazione contratti collettivi di lavoro
- Criteri generali e normativa per gli inquadramenti e le applicazione dei contratti collettivi di lavoro: fasc. per affare
- Determinazione dei ruoli e contratti: fasc. per affare

III.6 Retribuzioni e compensi
- Criteri generali e normativa per retribuzioni e compensi: fasc. per affare
- Anagrafe delle prestazioni: base di dati
- Ruoli degli stipendi: base di dati/tabulati
- Determinazione delle voci accessorie: fasc. personale
- Provvedimenti giudiziari di requisizione dello stipendio: fasc. per affare e fasc. personale
- Cessione del quinto dello stipendio: fasc. per affare e fasc. personale

III.7 Trattamento fiscale, contributivo e assicurativo
- Criteri generali e normativa per il trattamento fiscale, contributivo e assicurativo: fasc. per affare
- Determinazioni specifiche e provvedimenti circa il trattamento fiscale, contributivo e assicurativo: fasc. per affare
- Assicurazioni obbligatorie: fasc. personale

III.8 Tutela della salute e sicurezza sul luogo di lavoro
- Criteri generali e normativa per la tutela della salute e sicurezza sul luogo di lavoro: fasc. per affare
- Rilevazione dei rischi: fasc. per persona (uno per sede)
- Prevenzione infortuni: fasc. per affare
- Denunce di infortunio: fasc. per affare e fasc. personale
- Visite di medicina preventiva: fasc. per ciascuna campagna di visite. I referti delle singole visite, in busta chiusa, vanno inseriti nel fascicolo personale
- Verbali dei rappresentanti dei lavoratori per la sicurezza

III.9 Dichiarazioni di infermità ed equo indennizzo
- Criteri generali e normativa per le dichiarazioni di infermità: fasc. per affare
- Dichiarazioni di infermità e calcolo dell'indennizzo: fasc. per affare e fasc. personale

III.10 Indennità premio di servizio e trattamento di fine rapporto, quiescenza
- Criteri generali e normativa per il trattamento di fine rapporto: fasc. per affare
- Trattamento pensionistico e di fine rapporto: fasc. per affare e fasc. personale

III.11 Servizi al personale su richiesta
- Criteri generali e normativa per il servizi su richiesta: fasc. per affare
- Convenzioni stipulate dall'ATA: fasc. per affare
- Buoni pasto forniti dall'ATA: fasc. per attività
- Domande di servizi: fasc. per affare

III.12 Orario di lavoro, presenze e assenze
- Criteri generali e normativa per le assenze: fasc. per affare
- Domande e dichiarazioni dei dipendenti sull'orario e sulle assenze: fasc. personale
- Fogli firma; cartellini marcatempo; tabulati elettronici di rilevazione presenze: fasc. per attività
- Rilevazioni delle assenze per sciopero: fasc. per affare
- Part time: fasc. personale
- Permessi e aspettative: fasc. personale
- Diritto allo studio: fasc. personale
- Congedo ordinario e straordinario: fasc. personale
- Certificati medici di malattia: fasc. personale

III.13 Giudizi, responsabilità e provvedimenti disciplinari
- Criteri generali e normativa su provvedimenti disciplinari: fasc. per affare
- Provvedimenti disciplinari: fasc. per affare e fasc. personale

III.14 Formazione e aggiornamento professionale
- Criteri generali e normativa per la formazione e l'aggiornamento professionale: fasc. per affare
- Organizzazione di corsi di formazione e aggiornamento: fasc. per affare
- Partecipazione dei dipendenti a corsi: fasc. personale

III.15 Collaboratori esterni
- Criteri generali e normativa per il trattamento dei collaboratori esterni: fasc. per affare
- Elenco degli incarichi conferiti: repertorio
- Incarichi a contratto: fasc. per affare

Titolo IV. Risorse finanziarie e patrimoniali

IV.1 Bilancio preventivo e Piano esecutivo di gestione (PEG)
- Documento Unico di Programmazione (DUP): fasc. per affare
- Nota aggiornamento al DUP: fasc. per affare
- Bilancio preventivo: fasc. per affare
- Allegati del Bilancio preventivo
- Piano Esecutivo di Gestione: fasc. per affare
- Allegati del Piano Esecutivo di Gestione

IV.2 Gestione del bilancio e del PEG (con eventuali variazioni)
- Gestione del bilancio: fasc. per affare
- Variazioni di bilancio: fasc. per affare

IV.3 Gestione delle entrate: accertamento, riscossione, versamento
- Accertamenti delle entrate: fasc. per affare
- Riscossioni e versamenti
- Finanziamenti regionali
- Finanziamenti provinciali
- Finanziamenti comunali
- Finanziamenti di altri enti o imprese
- Contratti di mutuo: fasc. per affare
- Proventi da affitti e locazioni: fasc. per affare per ciascun immobile

- Pagamento diritti di riproduzione: fasc. per attività
- Reversali: repertorio annuale

IV.4 Gestione della spesa: impegno, liquidazione, ordinazione e pagamento
- Impegni di spesa: determinazioni dirigenziali, repertorio annuale
- Fatture ricevute: repertorio annuale
- Decreti di liquidazione: repertorio annuale
- Mandati di pagamento: repertorio annuale

IV.5 Partecipazioni finanziarie
- Gestione delle partecipazioni finanziarie: fasc. per affare

IV.6 Rendiconto della gestione; adempimenti e verifiche contabili
- Rendiconto della gestione
- Conto del bilancio
- Conto del patrimonio
- Conto economico

IV.7 Adempimenti fiscali, contributivi e assicurativi
- Mod. 770: fasc. annuale per attività
- Ricevute dei versamenti (IVA, IRPEF, ecc.): fasc. per attività per ciascuna imposta
- Pagamento dei premi dei contratti assicurativi

IV.8 Beni immobili
- Inventario dei beni immobili: registro
- Acquisizione di beni immobili: un fasc. per ciascun immobile
- Gestione dei beni immobili: manutenzione ordinaria
- Concessione in uso dei beni immobili
- Alienazione e dismissione di beni immobili: fasc. per affare

IV.9 Beni mobili
- Inventari dei beni mobili: un registro per ogni consegnatario
- Acquisizione di beni mobili: acquisto hardware e software, acquisti di beni e forniture varie: fasc. per affare
- Manutenzione di beni mobili
- Concessione in uso
- Alienazione e altre forme di dismissione di beni mobili

IV.10 Economato
- Acquisizione di beni e servizi con cassa economale: fasc. per affare
- Rendiconto periodico cassa economale: fasc. per affare
- Conto dell'economo: fasc. per affare
- Acquisizione di beni e servizi per il funzionamento dell'Ente non gestiti dall'Economo: fasc. per affare
- Elenco dei fornitori: repertorio

IV.11 Tesoreria
- Rapporti con il Tesoriere
- Giornale di cassa: repertorio annuale
- Mandati quietanzati inviati all'ATA al termine dell'esercizio finanziario: repertorio periodico

Titolo V. Affari legali

V.1 Contenzioso
- Cause civili: fasc. per affare
- Cause amministrative: fasc. per affare
- Cause penali: fasc. per affare
- Cause tributarie: fasc. per affare

V.2 Responsabilità civile e patrimoniale verso terzi; assicurazioni
- Contratti assicurativi: fasc. per affare
- Richieste e pratiche di risarcimento: fasc. per affare

V.3 Pareri e consulenze
- Pareri legali: fasc. per affare
- Consulenze agli uffici e strutture: fasc. per affare

Titolo VI. Gestione integrata dei rifiuti urbani e assimilati

VI.1 Pianificazione e studi
- Piano d'Ambito: fascicolo per affare
- Studi: fascicolo per affare
- Gestione finanziamenti regionali o di altri enti per realizzazione infrastrutture comunali: un fascicolo per ogni affare
- fascicolo per ogni affare (es. fascicolo per redazione Piano d'ambito, per ogni conferenza di servizio o richiesta parere su opere di terzi)

VI.2 Gestione servizio rifiuti, trattamento, smaltimento
- fascicolo per ogni affare

VI.3 Progetti di sensibilizzazione ambientale
- fascicolo per ogni affare

VI.4 Realizzazione opere e impianti
- fascicolo per ogni affare

Titolo VII. Oggetti diversi
Un fascicolo per ogni affare che non ha trovato una possibile collocazione nelle altri classi.

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 11

MODELLO DI CAMICIA

DI FASCICOLO CARTACEO

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

Area / Servizio _____

Anno apertura - Titolo . Classe . N° fascicolo
(es. 2016-4.10.1)

_____

Oggetto: _____

_____

_____

Anno chiusura _____

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 12

CONVENZIONE REGIONE MARCHE

E DISCIPLINARE TECNICO PER IL SERVIZIO

DI CONSERVAZIONE SOSTITUTIVA

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

DETERMINAZIONE N. 129 DEL 29 SETTEMBRE 2015

Oggetto:	Affidamento diretto alla Regione Marche tramite convenzionamento del servizio di conservazione digitale dei documenti informatici prodotti dall'ATA.

IL DIRETTORE
dott.ssa Elisabetta Cecchini

PREMESSO che:

- il Codice dell'amministrazione digitale "CAD" di cui al decreto legislativo n. 82 del 2005 ha normato la dematerializzazione dei documenti cartacei e la disponibilità degli stessi a livello informatico;
- la riproduzione dei documenti su supporti informatici è valida solo se viene garantita la conformità dei documenti agli originali nel rispetto delle regole tecniche stabilite dall'art. 71 del CAD (Codice dell'amministrazione digitale di cui al DLgs n. 82/2005) e dalla deliberazione CNIPA n. 11/2004;
- il 3 dicembre 2013 è stato emanato il DPCM con le nuove "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" che apporta modifiche alla deliberazione CNIPA n. 11/2004;
- tale DPCM:
    - introduce il concetto di "sistema di conservazione" che assicura la conservazione a norma dei documenti elettronici e la disponibilità dei fascicoli informatici, definendo le regole, le procedure, le tecnologie e i modelli organizzativi da adottare per la gestione di tali processi;
    - obbliga le pubbliche amministrazioni ad avvalersi esclusivamente dei servizi offerti da Conservatori accreditati dall'AGID con le modalità stabilite nella Circolare n. 65 del 10 aprile 2014, concedendo tuttavia alle strutture di conservazione esistenti alla data di emanazione del DPCM citato tre anni di tempo per adeguare i loro sistemi alle nuove disposizioni;

ATTESO che:

- per gli acquisti di beni e servizi sotto soglia comunitaria, l'ATA ha l'obbligo di avvalersi di convenzioni Consip e di far ricorso anche al mercato elettronico della pubblica amministrazione (M.E.P.A.) ovvero attraverso il mercato elettronico realizzato dalle centrali di committenza di riferimento;
- la legge 7 agosto 1990, n. 241 recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" stabilisce espressamente all'art. 15 che: "Anche al di fuori delle ipotesi previste dall'articolo 14, le amministrazioni pubbliche possono sempre concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune";
- la determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture n. 7 del 21 Ottobre 2010 su "Questioni interpretative concernenti la disciplina

dell'articolo 34 del d.lgs. 163/2006 relativa ai soggetti a cui possono essere affidati i contratti pubblici", conformemente a quanto in precedenza affermato dalla giurisprudenza comunitaria, ha ribadito la legittimità del ricorso a forme di cooperazione pubblico-pubblico attraverso cui più amministrazioni assumono impegni reciproci, realizzando congiuntamente le finalità istituzionali affidate loro, purché vengano rispettati una serie di presupposti;

- i presupposti richiesti ai fini della legittimità dell'impiego dello strumento convenzionale sono stati individuati nei seguenti punti: A) l'accordo deve regolare la realizzazione di un interesse pubblico, effettivamente comune ai partecipanti, che le Parti hanno l'obbligo di perseguire come compito principale, da valutarsi alla luce delle finalità istituzionali degli Enti coinvolti; B) alla base dell'accordo deve esserci una reale divisione di compiti e responsabilità; C) i movimenti finanziari tra i soggetti che sottoscrivono l'accordo devono configurarsi solo come ristoro delle spese sostenute, essendo escluso il pagamento di un vero e proprio corrispettivo, comprensivo di un margine di guadagno; D) il ricorso all'accordo non può interferire con il perseguimento dell'obiettivo principale delle norme comunitarie in tema di appalti pubblici, ossia la libera circolazione dei servizi e l'apertura alla concorrenza non falsata negli Stati membri;

RIENUTO di poter quindi ovviare all'utilizzo delle convenzioni Consip e del M.E.P.A. procedendo alla scelta di un Conservatore soggetto pubblico tramite convenzionamento;

VERIFICATA la possibilità di fatto di potersi rivolgere alla Regione Marche che ha istituito una struttura in grado di fornire idonee garanzie di sicurezza ed efficacia e che dispone della strumentazione tecnica necessaria e di personale adeguato allo scopo, in adesione al modello organizzativo che si sta affermando nel contesto nazionale dei cosiddetti depositi digitali, "Centri di conservazione digitale" o Poli archivistici, strutture dedicate alla conservazione per conto di più enti e organizzazioni, e quindi finalizzate in particolare a rispondere alle necessità di conservazione del patrimonio digitale di tutti gli enti locali del territorio marchigiano;

PRESO ATTO che:

- tale progetto, nato dall'analisi di best practice nazionali e internazionali (tra cui il progetto ParER della Regione Emilia Romagna e la soluzione open source proposta da Archivematica), si è concretizzato con la costituzione formale del Polo per la conservazione digitale Marche DigiP (Digital Preservation) con la Delibera di Giunta n. 167 del 14/02/2010;
- Marche DigiP (Digital Preservation) è una struttura che eroga servizi di conservazione dei documenti informatici e degli archivi digitali secondo il modello OAIS (Open Archival Information System) descritto nello standard ISO 14721:2012 e nel rispetto dei requisiti archivistici;
- per la conservazione dei propri documenti informatici la Regione Marche sta già utilizzando tale sistema;
- l'emanazione del DPCM 3 dicembre 2013 recante le nuove "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005" come suddetto concede alle strutture di conservazione esistenti alla data di emanazione del DPCM citato - tra le quali rientra il Polo Marche DigiP - tre anni di tempo per adeguare i loro sistemi alle nuove disposizioni;

- la Regione Marche, pur utilizzando sistemi già conformi alle specifiche nazionali ed agli standard di settore, ad oggi non risulta ancora tra i soggetti accreditati presso l'Agenzia per l'Italia Digitale, ma ha già verificato la fattibilità e predisposto un piano di lavoro con l'obiettivo di conseguire questo accreditamento prima del termine fissato dalla normativa vigente (11 aprile 2017) applicando infatti sistemi già in uso da enti già accreditati dall'AGID;

RITENUTO per quanto sopra che l'obbligo per le pubbliche amministrazioni ad avvalersi esclusivamente dei servizi offerti da Conservatori accreditati dall'AGID con le modalità stabilite nella Circolare n. 65 del 10 aprile 2014, possa ritenersi soddisfatto anche convenzionandosi con il Polo Marche DigiP della Regione Marche in virtù dei citati tre anni di tempo per adeguare i loro sistemi alle nuove disposizioni;

ATTESO che è pertanto interesse dell'ATA convenzionarsi con la Regione Marche per avvalersi di Marche DigiP per la conservazione digitale dei documenti informatici prodotti, secondo lo schema allegato alla presente determinazione, da considerarsi parte sostanziale e integrante della medesima;

ATTESO che al momento la Regione Marche ha previsto una prima convenzione di durata fino al 31/12/2015, periodo nel quale si procederà alle verifiche delle procedure tecniche, ossia della compatibilità del software di versamento utilizzato dall'ATA con le procedure del sistema Marche DigiP, e che successivamente la Regione proporrà una successiva convenzione che regolerà i rapporti anche dal punto di vista economico;

RILEVATA dall'allegata lettera che la Regione ha inviato ai Comuni la gratuità del servizio fino al 30/06/2016, mentre per i periodi successivi la Regione valuterà modalità di copertura con l'auspicabile obiettivo di ridurre gli oneri a carico degli Enti, indicativamente secondo lo schema tariffario già in uso in Emilia Romagna;

PRESO ATTO che dal tariffario dell'Emilia Romagna risulterebbero costi annui di euro 500,00 per una richiesta di spazio di conservazione fino a 200 gigabyte;

DATO ATTO che la fornitura sopra indicata rientra nella tipologia dei beni acquisibili mediante ricorso alle procedure in economia, ai sensi dell'art. 125 del D.Lgs. n. 163/2006 e dell'art. 13 del vigente Regolamento di Organizzazione;

REPUTATO, nell'ambito degli acquisti in economia di importo inferiore a quarantamila euro, di procedere con affidamento diretto da parte del responsabile del procedimento ad un fornitore, come consentito dall'art. 125, co. 11, del D.Lgs. n. 163/2006 e dall'art. 16, co. 6 del vigente Regolamento di Organizzazione, tanto più trattandosi di Ente pubblico;

CONSIDERATO che il presente procedimento non rientra nel campo di applicazione della L. n. 136/2010 sulla tracciabilità dei flussi finanziari trattandosi di convenzionamento con Ente pubblico;

PER QUANTO SOPRA ESPOSTO, VISTI:
- deliberazione CNIPA n. 11/2004;
- Codice dell'amministrazione digitale di cui al DLgs n. 82/2005

- DPCM 3 dicembre 2013 recante le nuove "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005";
- la L. n 488/1999;
- il D.Lgs. n. 267/2000, con particolare riferimento agli artt. 107 e 183;
- il D.Lgs. n. 163/2006 e ss.mm.ii. ed il D.P.R. n. 207/2010;
- la L. n. 296/2006 e ss.mm.ii., con particolare riferimento all'art. 1, co. 450, relativamente all'obbligo per le pubbliche amministrazioni di approvvigionamento di beni e servizi tramite il ricorso al mercato elettronico;
- il D.Lgs. n 95/2012, convertito in L. n. 135/2012, inerente la nullità per i contratti stipulati in violazione alle direttive sugli acquisti attraverso gli strumenti di acquisto messi a disposizione dal Consip S.p.a.;
- la legge 7 agosto 1990, n. 241;
- la determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture n. 7 del 21 Ottobre 2010;
- il Regolamento di organizzazione, approvato don Deliberazione dell'Assemblea n. 4 del 09.09.2013, con particolare riferimento al Titolo IV "Acquisizione di beni, servizi e lavori sotto soglia comunitaria";
- la L. n. 136/2010, recante il "Piano straordinario contro le mafie";
- il Decreto del Presidente n. 11 del 19.12.2014, di approvazione del "Piano triennale di prevenzione della corruzione 2014-2016, ai sensi della L. n. 190/2012;
- i Decreti del Presidente n. 3 del 23.03.2015 di approvazione del PEG per il triennio 2015-2017, n. 12 del 15.05.2015 e n. 19 del 03.08.2015 di variazione dello stesso;
- i pareri favorevoli, riportati in calce, in ordine alla regolarità tecnica e contabile di cui all'art. 147 bis, co. 1 del D.Lgs. n. 267/2000 come introdotto dall'art. 3, co. 1 del D.L. n. 174/2012;
- l'attestazione positiva, riportata in calce, di compatibilità dei pagamenti ai sensi dell'art. 9, co. 1, lett. a, punto 2, del D.L. n. 78/2009 convertito con modificazioni in L. n. 102/2009;

ACCERTATO che non sussistono situazioni di conflitto di interesse, ai sensi dell'art. 6-bis della L. n. 241/1990 da parte del sottoscritto, nei confronti dei destinatari del presente atto;

RITENUTO di dover disporre personalmente l'atto di che trattasi, poiché adempimento spettante al sottoscritto;

DETERMINA

1. Di approvare per i motivi già esposti in premessa, e che si richiamano integralmente, lo schema di Convenzione di collaborazione con la Regione Marche, ai sensi dell'art. 15 della legge n. 241 del 1990, finalizzato a disciplinare lo svolgimento della funzione di conservazione digitale dei documenti informatici prodotti dall'ATA, allegato al presente atto per farne parte integrante e sostanziale;
2. Di dare atto che la suddetta convenzione ha carattere provvisorio fino al 31/12/2015 finalizzato alla verifica delle procedure tecniche, ossia della compatibilità del software di versamento utilizzato dall'ATA con le procedure del sistema Marche DigiP, e che successivamente la

Regione proporrà una successiva convenzione che regolerà i rapporti anche dal punto di vista economico;

3. Di dare atto che il presente procedimento non rientra nel campo di applicazione della L. n. 136/2010 sulla tracciabilità dei flussi finanziari trattandosi di convenzionamento tra enti pubblici;
4. Di dare atto che il Responsabile del Procedimento, ai sensi dell'art. 10 del D.Lgs. n. 163/2006 e s.m.i., è la dott.ssa Elisabetta Cecchini – Direttore dell'Ente che provvederà alla sottoscrizione della Convenzione;
5. Di trasmettere il presente provvedimento al Responsabile del Servizio pianificazione campagne di comunicazione e rapporti con i media per la pubblicazione all'Albo pretorio on line dell'Ente.

RESPONSABILE ISTRUTTORIA (R.I.)
dott.ssa Simonetta Scaglia

RESPONSABILE PROCEDIMENTO (R.P.)
dott.ssa Elisabetta Cecchini

Il Direttore
dott.ssa Elisabetta Cecchini

SCHEMA DI CONVENZIONE CON GLI ENTI DEL TERRITORIO
PER I SERVIZI DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI

tra

la Regione Marche, rappresentata dal Dirigente della P.F. Sistemi Informativi e Telematici della Giunta Regionale, autorizzato alla sottoscrizione del presente atto con Delibera di Giunta Regionale 265 del 10/03/2014 esecutiva ai sensi di legge;

l'Ente
produttore_____

di seguito congiuntamente indicate "le Parti";

PREMESSO CHE:

- la Regione Marche previsto la costituzione del polo di conservazione con la Delibera di Giunta regionale n. 1039 del 30/07/2008 "Modalità Attuative del Programma Operativo (MAPO) della Regione Marche - POR-FESR - Competitività regionale e occupazione 2007-2013" e ha deliberato con atto di Giunta n.167 del 01/02/2010 la costituzione del Polo regionale di conservazione digitale denominato "Marche DigiP", d'ora in poi denominato DigiP;
- DigiP è la struttura individuata dalla Regione Marche per la fornitura della soluzione tecnologica, organizzativa, giuridica ed archivistica per la gestione e conservazione di archivi digitali della Amministrazione regionale e degli enti locali del territorio regionale;
- DigiP nasce con gli obiettivi di conservazione degli archivi digitali della Regione e degli enti regionali e rendere fruibili i contenuti digitali conservati da parte dei soggetti aventi diritto;
- in seguito all'aggiudicazione della procedura aperta per l'acquisizione di beni e servizi per la creazione e gestione del DigiP - la cui aggiudicazione efficace è stata formalizzata con DDPF n.119/INF del 22.08.2012 - esiste l'infrastruttura organizzativa, tecnologica e giuridica necessaria all'avvio dei servizi di archiviazione digitale a norma;
- la Regione Marche ha approvato con delibera di Giunta n. 265 del 10/03/2014 il presente "Schema di Convenzione" tra la Regione medesima e gli Enti locali delle Marche e loro forme associate, per l'avvio dei servizi di conservazione dei patrimoni documentali informatici da questi ultimi prodotti e mantenuti;
- ai sensi dell'art.15 della L.241/1990 e s.m.i. "*le amministrazioni pubbliche possono sempre concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attivita' di interesse comune*";
- la Regione Marche intende evolvere il proprio modello di servizio di conservazione nell'ottica del Cloud Computing per ottenere il beneficio delle economie di scala legate all'uso di tali tecnologie nel settore Pubblico;

- risulta di interesse dell'Ente produttore avvalersi del DigiP per la conservazione digitale dei documenti, quale soggetto in grado di fornire garanzie di sicurezza ed efficacia e che dispone della strumentazione tecnica necessaria e di personale adeguato allo scopo, stipulando apposita convenzione ai sul modello di Convenzione approvato con Deliberazione n. 265 del 10/03/2014 della Giunta Regionale delle Marche;
- tutti gli allegati previsti e richiamati all'interno della presente Convenzione, e segnatamente il Disciplinare Tecnico, costituiscono parte integrante ed essenziale della stessa;

Si conviene e si stipula quanto segue

CAPO I

DISPOSIZIONI GENERALI

Art. 1

(Oggetto dei servizi di conservazione)

1. L'ente produttore affida la conservazione dei propri documenti informatici, nel rispetto delle norme di legge, a DigiP, individuandolo come responsabile della conservazione dei documenti trasferiti in base alle specifiche definite nella presente convenzione e nei suoi allegati, parte integrante della stessa;
2. L'attività di conservazione svolta da DigiP si ispira ai principi indicati dall'art. 29 del D.Lgs. 42/2004 di coerente, coordinata e programmata attività di studio, prevenzione e manutenzione, e si ritiene in grado di soddisfare gli obblighi in capo all'Ente produttore di conservazione di documenti informatici ed in prospettiva di conservazione ed ordinamento dell'archivio nella sua organicità.

Art. 2

(Finalità)

La presente convenzione ha le seguenti finalità:

a. Creare le condizioni giuridico-organizzative per la conservazione dei documenti informatici dell'Ente produttore, nel rispetto delle finalità istituzionali degli enti;
b. Garantire economicità, efficienza ed efficacia alla funzione di conservazione dei documenti informatici;
c. Garantire una elevata qualità nei livelli di servizio anche a favore di eventuali utenti esterni per l'esercizio del diritto di accesso ai sensi della disciplina sull'accesso ai documenti amministrativi e del decreto legislativo n.196 del 2003, recante il "Codice in materia di protezione dei dati personali" o, in futuro, per ricerche storiche.

CAPO II

FUNZIONAMENTO E RESPONSABILITA'

Art. 3

(Obblighi delle parti)

1. DigiP si impegna alla conservazione dei documenti trasferiti assumendo la funzione di responsabile della conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione.
2. L'Ente produttore si impegna a depositare i documenti informatici nei modi e nelle forme definite da DigiP, garantendone l'autenticità e l'integrità nelle fasi di produzione e di

archiviazione corrente, effettuata nel rispetto delle norme sulla produzione e sui sistemi di gestione dei documenti informatici. In particolare garantisce che il trasferimento dei documenti informatici venga realizzato utilizzando formati compatibili con la funzione di conservazione e rispondenti a quanto previsto dalla normativa vigente.

3. L'Ente produttore mantiene la titolarità e la proprietà dei documenti depositati.
4. L'Ente produttore si impegna ad effettuare secondo diligenza e con la massima cura ed efficienza le attività di test previste e disciplinate nell'ambito della bozza di disciplinare tecnico. La durata complessiva della fase di test verrà concordata tra i responsabili degli Enti individuati negli allegati alla presente Convenzione. La durata complessiva della fase di test non potrà in nessun caso superare il limite di 60 giorni.
5. Entrambi i soggetti dichiarano che le attività previste dalla presente convenzione saranno effettuate nel rispetto dei principi di tutela da parte dello Stato dei beni archivistici come beni culturali e nel rispetto di quanto stabilito dal MIBAC (Soprintendenza archivistica). A tal fine copia della presente convenzione e della documentazione collegata sarà inviata a tutti gli Enti di competenza per gli opportuni adempimenti.
6. Il responsabile della conservazione è individuato nella figura del responsabile della conservazione del DigiP.

Art. 4

(Servizi offerti)

1. I servizi offerti dal DigiP riguardano la conservazione digitale, la restituzione per la consultazione o l'esibizione dei documenti a fini di accesso o per scopi storici, il supporto tecnico-archivistico. I servizi saranno erogati in base ad apposito Disciplinare Tecnico concordato tra i soggetti dei due enti competenti sia dal punto di vista informatico che archivistico.
2. Il Disciplinare Tecnico é redatto congiuntamente ed approvato rispettivamente dal DigiP e dall'Ente produttore. Esso, definito d'intesa con la Soprintendenza Archivistica della Regione Marche, individua in modo preciso e vincolante i tempi e le modalità di erogazione dei servizi, in particolare per quanto riguarda le specifiche operative dei sistemi di conservazione digitale e le modalità tecniche di restituzione dei documenti a fini di accesso e ricerca.
3. Il Disciplinare Tecnico conterrà l'individuazione dei referenti e responsabili di riferimento dei due enti per l'erogazione dei servizi oggetto della Convenzione stessa.
4. Il Disciplinare Tecnico potrà essere aggiornato in caso di modifiche nelle modalità di erogazione dei servizi anche a seguito di eventuali modifiche normative.
5. Il servizio di conservazione digitale e di restituzione dei documenti a fini di accesso e ricerca, che prevede lo svolgimento di procedure codificate, la certificazione dei processi di migrazione e l'adozione di idonee soluzioni tecnologiche e di sicurezza, è finalizzato sia alla conservazione dei documenti informatici, garantendone il mantenimento delle caratteristiche di autenticità, affidabilità, integrità, accessibilità, riproducibilità e intelligibilità all'interno del contesto proprio di produzione e archiviazione, sia alla organizzazione e inventariazione del patrimonio documentario digitale nella prospettiva di conservare l'archivio nella sua organicità per costituire, nei tempi e nei modi previsti dalla normativa, l'archivio storico prevedendo gli opportuni collegamenti logici e descrittivi tra documentazione informatica e documentazione cartacea
6. Il servizio di supporto tecnico archivistico erogato dal DigiP in accordo con la Sovrintendenza archivistica della Regione Marche verrà erogato al fine di consentire una corretta ed efficace integrazione con il polo.

Art. 5

(Accesso ai documenti conservati presso il DigiP)

1. L'accesso ai documenti conservati presso il DigiP avviene con i medesimi tempi e modalità previsti per i documenti conservati presso l'Ente produttore che mantiene la responsabilità del procedimento ai sensi del regolamento adottato per l'accesso ai documenti amministrativi e delle norme sull'accesso vigenti nel tempo.
2. Qualora la domanda di accesso venga presentata al DigiP, questi la trasmette immediatamente all'Ente produttore. DigiP è tenuto a fornire la propria collaborazione, se necessario, per il pieno rispetto dei tempi e delle modalità di accesso previste dalle norme.
3. DigiP, qualora gli venga richiesto, può consentire direttamente l'accesso a documenti soggetti a obblighi di pubblicazione, nel rispetto della normativa vigente.
4. Possono essere stipulati appositi accordi operativi fra i responsabili dei due enti per definire con maggior dettaglio modalità e obblighi reciproci, in particolare per quanto riguarda l'eventuale produzione di copie conformi cartacee, nel rispetto del principio per cui la copia conforme cartacea viene effettuata, se richiesta, dal soggetto che stampa il documento cartaceo traendolo dall'originale informatico.

CAPO III

RAPPORTI TRA SOGGETTI CONVENZIONATI

Art. 6

(Strumenti di consultazione e controllo)

1. DigiP consente all'Ente produttore l'accesso ai propri sistemi per verificare il corretto svolgimento dell'attività di conservazione e per consultare ed eventualmente estrarre i documenti depositati e le prove di conservazione, secondo le modalità tecniche previste nel Disciplinare Tecnico.
2. L'Ente produttore concorda con DigiP i nominativi e le funzioni del personale abilitato allo svolgimento della funzione di cui al comma 1.
3. DigiP consente alla Sovrintendenza archivistica l'accesso ai propri sistemi per rendere possibile ed operativo lo svolgimento della funzione di vigilanza e tutela prevista dalla legge ed effettuare le opportune verifiche sul corretto svolgimento dell'attività di conservazione.

Art. 7

(Oneri a carico delle parti, garanzie)

1. I servizi oggetto della presente convenzione sono forniti gratuitamente all'Ente produttore per tutta la durata della Convenzione stessa, prevista e disciplinata all'articolo 9.
2. Non sono previsti altri oneri a carico delle parti per il periodo di durata della presente convenzione.

Art. 8

(Trattamento dei dati personali)

1. L'Ente produttore è titolare del trattamento dei dati personali contenuti nei documenti dallo stesso prodotti. Al fine di consentire la fornitura dei servizi di cui al precedente art. 4, l'Ente produttore nomina DigiP quale responsabile esterno del trattamento dei dati personali necessari all'esecuzione della presente convenzione ed al compimento degli atti conseguenti.

2. DigiP accetta e si impegna, nel trattamento dei suddetti dati, ad attenersi alle istruzioni ed a svolgere i compiti indicati dall'Ente produttore nel Disciplinare tecnico;
3. Alla scadenza della convenzione, ovvero al termine di validità della stessa per qualsivoglia causa, la designazione a responsabile esterno del trattamento dei dati personali decade automaticamente.

Art. 9

(Decorrenza, durata, rinnovo della convenzione)

1. La presente convenzione ha durata fino al 31 Dicembre 2015 e dovrà essere espressamente rinnovata dalle parti alla sua naturale conclusione.
2. La data di effettiva attivazione dei servizi di conservazione dei documenti informatici verrà definita secondo quanto stabilito dai referenti e responsabili di riferimento dei due enti;
3. Alla scadenza naturale della presente Convenzione così come disciplinata al comma 1 del presente articolo, gli Enti sottoscrittori (Produttore e Conservatore), si impegnano a ridefinire la disciplina dell'art. 7 (Oneri a carico delle parti, garanzie).

Art. 10

(Modalità di restituzione degli archivi)

Al termine della durata naturale della presente Convenzione, tutti i documenti dell'Ente produttore depositati e tutte le prove dei processi di conservazione verranno restituiti all'Ente Produttore secondo le modalità previste nel disciplinare tecnico, unitamente alla documentazione indicante le specifiche tecniche degli archivi conservati così come del sistema di conservazione, al fine di agevolare il trasferimento degli stessi su diverso sistema di conservazione.

Ente produttore

…….

Regione Marche

P.F. Sistemi Informativi e Telematici della Giunta Regionale

Il Dirigente Serenella Carota

Giunta Regione Marche
Servizio Risorse Umane e Strumentali
P.F. Sistemi Informativi e Telematici

Ancona, lì 11 settembre 2015

AI SINDACI E SEGRETARI
DEI COMUNI

AI SEGRETARI DI PROVINCE E
UNIONI MONTANE

DEL TERRITORIO MARCHIGIANO

LORO SEDI

OGGETTO: Servizi del Polo di conservazione Marche DigiP agli enti locali

Gentili Sindaci e Segretari,

La Regione Marche ha avviato il progetto del Polo di conservazione regionale Marche DigiP, in adesione al modello organizzativo che si sta affermando nel contesto nazionale dei cosiddetti depositi digitali, "Centri di conservazione digitale" o Poli archivistici, strutture dedicate alla conservazione per conto di più enti e organizzazioni, e quindi finalizzate in particolare a rispondere alle necessità di conservazione del patrimonio digitale di tutti gli enti locali del territorio marchigiano.

La Regione Marche, ha previsto nell'ambito della programmazione POR 2007-2013 misura 2.1.2.11.02 "Sistema di conservazione documentale" un intervento specifico per la costruzione del sistema di conservazione, con un investimento di oltre 1.500.000 euro ed ha costituito formalmente il Polo per la conservazione digitale Marche DigiP (Digital Preservation) con la Delibera di Giunta n. 167 del 14/02/2010.

Marche DigiP (Marche Digital Preservation) è una struttura che eroga servizi di conservazione dei documenti informatici e degli archivi digitali secondo il modello OAIS (Open Archival Information System) descritto nello standard ISO 14721:2012 e nel rispetto dei requisiti archivistici.

Il progetto, nato dall'analisi di best practice nazionali e internazionali (tra cui il progetto ParER della Regione Emilia Romagna e la soluzione open source proposta da Archivematica) ha consolidato i suoi risultati e sta attualmente conservando i documenti informatici dell'ente Regione Marche.

Successivamente all'aggiudicazione della fornitura per la costruzione del Polo Marche DigiP, il 3 dicembre 2013 è stato emanato il DPCM con le nuove "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005". Tale DPCM definisce la natura e le funzioni del sistema di conservazione, i modelli organizzativi, gli standard e le specifiche tecniche; inoltre, obbliga le pubbliche amministrazioni ad avvalersi esclusivamente dei servizi offerti da Conservatori accreditati dall'AGID con le modalità stabilite nella Circolare n. 65 del 10 aprile 2014, concedendo tuttavia alle strutture di conservazione esistenti alla data di emanazione del DPCM citato - tra le quali rientra il Polo Marche DigiP - tre anni di tempo per adeguare i loro sistemi alle nuove disposizioni..

Giunta Regione Marche
Servizio Risorse Umane e Strumentali
P.F. Sistemi Informativi e Telematici

La Regione Marche, pur utilizzando sistemi già conformi alle specifiche nazionali ed agli standard di settore, ad oggi non risulta ancora tra i soggetti accreditati presso l'Agenzia per l'Italia Digitale, ma ha già verificato la fattibilità e predisposto un piano di lavoro con l'obiettivo di conseguire questo accreditamento prima del termine fissato dalla normativa vigente (11 aprile 2017) .

Per gli Enti in indirizzo che vogliano richiedere a questa struttura i servizi di conservazione digitale del loro patrimonio documentale, i costi saranno a carico del bilancio regionale fino al 30/06/2016, mentre per i periodi successivi si valuteranno modalità di copertura con l'auspicabile obiettivo di ridurre gli oneri a carico degli Enti.

Cordialmente.

La PO Sistemi Informativi per la dematerializzazione, la gestione dei flussi documentali e la trasparenza
(Cinzia Amici)

Il dirigente della
PF Sistemi Informativi e Telematici
(Serenella Carota)

PARERE DI REGOLARITÀ TECNICA

Ai sensi dell'art. 147 bis, comma 1 del D.Lgs. n. 267/2000, si esprime **parere favorevole** in ordine alla regolarità tecnica, attestando la regolarità della presente determinazione e la correttezza dell'azione amministrativa.

Jesi, lì 29.09.2015

Il Direttore
dott.ssa Elisabetta Cecchini

CERTIFICATO DI INIZIO PUBBLICAZIONE

DETERMINAZIONE N. 129 DEL 29.09.2015

OGGETTO: Affidamento diretto alla Regione Marche tramite convenzionamento del servizio di conservazione digitale dei documenti informatici prodotti dall'ATA.

Si certifica che l'atto di cui sopra viene oggi pubblicato all'Albo Pretorio on line di questa Amministrazione per 15 giorni interi e consecutivi.

Jesi, lì 26.11.2015

Il Direttore
dott.ssa Elisabetta Cecchini

REGIONE MARCHE

Disciplinare Tecnico per il servizio di conservazione

Ente produttore: [denominazione ente produttore]
Soggetto conservatore: Marche DigiP – Polo di conservazione regionale

Versione 1.0

Disciplinare tecnico per il servizio di conservazione

Versione 1.0

Firmatari	Ente

Modifiche rispetto alle precedenti versioni

Versione	Riferimento	Modifiche
1.0		

Indice

1. Premessa

Il presente Disciplinare Tecnico è redatto, d'intesa con la Regione Marche, in riferimento all'art. 4 della "Convenzione con gli enti del territorio per i servizi di conservazione dei documenti informatici" (d'ora in poi Convenzione), tra _____ (d'ora in poi Ente produttore) e REGIONE MARCHE, che regola nei suoi profili generali il rapporto tra l'Ente produttore e REGIONE MARCHE per lo svolgimento della funzione di conservazione dei documenti informatici affidati dall'Ente produttore a REGIONE MARCHE e più specificatamente al suo Servizio Polo di conservazione regionale Marche DigiP (d'ora in poi Marche DigiP).

Finalità del presente Disciplinare tecnico (d'ora in poi Disciplinare) è definire in modo preciso e vincolante le modalità operative di erogazione dei servizi da parte di Marche DigiP nei confronti dell'Ente produttore, in particolare per quanto riguarda le specifiche delle modalità tecniche per l'interoperabilità tra i sistemi dell'Ente produttore e i sistemi di conservazione digitale, le specifiche operative di questi ultimi e le modalità tecniche di restituzione dei documenti ai fini di accesso e ricerca.

In particolare, nel presente Disciplinare sono definiti i dati e i parametri che l'Ente produttore e Marche DigiP utilizzeranno nel contesto dei web service per l'interoperabilità con il sistema di conservazione, le stime dei flussi e dei volumi dei processi coinvolti, le modalità di esercizio del diritto di accesso, le modalità di ricerca, recupero e restituzione dei documenti conservati, gli aspetti tecnologici necessari a consentire il corretto svolgimento del processo di conservazione.

Definisce inoltre i referenti e i responsabili di riferimento sia dell'Ente produttore sia di Marche DigiP per l'erogazione dei servizi e la verifica del corretto svolgimento del processo di versamento dei documenti e di conservazione.

Definisce l'articolazione in Strutture (corrispondenti normalmente alle Aree Organizzative Omogenee, ma non escludendo altre ripartizioni) con cui l'Ente produttore si rapporta con Marche DigiP per il versamento dei documenti.

La definizione dei dati e dei parametri – e in genere di tutti gli elementi necessari alla corretta esecuzione del servizio di conservazione digitale – avviene di norma a livello di singola struttura interessata. Nel caso in cui gli elementi siano descritti a livello di Ente produttore, questi si applicano anche a tutte le strutture interessate.

Il Disciplinare costituisce, nelle sue versioni preliminari e non definitive, il documento di riferimento per lo svolgimento dei test che precedono l'attivazione del servizio di conservazione digitale. Il Disciplinare è rivisto e aggiornato ogniqualvolta intervengano modifiche o integrazioni relative agli oggetti trattati.

L'avvio del servizio di conservazione avverrà entro 3 giorni dal completamento dei test

Il Disciplinare e ogni sua successiva modifica sono inviati a cura di Marche DigiP alla Soprintendenza Archivistica per la Regione Marche in ottemperanza alle comunicazioni previste per il coordinamento delle attività in tema di conservazione dei documenti informatici.

All'Ente produttore è trasmessa ogni altra comunicazione inviata da Marche DigiP alla Soprintendenza Archivistica.

2. Referenti

2.1. Referenti Marche DigiP

Per quanto attiene ai rapporti generali con l'Ente produttore, Marche DigiP individua i seguenti referenti:

Nominativo	Ruolo e competenze	Contatti

2.2. Referenti Ente produttore

Per quanto attiene ai rapporti generali con Marche DigiP, l'Ente produttore individua i seguenti referenti:

Nominativo	Ruolo e competenze	Struttura e Contatti

N.B.: inserire al massimo n. 2 referenti.

3. Servizi di conservazione

3.1. Sistema di conservazione e modalità di versamento

Marche DigiP svolge il servizio di conservazione utilizzando il Sistema di conservazione DigiP (d'ora in poi Sistema di conservazione), il quale espone dei web service tanto per il versamento, quanto per il recupero/restituzione dei documenti conservati.

Le specifiche tecniche dei web service (inclusi i protocolli di comunicazione e le modalità di svolgimento delle sessioni di versamento) sono illustrate nel documento "Specifiche tecniche Servizio di Versamento DigiP" (d'ora in poi Specifiche), pubblicati all'indirizzo: **http://www.ecommunity.marche.it**, nella sezione "Polo di conservazione regionale" e quindi "Modalità di Attuazione".

Il collegamento telematico tra l'Ente produttore e Marche DigiP avviene attraverso la rete regionale. L'Ente produttore dovrà garantire una connettività adeguata.

Marche DigiP mette a disposizione dell'Ente produttore e, su sua richiesta, degli sviluppatori dei sistemi software versanti, un ambiente di test per effettuare le prove di versamento e recupero dei documenti.

I sistemi informatici di produzione, gestione e versamento dei documenti dell'Ente produttore sono descritti nel paragrafo 5.2.

L'Ente produttore invia i documenti in conservazione interfacciando i propri sistemi informatici con il Sistema di conservazione mediante i web service descritti nelle Specifiche e utilizzando i dati, i parametri e le informazioni definite nel presente Disciplinare.

Per determinate tipologie documentali e in casi eccezionali possono essere previste modalità di versamento alternative ai web service. Qualora tali modalità alternative fossero previste, sono definite e descritte nel presente Disciplinare.

L'Ente produttore ha l'onere di verificare il corretto completamento delle operazioni di versamento e conservazione al fine di segnalare entro 30 giorni eventuali difformità da quanto previsto nel presente Disciplinare.

3.2. Servizi di conservazione

Il processo di conservazione digitale si effettua su Pacchetti di versamento (SIP) che contengono aggregati logici definiti **unità documentarie (UD)**: queste ultime sono formate da uno o più documenti considerati come un tutto unico e costituiscono le unità elementari di cui si compone l'archivio dell'ente produttore.

Il Sistema di conservazione DigiP è stato progettato per accogliere Pacchetti di versamento in modalità backward compatibility con l'antecedente sistema di conservazione Sacer o in modalità SINCRO, personalizzabili. Tale sistema infatti è in grado di accogliere qualsiasi tipo di Pacchetto di Versamento così da garantire flessibilità e configurabilità.

4. Consultazione, restituzione e accesso

4.1. Consultazione e restituzione

L'Ente produttore può consultare le unità documentarie versate in Marche DigiP tramite interfaccia web, collegandosi all'indirizzo comunicato da Marche DigiP e autenticandosi tramite username e password preventivamente forniti da Marche DigiP.

Gli utenti da abilitare per l'accesso tramite interfaccia web al sistema di conservazione sono comunicati dai referenti dell'Ente produttore a Marche DigiP su apposito modulo, che provvede a inviare le credenziali di accesso via email ai diretti interessati.

L'accesso web consente all'Ente produttore di ricercare le unità documentarie versate e di effettuarne il download.

Inoltre, tramite l'interfaccia web, è possibile accedere a un servizio di monitoraggio in tempo reale dei versamenti effettuati, sia andati a buon fine che falliti.

4.2. Accesso a fini amministrativi

Non è previsto da parte di Marche DigiP né il rilascio di copie cartacee conformi agli originali digitali conservati, né l'accesso diretto alla documentazione da parte di colui che, dovendo tutelare situazioni giuridicamente rilevanti, abbia presentato istanza di consultazione.

Pertanto, in merito all'esercizio del diritto d'accesso ai documenti conservati da Marche DigiP, questo si limita a fornire all'Ente produttore, su precisa richiesta di quest'ultimo e senza che su di esso debba gravare alcun particolare onere, il documento informatico conservato, qualora per un qualsiasi motivo l'Ente produttore stesso abbia deciso di non acquisirlo direttamente mediante le modalità delineate ai paragrafi 4.1

Permane in carico allo stesso Ente produttore sia la responsabilità di valutare la fondatezza giuridica della domanda di accesso, sia l'onere di far pervenire il documento (o sua eventuale copia cartacea conforme) al soggetto richiedente la consultazione.

5. Ente produttore

5.1. Strutture versanti e Parametri per versamento

Le strutture cui afferisce la documentazione versata per la conservazione sono elencate in tabella.

Denominazione	Descrizione
[Denominazione della struttura]	Codice dell'Area Organizzativa Omogenea pubblicato nell'Indice delle pubbliche amministrazioni (http://www.indicepa.gov.it/)

5.1.1. Struttura: [denominazione struttura]

Descrizione sintetica della struttura, con l'indicazione degli strumenti di gestione documentale utilizzati.

5.2. Sistemi informatici

In tabella è riportato il sistema informatico utilizzato dall'Ente produttore per la produzione e gestione delle unità documentarie oggetto di conservazione digitale. Tale sistema, che nel contempo svolge il ruolo di applicativo versante, è definito nel sistema DigiP come utente con abilitazioni specifiche a chiamare i web service.

Sistema informatico	Versione e produttore	Tipologie documentali gestite
Es.: PALEO	[Versione dell'applicativo e denominazione del produttore]	Indicare quali tipologie di unità documentarie (vedi paragrafi 6.x) sono gestite dal sistema informatico

5.2.1. Sistema informatico [es.: PALEO]

Descrizione del sistema informatico con indicazione dell'architettura generale di funzionamento (web server, application server, database, file system, EDMS/ERMS, ecc.) con particolare riferimento alle modalità di memorizzazione e conservazione dei documenti e dei relativi metadati, nonché alle modalità di interfacciamento con il Sistema di conservazione.

6. Unità documentarie

Le unità documentarie versate in conservazione sono strutturate secondo lo schema descritto nelle Specifiche, che ne prevede l'articolazione in documenti (documento principale ed eventuali allegati, annessi, annotazioni) e componenti (file).

L'elenco delle tipologie di unità documentarie versate in conservazione è il seguente:

Tipologia unità documentaria	Struttura	Paragrafo
Denominazione unità documentaria		
Denominazione unità documentaria		

6.1. Tipologia unità documentaria 1

Documento	Tipologia Documento	Descrizione
Documento principale		
Allegati		
Annessi		
Annotazioni		

6.1.1. Dati per il versamento della [Tipologia UD 1]

La denominazione precisa delle chiavi, il formato dei valori, la loro struttura e tutte le informazioni tecniche di dettaglio sono indicati nelle Specifiche. In questa sede sono indicate la descrizione dei valori che possono assumere i metadati e i parametri nella chiamata dei servizi di versamento e, dove necessario, le logiche e i criteri utilizzati per la loro individuazione.

Inoltre l'obbligatorietà del metadato è indicata in grassetto con il valore "**SI**" quando è richiesta dall'interfaccia di versamento (vedi Specifiche) e in formato normale con il valore "SI" quando invece è definita in accordo tra Marche DigiP e l'Ente produttore per l'UD trattata.

6.1.1.1. Intestazione per la [Tipologia UD 1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
Versione	1.3	Versione dei web service di versamento	**SI**

Ambiente	MARCHE DIGIP MARCHE DIGIP_PRE MARCHE DIGIP_TEST	Ambiente assegnato da Marche DigiP per il versamento (in produzione il valore è MARCHE DIGIP, gli altri sono utilizzati nelle varie fasi in cui si articolano i test).	**SI**
Ente	Token	Denominazione dell'Ente produttore versante	**SI**
Struttura	Token	Codice AOO registrato nell'Indice PA. Se non è stata specificata alcuna AOO nell'Indice PA, riportare il codice IPA dell'Amministrazione	**SI**
UserID	PALEO_[…]	Utente versante, composto dal sistema descritto al paragrafo 5.2.1 da un codice identificante la tipologia di ente (C per Comune, P per Provincia, UM per Unione Montana) e dal nominativo dell'Ente (Es.: PALEO_C_ROCCASCURA)	**SI**

6.1.1.2. Identificazione univoca della [Tipologia UD 1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
Numero	Numero	Descrivere l'identificativo progressivo assegnato all'UD nell'ambito del Tipo Registro, soprattutto in riferimento all'identificazione dell'UD.	**SI**
Anno	Numero intero	Anno solare di riferimento con formato aaaa.	**SI**
TipoRegistro	Indicare il valore	Denominazione del registro nell'ambito del quale è registrata l'UD.	**SI**
TipologiaUnitaDocumentaria	Indicare il valore	Denominazione della tipologia dell'unità documentaria.	**SI**

6.1.1.3. Profilo archivistico della [Tipologia UD 1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
FascicoloPrincipale	Classifica Identificativo Oggetto	**Classifica**: indice di classificazione assegnato all'unità documentaria. I livelli sono tra loro separati da punto. Es: 1.2.3. **Identificativo**: stringa composta da Codice Classifica/Anno di Riferimento/Numero Progressivo. **Oggetto**: oggetto del fascicolo.	

Sottofascicolo (principale)	Identificativo Oggetto	**Identificativo**: stringa composta da Codice Classifica/Anno di Riferimento/Numero Progressivo. **Oggetto**: oggetto del sottofascicolo.	
FascicoloSecondario	Classifica Identificativo Oggetto	**Classifica**: classifica secondaria assegnata all'UD. I livelli sono tra loro separati da punto. Es: 1.2.3. **Identificativo**: stringa composta da Codice Classifica/Anno di Riferimento/Numero Progressivo. **Oggetto**: oggetto del fascicolo.	
Sottofascicolo (secondario)	Identificativo Oggetto	**Identificativo**: stringa composta da Codice Classifica/Anno di Riferimento/Numero Progressivo. **Oggetto**: oggetto del sottofascicolo.	

6.1.1.4. Profilo della [Tipologia UD 1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
Oggetto	Stringa	Descrivere (se necessario) cosa rappresenta l'Oggetto dell'UD.	
Data	Campo data	Descrivere cosa rappresenta la data dell'UD. Essa sarà espressa in formato aaaa/mm/gg.	
Cartaceo	false/true	Serve per indicare se l'originale dell'UD versata è in formato cartaceo o meno.	

6.1.1.5. Composizione della [Tipologia UD 1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
NumeroAllegati	Indicare il numero minimo/massimo (se rilevabile)	Indica il numero e la denominazione degli allegati tipizzati.	
NumeroAnnessi	Indicare il numero minimo/massimo (se rilevabile)	Indica il numero e la denominazione degli annessi tipizzati.	
NumeroAnnotazioni	Indicare il numero minimo/massimo (se rilevabile)	Indica il numero e la denominazione delle annotazioni tipizzate.	

6.1.1.6. Documento principale

6.1.1.6.1. Metadati di identificazione del documento principale di [UD1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
IDDocumento	Stringa alfanumerica	Identificativo assegnato dall'applicativo (ad es.: da PALEO) al documento principale, al fine di identificarlo in maniera univoca all'interno dello stesso applicativo versante.	**SI**

TipoDocumento	Indicare il valore che può assumere	Descrizione della tipologia documentaria. Il valore di tale metadato può anche coincidere con il valore assegnato al metadato TipologiaUnitaDocumentaria.	**SI**
TipoStruttura	Indicare il valore che può assumere	Descrive il tipo di struttura che caratterizza la tipologia di documento principale.	**SI**

6.1.1.6.2. Profilo del documento principale di [UD1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
Descrizione	Stringa	Descrivere cosa si intende per Descrizione.	
Autore	Stringa	Descrivere cosa si intende per Autore.	

6.1.1.6.3. Metadati specifici del documento principale di [UD1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
Denominazione chiave	Indicare il formato e/o gli eventuali valori che può assumere.	Descrivere il metadato.	

6.1.1.6.4. Componenti del documento principale di [UD1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
ID	Numero intero	Metadato utile al ricongiungimento della componente versata con il livello di appartenenza.	**SI**
OrdinePresentazione	Numero intero	Metadato che indica l'ordine di successione della singola componente versata rispetto alla struttura originale.	**SI**
TipoComponente	CONTENUTO (default)	Metadato che indica la tipologia di appartenenza della componente versata.	**SI**
TipoSupportoComponente	FILE (default)/METADATI	Metadato che indica il tipo di supporto della componente versata. Indicare i casi in cui è prevista la presenza di tipi supporto METADATI.	**SI**
NomeComponente	Stringa alfanumerica	Descrive come viene definito il nome del file, se viene creato dall'utente o generato dal sistema in base ad una specifica sintassi.	**SI**

FormatoFileVersato	Indicare quali sono i formati possibili del file (o rinviare al paragrafo 8 se sono possibili tutti quelli previsti)	Metadato che indica il formato del file versato.	**SI**
HashVersato		Indicare quale algoritmo di hash è utilizzato e con quale codifica è versato.	
IDComponenteVersato	Stringa alfanumerica	Metadato che descrive come è individuato il riferimento univoco del file nel sistema dell'ente produttore.	
UtilizzoDataFirmaPerRifTemp	false	Il sistema di conservazione utilizzerà la data ed ora di versamento per le verifiche sulla firma.	

6.1.1.7. Allegati/Annessi/Annotazioni della [Tipologia UD 1]

NB: In base alla complessità della struttura e della composizione dell'UD trattata, questa sezione può essere unica e descrivere al suo interno tutti gli allegati/annessi/annotazioni possibili per la tipologia di UD trattata, altrimenti annessi ed annotazioni possono essere descritti in ulteriori sezioni che replicano la struttura di questa (es: 6.1.1.10 Annessi; 6.1.1.11 Annotazioni, ecc.).

6.1.1.7.1. Metadati di identificazione Allegato/Annesso/Annotazione di [UD 1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
IDDocumento	Stringa alfanumerica	Identificativo assegnato dall'applicativo PALEO al documento principale, al fine di identificarlo in maniera univoca all'interno dello stesso applicativo versante.	**SI**
TipoDocumento	Indicare il valore che può assumere	Descrizione della tipologia documentaria. Il valore di tale metadato può anche coincidere con il valore assegnato al metadato TipologiaUnitaDocumentaria.	**SI**
TipoStruttura	Indicare il valore che può assumere	Descrive il tipo di struttura che caratterizza la tipologia di documento principale.	**SI**

6.1.1.7.2. Profilo dell'Allegato/Annesso/Annotazione di [UD1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
Descrizione	Stringa	Descrivere cosa si intende per Descrizione.	
Autore	Stringa	Descrivere cosa si intende per Autore.	

6.1.1.7.3. Metadati specifici Allegato/Annesso/Annotazione di [UD 1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
Denominazione chiave	Indicare il formato e/o gli eventuali valori che può assumere.	Descrivere il metadato.	

6.1.1.7.4. Componenti Allegato/Annesso/Annotazione di [UD 1]

CHIAVE	VALORE	DESCRIZIONE	OBBLIGATORIO
ID	Numero intero	Metadato utile al ricongiungimento della componente versata con il livello di appartenenza.	**SI**
OrdinePresentazione	Numero intero	Metadato che indica l'ordine di successione della singola componente versata rispetto alla struttura originale.	**SI**
TipoComponente	CONTENUTO (default)	Metadato che indica la tipologia di appartenenza della componente versata.	**SI**
TipoSupportoComponente	FILE (default)/METADATI	Metadato che indica il tipo di supporto della componente versata. Indicare i casi in cui è prevista la presenza di tipi supporto METADATI.	**SI**
NomeComponente	Stringa alfanumerica	Metadato che indica il nome della componente versata dunque, nel caso dell'Ente produttore in oggetto, il nome del file versato.	**SI**
FormatoFileVersato	Indicare quali sono i formati possibili del file (o rinviare al paragrafo 8 se sono possibili tutti quelli previsti)	Metadato che indica il formato del file versato.	**SI**
IDComponenteVersato	Stringa alfanumerica	Metadato che descrive come è individuato il riferimento univoco del file nel sistema dell'ente produttore.	
UtilizzoDataFirmaPerRifTemp	false	Il sistema di conservazione utilizzerà la data ed ora di versamento per le verifiche sulla firma.	

7. Modalità di svolgimento del servizio di conservazione

Il processo di conservazione avviene secondo le modalità descritte nel Manuale di conservazione, modalità che si possono sintetizzare come segue:

1. il Produttore trasmette il SIP nei modi definiti dall'accordo formale (memorizzato nel Sistema sotto forma di configurazione specifica del Produttore), in particolare il Produttore può scegliere se utilizzare un flusso di deposito all'interno di una zona di memorizzazione condivisa (file system remoto, FTP, etc..) oppure un servizio REST di versamento sincrono;
2. il Sistema rileva un nuovo trasferimento e
    a. trasferisce il SIP in una zona di lavoro temporanea, locale al servizio di ricezione, eventualmente decomprimendolo se compresso;
    b. trasferisce il SIP ad Archival Storage nella sezione corrispondente e ne notifica la ricezione al Produttore aggiungendolo alla lista dei SIP ricevuti;
    c. Il SIP ricevuto viene messo in coda per la validazione di qualità;
3. il Produttore può consultare la lista dei SIP ricevuti dal Sistema presente nell'area di deposito condivisa e verificarla;
4. il Sistema processa la coda dei SIP per l'analisi;
5. il Sistema recupera le Regole da applicare per la validazione in base al Produttore e alla tipologia documentale;
6. il Sistema valida il trasferimento del SIP applicando le regole di validazione attive selezionate al passo precedente;
7. i dati di validazione vengono raccolti temporaneamente nella zona di lavoro per i passi successivi;
8. il modulo di ricezione mette a disposizione del Produttore nella zona di deposito condivisa, coerentemente alla validazione, una ricevuta di presa in carico opzionalmente firmata (Rapporto di Versamento) o un esito negativo motivato;
9. in caso di successo il Sistema abilita il SIP per il passo successivo;
10. il Sistema genera un AIP a partire dalle informazioni presenti nel KIP, trasformandolo nel formato di IP scelto (attualmente lo standard ISO SINCRO) ;
11. il Sistema abilita il KIP al passo di generazione PDI;
12. il Sistema contrassegna l'IP come conforme agli accordi negoziati di (formato di) versamento.

7.1. Criteri per la creazione del pacchetto AIP

La creazione del pacchetto di archiviazione (AIP) avviene secondo le seguenti modalità:

1. il Sistema riceve la posizione temporanea nella zona di lavoro del SIP validato e spacchettato;
2. il Sistema estrae il contenuto informativo dal SIP e lo inserisce in una struttura di IP in

formato interno universale (Kernel Information Package – KIP, per la documentazione del formato vedi le note in Appendice);

3. il Sistema estrae le informazioni descrittive di conservazione (PDI) dal SIP e le aggiunge al KIP;

4. il Sistema integra eventualmente i PDI estratti con modifiche o inserimenti nel KIP;

5. il Sistema recupera le politiche e gli standard di archiviazione;

6. il Sistema, sulla base delle politiche e degli standard, esegue le necessarie conversioni, trasformazioni, riorganizzazioni sul SIP corrente e ne salva temporaneamente i risultati nel KIP;

7. il Sistema genera un AIP a partire dalle informazioni presenti nel KIP, trasformandolo nel formato di IP scelto (attualmente lo standard ISO SINCRO)

8. il Sistema abilita il KIP al passo di generazione PDI;

9. il Sistema contrassegna l'IP come conforme agli accordi negoziati di (formato di) versamento.

8. Formati file

Nella tabella che segue sono individuati i formati dei file relativi ai componenti delle unità documentarie inviate in conservazione:

Formato file	Descrizione

Elenco degli allegati al presente Disciplinare:

ALLEGATO A - Scheda tecnica connettività per il servizio di conservazione

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 13

MANUALE DEI PROCESSI

PER LA CONSERVAZIONE DIGITALE

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

Manuale di conservazione

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	05/10/2015	Roberta Rosatone	*Supporto Archivistico*
Verifica	09/10/2015	Davide Madonnini	*Supporto Archivistico Enti*
Approvazione			

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Vers. 1.0 / Rev. 01	10/10/2015	Prima versione	
Vers. 1.0 / Rev. 02	13/10/2015	Revisione descrizione responsabili	
Vers. 1.0 / Rev. 03	20/10/2015	Revisione descrizione componenti fisiche	
Vers. 1.0 / Rev. 04	14/01/2016	Revisione per osservazioni AGID	
Vers. 1.0 / Rev. 05	16/02/2016	Revisione per osservazioni AGID	
Vers. 1.0 / Rev. 06	03/03/2016	Revisione per osservazioni AGID	

INDICE DEL DOCUMENTO

INDICE DELLE FIGURE

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente manuale descrive il sistema di conservazione dei documenti informatici realizzato sulla base delle Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis, 23 -ter, comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 di cui al DPCM 3 dicembre 2013.

Esso definisce, in particolare:

- i soggetti coinvolti nel processo di conservazione;
- gli obblighi e le responsabilità;
- l'oggetto della conservazione;
- il processo di conservazione;
- le modalità attuate per garantire la conservazione permanente dei documenti;
- le modalità per ottenere l'esibizione di un documento conservato.

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Aggregazione documentale informatica: aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.

Archivio informatico: archivi di documenti memorizzati con procedure informatiche.

Conservatore accreditato: soggetto, pubblico o privato che svolge attività di conservazione dei documenti informatici e certificazione dei relativi processi anche per conto di terzi, che hanno ottenuto l'accreditamento presso l'Agenzia per l'Italia Digitale, come da art. 44bis del vigente CAD.

Disciplinare Tecnico: documento redatto da ogni Produttore, che definisce le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei Documenti informatici.

Dispositivo sicuro per la creazione di una firma: dispositivi, che utilizzano procedure per la generazione delle firme come da art. 44bis del vigente CAD.

Documento: tutti i libri, le carte, le mappe, le fotografie o gli altri materiali documentari, indipendentemente dalla forma o dalle loro caratteristiche, prodotti o ricevuti da ogni pubblica o privata istituzione, nello svolgimento delle sue funzioni istituzionali o in connessione con la conduzione dei suoi affari particolari, e conservati, o degni di essere conservati, dalla stessa istituzione o dal suo successore, come testimonianza delle sue funzioni, della sua politica, delle decisioni, procedure, operazioni, o altre attività, o a causa del valore informativo dei dati ivi contenuti.

Documento conservato: documento sottoposto al processo di conservazione.

Documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Esibizione: operazione che consente di visualizzare un documento conservato e di ottenerne copia.

Evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.

Fascicolo informatico: aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.

Firma detached: firma digitale che è tenuta separata dai dati firmati, a differenza della firma digitale completa che è inglobata nel file stesso. Ciò permette di poter lavorare con il file originale senza dover aprire un file firmato digitalmente, ma ovviamente una qualsiasi modifica al file originale interrompe lo stretto legame con la firma, nel senso che un file differente non possiederà

la medesima firma (Fonte: Wikipedia).

Firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (CAD).

Firma elettronica qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (CAD).

Firma digitale: il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (DPR 445/2000).

Funzione di hash: una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.

Impronta: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.

Gestione informatica dei documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici (CAD).

Identificativo univoco universale (UUID): universally unique identifier o UUID è un identificativo standard ed è documentato come parte dell'ISO/IEC 11578:1996 "Information technology – Open Systems Interconnection – Remote Procedure Call (RPC)" e più recentemente in ITU-T Rec. X.667 | ISO/IEC 9834-8:2005.

Indice del Pacchetto di archiviazione (IPdA): l'evidenza informatica associata ad ogni Pacchetto di archiviazione, contenente un insieme di informazioni articolate in uno Schema XML (UNISINCRO).

Marca temporale: il riferimento temporale che consente la validazione temporale.

Metadati: elementi che descrivono il contesto, il contenuto e la struttura dei documenti e la loro gestione nel tempo (ISO 15489).

OAIS: ISO 14721:2012: Space data and information transfer systems -- Open archival information system - Reference model, OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.

Pacchetto di versamento (SIP): il pacchetto informativo inviato ad un OAIS dal Produttore.

Pacchetto di archiviazione (AIP): il pacchetto informativo conservato in un OAIS..

Pacchetto di distribuzione (DIP): il pacchetto informativo inviato ad un Utente da un OAIS.

Pacchetto informativo (IP): contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.

Rapporto di versamento: documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

Riferimento temporale: informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (D.P.C.M. 30 marzo 2009).

Scarto: operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti per i quali non sussista l'obbligo di conservazione e che siano stati considerati irrilevanti dal punto di vista amministrativa e della ricerca.

Soggetto produttore: persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.

Validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi (CAD).

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 NORMATIVA

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- Deliberazione della Giunta Regionale n. 1039 del 30 luglio 2008 - Modalità Attuative del Programma Operativo (MAPO) della Regione Marche - POR-FESR - Competitività regionale e occupazione 2007-2013";
- Deliberazione del Consiglio Regionale n. 95 del 15 luglio del 2008 - Piano Telematico Regionale per lo sviluppo della banda larga ed il superamento del digital divide;

- Deliberazione della Giunta Regionale 1759 del 1 dicembre 2008 - Avvio della sperimentazione e dell'analisi finalizzata alla definizione del sistema di conservazione dei documenti cartacei e digitali della Regione Marche;
- Deliberazione della Giunta Regionale n. 252 del 23 febbraio 2009 - Programma Attuativo Regionale PAR FAS 2007-2013;
- Deliberazione della Giunta Regionale n. 1925 del 17 novembre 2009 - Partecipazione al partenariato interregionale con le Regioni Liguria, Piemonte, Lombardia, Emilia Romagna, Marche, Abruzzo, Campania, Puglia, Sicilia e la Provincia Autonoma di Trento ed il CISIS per la cooperazione nella realizzazione del progetto interregionale "PRODE-PROGETTO Dematerializzazione;
- Deliberazione della Giunta Regionale n. 167 del 14 febbraio 2010 - Definizione delle modalità operative di attuazione del polo di conservazione digitale della Regione Marche;
- Decreto della P.F. Sistemi informativi e telematici n. 213/INF_02 del 30 novembre 2010 - Procedura aperta per l'acquisizione di beni e servizi per la creazione e gestione del Polo regionale di conservazione degli archivi digitale;
- Decreto della P.F. Sistemi informativi e telematici n. 119/INF del 22 agosto 2012 – Aggiudicazione della procedura aperta e costruzione dell'infrastruttura organizzativa, tecnologica e giuridica per l'avvio dei servizi di archiviazione digitale a norma;
- Deliberazione della Giunta Regionale n. 265 del 10 marzo 2014 - Avvio dei servizi del Polo di conservazione digitale Marche DigiP;

Torna al sommario

3.2 STANDARD

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and

Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- ISO 15489 Record management – Code of practice

Torna al sommario

4. RUOLI E RESPONSABILITÀ

Il DPCM 3 dicembre 2013 individua, all'art. 6, i seguenti ruoli: Produttore, Utente e Responsabile della conservazione.
Il Produttore, nelle PA identificato con la figura del responsabile della gestione documentale, produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.
L'utente è colui che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di suo interesse.
Il Responsabile della conservazione, è il soggetto responsabile dell'insieme delle attività elencate nell'articolo 7, comma 1 delle regole tecniche del sistema di conservazione. Il Responsabile della conservazione può affidare le attività definite previste dall'art. 7 del DPCM 3 Dicembre 2013 al Responsabile del servizio di conservazione.
Nel seguito è esplicitato l'assetto dei ruoli e delle responsabilità all'interno del Polo DigiP.

Ruolo	Nominativo	Attività associate al ruolo	Note
Responsabile del servizio di conservazione	Serenella Carota	- Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - Corretta erogazione del servizio di conservazione all'ente produttore; - Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015
Responsabile della funzione archivistica di conservazione	Mauro Ercoli	- Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015

		- Collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	
Responsabile del trattamento dei dati	Massimo Trojani	- Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015
Responsabile della sicurezza dei sistemi per la conservazione	Maria Laura Maggiulli	- Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - Segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015
Responsabile dei sistemi informativi per la conservazione	Cinzia Amici	- Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; - Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; - Segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; - Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; - Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Cinzia Amici	- Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; - Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; - Monitoraggio degli SLA relativi alla	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo

		manutenzione del sistema di conservazione; - Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; - Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	addendum contrattuale del 22/12/2015

Torna al sommario

4.1 PUBBLICO UFFICIALE

Il ruolo di Pubblico Ufficiale è svolto da personale di Regione Marche appositamente designato.
Il ruolo di Pubblico Ufficiale, per i casi in cui è previsto l'intervento di soggetto diverso della stessa amministrazione, sarà svolto da altro dirigente all'uopo individuato o da altro soggetto da quest'ultimo designato.

Torna al sommario

4.2 CERTIFICATION AUTHORITY

I certificarti di firma digitale utilizzati nel processo di conservazione sono forniti da Actalis S.p.A.

Torna al sommario

4.3 SOPRINTENDENZA ARCHIVISTICA PER LE MARCHE

Esercita funzioni di tutela e vigilanza sugli archivi degli enti pubblici territoriali e non e di enti privati dichiarati di interesse storico particolarmente importante (ai sensi dell'art. 4 e dell'art. 18 del D.lgs. 22 gen. 2004, n. 42 Codice dei beni culturali e del paesaggio e successivi aggiornamenti), autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del D.Lgs 42/2004.

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 ORGANIGRAMMA

Il polo archivistico DigiP svolge per conto degli enti convenzionati il servizio di conservazione dei documenti e degli archivi informatici, con la finalità principale di garantirne la validità giuridica, attivando i trattamenti previsti dalla normativa in vigore. Allo scopo di garantire tale servizio il Polo si avvale di un sistema applicativo e di un'apposita organizzazione con personale altamente qualificato e del supporto di esperti esterni di comprovata esperienza in materia, dotati di competenze specializzate.

Figura 1 – Organigramma

Torna al sommario

5.2 STRUTTURE ORGANIZZATIVE

A supporto della struttura organizzativa indicata precedentemente il modello organizzativo sotteso al Polo Regione Marche DigiP prevede l'interazione dei seguenti soggetti:

- **Ente produttore**: produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di. Il rapporto tra soggetto produttore e Polo Marche DigiP è disciplinato da specifici contratti di servizio; può richiedere i servizi di consulenza offerti dalla Unità di Gestione del Polo per la definizione delle politiche di dematerializzazione e conservazione.

- **Comitato Regionale Utilizzatori (CRU)**: è un comitato inter-ente formato dalla Regione Marche e da altri enti del territorio rappresentativi delle diverse tipologie di soggetti che interagiscono con il Polo Marche DigiP; collabora alla valutazione dei livelli qualitativi dei servizi offerti (*customer satisfaction*), all'identificazione delle esigenze degli utilizzatori e alla formulazione di eventuali richieste di servizio e/o proposte di miglioramento.

- **Comitato Scientifico (CS)**: definisce gli indicatori e gli strumenti per assicurare la qualità dei servizi erogati; approva la documentazione elaborata dall' Unità di Progettazione, il piano di audit e monitoraggio; assicura il monitoraggio della evoluzione tecnologica, normativa e degli standard fornendo il know how per l'aggiornamento del modello conservativo e tecnologico.

- **Unità di Progettazione (UP)**: è formata da figure professionali che dispongono delle necessarie competenze giuridiche, archivistiche, informatiche e da referenti di dominio nelle aree tematiche per le quali si registra la maggiore produzione di documenti informatici (salute, servizi a cittadini/imprese, gestione delle risorse umane, strumentali e materiali, atti amministrativi). All'Unità di Progettazione è demandata:
    - l'elaborazione delle procedure e i processi che costituiscono il modello conservativo digitale del Polo;
    - la definizione ed implementazione del piano self-audit, di monitoraggio e di documentazione dell'attività;
    - la definizione e progettazione e pianificazione dell'aggiornamento tecnologico e professionale del personale del Polo Marche DigiP;
    - l'elaborazione degli schemi di contratto di servizio;
    - la supervisione e il coordinamento delle attività dell'Unità di Gestione e dell'Unità Data Center.

- **Unità di Gestione (UG)**: implementa e gestisce il modello conservativo digitale disegnato dall'Unità di Progettazione; rende disponibile un servizio di help desk sulle tematiche di archiviazione e conservazione, interagendo con gli enti produttori.

- **Unità Data Center**: è formata da figure professionali idonee che svolgono le attività di natura tecnologica assicurando il corretto funzionamento del Polo Marche DigiP con modalità e tempi definiti dai responsabili del sistema.

Per rispondere altresì agli orientamenti governativi nazionali ed europei in materia di Agenda digitale e nel contempo dare piena operatività ai servizi di DigiP, è stata istituita la Community network degli enti utilizzatori dei servizi denominata **DigiPCommunity**, ovvero una comunità dinamica di settore che si aggrega secondo un modello a geometria variabile e condivide le informazioni contenute nella knowledge base attenendosi ad ontologie semantiche. Tale community promuove ai fini della conservazione di archivi digitali:

- il trasferimento tecnologico e lo scambio di conoscenza tra i portatori di interesse del sistema;
- la fornitura di strumenti condivisi per superare il limite attuale dei processi di automazione dei procedimenti amministrativi;
- funzioni di promozione sul territorio per creare un potenziale bacino di utenti consapevoli dei reali vantaggi del modello di lavoro a rete che vede DigiP come infrastruttura abilitante.

Il servizio riguarda principalmente, ma non esclusivamente, i documenti sottoscritti con firma digitale, ed ha inizio nel momento in cui il documento entra nel patrimonio documentario dell'ente. Il servizio ha come output primario la restituzione da parte del conservatore di documenti correttamente conservati, principalmente per finalità di esibizione.

Il servizio riguarda i documenti digitali e costitutivi dell'archivio informatico dell'ente (con particolare attenzione per il documenti sottoscritti con firma digitale).
Il servizio fornisce attività finalizzate a garantire un primo consolidamento dei documenti informatici e delle loro aggregazioni per l'eventuale esibizione (soprattutto con riferimento alle categorie individuate in seguito) e per supportare i successivi processi di conservazione nel tempo a fini amministrativi e di ricerca e previe operazioni di selezione e scarto.

L'applicativo dell'ente versante può eseguire il versamento del documento in conservazione (e dei metadati di contesto amministrativo e archivistico) nel momento in cui questo viene acquisito nell'archivio corrente dell'Ente oppure eseguire il versamento in un momento successivo, attraverso un'estrazione dei documenti presenti in archivio (tipicamente con una procedura batch). Il modello si riferisce sia ai documenti che costituiscono l'archivio, quindi sia quelli interni prodotti all'interno dell'ente (mantenuti internamente o spediti a soggetti terzi), sia i documenti ricevuti da soggetti terzi in varie modalità.

La realizzazione del sistema di conservazione è basata sul modello di OAIS e garantisce la conservazione di documenti digitali per conto di più enti e organizzazioni assicurando i più elevati livelli di sicurezza.

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 OGGETTI CONSERVATI

Di seguito vengono elencate le tipologie di documenti per la cui accettazione è attualmente configurato il sistema di conservazione DigiP:

- Documento protocollato
- Documento non protocollato
- Registro giornaliero di protocollo

Il Polo Marche DigiP accetta i formati elencati nell'Allegato n. 2 al DPCM 3/12/2013 e, inoltre, è in grado di gestire, su richiesta del soggetto produttore e previa valutazione e approvazione da parte del Polo Marche DigiP, anche formati non compresi nel suddetto elenco, ma specificati nel manuale di conservazione del soggetto produttore e riportati nel disciplinare tecnico.
Per i file opportunamente elencati nel disciplinare tecnico, che sono trasmessi al sistema di conservazione in un formato diverso da quelli specificati secondo il processo precedentemente descritto sarà garantita esclusivamente la ricerca e il recupero con garanzia dell'integrità binaria.

Per quanto riguarda i metadati si fa riferimento all'Allegato n. 5 del DPCM 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione.
Per quanto riguarda le politiche di conservazione si rimanda alle specificità del contratto definite nel Disciplinare Tecnico.

Torna al sommario

6.2 PACCHETTO DI VERSAMENTO (SIP)

Il Sistema di conservazione DigiP è stato progettato per accogliere Pacchetti di versamento (SIP – Submission Information Package) disegnati principalmente secondo lo standard SINCRO.
Tuttavia il sistema è altamente configurabile e personalizzabile ed è quindi in grado di accogliere qualsiasi tipo di Pacchetto di Versamento, garantendo in tal modo un elevato livello di flessibilità. Questa caratteristica ha permesso fin da subito la compatibilità (sebbene con alcune limitazioni, ad esempio il vincolo di 1 SIP => 1 documento) con il Sistema di conservazione preesistente.
Il SIP è definito da:

- un contenitore, dipendente dal canale trasmissivo scelto, che racchiude i contenuti del pacchetto informativo (es: file in formato zip, HTTP Request di tipo POST ...);
- un file XML, descrittore del contenuto, dei metadati del Produttore e delle eventuali aggregazioni; detto indice può essere validato contro il proprio schema XSD;

- l'insieme dei file elencati nell'indice, con i propri metadati.

Il caricamento di un pacchetto di versamento (SIP) può avvenire in tre diverse modalità, dipendentemente dagli accordi di servizio:

- **Flusso**: i pacchetti SIP, definiti come file .zip, vengono posizionati in una specifica cartella ftp assegnata all'utente (Soggetto Produttore). Il sistema tramite periodici controlli troverà il file e avvierà il processo di versamento.
- **Form web**: l'utente versatore, autenticato ed autorizzato, inserisce tramite apposita form del sistema il testo dell'indice descrittore in una casella di testo e allega i file associati.
- **Interfaccia REST**: l'applicazione versante, autenticata ed autorizzata, trasmette al sistema i pacchetti di versamento utilizzando l'apposita interfaccia webservice REST.

Il Soggetto produttore avrà la possibilità di monitorare in tempo reale la gestione dei Pacchetti di versamento tramite apposito portale al quale potrà accedere con credenziali personali fornite dal Polo. Il portale DigiP permette, infatti, di controllare la Data del versamento, i documenti Ricevuti, i documenti Presi in carico, il Rapporto di versamento e i Pacchetti di Archiviazione. Informazioni, queste, racchiuse in un Registro dei pacchetti che è possibile scaricare in formato excel, che riportano i dettagli dei Pacchetti e dei log. Dal medesimo portale sarà possibile visualizzare anche i Pacchetti di Distribuzione.
Per i dettagli tecnici si rimanda al documento allegato "Manuale di Utilizzo DigiP".

Torna al sommario

6.3 PACCHETTO DI ARCHIVIAZIONE (AIP)

Il sistema di conservazione DigiP è conforme allo standard OAIS ISO 14721:2012 e in particolare per tutto quanto riguarda l'acquisizione dei Pacchetti di Versamento (SIP- Submission Information package) e la loro trasformazione in Pacchetti di archiviazione (AIP - Archival Information Package).

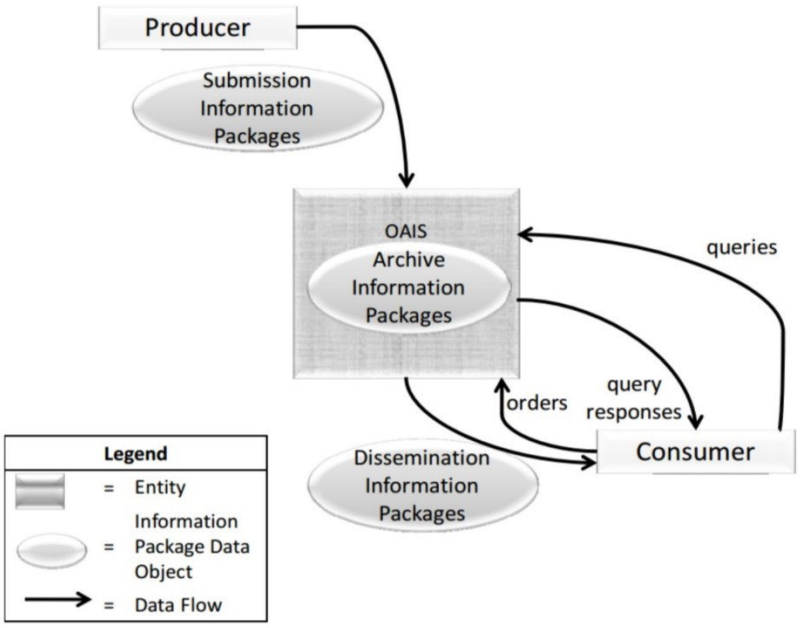


Figura 2 - Modello OAIS

Il sistema di conservazione DigiP individua nella fase di Ingest il momento in cui il SIP conferito dal Soggetto Produttore viene validato e quindi trasformato in AIP. Durante questo processo non banale, i risultati delle validazioni e delle conversioni di formato richieste dagli accordi di servizio e dalle politiche prestabilite vengono raccolti e aggregati in una struttura di IP idonea alla successiva generazione dei corrispondenti Pacchetti di archiviazione. Questa struttura transitoria identificata come KIP – Kernel Information Package - è indipendente dai formati scelti per l'archiviazione. La struttura di questi ultimi segue lo standard SINCRO così come indicato nelle Regole tecniche in materia di conservazione.

Si riporta di seguito la struttura dell'indice del Pacchetto di Archiviazione:

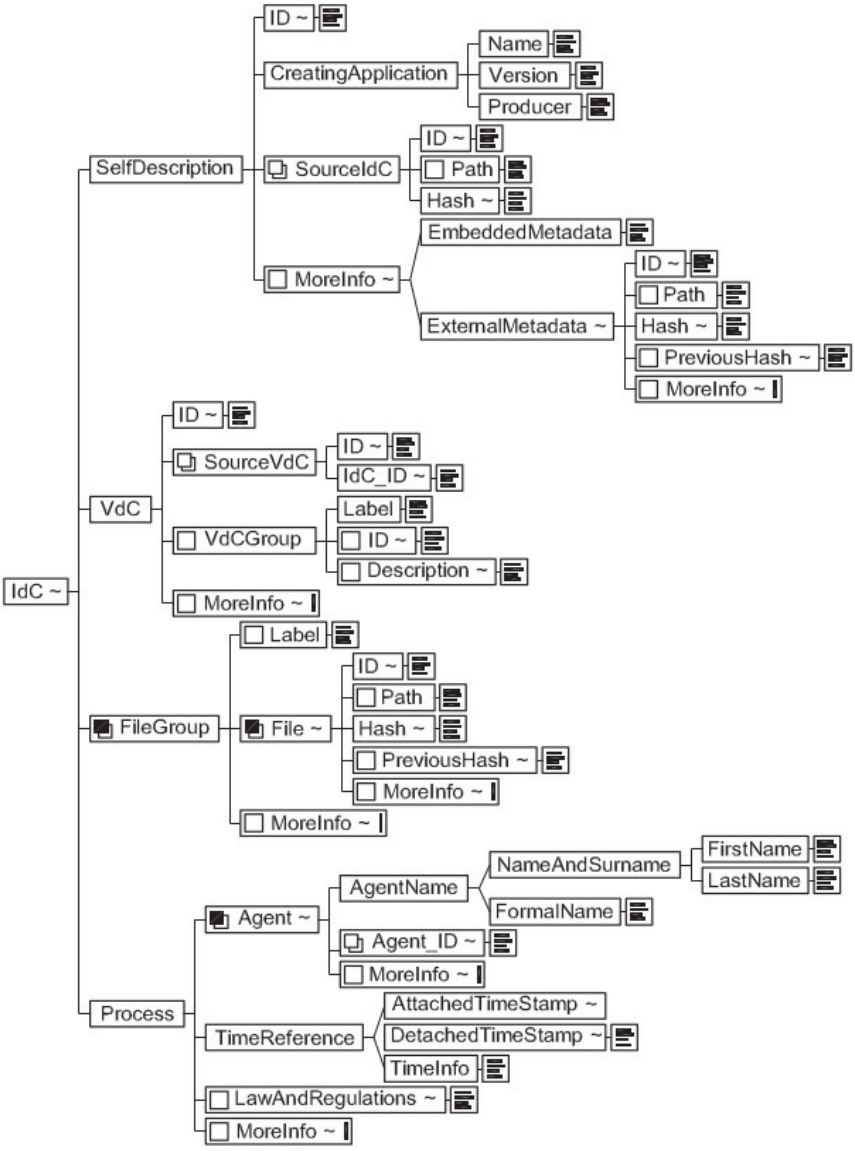


Figura 3 - Indice PdA

Il tag MoreInfo nella struttura SINCRO rappresenta la naturale estensione dello schema e nell'implementazione attuale del Sistema accoglie le tipologie di metadati previste dal modello OAIS che non sono contemplati da SINCRO e tutti i metadati descrittivi specifici del documento aggiunti dal Produttore.

Torna al sommario

6.4 PACCHETTO DI DISTRIBUZIONE (DIP)

I pacchetti di distribuzione (DIP – Dissemination Information Package) vengono creati a seguito

della richiesta da parte di un utente.
Per la formazione di tali pacchetti il sistema DigiP effettua un processo di riconversione dall'AIP al KIP.

La struttura del DIP è conforme allo standard SinCRO, soprattutto per quanto riguarda l'interoperabilità con altri sistemi di conservazione.
Per gli utenti consultatori tale struttura è dipendente anche dagli accordi fra il Polo DigiP ed il produttore dei documenti

Per i dettagli della struttura del DIP e le politiche di distribuzione si rimanda agli allegati "Manuale di Utilizzo DigiP" e "Disciplinare Tecnico".

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

Il sistema di conservazione DigiP, conforme allo standard OAIS è composto dalle seguenti aree funzionali:

1. INGEST, dove si tratta il flusso di documenti dal Produttore al Polo;
2. ARCHIVAL STORAGE, che racchiude le funzionalità di base per garantire la persistenza dei documenti;
3. DATA MANAGEMENT, l'unità di gestione dei metadati e del catalogo di ricerca;
4. ADMINISTRATION, per la gestione del Sistema da parte degli Amministratori;
5. PRESERVATION PLANNING, funzionalità di previsione e monitoraggio degli utenti e degli oggetti del Sistema;
6. ACCESS, dove si gestisce il flusso di richieste di documenti in uscita e la ricerca da parte del Consumatore.

Nel seguito sono descritte le funzioni dei processi di gestione relativi alle suddette aree funzionali.

Torna al sommario

7.1 INGEST

Questa area funzionale è costituita dall'insieme dei processi che sovraintendono l'accettazione delle risorse digitali inviate dai Produttori e della loro preparazione per l'inclusione nel sistema di archiviazione.
I suoi passi procedurali sono descritti nei paragrafi successivi.

Torna al sommario

7.1.1 Trasferimento di SIP

Passi procedurali:

- il Produttore trasmette il SIP nei modi definiti dall'accordo formale (memorizzato nel Sistema sotto forma di configurazione specifica del Produttore), in particolare il Produttore può scegliere se utilizzare un flusso di deposito all'interno di una zona di memorizzazione condivisa (file system remoto, FTP, etc..) oppure un servizio REST di versamento asincrono;
- il Sistema rileva un nuovo trasferimento e
    - verifica la corrispondenza tra il Soggetto Produttore indicato nei metadati del SIP con l'utente versatore che ha conferito il pacchetto stesso e ne lascia traccia tra i log

applicativi. In caso di controllo positivo il SIP viene validato formalmente e in caso di conformità:

- trasferisce il SIP localmente al servizio di ricezione: indipendentemente dal metodo di conferimento scelto dal Produttore, i Pacchetti Informativi vengono depositati in una zona temporanea di lavoro appositamente configurata e segregata sulla base del nome in codice (scelto univocamente all'interno del Sistema) del Produttore;
- trasferisce il SIP ad Archival Storage nella sezione corrispondente e ne notifica la ricezione al Produttore aggiungendolo alla lista dei SIP ricevuti ricevuti (documento csv – registro giornaliero dei sip versati per Soggetto Produttore);
- il SIP ricevuto viene messo in coda per la validazione di qualità (UC 1.2);

o i SIP non attribuibili ad alcun Soggetto Produttore o non conformi vengono spostati in una zona terminale (denominata "cestino") per le valutazioni in merito alle cause di mancata conformità da parte degli Utenti abilitati. Si prevede un periodo configurabile di ritenzione dei SIP cestinati, trascorso il quale saranno eliminati fisicamente dal Sistema senza ulteriori formalità.

- il Produttore può consultare la lista dei SIP ricevuti dal Sistema, lista presente sia nell'area di deposito condivisa (condivisa tra Soggetto Produttore e Polo) che nell'area Ingest accessibile dal sito web, e verificarla.

Quando il trasferimento è completato il Sistema abilita i successivi casi d'uso.

Torna al sommario

7.1.2 Quality Assurance

Passi procedurali:

- il Sistema processa la coda dei SIP ricevuti sottoponendoli all'analisi dei formati dei file in essi contenuti ed alla verifica delle eventuali firme digitali con conseguente recupero dei dati dei firmatari;
- il Sistema recupera le Regole da applicare per la validazione in base al Produttore e alla tipologia documentale;
- il Sistema valida il trasferimento del SIP applicando le regole di validazione attive selezionate al passo precedente utilizzando i risultati delle analisi dei formati e delle verifiche già effettuate;

- i dati derivati dalla validazione confluiranno sia nel Rapporto di versamento, sia tra i metadati del futuro AIP;
- il Sistema emette, a seconda dell'esito della validazione, una ricevuta di presa in carico (validazione positiva) oppure una comunicazione di anomalia (validazione negativa con descrizione delle anomalie) opzionalmente firmata (Rapporto di Versamento, per i contenuti vedi figura) a disposizione del Produttore sia nella zona di deposito condivisa che scaricabile dall'interfaccia web. Prima dell'apposizione eventuale della firma digitale, il Rapporto di versamento è (opzionalmente) protocollato dal Sistema di Protocollo dell'Ente Polo. La segnatura di protocollo così ottenuta rappresenta un valido riferimento temporale opponibile a terzi in quanto il Sistema di Protocollo che lo ha prodotto è il Protocollo Informatico di un ente pubblico. La marcatura temporale ottenuta per tramite del Protocollo viene mantenuta in associazione con il SIP e inclusa tra i metadati del Pacchetto di Archiviazione prima della necessaria apposizione della firma digitale del Conservatore. Il Rapporto di Versamento viene inoltre aggiunto al contenuto informativo del SIP originale. Questa parte del processo di acquisizione garantisce la qualità del trasferimento nei confronti di Terzi.

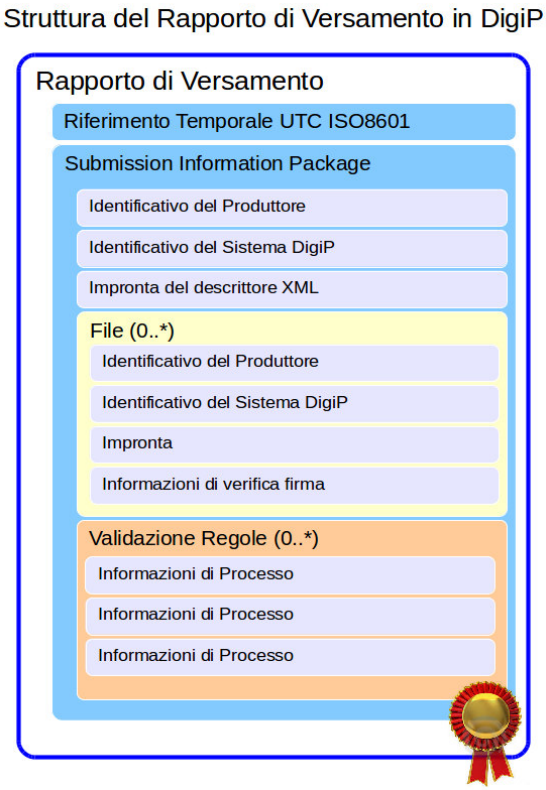


Figura 4 - Struttura RdV

- in caso di successo il Sistema abilita il SIP per il passo successivo.

Torna al sommario

7.1.3 Generazione di AIP

Passi procedurali:

- il Sistema riceve la posizione temporanea nella zona di lavoro del SIP validato e spacchettato;
- il Sistema estrae il contenuto informativo dal SIP e lo inserisce in una struttura di IP in formato interno universale KIP (Kernel Information Package):
    - il Sistema estrae le informazioni descrittive di conservazione (PDI) dal SIP e le aggiunge al KIP;
    - il Sistema integra eventualmente i PDI estratti con modifiche o inserimenti nel KIP;
    - il Sistema recupera le politiche e gli standard di archiviazione;
    - il Sistema, sulla base delle politiche e degli standard, esegue le necessarie conversioni, trasformazioni, riorganizzazioni sul SIP corrente e ne salva temporaneamente i risultati nel KIP;
    - al termine del processo di generazione la documentazione delle operazioni effettuate sul SIP viene inserita nel KIP
- il KIP viene trasformato tramite XSLT nel formato di IP scelto (attualmente lo standard ISO SINCRO), per come è stato progettato il ruolo del KIP tale trasformazione è reversibile;
- il Sistema abilita il KIP al passo di generazione PDI verso Data Management (compilazione del catalogo di ricerca con le chiavi dei metadati);
- in caso di successo complessivo il Sistema contrassegna l'IP come conforme agli accordi negoziati di (formato di) versamento, con il risultato che il Sistema ha generato un AIP a partire dal SIP; l'AIP testé generato viene persistito dall'Archival Storage ed associato ad un identificativo univoco della posizione di memorizzazione;
- eventuali fallimenti occorsi durante il processo sono tracciati nello stato di avanzamento da SIP ad AIP, lasciando all'utente Amministratore la possibilità di ripristinare la situazione ad un punto noto e rilanciare il processo stesso.

Torna al sommario

7.2 ARCHIVAL STORAGE

La funzione gestisce l'immagazzinamento a lungo termine delle risorse digitali affidate al sistema. Si tratta di un'area funzionale non direttamente acceduta dagli Utenti del sistema e pertanto il suo ruolo è accennato sinteticamente di seguito.

Alla richiesta di memorizzazione di un contenuto informativo proveniente dall'area funzionale Ingest, il Sistema seleziona e prepara il corretto dispositivo di memorizzazione recuperando l'informazione dalla configurazione del Soggetto Produttore e si predispone per ricevere l'informazione in streaming. Al termine del trasferimento dello stream di informazioni il Sistema notifica al chiamante la correttezza della procedura comunicando l'identificativo univoco sotto il quale è memorizzato il contenuto informativo.
L'identificativo unico del contenuto informativo memorizzato all'interno di Archival Storage è rappresentato dall'indirizzo univoco composto da:

- un identificativo unico universale che contiene riferimenti al partizionamento ed alla segregazione;
- una gerarchia a otto livelli derivata dal partizionamento di un UUID;
- l'impronta del contenuto informativo.

Il recupero dei contenuti memorizzati all'interno di Archival Storage avviene sempre tramite l'identificativo unico della risorsa.

Completano le funzionalità di memorizzazione e di recupero delle informazioni la funzione amministrativa di controllo degli errori e di calcolo delle statistiche di memorizzazione.

Torna al sommario

7.3 DATA MANAGEMENT

La funzione di Data Management gestisce il database dei metadati (descrittivi e PDI) inclusi nel catalogo di ricerca ed i dati amministrativi e statistici del sistema.
Il suo ruolo all'interno del processo di conservazione è finalizzato al mantenimento di informazioni sul processo stesso, che verranno incluse tra i metadati dell'IP, e all'ottimizzazione (denormalizzazione rispetto al pacchetto di archiviazione) dei percorsi di ricerca mediante chiavi multiple.
La natura dinamica del Data Management permette inoltre di tracciare il log forensico delle attività in corso sull'intera applicazione Polo DigiP e di restituire reportistiche in tempo reale. Il report può essere di due tipologie: generato da una ricerca per metadati (access) o dall'analizzatore pianificato di coerenza e integrità con i dati statistici (numero file, dimensione file…) accessibile da Administration.
Il data management è specifico dell'applicativo e non gestisce i dati rilevanti alla conservazione.

Torna al sommario

7.4 ADMINISTRATION

L'area funzionale Administration raggruppa l'insieme delle funzioni rivolte alla gestione delle configurazioni del Sistema, al monitoraggio, all'interazione con gli utenti, agli accordi di servizio con i produttori ed al mantenimento degli standard di archiviazione definiti.

Torna al sommario

7.4.1 Negoziazione accordo di versamento

Opera sulla base delle politiche di versamento negoziate tra il Produttore ed il Polo Marche DigiP in particolare:

- il Sistema mantiene la configurazione della struttura dei SIP;
- il Sistema mantiene la configurazione dei parametri di interazione tra Soggetto Produttore e l'Applicazione Polo DigiP;
- il Sistema valuta il design del SIP come parte del processo di approvazione del versamento.

Nota: l'ultimo passo è implementato tramite la SandBox nel modulo di Preservation Planning.

Torna al sommario

7.4.2 Monitor della configurazione del Sistema

Si tratta di una funzione di monitoraggio del sistema che richiama funzionalità sviluppate nei rispettivi moduli di competenza, in particolare:

- il Sistema raccoglie informazioni di sistema dal modulo Data Management;
- il Sistema raccoglie statistiche dal modulo Archival Storage;
- il Sistema permette di monitorare le operazioni di sistema;
- il Sistema permette di monitorare l'utilizzo di sistema.

Il sistema archivio viene valutato nelle configurazioni correnti.

Torna al sommario

7.4.3 Definizione di standard e politiche

Il Sistema permette di configurare gli standard e le politiche sulla base delle informazioni ricevute, tra cui:

- Formati

- Documentazione e metadati descrittivi
- Obiettivi della migrazione
- Politiche di gestione della memorizzazione
- Politiche di migrazione
- Politiche di sicurezza
- Politiche di evoluzione del Sistema

Torna al sommario

7.4.4 Visualizzazione degli AIP

Si tratta di una funzionalità di monitoraggio sul processo di conservazione, grazie alla quale l'AIP è reso in formato ispezionabile.

Torna al sommario

7.4.5 Processo di Scarto AIP

Si tratta di una funzione avanzata di gestione del patrimonio informativo già acquisito, prevista dalla normativa. Quando si creano i presupposti l'Amministratore crea un nuovo processo di scarto, specificando gli estremi del documento di autorizzazione allo scarto. A questo punto il processo è in corso e:

- il Sistema identifica gli AIP scartabili in base al massimario di scarto (vedi configurazione della tipologia documentale);
- l'Amministratore seleziona per lo scarto tra gli elementi identificati al passo precedente;
- al termine della selezione (multipla) l'Amministratore lancia il processo (asincrono) di scarto;
- il Contenuto Informativo dell'AIP è rimosso fisicamente dal Sistema, insieme a tutti i SIP e i DIP corrispondenti. Il rapporto prodotto al termine del processo di scarto viene mantenuto nel Sistema ed associato ai metadati degli AIP scartati.

In caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo, secondo quanto disposto dall’art. 21, comma 1, lettera d del Codice dei beni culturali.

Torna al sommario

7.4.6 Migrazione

In ogni momento la funzione di migrazione è attivabile per singolo Produttore: di ogni file di formato obsoleto viene creata una versione in formato migrato che lo sostituisce in una nuova revisione del AIP.

Torna al sommario

7.4.7 Riversamento

Tutti gli AIP sono resi disponibili sotto forma di DIP standard, per essere riversati su un nuovo Sistema di conservazione, senza eliminare alcuna informazione dal Sistema corrente.

Torna al sommario

7.5 PRESERVATION PLANNING

E' l'area funzionale che si occupa della progettazione della strategia di conservazione del sistema e delle sue modifiche a fronte dei cambiamenti tecnologici riguardanti gli oggetti archiviati e del mutamento dei bisogni espressi dalla Comunità di riferimento.

Torna al sommario

7.5.1 Osservazione della Comunità designata

E' una funzionalità di indagine/feedback mediante questionari. Gli attori sono il Sistema Polo Marche DigiP, il Produttore, il Consumatore.
La procedura invia le specifiche di conservazione al modulo funzionale che si occupa di design del packaging e di piani di migrazione; invia reports, avvisi e standard emergenti al modulo funzionale di sviluppo strategie di conservazione.

Torna al sommario

7.5.2 Prototipazione

La funzione è svolta dal componente del sistema denominato SandBox ed è una funzione ad euristica esplorativa. Il risultato della prototipazione è disponibile istantaneamente per essere esportato in ambiente di produzione.

Torna al sommario

7.5.3 Sviluppo di strategie di conservazione

Sono funzioni parzialmente automatizzabili, per le quali si prevede l'uso massivo della SandBox.

Torna al sommario

7.5.4 Sviluppo di standard di conservazione

La funzionalità, appoggiandosi sempre sul componente SandBox, segue il medesimo iter della Prototipazione.

Torna al sommario

7.5.5 Sviluppo di standard di migrazione

E' un insieme di funzioni eterogenee per le quali viene fornito a tecniche "what-if" esplorabili tramite la SandBox durante le fasi di prototipazione e design, sia degli IP che del software di trasformazione/migrazione di standard di formato per l'IP.
La funzionalità mette istantaneamente a disposizione dell'utente amministratore gli artefatti studiati, per l'installazione in ambiente reale di produzione.

Torna al sommario

7.5.6 Sviluppo di Packaging design

E' una funzione basata sulle funzionalità di indagine fornite dalla SandBox e consente di produrre AIP/SIP destinati a implementare l'accordo di versamento.

Torna al sommario

7.6 ACCESS

Attraverso l'area funzionale Access gli utenti del sistema possono ricercare, richiedere ed ottenere i diversi tipi di oggetti informativi conservati dal sistema stesso. Rappresenta inoltre il canale preferenziale per il monitoraggio della Comunità di Riferimento, attraverso il quale vengono somministrati i questionari e forniti i feedback.

Torna al sommario

7.6.1 Generazione di DIP

La funzione, a seguito di una richiesta specifica da parte di un utente, recupera l'AIP ricercato/selezionato e genera un DIP, notificando il completamento del recupero al modulo di

accesso. Durante questo processo non banale i risultati delle conversioni di formato richieste dagli accordi di servizio e dalle politiche prestabilite vengono raccolti e aggregati in una struttura di IP idonea alla successiva generazione dei corrispondenti Pacchetti di Distribuzione.
Questa struttura transitoria identificata come KIP – Kernel Information Package - è indipendente dai formati scelti per la disseminazione e viene gestita in un'apposita area di lavoro dedicata. Il processo di trasformazione da AIP a KIP è la funzione inversa della trasformazione da KIP ad AIP: questo garantisce coerenza e consistenza ai pacchetti destinazione.
La struttura del Pacchetto di Distribuzione segue lo standard SINCRO, così come indicato nelle Regole tecniche in materia di conservazione, per interoperabilità tra Conservatori. Resta comunque possibile configurare una diversa conversione per tutti i casi in cui sia necessario adeguare i Pacchetti di Distribuzione alla Comunità di riferimento.
I Pacchetti così costituiti sono resi disponibili per la fruizione singolarmente via web o attraverso un canale FTP dedicato in via massiva, ma senza precludere la possibilità di accordo di servizio per la fornitura di supporti rimovibili (CD, DVD, BlueRay ...), in alternativa al canale FTP.
E' inoltre possibile prevedere un tempo massimo di ritenzione dei Pacchetti di Distribuzione, tempo oltre il quale i DIP possono essere eliminati dal Sistema.

Torna al sommario

7.7 RICHIESTE DI DUPLICATI E COPIE INFORMATICHE DEI DOCUMENTI CONSERVATI, ATTESTAZIONE DI CONFORMITÀ

Il modulo Access consente agli utenti autorizzati di ottenere una copia (o duplicato, nel caso in cui non siano necessarie conversioni di formato) dei documenti conservati tramite la richiesta di generazione DIP. Al momento non è prevista l'espressa richiesta di attestazione di conformità per i documenti prodotti dalla disseminazione pertanto, ove richiesto, si procederà esternamente al Sistema con la creazione di un supporto (CD, DVD, e-mail …) contenente sia il DIP che l'attestazione richiesta nella forma attualmente ritenuta valida ai fini legali. Il sistema può fornire tutti gli elementi necessari ad evadere simili richieste (ad es.: impronta Hash del DIP, etc.).

Nel caso in cui venga richiesto l'utilizzo di supporti fisici rimovibili per la trasmissione dei pacchetti di distribuzione, il personale incaricato del trasporto dei supporti fisici viene scelto sulla base dei requisiti definiti dal Responsabile del servizio di conservazione.
Si precisa che tali supporti fisici non presentano riferimenti esterni tali da permettere l'identificazione dell'ente produttore, dei dati contenuti e della loro tipologia. Inoltre, il tipo di contenitore individuato per i DIP permette di impostare credenziali crittografiche tali da proteggere i dati in essi contenuti limitatamente alla distribuzione tramite supporti fisici.

Torna al sommario

7.8 PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI

Il Sistema di conservazione DigiP è pienamente conforme al dpcm 3 dicembre 2013 e rispondente all'art. 9 comma 1, lett. h), nel quale viene dichiarato che il sistema di conservazione garantisce "ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione". DigiP, infatti, assicura l'interoperabilità e la trasferibilità sia in fase di acquisizione dei Pacchetti da parte di altro conservatore, sia in fase di trasmissione ad altro soggetto conservatore. DigiP, inoltre, come specificato in precedenza, risponde allo standard UNI 11386:2010 SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

8.1 COMPONENTI LOGICHE

Il processo di conservazione è realizzato tramite il sistema DigiP che si compone dei moduli descritti precedentemente:

- Ingest
- Archival Storage
- Data management
- Administration
- Preservation Planning
- Access

Di seguito lo schema rappresentativo delle aree funzionali di DigiP. Si noti a tale proposito come le aree funzionali di base (Archival Storage e Data Management) corrispondano - nella metafora di un Sistema vivente - ai piedi del Sistema, le aree funzionali responsabili delle operazioni di I/O siano le braccia, l'area di amministrazione identificata dalle funzioni razionali del cervello ed il cuore dell'Archivio – l'area Preservation Planning.

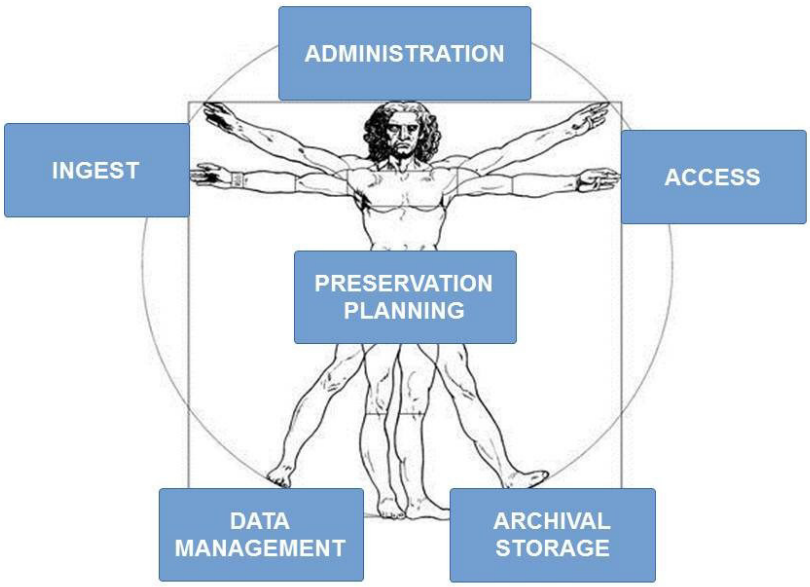


Figura 5 – Aree funzionali DigiP

La soluzione implementata per il Sistema Polo Marche DigiP combina e armonizza i seguenti pattern emergenti:

- Domain driven design component-based (per la parte generale), consente di rilasciare in successione moduli verticali come componenti dell'applicazione garantendo comunque i passi di integrazione con il software prodotto. Il partizionamento del dominio in contesti limitati e aggregati è naturale conseguenza della riorganizzazione delle classi del dominio.
- CQRS-based (per le parti comuni), la diversificazione dei percorsi di lettura e scrittura segue la struttura tipica del modello OAIS e ne rinforza l'implementazione aderente allo standard.

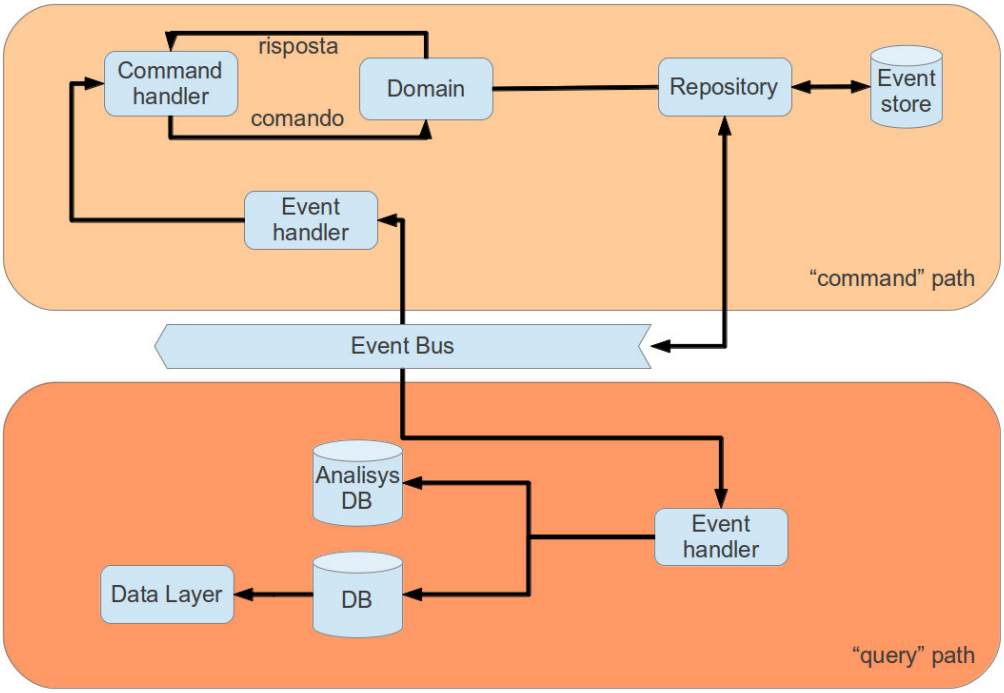


Figura 6 – Schema di principio del Pattern Command Query Responsibility Segregation (CQRS)

- Event Driven (per le parti di comunicazione inter-processo), il disaccoppiamento esteso anche ai processi e la scelta di un modello di comunicazione asincrono aumenta la scalabilità complessiva e riduce l'incidenza del single-point-of-failure.
- Rule-based (per le parti decisionali), la scrittura delle regole di business in una forma comprensibile all'uomo e che mantiene la possibilità di elaborazione automatica e condizionale realizza il requisito di flessibilità e di configurabilità, permettendo allo stesso tempo al Sistema Polo Marche DigiP di essere sempre in linea con le tecnologie e la Comunità di riferimento.

Torna al sommario

8.2 COMPONENTI TECNOLOGICHE

L'immagine che segue schematizza dal punto di vista tecnologico le principali componenti del Sistema di conservazione di DigiP.

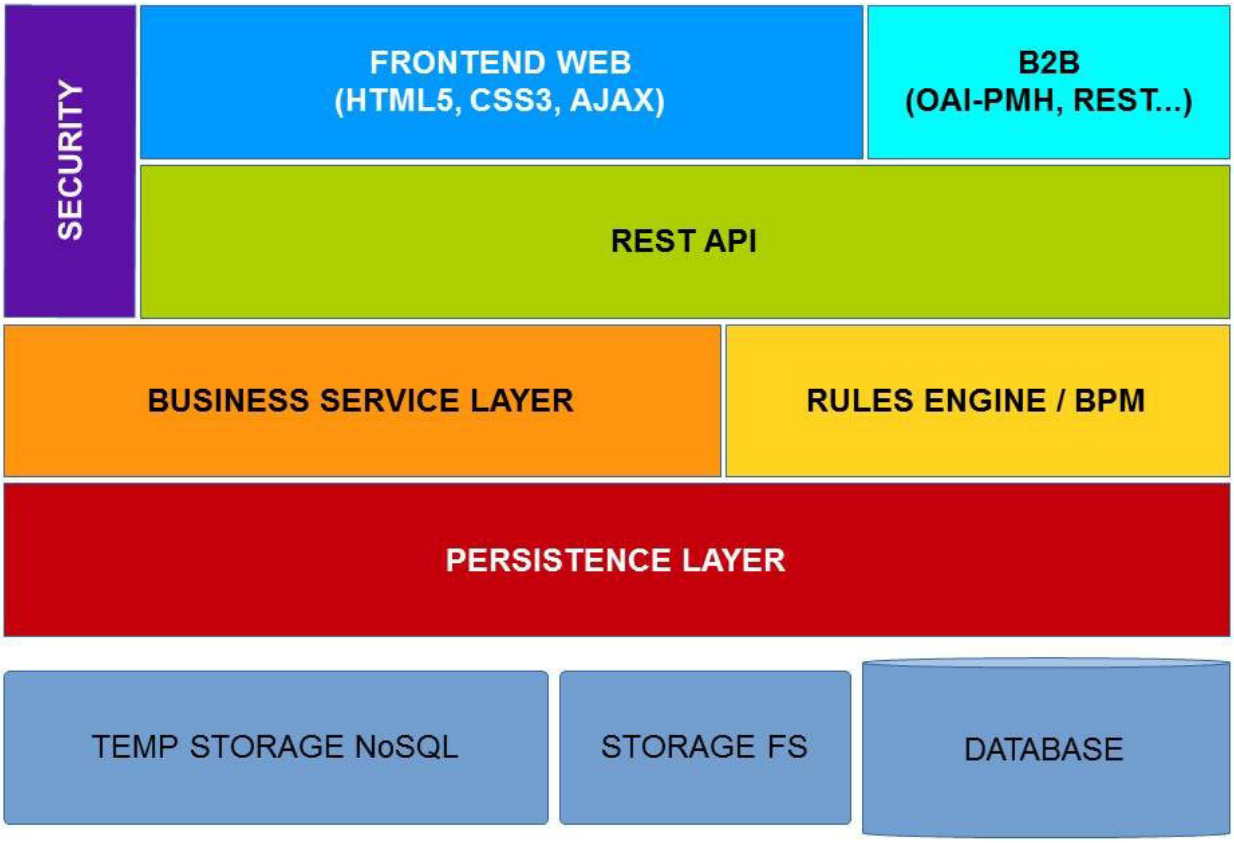


Figura 7 - Componenti tecnologiche e livelli architetturali di DigiP

Trattandosi di una web application verticale, in modo del tutto naturale sono state identificate responsabilità diverse nei diversi strati del software che realizzano le funzionalità elencate in OAIS, quindi è stata definita l'architettura a tre livelli come illustrata in figura:

1. Il livello di presentazione, costituito da:
   - un sistema di sicurezza integrabile a livello di container con il Portale Servizi di Regione Marche (Cohesion);
   - le interfacce web user-oriented realizzate in HTML5, personalizzate con i fogli stile CSS e dinamicizzate mediante l'impiego di Ajax (librerie Dojo);
   - l'interfaccia standard REST per le comunicazioni B2B interoperabili;

- uno strato intermedio di servizi REST, allo scopo di disaccoppiare client e server migliorando la scalabilità, la configurabilità e la robustezza del sistema.

2. Il livello di business logic, costituito da:
   - servizi generali e specializzati, invocati direttamente dai servizi REST per l'implementazione delle funzionalità OAIS;
   - un gestore di processi come implementazione ampiamente configurabile dei workflow e dei controlli a cui sono soggetti i diversi Information Package (IP). La realizzazione prevede l'impiego di un message broker ad alte prestazioni (RabbitMQ), inoltre è previsto un modulo per estendere l'implementazione di workflow personalizzati basati su BPM (modulo workflow).
3. Il livello della persistenza, diversificato tra
   - deposito temporaneo ad alta disponibilità, dove i diversi IP vengono parcheggiati in attesa del completamento dei controlli previsti, capace di accogliere notevoli picchi di versamento parallelo, per il momento identificato da una porzione condivisa del file system del nodo;
   - storage di grande capacità, dove vengono mantenuti inalterati i diversi IP, predisposto per diversificare la memorizzazione in base alla priorità/qualità del supporto;
   - database, ottimizzato per le ricerche di catalogo, dove vengono raccolti e organizzati tutti i metadati.

I componenti software utilizzati sono i seguenti:

- Server: Apache Tomcat;
- Database: PostgreSql;
- Storage FS e Temp Storage NoSql: Jackrabbit (JCR 2.0), file system;
- Persistence layer: realizzato su ORM (Object-Relational Mapping) e precisamente Hibernate 3.6.x;
- Business service layer: realizzato su Spring 3.1.x;
- Rules Engine / BPM: realizzato con l'impiego di RabbitMQ.

Torna al sommario

8.3 COMPONENTI FISICHE

Dal punto di vista tecnico il sistema è progettato e realizzato in maniera da fornire un'elevata continuità di servizio, garantire l'integrità degli oggetti conservati, gestire grandi volumi di dati, mantenere performance stabili indipendentemente dai volumi di attività ed assicurare la riservatezza degli accessi.

Il Sistema è sviluppato con tecnologie di larga diffusione open source con eccezione del software di gestione del mirroring degli storage che è legato alla tecnologia degli storage stessi e del software di backup su nastro.

L'immagine che segue schematizza le principali componenti infrastrutturali del Sistema di conservazione di DigiP e le principali relazioni con altri sistemi interessati dal processo di conservazione descritto nelle sezioni precedenti del presente Manuale.

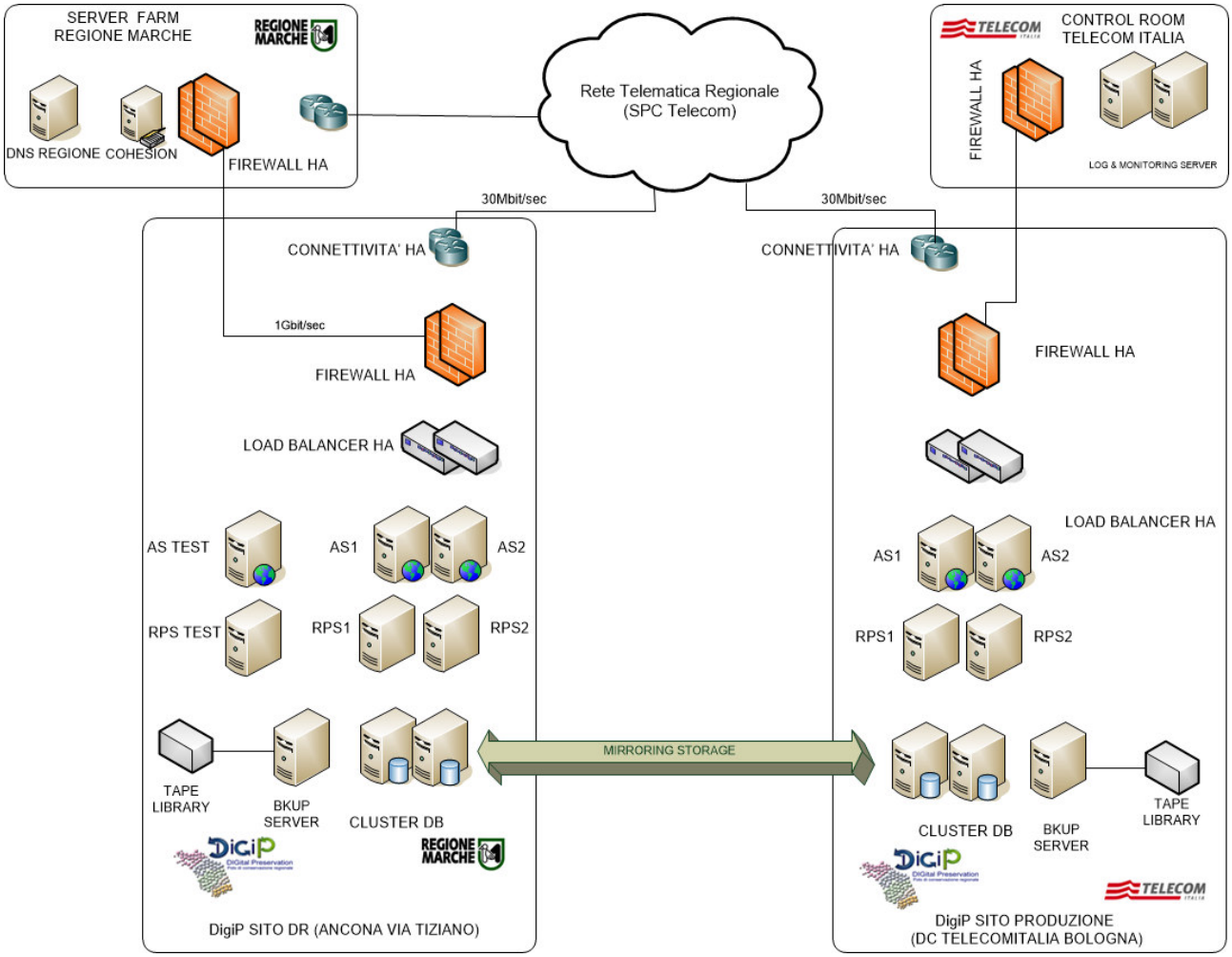


Figura 8 - Componenti fisiche

Il Sistema è realizzato su due siti che distano circa 200 chilometri l'uno dall'altro: un sito primario, (produzione) installato presso il Data Center di Telecom Italia a Bologna, che svolge funzioni di normale operatività e un sito secondario installato presso una sala dedicata nella Server Farm di Regione Marche, che ha lo scopo di subentrare come sito di Disaster Recovery nel caso di caduta irreparabile del sito primario. I due siti sono gestiti dalla Control Room di Telecom Italia.

Entrambi i siti sono interconnessi alla Rete Telematica Regionale della Regione Marche mediante accessi in fibra ottica totalmente ridondati.

La Rete Telematica Regionale della Regione Marche è l'infrastruttura principale per trasporto dati attraverso la quale è possibile usufruire dei servizi DigiP.
Enti contribuitori non dotati di accesso alla rete telematica regionale possono connettersi al sistema via rete pubblica INTERNET attraverso un SISTEMA di FRONT END .

La figura sottostante illustra l'interconnessione dei siti primario e Disaster Recovery DigiP alla Rete Telematica Regionale.

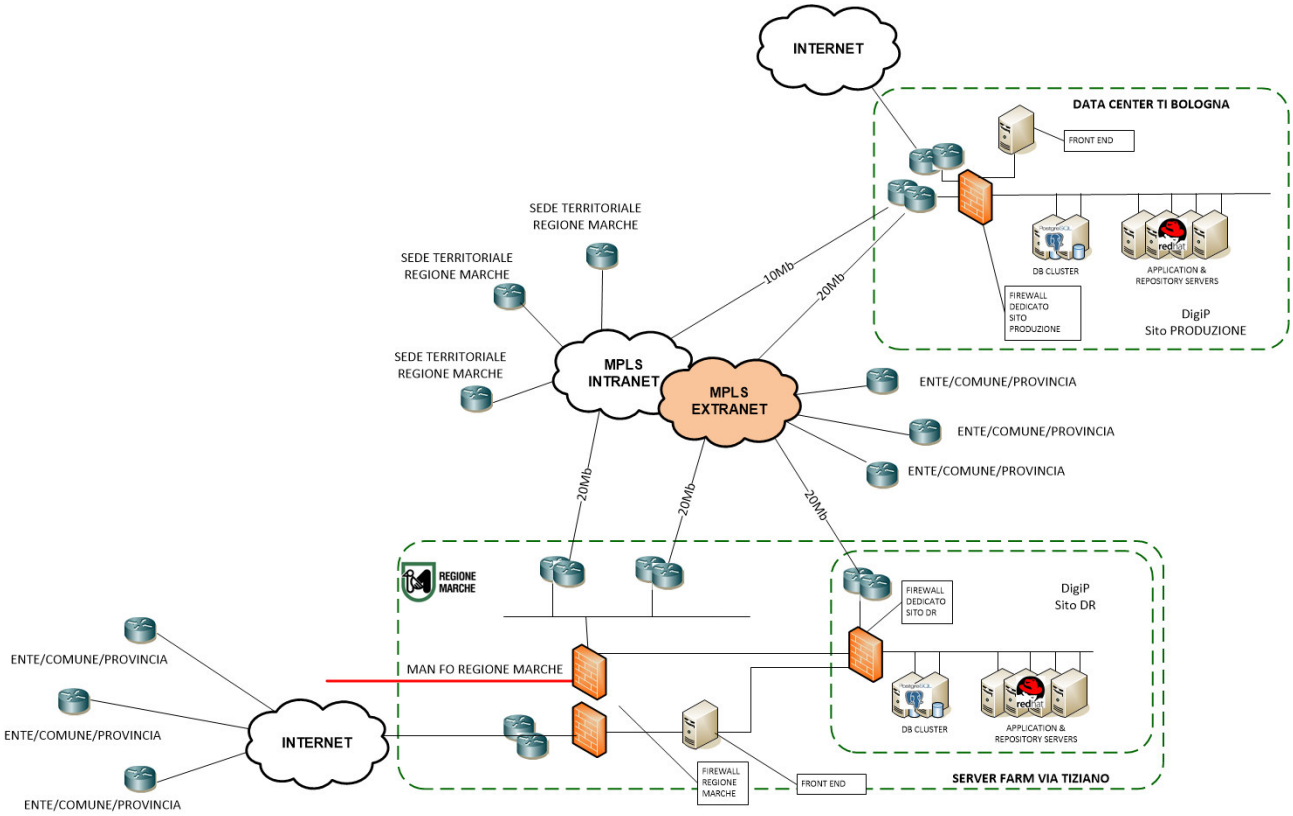


Figura 9 - Interconnessioni sito primario/DR alla Rete Telematica Regionale

Tutti i componenti del sito primario e Disaster Recovery sono ridondati.

Alcuni sistemi di supporto, impiegati dalla Control Room di Telecom Italia sono installati (sistemi di log & monitoring), ridondati, presso le server farm Telecom Italia di Rozzano e Pomezia.

La Control Room di Telecom Italia è direttamente connessa, mediante collegamenti specializzati, protetti da opportuni separation firewall, al sito di Disaster Recovery .

La figura sottostante illustra la modalità di connessione della Control Room alle installazioni DigiP.

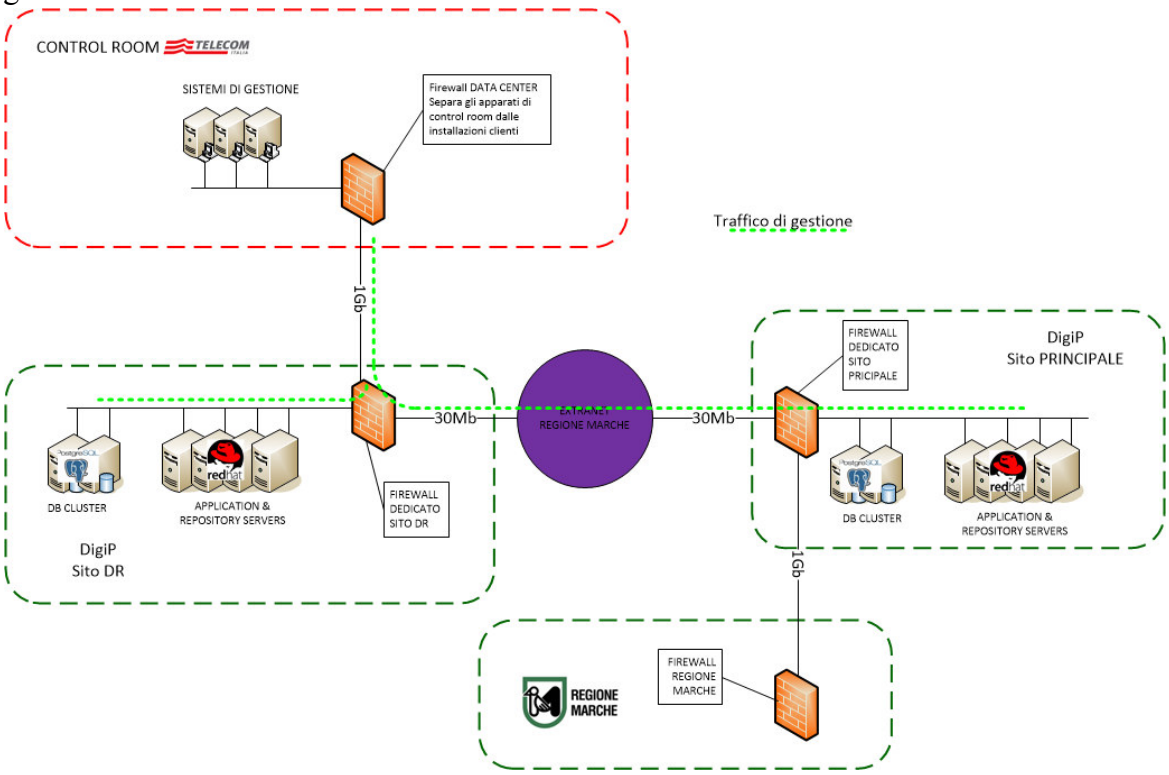


Figura 10 - Modalità di connessione Control Room a DigiP

In situazione di funzionamento normale il Sistema è attivo solo sul sito primario; il sito secondario si limita a replicare le informazioni del sito primario in maniera asincrona man mano che vengono generate e a compiere funzioni di backup.

In caso di caduta irreparabile del sito primario (disastro) il sito secondario viene posto in stato di attività e vi si reindirizza il traffico.

I sistemi di sviluppo risiedono presso la server farm di Regione Marche su ambienti fisicamente diversi da quelli che ospitano il sito primario DiGiP.

Torna al sommario

8.4 CARATTERISTICHE TECNICHE DEL SITO PRIMARIO

Lo schema illustra le componenti del sito di produzione

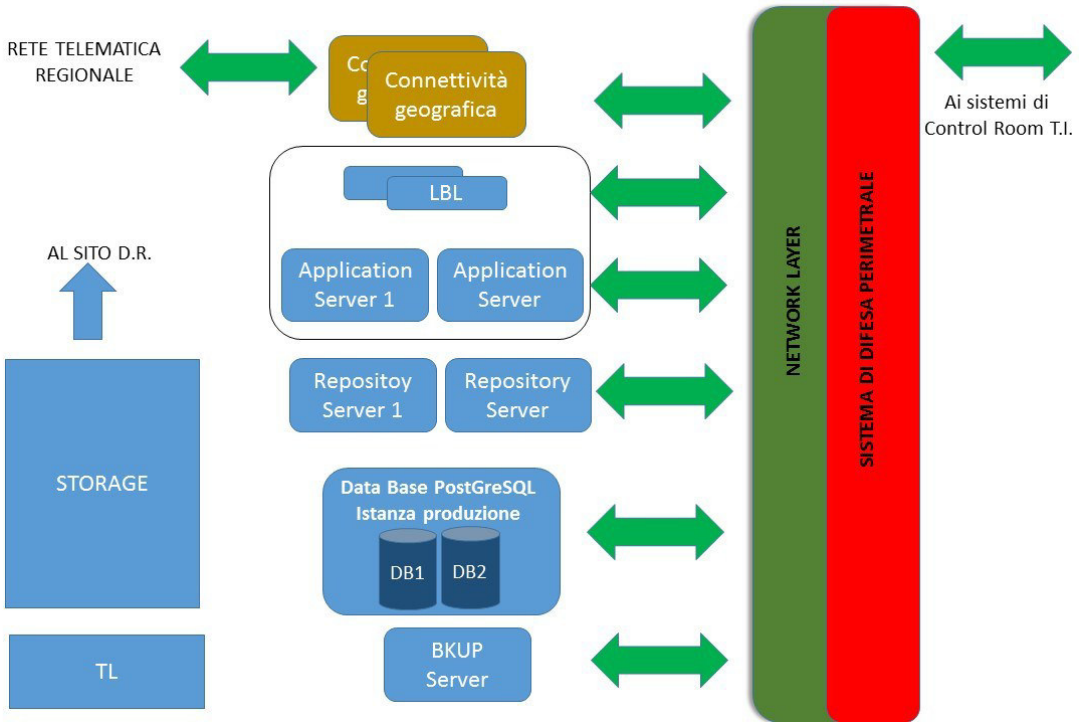


Figura 11 - Componenti sito di produzione

- **Connettività geografica**, costituita da collegamenti in fibra ottica (30Mbit/sec) totalmente ridondati su percorso fisico differenziato che consentono l'esposizione del servizio DigiP sulla Rete Telematica Regionale e l'allineamento degli storage dei due siti DigiP;
- **Network Layer** (CISCO), costituito da una coppia di switch, che provvede all'interconnessione delle varie componenti del sistema;
- **Sistema di difesa perimetrale** (FORTINET) in cluster, che si occupa di separare i veri layer del sistema;
- **Bilanciatore di carico LBL** (CISCO) in cluster, che si occupa di ripartire il carico sulla coppia di application server;
- **Application server TOMCAT** la batteria di application server è composta da due server;
- **Repository Server JACKRABBIT**la batteria di application server è composta da due server;
- **Data Base PostGreSQL** in cluster di sistema operativo;Il Cluster ospita due distinte istanze PostgreSQL una per il DB di Produzione e una per quello di test/pre-produzione

- **Sistema di Storage** composto da un apprato IBM Storewize V700 dotato di una capacità lorda di 24 TB
- **Sistema di Backup** composto da un backup server (Symantec) e una tape library IBM TS3100.

Gli accessi al sistema avvengono esclusivamente passando da firewall tramite protocolli sicuri (HTTPS e FTPS).
Lo ***storage*** su disco è suddiviso in due categorie:

- **Data Base** per la *memorizzazione* delle informazioni e di parte degli ***Oggetti-dati*** conservati in forma di Bytea (ByteArray);
- **File system** per la *memorizzazione* temporanea degli ***Oggetti-dati*** che, in base alle politiche configurate nel sistema, verranno archiviati su cassette; il ***file system*** contiene inoltre tutti i file di servizio (log, configurazioni, ecc.);

Lo ***storage*** su disco è ospitato su uno storage array ed è costituito da un'area di storage primario con dischi ad alta velocità e da un'area di storage secondario con dischi a media velocità; in questo modo è possibile ottimizzare la distribuzione dei dati sui dischi in ragione delle necessità applicative.

Lo ***storage*** su nastri magnetici (backup) si basa su un sistema a cassette (***tape library***), completamente governato da Symantc Backup Exec che gestisce cassette in standard LTO4 su cui vengono mantenuti in **modalità di backup**, i backup full e gli archive log del Data Base, immediatamente disponibili per qualsiasi attività di restore che si rendesse necessaria.

La replica dei dati sul sito secondario è garantita dalla tecnologia Remote Mirroring di IBM in modalità Global Mirroring.

Global Mirroring è una modalità di scrittura asincrona che assicura che le richieste di scrittura vengono effettuate sul sito remoto nello stesso ordine nel quale sono state effettuate sul sito principale, garantendo in questo modo la consistenza dei dati.

Global Mirroring è in grado di assicurare un RPO prossimo allo zero.

La funzionalità di Change Volume (specifica dei sistemi V7000) garantisce il corretto funzionamento del Global Mirroring anche in presenza di sovraccarico della rete di collegamento fra i due siti.

Torna al sommario

8.5 CARATTERISTICHE TECNICHE DEL SITO DI DISASTER RECOVERY

Il sito di disaster recovery, ubicato presso la Server Farm Regionale di Via Tiziano ad Ancona è realizzato in maniera speculare rispetto al sito principale , sul sito di Disaster Recovery è presente un Ambiente di PRE-PRODUZIONE.
L'immagine che segue schematizza le principali componenti tecniche del sito secondario di disaster recovery di DigiP

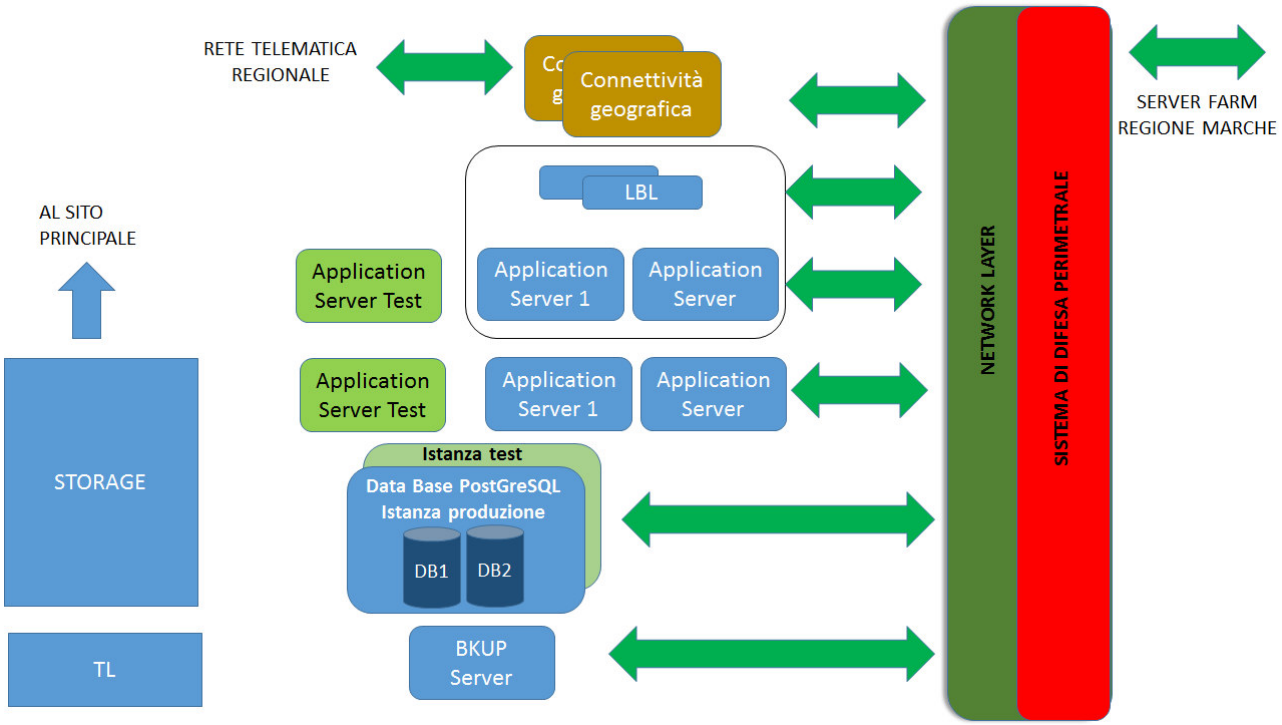


Figura 12 - Componenti tecniche sito disaster recivery DigiP

Il Sistema è sviluppato in Java su sistemi operativi Red Hat utilizzando i seguenti componenti principali:

- **Connettività geografica**, costituita da collegamenti in fibra ottica (30Mbit/sec) totalmente ridondati su percorso fisico differenziato che consentono l'esposizione del servizio DigiP sulla Rete Telematica Regionale e l'allineamento degli storage dei due siti DigiP;
- **Network Layer** (CISCO), costituito da una coppia di switch, che provvede all'interconnessione delle varie componenti del sistema;
- **Sistema di difesa perimetrale** (FORTINET) in cluster, che si occupa di separare i veri layer del sistema;

- **Bilanciatore di carico LBL** (CISCO) in cluster, che si occupa di ripartire il carico sulla coppia di application server;
- **Application server TOMCAT** la batteria di application server è composta da tre server;dei quali uno è dedicato all'ambiente di PRE-PRODUZIONE
- **Repository Server JACKRABBIT** la batteria di application server è composta da tre server;dei quali uno è dedicato all'ambiente di PRE-PRODUZIONE
- **Data Base PostGreSQL** in cluster di sistema operativo; il Cluster ospita due distinte istanze PostgreSQL una per il DB di Produzione e una per quello di test/pre-produzione
- **Sistema di Storage** composto da un apparato IBM Storewize V700 dotato di una capacità lorda di 24 TB
- **Sistema di Bkup** composto da un backup server (Symantec) e una tape library IBM TS3100.

Il sistema di storage è configurato in modo speculare a quello del sito principale e sincronizzato con quest'ultimo tramite i meccanismi di mirroring dell'apparato.

Torna al sommario

8.6 PROCEDURE DI GESTIONE E DI EVOLUZIONE

Le procedure di gestione ed evoluzione del sistema sono affidate ad un insieme di unità funzionali:

- **Unita di Gestione:** che esegue la normale attività di conduzione del sistema.
- **Unità di Progettazione e Sviluppo Software:** che si occupa della manutenzione correttiva ed evolutiva del software di conservazione.
- **Unità Data Center:** incaricata della gestione sistemistica infrastrutturale.
- **Supporti di secondo livello**: costituiti dai Comptence Center di Telecom Italia che cooperano con l'Unità Data Center nella rimozione di guasti e anomalie infrastrutturali.
- **Unità di Progettazione infrastrutturale**: che cura la progettazione e l'implementazione dell'evoluzione dell'infrastruttura HW.

Torna al sommario

8.7 CONDUZIONE E MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE

L'Unità di Gestione (UG) è il gruppo di lavoro che gestisce operativamente il funzionamento quotidiano del sistema di conservazione e costituisce inoltre il punto di riferimento per gli utenti finali del sistema stesso.

Oltre all'esecuzione dei processi descritti nel Manuale della Conservazione (ad esempio il controllo della corretta esecuzione delle regole di formazione degli AIP di conservazione, l'abilitazione di

nuovi utenti, ecc.), l'UG si occuperà delle funzioni di help desk verso gli Enti produttori (I° livello) sulle tematiche operative di conservazione ed archiviazione.

Torna al sommario

8.8 GESTIONE E CONSERVAZIONE DEI LOG

Il sistema di gestione e conservazione dei log si basa sul prodotto Syslog-ng Store Box di Balabit. Di seguito l'architettura logica:

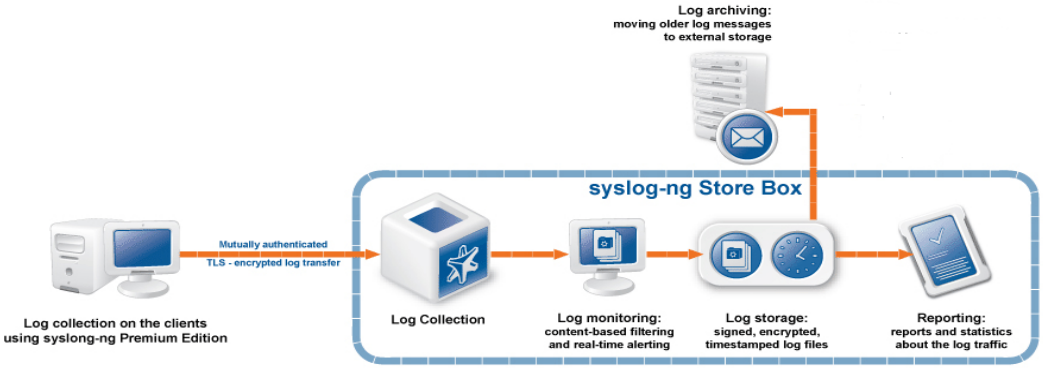


Figura 13 - Architettura logica

Sui sistemi in perimetro vengono attivate le funzionalità standard di sistema operativo di logging degli accessi (login/logoff). Sui DB server viene inoltre attivato il tracciamento degli accessi al DB, mediante la soluzione TOLL, integrabile con syslog-ng.

Su ciascun server in perimetro viene installata la componente client di syslog-ng PE 3.0

Presso i Data Center di T.I viene predisposta una coppia di Syslog-ng Store Box (SSB5000) in configurazione HA.

I syslog-ng client inviano, in modo sincrono e sicuro (canale cifrato, controllo integrità) gli eventi di loging/logoff al SSB di riferimento.

I log di accesso raccolti (archiviazione cifrata) sono fruibili mediante accesso al SSB, previa disponibilità della chiave privata di cifratura. Su specifica richiesta del Cliente potranno essere forniti i log di pertinenza in formato leggibile.

I log ricevuti dagli host remoti sono memorizzati in file binari compressi, cifrati, firmati e timestamped; sono inoltre sottoposti a backup su storage/server esterni.

E' previsto, mediante analoga modalità, il tracciamento degli accessi e di tutte le attività effettuate sul server SSB (conservazione dei log di accesso e delle attività effettuate su file cifrati).

E' prevista una gestione di tipo RBAC (Role-Based Access Control) dei privilegi degli utenti di sistema.

Syslog-Ng ha la funzionalità del "buffering" che permette di archiviare i messaggi localmente (lato syslog-ng client) e di rispedirli quando la connessione con il server di raccolta si è ristabilita dopo un eventuale fault, garantendo di fatto la continuità di registrazione degli eventi.
È possibile gestire i log ricevuti in path separati e configurabili sulla base delle sorgenti dati (IP o hostname).

Il servizio garantisce la tenuta in linea dei dati riferiti ai 6 mesi precedenti quello in corso.

Torna al sommario

8.9 MONITORAGGIO DEL SISTEMA DI CONSERVAZIONE

Il monitoraggio infrastrutturale del sistema è affidato all'Unità Data Center che si compone di una Unità di Presidio della sala dati del sito principale e da un insieme di strutture centralizzate di Telecom Italia che collaborano nella gestione sistemistica dell'infrastruttura:

L'Unità di Presidio cura tutte le attività On Site, quali:

- gestione degli accessi fisici alla sala macchine del sito principale;
- la verifica visiva dello stato del sistema;
- controllo dei bkup;
- controllo dello stato di allineamento dei sistemi di storage dei due siti;
- verifica dell'operato delle ditte manutentrici dell'hardware;
- collabora con le strutture centralizzate per la risoluzione dei guasti di sistema.

La Control Room di Telecom Italia si occupa di tutta l'attività di gestione sistemistica, dal sistema operativo al middleware, e cura le attività di log & monitoring sistemistico.

Il Centro Nazionale Assistenza e il NOC (Network Operation Center) di T.I. si occupano della gestione sistemistica del network Layer (Switch e Bilanciatori).

Il Centro Nazionale Assistenza e il SOC (Security Operation Center) di T.I hanno in carico la gestione degli apparati di sicurezza perimetrale.

Il Centro di Gestione TIDS (Telecom Italia Digital solution ex PathNET) ha la responsabilità del corretto funzionamento delle linee di interconnessione alla Rete Telematica della Regione Marche.

Tutte le componenti dell'Unità Data Center sono supportate dai Competence Center di Telecom Italia che costituiscono l'HelpDesk di secondo livello per la componente infrastrutturale.

Torna al sommario

8.10 CHANGE MANAGEMENT

Le attività di change management sono classificate in attività di tipo ordinario o evolutivo.
Il change management ordinario comprende tutte quelle attività hardware e software che non alterano l'architettura del sistema. Tali attività non richiedono di norma il coinvolgimento dell'Unità di Progettazione Infrastrutturale e sono eseguite dall'Unità Data Center direttamente o con il supporto del fornitore.

Tutte le attività di change management ordinario vengono tracciate e documentate dalla richiesta all'espletamento.

Le attività di change management evolutivo hanno un impatto sull'architettura del sistema, richiedono uno studio di fattibilità e la redazione di un' apposito progetto che dovrà essere approvato da Regione Marche.
Le attività di change management evolutivo sono eseguite dall'Unità Data Center direttamente o con il supporto di un fornitore.
Tutte le attività di change management evolutivo vengono tracciate e documentate dalla richiesta all'espletamento.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

9.1 VERIFICA PERIODICA DI CONFORMITÀ A NORMATIVA E STANDARD DI RIFERIMENTO

La struttura di progetto costituita dal Comitato Scientifico procederà periodicamente ad eseguire audit interni sull'intero sistema al fine di verificarne la conformità alla normativa cogente ed agli standard di riferimento.

Torna al sommario

9.2 PROCEDURE DI MONITORAGGIO

Vengono prodotti dal personale delle strutture di costituenti l'Unità Data Center e resi disponibili periodicamente report di monitoraggio tecnico, su tutte le aree infrastrutturali (rete, server, storage, database, backup). Si tratta di report tra loro eterogenei, prodotti dal software di base dei sistemi e dal software di monitoraggio tecnico installato sui medesimi.

Periodicamente i report di monitoraggio tecnico vengono esaminati congiuntamente all'Unità di Progetto con lo scopo di individuare eventuali aree di miglioramento negli aspetti tecnici dell'applicativo.

Torna al sommario

9.3 VERIFICA E MANTENIMENTO DELL'INTEGRITÀ DEGLI ARCHIVI

Le procedure di monitoraggio illustrate nel paragrafo precedente, le politiche di conservazione dei backup illustrate nel Piano della Sicurezza e le caratteristiche delle tecnologie utilizzate garantiscono la completa integrità di quanto archiviato in DigiP, ovvero di quanto depositato nel Data Base, nel file system e negli archivi su cassetta, una volta che sia stato duplicato nel sito di Disaster Recovery e salvato tramite opportuno backup sia nel sito primario che nel sito secondario.
Le funzionalità di Archiviazione consentono:

- l'amministrazione del data base, che si basa sulle funzionalità del data base e si occupa di gestire tutti i dati che transitano nel sistema, a parte i file memorizzati nel file system. Gli accessi al data base sono effettuati tramite opportuni moduli applicativi, che garantiscono l'indipendenza dell'applicativo dallo specifico data base (purché sql) e dalla sua specifica release;
- la manutenzione del data base. Le funzionalità di remote mirroring dello storage assicurano la replica del data base e del file system del repository nel sito di disaster recovery, mentre le funzionalità di recovery management consentono backup del data base completi e

incrementali, a caldo, secondo le politiche di sicurezza descritte nel piano della sicurezza. la gestione sistemistica del data base è effettuata tramite prodotti certificati, ed è tracciata nel log di sistema. il data base fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificare attività di manutenzione del data base stesso e degli applicativi che lo utilizzano;

- il controllo dell'integrità del data base, che avviene sfruttando funzionalità native del data base. Per quanto attiene alla componente di data base degli archivi, l'integrità è garantita dalle funzionalità intrinseche di PostGreSQL per tutti i metadati descrittivi, in particolare dalle funzionalità di backup del data base e di raccolta degli archive log (file WAL).

Per quanto attiene invece alla componente di file system degli archivi, l'integrità è garantita da funzionalità intrinseche del modulo di archiving di Symantec Backup Exec per tutti i dati archiviati su cassetta.

Qualora nonostante le garanzie fornite dalle tecnologie impiegate si verificassero anomalie nell'integrità degli archivi, sono previste le opportune procedure applicative di ripristino illustrate nel paragrafo seguente.

Non sono considerati facenti parte del Sistema, e quindi non fruiscono della stessa garanzia di integrità, i dati in ingresso presenti su aree temporanee (es. spazi FTP, ecc.), per i quali le procedure di soluzione di cui al paragrafo seguente prevedono la ritrasmissione nel caso di anomalie.

Il Piano della Sicurezza di DigiP descrive le modalità con cui DigiP assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i back up degli archivi, il Disaster Recovery e la Continuità Operativa.

Torna al sommario

9.4 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE

Le anomalie vengono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che l'ha generata nel processo di conservazione; quindi oltre alle procedure atte a garantire l'integrità degli archivi, nel senso indicato al paragrafo precedente, esistono anche procedure atte a risolvere anomalie in altre componenti del sistema che registrano dati in DigiP.

Le caratteristiche comuni e le specificità delle procedure di risoluzione delle anomalie dipendono da diversi fattori organizzativi e tecnologici:

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nel

File System operano in modalità transazionale;

- il backup del Data Base assicura il restore all'ultima transazione completata correttamente;
- il File System di DigiP è sottoposto a backup full a caldo con frequenza quindicinale. Non è quindi possibile far fronte a tutte le possibili anomalie con le stesse procedure, ma sono necessarie procedure specifiche secondo la natura dell'anomalia stessa.

La tabella seguente illustra le misure adottate per risolvere eventuali anomalie, classificate in ragione della collocazione delle informazioni nell'ambito del sistema nel momento in cui si è verificata l'anomalia:

File System del PreIngest	Si richiede la ritrasmissione dei SIP
Data Base di DigiP	Si effettua la restore tramite le funzioni standard di PostGres dal sito primario o dal sito secondario (nel caso di indisponibilità del DB primario)
File System di DigiP	Si effettua la restore tramite le funzioni standard del file server per tutti i file inseriti nel *file system* fino all'ultimo back up; per i file inseriti successivamente all'ultimo back up si eseguono opportune procedure di quadratura tra Data Base e *file system*, che provvedono a riportare il sistema in stato di congruenza. Le procedure di recupero debbono essere eseguite sia sul sito primario che sul secondario.

Torna al sommario

ALLEGATI

PIANO DELLA SICUREZZA

MANUALE DI UTILIZZO DIGIP

DISCIPLINARE TECNICO

PROGETTO REGIONALE DI CONSERVAZIONE DEGLI ARCHIVI DIGITALI

POLO MARCHE DIGIP

Sistema informatico per il Polo DigiP

Manuale d'uso

DigiP Versione 1.3.11

TELECOM ITALIA S.p.A. – Piazza Affari, 2 - 20123 Milano www.telecomitalia.com – Cap. Sociale 10.688.746.056,45 Euro – CF e Piva 00488410010
UNIMATICA S.p.A. - Via C.Colombo, 21 - 40131 Bologna (Italy) - Tel: +39.051.4195011 – Fax: +39.051.4195050 www.unimaticaspa.it - Cap.Sociale 500.000,00 Euro i.v. - CF. RI. Piva 02098391200 - REA BO 413696

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
1.0	05/02/15	Versione preliminare	Annachiara Coviello	Stefano Ghedini
1.1	10/03/16	Revisione documento	Annachiara Coviello	Stefano Ghedini
1.2	26/08/16	Revisione documento	Annachiara Coviello	Stefano Ghedini

Indice Generale

Introduzione

Il presente documento ha lo scopo di fornire una guida all'utilizzo del sistema informatico del Polo Regionale di conservazione degli archivi digitali di Regione Marche – DigiP, da qui identificato come sistema “Polo Marche DigiP”.

Nel presente documento verranno quindi illustrate le procedure per un corretto funzionamento dell'applicativo.

Il manuale verrà suddiviso nelle seguenti macro tematiche:

- Struttura generale del sistema
- Funzionamento generale del sistema per effettuare un versamento
- Configurazione del sistema
- Compiti e responsabilità dei diversi ruoli assegnati agli utenti
- Manuale per gli utenti

1. Struttura generale del sistema

Il sistema informatico del Polo Regionale – Digip – si pone come obiettivo la conservazione degli archivi digitali della Regione Marche. L'aspetto funzionale del Sistema è in linea di principio compatibile con l'organizzazione e le funzionalità necessarie per essere un archivio digitale in standard OAIS.

La struttura dell'applicativo si compone di parti utili per lo scambio di informazioni tra l'utente e il sistema:

- File System
- Maschere
- Database
- Repository

1.1 File System

Il sistema Digip utilizza per diversi fini operativi cartelle e file.

- Vengono utilizzate cartelle FTP per gestire lo scambio di informazioni tra utente e sistema. Queste cartelle sono definite al momento della configurazione e comunicate all'utente in fase di attivazione. Per esempio chi utilizza l'applicativo può avere la possibilità di caricare pacchetti di versamento (SIP) copiandoli direttamente nella cartella predisposta. Su questo stesso canale riceverà poi dal sistema un file contenente il rapporto di versamento, dove è comunicata l'avvenuta archiviazione dei documenti o il dettaglio dei problemi riscontrati.
- L'applicativo utilizza le cartelle come ambiente di lavoro: sono il punto di salvataggio di risultati intermedi o definitivi durante tutto il processo di caricamento. Un utente abilitato può avere accesso a queste cartelle per monitorare il corretto procedersi delle funzioni. L' ambiente viene sempre pulito una volta archiviati i pacchetti (AIP).
- Sono presenti cartelle contenenti file di properties e file funzionali.
- Sono definite dalle configurazioni directory utili per procedure come: migrazione, generazione di pacchetti DIP, creazione di report, sandBox.

1.2 Maschere

Le maschere sono le interfacce tramite cui l'utente può visualizzare e gestire tutto il funzionamento del sistema. Alcuni esempi: impostazione delle configurazione, monitoraggio dei versamenti, avvio di procedura parallele ai versamenti, compilazione di questionari. L'accesso a queste maschere viene fatto tramite autenticazione definita e rilasciata in fase di attivazione a tutti gli utenti appartenenti ad uno specifico Ente. L' accesso all'applicativo non implica la visualizzazione e l'utilizzo di tutto il sistema, poiché questo è vincolato dalla definizione di ruoli che un utente possiede. Ad ogni utente infatti sono assegnati uno o più casi d'uso che danno accesso a differenti funzionalità. Questo aspetto viene affrontato in modo esaustivo nel successivo paragrafo *"Compiti e responsabilità dei diversi ruoli assegnati agli utenti".*

1.3 Database

Il database utilizzato per la conservazione dei metadati è PostgreSql, ultima versione stabile.
Le tabelle generate sono definite secondo la struttura definita dal modello OAIS e per esigenze di programmazione. L'accesso al database per la consultazione dei dati è riservato ai soli utenti a cui viene data l'autorizzazione. Si sottolinea che gran parte delle informazioni persistite sono visibili e consultabili tramite interfaccia grafica. Modifiche alle tabelle invece sono permesse solo a livello sistemistico.

1.4 Repository

L'applicativo utilizza un repository dove mantenere fisicamente tutti gli elementi che sono stati utilizzati durante il processo di archiviazione. Tutti i file appartenenti al pacchetto di versamento (SIP) o di archiviazione (AIP) vengono memorizzati dal sistema su uno storage Jackrabbit (JCR 2.0), come inputstream . L'utente autorizzato può recuperare gli elementi tramite l'indirizzo del nodo (storeAddress), valore definito dal sistema al momento del caricamento e memorizzato sul database.

2. Funzionamento generale del sistema

2.1 Versamento

Il caricamento di un pacchetto di versamento (SIP) può avvenire tramite flusso o tramite versamento Web (chiamata Rest). L'utente a seconda degli accordi presi con l'azienda conservatrice avrà quindi queste due possibilità.

Caricamento tramite FLUSSO: il produttore posiziona dentro una specifica cartella FTP, assegnata al *Soggetto Produttore* al momento dell'attivazione, i pacchetti SIP, definiti come:

- pacchetto .zip contenente
- un file XML di indice definito secondo il modello XSD di riferimento. (Ad oggi per questa modalità di versamento è accettato solamente il modello SINCRO).
- tanti file allegati quanti ne definisce l'indice. Il formato deve essere conforme agli accordi.

Attenzione si precisa che:

- il nome dei pacchetti SIP che si vogliono versare deve essere univoco, salvo nel caso di caricamento di uno precedentemente andato in errore
- si deve mantenere la coerenza tra la descrizione dei file definiti nell'indice e quelli effettivamente allegati.

Il sistema tramite periodici controlli, trovato il file, avvierà il processo di versamento. L'applicativo poi risponderà al soggetto versatore posizionando in una cartella *shared* (denominata RDV) due tipi di file definiti come segue:

- RDC_*nomedelSIP*.csv : un file csv per ogni versamento nel quale è definito il SIP che il sistema ha preso in carico per procedere all'archiviazione dei suoi dati. In questo file viene definito un ID univoco che è fondamentale per la ricerca e la gestione dei dettagli del singolo versamento. Nel caso il rapporto di carico, RDC, sia già presente (ad esempio per una esecuzione precedente fallita) viene comunque aggiunta la nuova riga alla fine del file.
  Nel file vengono specificati i seguenti campi:
  - Date/Time: data di creazione del rapporto di carico, in formato YYY-MM-DD HH:mm:ss

- Soggetto produttore: nome ente che sta effettuando il versamento
- Nome SIP: nome del pacchetto SIP versato
- ID SIP: identificativo univoco del pacchetto SIP versato
- Data Versamento: data del versamento, in formato YYY-MM-DD HH:mm:ss
- Codice Esito: codice esito della presa in carico del SIP. Può avere tre valori: OK (pacchetto preso in carica), WARN (pacchetto preso in carica, ma il sistema ha riscontrato anomalie non bloccanti), ERROR (pacchetto rifiutato dal sistema e non preso in carica)
- Messaggio: messaggio descrittivo sull'esito della presa in carica del SIP

- *RDV_idUnivocoSIP.xml:* un file per ogni versamento effettuato e preso in carica dal sistema. E' il rapporto di versamento di ogni singolo SIP. (Per la struttura vedere **Allegato n.1**). Grazie a questo file l'utente può controllare se il pacchetto versato è formalmente corretto per lo standard richiesto. Fino a questo momento infatti la responsabilità della corretta archiviazione dei file è a carico dell'utente il quale deve rispettare le regole e i modelli definiti dagli accordi. In caso contrario vengono segnalati gli errori e il sistema non archivierà i SIP. Superati i controlli il sistema procederà con l'archiviazione. Da questo punto in avanti la responsabilità è dell'azienda conservatrice, la quale provvederà alla correzione di eventuali errori.

Una volta depositati sulla cartella, entrambi i file, possono essere gestiti dall'utente che può visualizzarli, copiarli, spostarli o eliminarli. Il sistema non si prende cura di eliminare file vecchi o non utilizzati.

NOTA: se autorizzati ad accedere alle interfacce dell'applicativo l'utente ha la possibilità di caricare il pacchetto zip e di recuperare i file RDC e RDV direttamente tramite una maschera apposita. Per i dettagli vedere il paragrafo *Versamento ZIP.*

Definizione cartella FTP: il protocollo utilizzato è SFTP. Sono attivi esclusivamente gli utenti definiti in DigiP e il servizio gira in una macchina Docker (con lettura dei dati via SQL).
Il servizio è composto dai seguenti processi:
- un demone "sftp" che resta in ascolto e utilizza "utente", "password" e "userpath" per la costruzione dei parametri di connessione, salvando i file su storage locale (su percorso in funzione del login utente)
- un servizio che gira ogni 5 minuti dalla macchina che ha il servizio esposto e si collega al server SQL per ottenere l'elenco degli utenti e dei percorsi attivi , quindi allinea" (con rsync) le cartelle:

- le cartelle */home/digipark/...*/RDV da "pubblico" -> "APS"
- le cartelle */home/digipark/...*/RIVERSAMENTO da "pubblico" -> "APS"
- le cartelle */home/digipark/...*/SIP da "APS" -> "pubblico"

Il DB e lo storage locali sono persistenti, il demone gira in una sandbox docker che all'avvio carica le configurazioni e il filesystem persistente "ricreando da zero tutto l'ambiente di processo".

Caricamento tramite WEB-REST: l'utente autorizzato effettua i caricamenti via web tramite maschere specifiche oppure trasmettendo i versamenti al sistema tramite chiamata rest. Per i dettagli sulla modalità di versamento si rimanda al paragrafo *Versamento Web* e *Versamento Web RPG*.

Si specifica che il nome del pacchetto SIP sarà definito come WS_CHIAVE:

WS_Numero-Anno-TipoRegistro : valori definiti nell'indice sotto il tag <Chiave>.

In questo caso il sistema risponderà all'utente in due momenti: subito dopo il versamento tramite la visualizzazione di un messaggio a video (definito graficamente a partire dal file xml generato secondo il modello **Allegato n.2** o **Allegato n.3**) e dopo la validazione delle regole tramite la creazione del file RDV definito sopra che può essere visualizzato direttamente da interfaccia, tramite la maschera *Esiti Versamenti.*

Per entrambe le modalità l'utente, con ruolo di amministratore o di ingest, può monitorare il processo e il completamento di questo tramite la specifica interfaccia *Esiti Versamenti.* La ricerca è per data versamento e, tramite l'identificativo e il nome del pacchetto, si può visualizzare lo stato del processo, i dettagli e scaricare il rapporto di versamento.

Vengono mostrati di seguito i **passaggi operativi** eseguiti dal sistema:

- il sistema rileva un nuovo versamento (via Flusso o via Rest) e trasferisce il SIP in una cartella di lavoro temporanea;
- fa i primi controlli sugli oggetti ricevuti se sono conformi agli accordi presi con l'Ente: se corretti prende in carica il versamento e procede, altrimenti sposta tutto in una specifica zona denominata Cestino;
- memorizza il SIP in una sezione specifica dell' Archival Storage e notifica l'avvenuta ricezione del versamento al produttore;
- Il SIP passa al processo per il controllo della qualità: il sistema recupera ed esegue le Regole da applicare per la validazione in base al soggetto produttore e al tipo di documento che sta versando;
- il sistema elabora una ricevuta di presa in carico opzionalmente firmata (Rapporto di Versamento) e ne salva una copia sul repository;
- Se le regole sono state tutte validate correttamente il sistema recupera ed esegue le trasformazioni opportune per rendere i file conformi agli accordi per l'archiviazione (attualmente lo standard ISO SINCRO);
- il sistema genera un AIP e memorizza gli oggetti in una sezione specifica dell' Archival Storage.

Versione e controlli per il versamento WEB Service

Un pacchetto che viene versato via web service segue opportuni controlli e procedure a seconda della versione specificata nell'indice del pacchetto. Di seguito i dettagli:

v 1.3:

- controllo della lunghezza massima del nome del file definito nell'indice xml
- controllo e renaming dei nomi doppi dei file definiti nell'indice xml
- controllo numero dei file allegati con numero dei file dichiarati nell'indice xml

v 1.4:

- controllo della lunghezza massima del nome del file definito nell'indice xml
- controllo e renaming dei nomi doppi dei file definiti nell'indice xml
- controllo numero dei file allegati con numero dei file dichiarati nell'indice xml
- inserimento del valore dell'identificativo del pacchetto (UUID) nel rapporto di carico

v 1.5:

- controllo della lunghezza massima del nome del file definito dai file allegati
- controllo e renaming dei nomi doppi dei file definito dai file allegati
- controllo numero e nome dei file allegati con numero e nome dei file dichiarati nell'indice xml
- inserimento del valore dell'identificativo del pacchetto (UUID) nel rapporto di carico

v 1.6:

- controllo della lunghezza massima del nome del file definito dai file allegati
- controllo e renaming dei nomi doppi dei file definito dai file allegati
- controllo numero e nome dei file allegati con numero e nome dei file dichiarati nell'indice xml
- inserimento del valore dell'identificativo del pacchetto (UUID) nel rapporto di carico
- gestione del livello di riservatezza inserito nell'indice xml (valori da 0 a 127)

2.2 Modifica

Una volta archiviati i pacchetti di versamento è possibile effettuare delle specifiche modifiche. Queste possono essere fatte sulla base di accordi presi tra l'ente e l'azienda conservatrice e soprattutto rispettando le normative sulla conservazione.

Vediamo di seguito in dettaglio la procedura nelle due modalità di versamento.

Modifica tramite FLUSSO: il produttore posiziona dentro una specifica cartella FTP, assegnata al *Soggetto Produttore* al momento dell'attivazione, i pacchetti SIP di modifica, definiti come:

- pacchetto .zip, con lo stesso nome del precedente SIP da modificare, contenente
- un file XML di indice definito secondo il modello XSD di riferimento (SINCRO), dove devono essere inseriti:
  - obbligatoriamente i tag di <sincro:SourceIdC> con le informazioni relative all'AIP che si vuole modificare:
    - <sincro:ID>: inserire il valore dell'identificativo univoco dell'AIP
    - <sincro:Path>: inserire l'indirizzo (store address) del pacchetto AIP
    - <sincro:Hash sincro:function="SHA-1">: inserire valore dell'hash del pacchetto AIP
  - metadati in aggiunta o modifica. Nel secondo caso associare il valore al tag corretto che si vuole modificare
  - esclusivamente i file in aggiunta con i relativi metadati.
- tanti file allegati quanti ne definisce l'indice. Il formato deve essere conforme agli accordi.

Il sistema trovato il file avvierà il processo di modifica. L'applicativo prima di procedere farà opportuni controlli sull'esistenza dell' AIP dichiarato da modificare. Nel caso l'identificativo fosse sbagliato non procederà alla modifica, ma sposterà tutto nel cestino.

Attenzione: se si cambia nome al pacchetto e se i tag definiti sopra non vengono valorizzati il sistema riconoscerà il SIP come un versamento normale, e non come una modifica, e procederà all'archiviazione.

Modifica tramite WEB-REST: l'utente autorizzato trasmette al sistema i pacchetti di versamento per la modifica tramite una specifica chiamata Rest.

L'utente per effettuare il versamento di modifica dovrà:

- inserire la VERSIONE corretta per la validazione XSD dell'indice
- inserire corrette credenziali (LOGINNAME e PASSWORD), con ruolo ingest
- copia e incolla dell'indice descrittore per un versamento di tipo aggiunta\modifica dove inserire:
  - obbligatoriamente la CHIAVE (*Numero-Anno-TipoRegistro)* del pacchetto deve essere la stessa del precedente versamento che si vuole modificare
  - metadati in aggiunta o modifica. Nel secondo caso associare il valore al tag corretto che si vuole modificare
  - esclusivamente i file in aggiunta, con i relativi metadati
- fare upload dei file da aggiungere, se presenti
- inviare e attendere la risposta di corretto caricamento.

Vengono mostrati di seguito i **passaggi operativi** eseguiti dal sistema per la modifica:

- il sistema rileva un nuovo versamento di tipo modifica (via Flusso o via Rest) e trasferisce il SIP in una cartella di lavoro temporanea;
- controlla se in archivio esiste il pacchetto da modificare con la stessa chiave. Lo recupera e procede alla trasformazione xslt dell'indice AIP nel formato KIP e lo pone nella cartella di lavoro.
- fa i primi controlli sugli oggetti ricevuti se sono conformi agli accordi presi con l'Ente, se corretti procede;
- Il SIP_modifica passa al processo per il controllo della qualità: il sistema recupera ed esegue le regole da applicare per la validazione in base al soggetto produttore e al tipo di documento che sta versando;
- il sistema elabora una ricevuta di presa in carico opzionalmente firmata (Rapporto di Versamento) e ne salva una copia sul repository;
- se le regole sono state tutte validate correttamente il sistema recupera ed esegue le trasformazioni opportune per rendere i file conformi agli accordi per l'archiviazione (attualmente lo standard ISO SINCRO);
- il sistema genera un nuovo AIP dove sono presenti tutti i metadati del precedente pacchetto con le opportune modifiche, se presenti, e tutti i nuovi metadati aggiunti, se presenti. Memorizza gli oggetti in una sezione specifica dell' Archival Storage;
- il sistema setta a false, non più valido, l'AIP originale che è stato modificato.

- si precisa che gli AIP non vengono cancellati, ma in archivio saranno presenti entrambi i pacchetti, l'originale e il modificato. Il primo risulterà non più valido e potrà essere visualizzato durante la ricerca solo come *reference* del nuovo pacchetto.

3. Configurazione del sistema

Prima di iniziare a versare pacchetti SIP è indispensabile configurare il sistema.
Di seguito l'elenco delle configurazioni da valorizzare per il corretto funzionamento del programma:

- **Soggetto produttore**: si definisce un soggetto produttore per ogni nuovo cliente
- **Utente:** si definiscono utenti utilizzatori dell'applicativo e i loro ruoli specifici, a seconda delle responsabilità
- **Configurazioni globali:** si definiscono parametri globali per il corretto funzionamento di tutte le componenti del sistema (livello sistemistico)
- **Configurazioni soggetto produttore:** si definiscono parametri per soggetto produttore, un modello di archiviazione concordato con l'utente
- **Configurazioni tag:** per ciascun soggetto produttore si definiscono nomi di Tag. Questi sono utili al processo di archiviazione e nella ricerca di metadati persistiti sul database
- **Tipologia documentale:** per ogni soggetto produttore si definiscono tipologie documentali relative al tipo di documenti che si prevede di versare
- **Gestione policy:** per ogni soggetto produttore e tipologia documentale si definiscono policy suddivise in rule, transformation e standard. Queste sono utili per controllare e modificare i versamenti effettuati, in quanto devono rispettare un corretto modello archivistico
- **Configurazione file xslt:** si definiscono file di trasformazione xslt utili al processo per una corretta produzione di file di indice per la conservazione

Tutte queste configurazioni sono gestite dall'amministratore di sistema in accordo con l'ente. La definizione e la modifica avvengono tramite query dirette al database o se possibile attraverso maschere web apposite.

3.1 Soggetto produttore

Tramite il termine soggetto produttore si definisce la partizione per Ente/Cliente del polo archivistico. Ogni Ente infatti ha un preciso soggetto produttore di riferimento. Questo valore è indispensabile per la corretta archiviazione dei documenti. Legato a questo infatti è collegato tutto il sistema di definizione degli Information Package. La sua corretta definizione comporta un corretto salvataggio e un corretto recupero di tutta la documentazione salvata per determinati clienti.

Definizione soggetto produttore:

NOME CAMPO TABELLA	VALORE IPOTETICO	SIGNIFICATO DEL CAMPO
SOGGETTO PRODUTTORE (ID)	soggetto produttore_id	Valore identificativo univoco per ciascun soggetto produttore (primary key)
NOME	soggetto produttore_nomeEnte	Nome univoco dato a ciascun soggetto produttore che definisce l'ente di riferimento
DESCRIZIONE	soggetto produttore di Test	Parte descrittiva utile alla comprensione del relativo soggetto produttore appena creato. Es. a quale ente/cliente ci stiamo riferendo,

		se ci sono note particolari ecc..

3.2 Utenti

Ogni ente/cliente prevede un numero non definito di utenti che possono usare l'applicativo. Ognuno di questi utenti potrebbe avere aree di responsabilità differenti e sopratutto una visione limitata dell'applicativo e dei pacchetti di archiviazione per motivi di sicurezza. Per gestire ciò quando viene creato un utente vengono legati ad esso uno o più ruoli e un livello di riservatezza (questo tema verrà sviluppato ampiamente nella sezione *Compiti e responsabilità dei diversi ruoli assegnati agli utenti*).

Definizione utente:

NOME CAMPO TABELLA	VALORE IPOTETICO	SIGNIFICATO DEL CAMPO
ID	123456789	Valore identificativo univoco per ciascun utente (primary key)
NOME	nome_utente	Nome univoco che identifica ciascun utente
MAIL	mail_utente	Indirizzo mail relativo all'utente di riferimento. Questo indirizzo servirà per l'invio di questionari, di comunicazioni e per un eventuale cambio di password
SOGGETTO PRODUTTORE_ID	soggetto produttore_id	Identificativo del soggetto produttore a cui l'utente fa riferimento (foreign key)
RISERVATEZZA	Da 0 a 127	Numero intero che definisce il livello di riservatezza a cui può accedere l'utente. Precisamente l'accesso ai documenti è permesso per un livello < o uguale al livello di riservatezza
CODICE FISCALE	aaa12bb345cc6	Codice fiscale dell'utente
Ip	123.08.08	Identifica l'indirizzo Ip dell'utente

A ciascun utente inoltre vengono assegnate le credenziali di accesso al sistema definite da:

username: corrisponde al nome dell'utente salvato sul database

password: valore deciso dall'utente (di almeno 6 caratteri) e salvato in modo crittografato sul database

3.3 Configurazioni globali

Di seguito l'elenco dei parametri globali indispensabili per il processo di caricamento dei pacchetti di versamento.

NOME PARAMETRO	VALORE PARAMETRO IPOTETICO	SIGNIFICATO PARAMETRO
AMQP_USERNAME	guest	Credenziali RabbitMQ
AMQP_PASSWORD	guest	Credenziali RabbitMQ

AMQP_HOST	localhost	Host RabbitMQ
AMQP_PORT	5672	Porta RabbitMQ
PATH_WORK_DIRECTORY	/home/digipark/work	Directory di lavoro per il sistema, dove vengono salvati i risultati parziali del processo
QST_PERC_BLOCKER	5	Percentuale sul totale delle risposte del questionario per definire se l'argomento della domanda relativa è un problema bloccante ai fini del processo
QST_PERC_CRITICAL	10	Percentuale sul totale delle risposte del questionario per definire se l'argomento della domanda relativa è un problema critico ai fini del processo
QST_PERC_MAJOR	50	Percentuale sul totale delle risposte del questionario per definire se l'argomento della domanda relativa è un problema di livello major ai fini del processo
QST_PERC_MINOR	50	Percentuale sul totale delle risposte del questionario per definire se l'argomento della domanda relativa è un problema minor ai fini del processo
QST_MAIL_HOST	mail.unimaticaspa.it	Host da cui parte la mail per comunicare con gli utenti
QST_MAIL_ENVELOPEFROM	digipark@unimaticaspa.it	Indirizzo digipark da cui parte la mail per comunicare con gli utenti
QST_MAIL_SUBJECT	Questionario Digipark	Oggetto della mail
QST_MAIL_PORT	25	Porta per la gestione della mail
QST_ABBR_LENGHT	50	Numero massimo di caratteri per la visualizzazione nelle maschere della descrizione del questionario
PATH_WORK_SANDBOX	/home/digipark/sandbox	Directory usata del sistema dove vengono gestiti e salvati solo i lavori della sandBox
PATH_WORK_DIRECTORY_DIP	/home/digipark/work/dip	Directory usata del sistema dove vengono salvati solo i lavori per la gestione dei DIP
PATH_WORK_DIRECTORY_MIGRATION	/home/digipark/work/ migration	Directory usata del sistema dove vengono gestiti e salvati solo i lavori relativi al processo di migrazione
VERIFICA_FIRMA_SERVICE_URL	https://web1.unimaticaspa.it/ uniserv-test/services/ uniservService20	Service_URL per la verifica di un file firmato
VERIFICA_FIRMA_ENTE	settoreconservazione	Ente per la verifica della firma
VERIFICA_PROVIDER	unimatica	Provider per la verifica della firma

FIRMA_SERVICE_URL	https://web1.unimaticaspa.it/uniserv-test/services/Uniserv40Services	Service_URL per effettuare la firma di un file
FIRMA_USERNAME	settoreconservazione	Credenziali per firmare un documento
FIRMA_PASSWORD	settoreconservazione	Credenziali per firmare un documento
FIRMA_CREDENZIALE	collaudo	Credenziali per firmare un documento
FIRMA_PROVIDER	unimatica	Provider per firmare un documento
RECUPERO_QUEUE_RUNNING	2	Numero di giorni che devono passare prima di avviare un processo di ripristino di una coda che ha interrotto i lavori, non per motivi procedurali.
MINUTES_BETWEEN_BATCH_PROCESS	100	Minuti di intervallo tra la fine di un processo e l'inizio di un altro
PROT_SERVICE_URL	https://paleotest.regionemarche.intra/PaleoWebServices R_MARCHE/PaleoWebService.svc?wsdl	Url per la chiamata al sistema di protocollo regionale Paleo per la protocollazione del Rapporto di Versamento
PROT_USERID	Polo.versamento	UserID per l'accesso al sistema di protocollo regionale Paleo
PROT_PASSWORD	password	Password di accesso al sistema di protocollo regionale Paleo
PROT_COD_AMM	r_marche	Codice amministratore per l'accesso al sistema di protocollo regionale Paleo
PROT_OPERATORE_COGNOME	polo	Cognome operatore che accede al sistema di protocollo regionale Paleo
PROT_OPERATORE_NOME	versamento	Nome operatore che accede al sistema di protocollo regionale Paleo
PROT_OPERATORE_RUOLO	protocollista	Ruolo operatore che accede al sistema di protocollo regionale Paleo
PROT_OPERATORE_CODICE_UO	INF	Codice unità organizzativa del sistema di protocollo regionale Paleo
ALGORITMO_HASH_NOME_RULE	MD5	Algoritmo per il controllo hash nell'applicazione delle regole
ALGORITMO_HASH_NOME_TRANSFORMATION	MD5	Algoritmo per il controllo hash nell'applicazione delle trasformazioni
CODIFICA_HASH_NOME_RULE	B64	Codifica per il controllo hash nell'applicazione delle regole
CODIFICA_HASH_NOME_TRANSFORMATIO	B64	Codifica per il controllo hash nell'applicazione delle

N		trasformazioni
VERSIONE_VERSAMENTO	1.3	Numero versione del file xsd per la validazione degli indici di versamento
TEMA	test_clienti	Identificativo per la scelta del CSS da utilizzare per l'interfaccia grafica
QUEUE_SUBMISSION_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_SUBMISSION_CONSUMER
QUEUE_LOAD_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_LOAD_CONSUMER
QUEUE_PROCESS_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_PROCESS_CONSUMER
QUEUE_GESTIONE_ESITI_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_GESTIONE_ESITI_CONSUMER
QUEUE_GENERATE_AIP_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_GENERATE_AIP_CONSUMER
QUEUE_INGEST_MONITOR_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_INGEST_MONITOR_CONSUMER
QUEUE_DIP_REQUEST_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_DIP_REQUEST_CONSUMER
QUEUE_GENERATE_DIP_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_GENERATE_DIP_CONSUMER
QUEUE_DISCARD_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_DISCARD_CONSUMER
QUEUE_MIGRATION_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_MIGRATION_CONSUMER
QUEUE_PROCESS_CHECK_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_PROCESS_CHECK_CONSUMER
QUEUE_RIVERSAMENTO_REQUEST_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_RIVERSAMENTO_REQUEST_CONSUMER
QUEUE_SYSTEM_MONITOR_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_SYSTEM_MONITOR_CONSUMER
QUEUE_GENERATE_REPORT_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_GENERATE_REPORT_CONSUMER
QUEUE_DELETE_DIP_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_DELETE_DIP_CONSUMER

QUEUE_PUBBLICA_QUESTIONARIO_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_PUBBLICA_QUESTIONARIO_CONSUMER
QUEUE_MODIFY_CONSUMER	1	Numero di worker attivi sulla coda QUEUE_MODIFY_CONSUMER
LOGIN_LOCALE	True / False	Settato a *true* prevede l'accesso alle maschere tramite il login “Database interno” oltre all'identificazione Coesion
TRASHCAN_PATH	/home/digip/work/trash	Path di riferimento per il recupero dei SIP scartati e finiti nel cestino
DEFAULT_ENCODING	UTF-8	Valore di default per codifica encoding
MINUTI_LATENZA_INGEST	60	Minuti oltre i quali il sistema processa pacchetti SIP che risultano già presi in carico
AMBIENTE	MARCHE DIGIP	Identifica l'ambiente di lavoro
MAX_LENGTH_FILENAME	255	Lunghezza massima per il nome dei file allegati
FORMAT_DETECTOR_MAX_THREADS	20	Numero max thread in parallelo
CUSTOM_LEVEL_LOGGER	ERROR \ WARNING	Livello di logger
MINUTI_VALIDITA_TOKEN_PASSWORD	30	Minuti di validità del token che permette il reset della password
PATH_KEYSTORE	/home/digipark/work	Path dove si trova il keystore che contiene una chiave AES per la crittografie dei file
PWD_KEYSTORE	123456789	Password per accedere alla chiave AES per la crittografia dei file
CIFRATURA_STORE	ENCRYPTED \ NONE	Parametro che decide se i file devono essere salvati criptati o non criptati
QUEUE_EXECUTOR_POOL	200	Numero thread pool

3.4 Configurazioni per soggetto produttore

Di seguito l'elenco dei parametri da configurare per ogni singolo *soggetto produttore* indispensabili per il processo di caricamento dei pacchetti di versamento.

NOME PARAMETRO	VALORE PARAMETRO IPOTETICO	SIGNIFICATO PARAMETRO
DEFAULT_STORAGE	jcrRepository	Nome dello storage utilizzato
DEFAULT_PROVISIONING	FLUSSO / REST	Modalità di versamento dei SIP
DESCRITTORE_SIP	indiceSIP.xml	Nome del file indice descrittore presente nel pacchetto di versamento SIP

DESCRITTORE_AIP	indiceAIP.xml	Nome del file indice descrittore presente nel pacchetto di archiviazione AIP
DESCRITTORE_DIP	indiceDIP.xml	Nome del file indice descrittore presente nel pacchetto di distribuzione DIP
PATH_SHARED_DIRECTORY	/home/digipark/soggetto produttore/digip	Cartella FTP che serve da interscambio tra l'utente e il sistema
PATH_XSLT_FITS	/home/digipark/XSLT/ xslt_fits.xslt	Path del file di trasformazione XSLT che adatta il file generato dal tool Fits in un formato comodo al processo
PATH_XSLT_KIP_AIP	/home/digipark/XSLT/ xslt_KIP-AIP.xslt	Path del file di trasformazione XSLT che adatta il file KIP, risultato dei vari processi di trasformazione avvenuti al SIP, ad un formato standard (sincro) per l' AIP
PATH_XSLT_AIP_KIP	/home/digipark/XSLT/ xslt_AIP-KIP.xslt	Path del file di trasformazione XSLT che adatta il file di indice di un AIP ad un formato comodo al processo che denominiamo come KIP
PATH_XSLT_KIP_DIP	/home/digipark/XSLT/ xslt_KIP-DIP.xslt	Path del file di trasformazione XSLT che adatta il file di indice ad un formato comodo al processo che denominiamo come KIP
PATH_RIVERSAMENTO	/home/digipark/work/ riversamento	Directory usata dal sistema dove vengono salvati solo i risultati del processo di riversamento, generazione dei DIP
PRODUZIONE_REPORT	ABILITATO / DISABILITATO	Flag che abilita o disabilita la produzione di un report periodico che descrive l'andamento del sistema
PERIODO_REPORTING	30	Numero di giorni che scandiscono la produzione di un report per descrivere l'andamento del sistema
GESTIONE_RECORD_REPORT	CANCELLA / CONSERVA	Flag che decide se cancellare o mantenere i record sul database, relativi alla produzione dei report periodici di sistema
DIRECTORY_REPORT_CSV	/home/digipark/csvReport	Cartella dove verranno salvati tutti i report periodici di sistema generati
VERIFICA_FIRMA	ABILITATA / DISABILITATA	Flag che abilita o disabilita la verifica dei file firmati
PROFILO_VERIFICA_FIRMA	default / ControlloTotale	Profilo definito per applicare la verifica della firma
FIRMA_RDV	ABILITATA / DISABILITATA	Flag che abilita o disabilita la firma del rapporto di versamento
FIRMA_AIP	ABILITATA / DISABILITATA	Flag che abilita o disabilita la firma

		dell'indice dell'AIP
RISERVATEZZA_DEFAULT	0	Valore che definisce un livello di riservatezza del pacchetto di versamento e di conseguenza di archiviazione nel caso non sia specificato tra i metadati del SIP. Il valore 0 è il valore più basso e quindi tutti potranno accedere ai file che hanno questo livello di riservatezza, il valore massimo è 127 e solo gli utenti a cui è associato questo valore potranno consultare i documenti
PERIODO_CONSERVAZIONE_DIP	30	Numero di giorni di conservazione dei pacchetti di distribuzione DIP. Passati questi giorni vengono cancellati i file dalle cartelle e dal repository e settati a false sul database.
PROTOCOLLAZIONE_RDV	ABILITATA / DISABILITATA	Flag che abilita o disabilita la protocollazione del rapporto di versamento
PROT_CODICE_REGISTRO	GRM	Codice Registro di protocollazione
PROT_CODICE_FASCICOLO	150.30.130/2015/INF/278	Codice Fascicolo di protocollazione
PROT_COGNOME_DESTINATARIO	Digip	Cognome destinatario per la protocollazione
PROT_EMAIL_DESTINATARIO	digip@regione.marche.it	Indirizzo mail del destinatario per la protocollazione
ALGORITMO_HASH	SHA-1	Definizione dell'algoritmo per il calcolo dell'hash
CODIFICA_HASH	HEX	Definizione della codifica per il calcolo dell'hash
INGEST_HASH_CHECK_LEVEL	ERROR_EXISTS	Livello controllo hash per la rule CONTROLLO_HASH
INGEST_HASH_CHECK_ENABLE	true	Abilitazione controllo hash di un file con quanto dichiarato nell'indice.
DEFAULT_ENCODING	windows-1252	Valore di default per la codifica encoding
TIPOLOGIA_DOCUMENTALE_MODIFICA	Registro giornaliero di protocollo	Tipologia documentale del documento di modifica
TIPOLOGIA_DOCUMENTALE_RPG	Registro giornaliero di protocollo	Tipologia documentale dei documenti di Registro giornaliero di protocollo

3.5 Configurazione Tag

Di seguito sono elencati i nomi di Tag utili ai fini del processo di archiviazione, ma anche per una maggiore praticità nella ricerca dei metadati memorizzati sul database.

Tag riferiti ai metadati del file di indice riferiti al pacchetto SIP:

NOME TAG	VALORE TAG IPOTETICO	SIGNIFICATO TAG
ID_DESCRITTORE_ORIGINE	ID_descrittore_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive il metadato identificativo (ID), presente sul file indice del SIP.
PATH_DESCRITTORE_ORIGINE	Path_descrittore_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive il metadato path, presente sul file indice del SIP.
HASH_DESCRITTORE_ORIGINE	Hash_descrittore_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive il metadato hash, presente sul file indice del SIP.

Tag riferiti ai metadati dei file allegati (originali) appartenenti al pacchetto SIP:

NOME TAG	VALORE TAG IPOTETICO	SIGNIFICATO TAG
FILEGROUP_ORIGINE	FileGroup_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive il metadato file group, presente sul file indice del SIP.
FILENAME_ORIGINE	FileName_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive il metadato nome file originale, presente sul file indice del SIP.
PATH_FILE_ORIGINE	Path_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive il metadato path del file originale, presente sul file indice del SIP.
HASH_FILE_ORIGINE	Hash_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive il metadato hash del file originale, presente sul file indice del SIP.
DATADOCUMENTO_ORIGINE	dataDocumento_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive la data originale di creazione del file di origine, presente sul file indice del SIP
ESTENSIONEFORMATO_ORIGINE	EstensioneFormato_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive l'estensione del file originale, presente sul file indice del SIP.

FORMATOFILE_ORIGINE	FormatoFile_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive il formato del file di origine, presente sul file indice del SIP.
MIMETYPE_ORIGINE	Mimetype_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive il mimetype del file di origine, presente sul file indice del SIP.
IDDOCUMENTO_ORIGINE	ID_Documento_origine	Tag che sarà presente sul file indice AIP e sul database e che descrive l'id documento del file di origine, presente sul file indice del SIP.

Tag riferiti ai metadati dei file che hanno subito trasformazioni o modifiche appartenenti al pacchetto AIP:

NOME TAG	VALORE TAG IPOTETICO	SIGNIFICATO TAG
FILEDIRECTORYWORK_AIP	FileDirectoryWork_aip	Tag che sarà presente sul file indice AIP e sul database e che descrive la directory di lavoro dell'AIP, dove verrà posto il file trasformato tramite conversion.
FILENAME_AIP	FileName_aip	Tag che sarà presente sul file indice AIP e sul database e che descrive il nome del file allegato dell'AIP dopo aver subito una trasformazione.
FORMATOFILE_AIP	FormatoFile_aip	Tag che sarà presente sul file indice AIP e sul database e che descrive il formato del file allegato dell'AIP dopo aver subito una trasformazione
MIMETYPE_AIP	Mimetype_aip	Tag che sarà presente sul file indice AIP e sul database e che descrive il mimetype del file allegato dell'AIP dopo aver subito una trasformazione
ESTENSIONEFORMATO_AIP	EstensioneFormato_aip	Tag che sarà presente sul file indice AIP e sul database e che descrive l'estensione del file allegato dell'AIP dopo aver subito una trasformazione
STOREADDRESS_FILE_AIP	StoreAddressFile_aip	Tag che sarà presente sul file indice AIP e sul database e che descrive lo store address del file allegato dell'AIP dopo aver subito una trasformazione
HASH_FILE_AIP	HashFile_aip	Tag che sarà presente sul file indice AIP e sul database e che descrive l'hash del file allegato dell'AIP dopo aver subito una trasformazione
UUID_SIP_TRANSFORM	UuidIP_trasform	Tag che sarà presente sul file indice AIP e sul database e che descrive l'id del SIP di

		riferimento da cui è stato definito l'AIP. Il tag viene utilizzato quando il SIP subisce una trasformazione.

Tag che descrive l'ID del SIP di origine per l'AIP:

NOME TAG	VALORE TAG IPOTETICO	SIGNIFICATO TAG
SIP_UUID	SipUuid	Tag che sarà presente sul file indice AIP e sul database e che descrive l'id del SIP di riferimento da cui è stato definito l'AIP

Tag definiti nel file descrittore del SIP:

NOME TAG	VALORE TAG IPOTETICO	SIGNIFICATO TAG
TAG_DESCRITTORE_FILE	sincro:File	Tag presente sul file descrittore SIP per identificare il corpo dei metadati riferiti ai file allegati
TAG_DESCRITTORE_FILENAME	sincro:ID	Tag presente sul file descrittore SIP per identificare il nome del file allegato
TAG_DESCRITTORE_INTESTAZIONE_CHIAVE	Intestazione	Tag presente sul file descrittore SIP per identificare il corpo dove si trovano le chiavi per l'identificativo del file (solo per i file no sincro)
TAG_DESCRITTORE_CHIAVE	Chiave	Tag presente sul file descrittore SIP per identificare la chiave del file (solo per i file no sincro)
TIPOLOGIA_DOCUMENTALE	sincro:TipologiaDocumentale	Tag presente sul file descrittore SIP per identificare la tipologia documentale
NUMERO_SIP_ORIGINE	Numero	Tag presente sul file descrittore SIP per identificare il numero del file (solo per i file no sincro)
ANNO_SIP_ORIGINE	Anno	Tag presente sul file descrittore SIP per identificare l'anno del file (solo per i file no sincro)
TIPOREGISTRO_SIP_ORIGINE	TipoRegistro	Tag presente sul file descrittore SIP per identificare il tipo registro
RISERVATEZZA_TAG	sincro:riservatezza	Tag presente sul file descrittore SIP per identificare il livello di riservatezza
TAG_DESCRITTORE_HASH_VERSATO	HashVersato	Tag presente sul file descrittore SIP per identificare hash
TAG_DESCRITTORE_COMPONENTE	Componente	Tag presente sul file descrittore SIP per

		identificare il componente
ATTR_DESCRITTORE_HASH_ALGORITHM	algoritmo	Attributo che identifica l'algoritmo per il calcolo dell' hash
ATTR_DESCRITTORE_HASH_ENCODING	codifica	Attributo che identifica la codifica per il calcolo dell' hash
TAG_DESCRITTORE_OGGETTO_SIP	Oggetto	Tag presente sul file descrittore SIP per identificare l'oggetto
TAG_DESCRITTORE_AIP_DA_MODIFICARE	sincro:SourceIdC	Tag presente sul file descrittore di modifica per definire il gruppo di tag che identificano il pacchetto AIP che deve essere modificato
TAG_ID_AIP_DA_MODIFICARE	sincro:ID	Tag presente sul file descrittore di modifica per definire l' identificativo del pacchetto AIP che deve essere modificato

Tag definiti nel file descrittore dell' AIP per il recupero e la persistenza dei metadati del packaging information:

NOME TAG	VALORE TAG IPOTETICO	SIGNIFICATO TAG
DESCRITTORE_PACKINF_VDC_AIP	sincro:VdC	Tag presente nel file indice dell' AIP per ritrovare il blocco dove sono presenti tutti i metadati riferiti al packaging information. Serve per recuperare e persistere sul database questi metadati (si basa sul modello standard sincro)
DESCRITTORE_PACKINF_MOREINFO_AIP	sincro:MoreInfo	Tag presente nel file indice dell' AIP per ritrovare il blocco dove sono presenti tutti i metadati riferiti al packaging information. Serve per recuperare e persistere sul database questi metadati (si basa sul modello standard sincro)
DESCRITTORE_PACKINF_MOREINFO_EMBEDDED_METADATA_AIP	sincro:EmbeddedMetadata	Tag presente nel file indice dell' AIP per ritrovare il blocco dove sono presenti tutti i metadati riferiti al packaging information. Serve per recuperare e persistere sul database questi metadati (si basa sul modello standard sincro, sottostruttura del tag sincro:MoreInfo)

Tag definiti nel file descrittore del DIP

NOME TAG	VALORE TAG IPOTETICO	SIGNIFICATO TAG
FILEDIRECTORYWORK_DIP	FileDirectoryWork_dip	Tag che sarà presente sul file indice DIP e che descrive la directory di lavoro dove verrà posto il file che ha subito una transformation.

FILENAME_DIP	FileName_dip	Tag che sarà presente sul file indice DIP e che descrive il nuovo nome del file allegato dopo aver subito la trasformazione conversion.
FORMATOFILE_DIP	FormatoFile_dip	Tag che sarà presente sul file indice DIP e che descrive il nuovo formato del file allegato dopo aver subito la trasformazione conversion.
MIMETYPE_DIP	Mimetype_dip	Tag che sarà presente sul file indice DIP e che descrive il nuovo mimetype del file allegato dopo aver subito la trasformazione conversion.
ESTENSIONEFORMATO_DIP	EstensioneFormato_dip	Tag che sarà presente sul file indice DIP e che descrive la nuova estensione del formato del file allegato dopo aver subito la trasformazione conversion.
STOREADDRESS_FILE_DIP	StoreAddressFile_dip	Tag che sarà presente sul file indice DIP e che descrive lo store address, indirizzo del repository dove è stato salvato il pacchetto DIP
HASH_FILE_DIP	HashFile_dip	Tag che sarà presente sul file indice DIP e che descrive il nuovo hash del file allegato dopo aver subito una trasformazione.
UUID_AIP_TRANSFORM	UuidIP_trasform	Tag che sarà presente sul file indice DIP e che descrive l'id dell'AIP di riferimento da cui è stato definito il DIP
AIP_UUID	aip_uuid	Tag che sarà presente sul file indice DIP e che descrive l'id dell'AIP di riferimento da cui è stato definito il DIP
AIP_UUID_MODIFICATO	AipUuid_modificato	Tag che identifica l'uuid dell'AIP modificato

Tag riferiti alla migrazione:

NOME TAG	VALORE TAG IPOTETICO	SIGNIFICATO TAG
MIGRAZIONE_AIP_UUID	MigrazioneAipUuid	Tag che identifica l'id dell'AIP che è stato migrato
MIGRAZIONE_TAG_FILE	sincro:File	Tag presente sul file descrittore AIP per identificare il corpo dei metadati riferiti ai file allegati
MIGRAZIONE_TAG_NOMEFILE	sincro:ID	Tag presente sul file descrittore AIP per identificare il nome del file allegato
MIGRAZIONE_TAG_PATH	sincro:Path	Tag presente sul file descrittore AIP per

		identificare il path del file allegato
MIGRAZIONE_TAG_HASH	sincro:Hash	Tag presente sul file descrittore AIP per identificare l'hash del file allegato

3.6 Tipologia documentale

La tipologia documentale definisce il tipo di documento che si vuole archiviare. Per ogni soggetto produttore il sistema prevede che bisogna definire tutte le tipologie documentali che si vogliono versare. Legate a queste infatti potrebbero variare i modelli di conservazione. Per questi motivi ogni tipologia documentale prevede anche precise policy.

Definire una tipologia documentale:

NOME CAMPO TABELLA	VALORE IPOTETICO	SIGNIFICATO DEL CAMPO
ID	123456789	Valore identificativo univoco per ciascuna tipologia documentale (primary key)
NOME	Documento protocollato	Nome della tipologia documentale specifica
SOGGETTO PRODUTTORE_ID	soggetto produttore_id	Identificativo del soggetto produttore a cui la tipologia documentale fa riferimento (foreign key)
DURATA CONSERVAZIONE	Da 0 a infinito	Numero di anni previsti per la conservazione dei pacchetti, per quella specifica tipologia documentale

3.7 Gestione delle policy

Le Policy sono una tipica azione standard di qualità (e quindi testata ed approvata) che viene applicata in confini delimitati e soltanto al verificarsi di ben determinate condizioni. Ogni policy è definita per soggetto produttore e per tipologia documentale. Una policy è suddivisa in rule, transformation e standard. Le rule sono regole di controllo per verificare la corretta struttura dei versamenti effettuati da parte degli utenti. Le trasformazioni invece sono processi che modificano la struttura dei file per avere una conservazione che segua i parametri definiti dalla convenzione. Gli standard sono normative approvate, alla base di una policy, possono essere intesi come documentazione consultabile.

Definizione policy:

NOME CAMPO TABELLA	VALORE IPOTETICO	SIGNIFICATO DEL CAMPO
ID	123456789	Valore identificativo univoco definito per ciascuna policy (primary key)
VERSION	Valore progressivo intero a partire da 1	Valore intero progressivo che definisce e tiene traccia delle variazioni delle policy. Il numero più alto è relativo all'ultima versione e quindi alla policy in uso
DESCRIPTION	Policy di test	Testo che serve a spiegare l'obiettivo della

		policy di riferimento
SOGGETTO PRODUTTORE_ID	soggetto produttore_id	Identificativo del soggetto produttore a cui la policy fa riferimento (foreign key)
CONTESTO	QA_SIP QA_AIP QA_DIP MIG_AIP	Il contesto si riferisce all'ambito di applicazione della policy. Nello specifico può essere applicato ad un pacchetto SIP (QA_SIP), ad un pacchetto AIP (QA_AIP), per un processo di riversamento (QA_DIP) o di migrazione (MIG_AIP).
TIPOLOGIA_DOCUMENTALE_ID	tipologia_documentale_id	Identificativo della tipologia documentale a cui la policy fa riferimento (foreign key)
ATTIVA	TRUE/FALSE	Flag che definisce se una policy è attiva e quindi da applicare

Definizione regole:

NOME CAMPO TABELLA	VALORE IPOTETICO	SIGNIFICATO DEL CAMPO
ID	123456789	Valore identificativo univoco definito per ciascuna rule (primary key)
NOME	nome_regola	Nome che identifica il tipo di regola che si vuole applicare
VERSION	Valore progressivo intero a partire da 1	Valore intero progressivo che definisce e tiene traccia delle variazioni delle regole. Il numero più alto è relativo all'ultima versione e quindi alla rule in uso
RULE	Definizione della regola	A seconda del tipo di regola viene inserita la definizione. es.Per una regola XSD verrà salvato il file xsd di trasformazione, per una regola che controlla i formati verranno inserite le estensioni dei file accettati (es .pdf .xml .jpeg)
TIPO RULE	XSD FORMATO_METADATI FORMATO_FILE RULE	Viene definito il tipo di regola che vuole essere applicata tra quelle elencate: validazione xsd del file indice (XSD), controllo dell'estensione dei formati dei file allegati definiti all'interno del file di indice (FORMATO_METADATI), controllo del formato dei file allegati se sono accettabili (FORMATO_FILE), controllo se alcuni metadati definiti nel file indice rispettano la regular expression definita dalla regola (RULE)
ATTIVA	TRUE/FALSE	Definisce se la regola è attiva e quindi applicabile oppure no

POLICY_ID	policy_id	Identificativo della policy a cui la rule fa riferimento (foreign key)
CONTESTO	FILE METADATI CROSS	Definisce se la regola deve essere applicata a tutti i file allegati (FILE), solo al file di indice e ai suoi metadati (METADATI), ad entrambi (CROSS)
RuleTARGET	nome_tag	Nome del tag a cui deve essere applicata la regola di tipo RULE

Definizione trasformazione:

NOME CAMPO TABELLA	VALORE IPOTETICO	SIGNIFICATO DEL CAMPO
ID	123456789	Valore identificativo univoco definito per ciascuna transformation (primary key)
NOME	nome_trasformazione	Nome che identifica il tipo di trasformazione che si vuole applicare
VERSION	Valore progressivo intero a partire da 1	Valore intero progressivo che definisce e tiene traccia delle variazioni delle trasformazioni. Il numero più alto è relativo all'ultima versione e quindi alla trasformazione in uso
TRASFORMAZIONE	Definizione della trasformazione	A seconda del tipo di trasformazione viene inserita la definizione. es.Per una trasformazione XSLT verrà salvato il file xslt di trasformazione, per una conversion viene salvato l'id del convertitore di riferimento, per una identity viene scritto il formato del file da non convertire (es.Portable Document Format)
TIPO TRASFORMAZIONE	XSLT CONVERSION IDENTITY_FILE IDENTITY	Viene definito il tipo di trasformazione che vuole essere applicata tra quelle elencate: trasformazione xslt di un file (XSLT), conversione di un file in un altro formato (CONVERSION), mantenere il formato del file uguale all'originale (IDENTITY_FILE), mantenere la struttura del file di indice uguale all'originale (IDENTITY)
ATTIVA	TRUE/FALSE	Definisce se la trasformazione è attiva e quindi applicabile oppure no
POLICY_ID	policy_id	Identificativo della policy a cui la trasformazione fa riferimento (foreign key)
CONTESTO	FILE METADATI	Definisce se la trasformazione deve essere applicata a tutti i file allegati (FILE), solo al file di indice e ai suoi metadati

	CROSS	(METADATI), ad entrambi (CROSS)

Definizione standard:

NOME CAMPO TABELLA	VALORE IPOTETICO	SIGNIFICATO DEL CAMPO
ID	123456789	Valore identificativo univoco definito per ciascuno standard (primary key)
VERSION	Valore progressivo intero a partire da 1	Valore intero progressivo che definisce e tiene traccia delle variazioni degli standard. Il numero più alto è relativo all'ultima versione e quindi allo standard in uso
DESCRIPTION	Standard di test	Testo che serve a spiegare il contenuto di uno standard
CONTENT	Testo della normativa	Testo della normativa
ATTIVA	TRUE/FALSE	Definisce se lo standard è attivo e quindi applicabile oppure no
POLICY_ID	policy_id	Identificativo della policy a cui lo standard fa riferimento (foreign key)

3.8 Configurazione file xslt

Il processo di archiviazione utilizza file di trasformazione XSLT per convertire in una struttura ben definita file XML. Questa procedura serve a conservare documenti in formati formalmente corretti, permettendo all'utente di versare file di indice strutturati in modi differenti. Il processo infatti prende in input file xml di diversi modelli e li converte in un modello unico, che è quello richiesto dalle specifiche di archiviazione.

I file di trasformazione sono salvati in cartelle specifiche definite dai parametri di configurazione per soggetto produttore (es. *PATH_XSLT_XX*).

Esaminiamo i singoli file.

XSLT_FITS.XSLT: file di trasformazione che prende il file output del tool FITS e lo ristruttura in un modello standard comodo al sistema.

XSLT_KIP-AIP.XSLT: file di trasformazione che prende il file KIP e lo converte in indice AIP, in un modello standard per la conservazione (es. sincro).

XSLT_AIP-KIP.XSLT: file di trasformazione che prende l'indice del pacchetto di archiviazione AIP e lo riorganizza in un modello comodo al sistema che denominiamo come KIP.

XSLT_KIP-DIP.XSLT: file di trasformazione che prende il file KIP e lo converte in indice DIP, in un modello standard per la conservazione (es. sincro).

NOTA: con il termine file KIP si intende un modello standard di file xml. Viene utilizzato dal sistema per agevolare i processi intermedi per la generazione corretta di un pacchetto di archiviazione

4. Compiti e responsabilità dei diversi ruoli assegnati agli utenti

In questo paragrafo verranno esaminati nel dettaglio i compiti e le responsabilità dei diversi ruoli che possono essere assegnati agli utenti.

I ruoli possibili sono i seguenti:

- ADMINISTRATION: l'utente admin si occupa di tutta la parte di amministrazione, configurazione e visualizzazione di tutti i processi
- INGEST: l'utente ingest si occupa della ricezione dei pacchetti di versamento (SIP) trasmessi dall'Ente produttore; verifica l'integrità e la completezza dei pacchetti; mette a disposizione del produttore il Rapporto di Versamento (RdV); genera i pacchetti di archiviazione (AIP). Può consultare la lista dei SIP ricevuti dal sistema ed effettuare il download degli stessi. Periodicamente poi viene richiesta la compilazione di un questionario con domande specifiche al suo ambito di lavoro
- ACCESS: l'utente access gestisce il flusso di richieste di documenti in uscita e la ricerca da parte dell'Ente produttore. Può consultare i documenti archiviati e conservati ed effettuarne il download tramite la generazione del pacchetto di distribuzione (DIP). Periodicamente poi viene richiesta la compilazione di un questionario con domande specifiche al suo ambito di lavoro
- PRESERVATION PLANNING: l'utente con ruolo preservation planning ricerca e favorisce il miglioramento del sistema attraverso la gestione di tutto quello che riguarda la stesura del questionario, la raccolta delle risposte, la creazione di attività e il controllo di vecchie e nuove funzionalità attraverso l'utilizzo della sandBox

Per ogni ruolo sono assegnati all'utente dei casi d'uso, cioè le singole attività che si possono fare in quello specifico ambito. Un utente quindi potrà visualizzare tutte le maschere relative ai casi d'uso dei ruoli a lui assegnati e gestirne le attività.

4.1 Ruolo Administration

L'amministratore gestisce una parte fondamentale del sistema, tutta la parte di configurazione e di controllo del sistema.

Gli utenti che hanno questo ruolo possono avere i seguenti casi d'uso.

- **Configurazioni:** definire i parametri globali per la configurazione del sistema;
- **Soggetto Produttore**: visualizzare, creare e modificare soggetti produttore
- **Dati Accordo:** definire i dettagli dell'accordo di versamento
- **Utenti:** visualizzare, creare, modificare un utente e assegnargli i ruoli
- **Esiti versamenti:** visualizzare lo stato dei versamenti
- **Visualizza AIP:** visualizzare nel dettaglio gli AIP creati e ricercare i metadati relativi
- **Gestione Policy:** visualizzare, creare e modificare le policy, le rule, le transformation e gli standard
- **Tipologia Documentale:** visualizzare, creare modificare la tipologia documentale
- **Pannello di Controllo:** avviare processi per visualizzare lo stato attuale del sistema
- **Configurazione Tag:** visualizzare e modificare il valore dei Tag utili ai processi
- **Configurazione ricerca:** visualizzare, modificare e selezionare l'etichetta per i parametri di ricerca semplice e avanzata

- **Gestione DIP:** avviare e monitorare il riversamento (da AIP a DIP)
- **Migrazione AIP:** avviare e monitorare una migrazione di AIP
- **Processo Di Scarto:** avviare e monitorare un processo di scarto

4.2 Ruolo Preservation Planning

Gli utenti che hanno il ruolo di Preservation Planning possono avere i seguenti casi d'uso.

- **Gestione Questionario:** creare, modificare e pubblicare i questionari da sottoporre ai produttori
- **Gestione Attività:** creare, modificare e visualizzare attività
- **Community:** creare, modificare, visualizzare ed eliminare community
- **Sandbox:** gestire tutta la parte relativa alla SandBox.

4.3 Ruolo Ingest

L' Ingest è il ruolo del Produttore che gestisce il processo di caricamento dei SIP.

Gli utenti che hanno questo ruolo possono avere i seguenti casi d'uso.

- **Elenco Questionari:** compilare questionari inerenti al lavoro svolto
- **Esiti Versamenti:** visualizzare l'andamento dei versamenti dei SIP, recupera il rapporto di versamento (RDV)
- **Versamento Web:** effettuare versamenti SIP tramite upload via WEB, (versamento Rest)
- **Versamento Web RPG:** effettuare specifici versamenti SIP tramite upload via WEB, con tipologia documentale *Registro giornaliero di protocollo, (versamento Rest)*
- **Versamento ZIP:** effettuare specifici versamenti di pacchetti zip, (versamento via Flusso).

4.4 Ruolo Access

L'utente a cui è stato dato il ruolo di Access ha la possibilità di eseguire query di ricerca e richiedere al sistema la generazione di DIP.

Gli utenti che hanno questo ruolo possono avere i seguenti casi d'uso.

- **Elenco Questionari:** compilare questionario inerenti al lavoro svolto
- **Gestione DIP:** generare e recuperare DIP
- **Ricerca Semplice:** ricercare e recuperare AIP tramite i suoi metadati e generare DIP
- **Ricerca Avanzata:** ricercare e recuperare AIP tramite i suoi metadati e generare DIP

5. Manuale per gli utenti

5.1 Accesso al Sistema

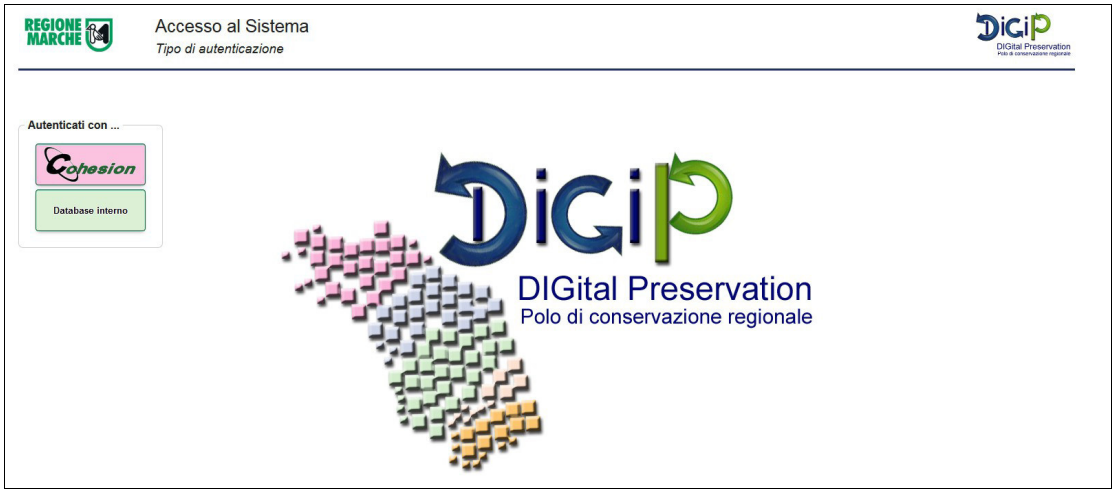
L’ accesso all'applicativo DigiP avviene tramite il framework di autenticazione Cohesion.

Vediamo di seguito i passaggi.

NOTA: si precisa che l'applicativo è compatibile con i browser Chrome, Safari, Mozilla Firefox, Opera e solo dalla versione 9 in poi di Internet Explorer.

Modalità di accesso:

- collegarsi all'applicativo DigiP attraverso l'indirizzo comunicato da Marche DigiP
- l'utente visualizzerà la seguente maschera di Accesso al sistema



- cliccare sul pulsante Cohesion 

- l'utente visualizzerà la schermata sotto e dovrà autenticarsi con una delle seguenti modalità: Smart Card, Pin Cohesion, Otp Cohesion

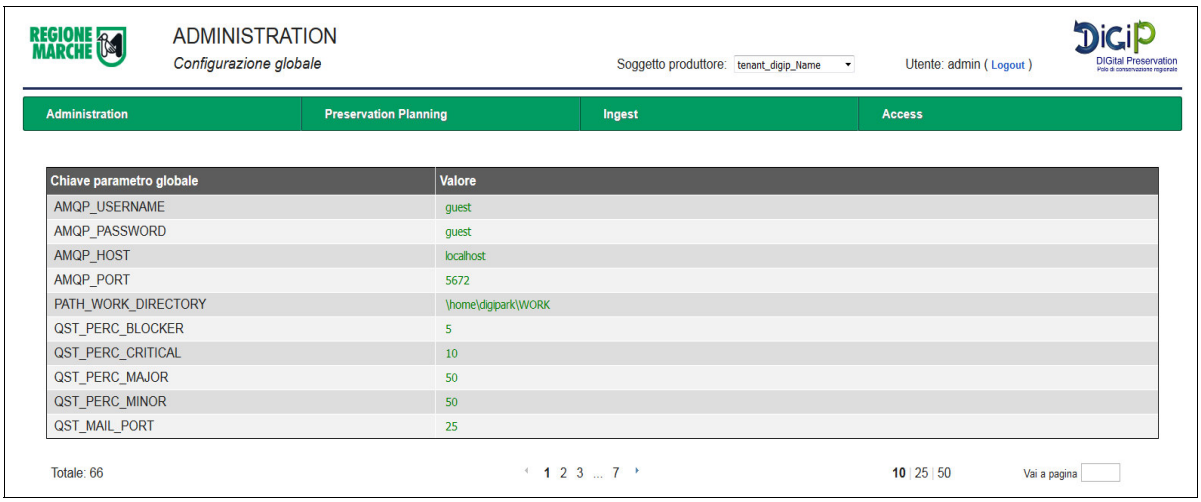
NOTA: una volta autenticati è possibile navigare il sistema. Si precisa che verranno visualizzate **solo** le maschere relative ai ruoli e casi d'uso assegnati all'utente registrato.

5.2 Area Administration

Di seguito sono illustrati tutti i casi d'uso relativi al ruolo di amministratore. Si precisa che è possibile che un utente non visualizzi tutte le maschere poichè non gli sono state assegnate quelle specifiche attività.

Configurazioni

Definizione. La maschera denominata *Configurazioni* permette all'utente amministratore di visualizzare e modificare i parametri globali di configurazione. Come mostra l'immagine, la tabella presenta l'elenco di tutti i parametri per chiave e valore parametro.



Operazioni:

1. **Creazione.** I nuovi parametri vengono creati direttamente sul database a livello sistemistico. Non è possibile inserirne di nuovi via interfaccia grafica.

2. **Modifica.** E' possibile modificare solamente il valore del parametro e non la chiave, per motivi applicativi. L'utente amministratore dovrà semplicemente cliccare sul campo che desidera cambiare, la cella diventerà editabile e quindi potrà sostituire il nuovo dato al vecchio.

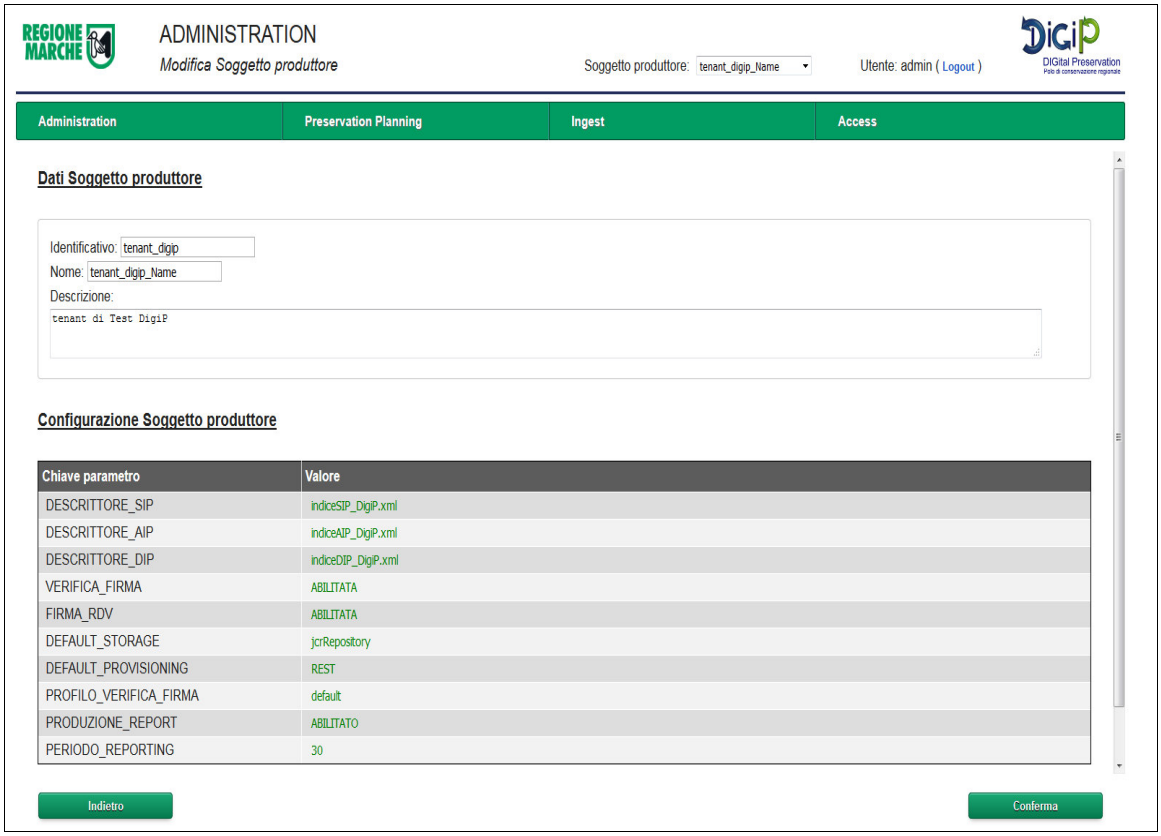
Soggetto Produttore

Definizione. La maschera denominata *Soggetto Produttore* permette all'utente amministratore di visualizzare, creare e modificare i Soggetti Produttori. La tabella presenta l'identificativo, il nome e una descrizione di tutti i Soggetti Produttori. Inoltre è presente un pulsante di modifica per ogni elemento e un pulsante di creazione.

Nota: Cliccando sulla lente di ingrandimento, presente nella colonna *Nome*, è possibile effettuare una ricerca per nome soggetto produttore.

Operazioni:

1. **Creazione.** E' possibile creare via interfaccia un nuovo Soggetto Produttore cliccando sul pulsante *Nuovo Soggetto Produttore*. Si aprirà quindi una maschera. Inserire opportunamente *Identificativo*, *Nome* e *Descrizione* nelle caselle di testo e premere il pulsante *Conferma*. Apparirà una tabella di configurazione. In questa tabella è possibile settare il valore dei parametri specifici per ogni Soggetto Produttore, cliccando direttamente sulla cella che diventerà editabile. Tornando alla schermata precedente il Soggetto Produttore appena creato sarà presente nell'elenco.
2. **Modifica.** E' possibile modificare un Soggetto Produttore cliccando sul relativo tasto *Modifica*. Si aprirà una nuova schermata dove verranno visualizzati i dettagli del Soggetto Produttore di riferimento. E' possibile modificare i valori dei campi *Nome*, *Descrizione* e *Configurazioni* cliccando sul campo ed editando il testo. Non è possibile modificare l'dentificativo per vincoli del database. Premendo il pulsante *Conferma* i nuovi valori verranno automaticamente modificati e persistiti.



Dati Accordo

Definizione. La maschera denominata *Dati Accordo* permette all'utente amministratore di visualizzare, inserire e modificare i Dati Accordo tra sistema e ente. I dati sono definiti per ogni soggetto produttore, per visualizzarli cliccare il rispettivo pulsante *Visualizza dati accordo*. Verrà visualizzato un elenco chiave\valore di parametri di accordo. E' presente un pulsante per la creazione di un nuovo valore.

Operazioni:

1. **Creazione.** E' possibile creare nuovi parametri di accordo cliccando sul pulsante *Inserisci Nuovo Dato*. Si aprirà una nuova maschera. Inserire opportunamente nelle caselle di testo una chiave identificativa e il valore correlato, premere il pulsante *Conferma*. Tornando alla schermata precedente il nuovo dato sarà presente nell'elenco.
2. **Modifica.** E' possibile modificare il valore di un dato già inserito in precedenza cliccando sul campo ed editando il testo. Non è possibile modificare la chiave per vincoli applicativi.

Utenti

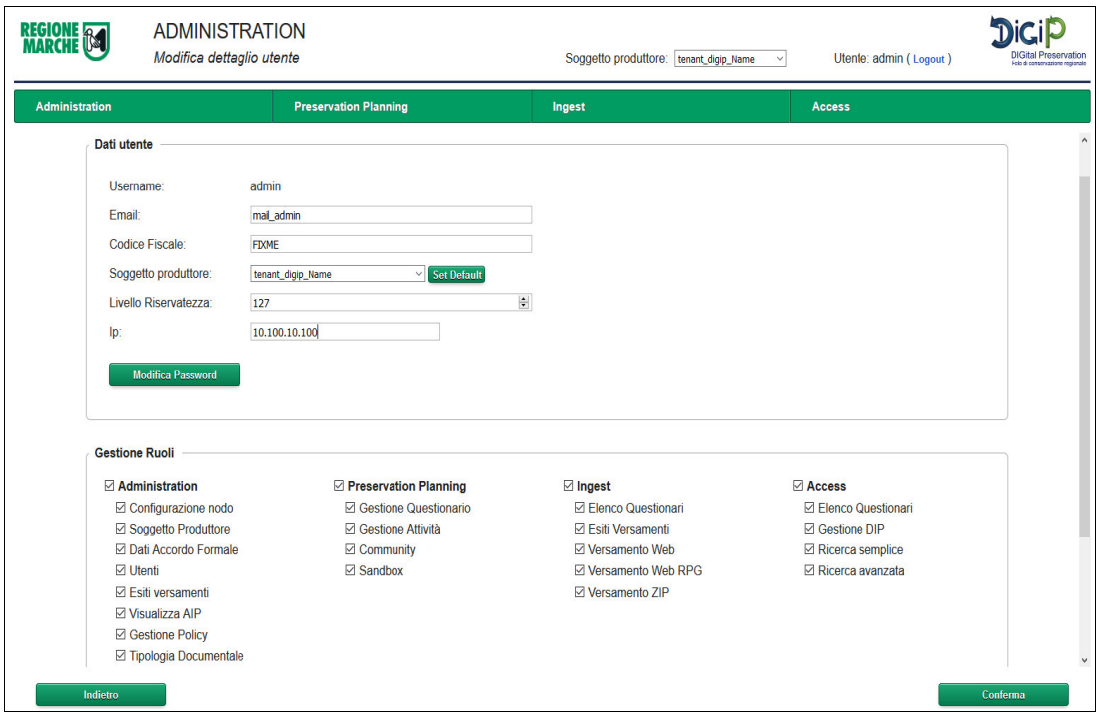
Definizione. La maschera denominata *Utenti* permette all'amministratore di visualizzare, inserire, modificare ed eliminare utenti che utilizzano l'applicativo. Come mostra l'immagine, la tabella presenta l'identificativo, il nome e la mail di tutti gli utenti. Inoltre è presente un pulsante di modifica

per ogni elemento, un pulsante di creazione e un pulsante di gestione dei dati personali dell'utente autenticato.

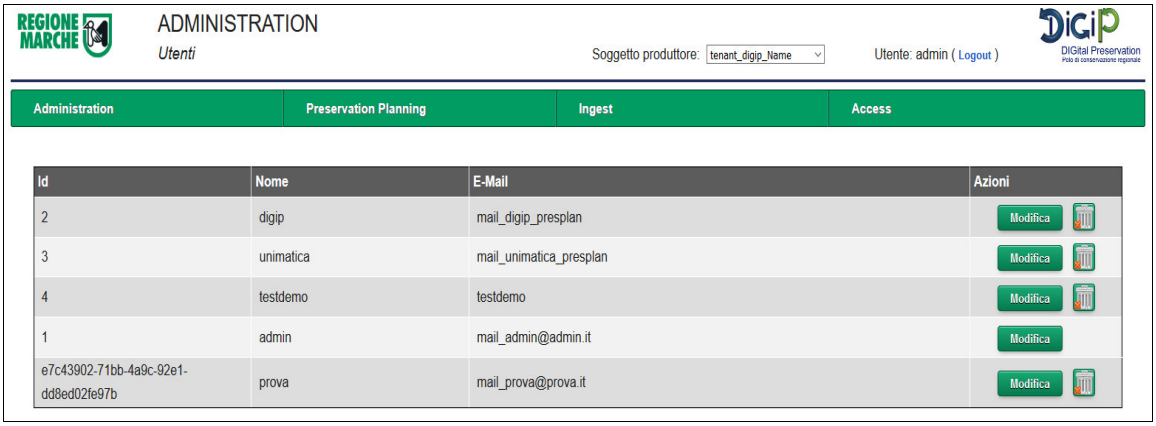
Operazioni:

1. **Creazione.** E' possibile creare nuovi utenti cliccando sul pulsante *Nuovo Utente*. Si aprirà una nuova maschera. Inserire opportunamente nelle caselle di testo *username*, *password*, *email* e *codice fiscale.* Selezionare il Soggetto Produttore di riferimento e il livello di riservatezza, cioè a che livello l'utente potrà visualizzare i pacchetti versati. A seconda delle attività che un utente può eseguire selezionare con un flag i ruoli e i relativi casi d'uso. Una volta concluso premere il pulsante *Conferma*. Tornando alla schermata precedente il nuovo utente sarà presente nell'elenco.
NOTA: la password da inserire deve essere almeno di 6 caratteri; l' username è univoco quindi se già presente nel database verrà rifiutato dal sistema.

2. **Modifica.** E' possibile modificare un Utente cliccando sul relativo tasto *Modifica*. Si aprirà una nuova schermata dove verranno visualizzati i dettagli. E' possibile modificare i valori dei campi *email* , *codice fiscale*, editando il testo, il *soggetto produttore e* il *livello di riservatezza* selezionandone uno diverso, i *ruoli-casi d'uso* inserendo o togliendo flag. Non è possibile modificare l'username per vincoli del database. I pulsanti *Set Default* e *Modifica Password* permettono rispettivamente di settare il Soggetto Produttore di default e di modificare la password di accesso. Premendo il pulsante *Conferma* i nuovi valori dell'utente verranno automaticamente modificati e persistiti.



3. **Eliminazione:** è possibile eliminare un utente cliccando sulla relativa icona del cestino che si trova sulla tabella. Verrà chiesta una conferma di eliminazione. Una volta confermato l'utente non sarà più visualizzato dalla maschera.

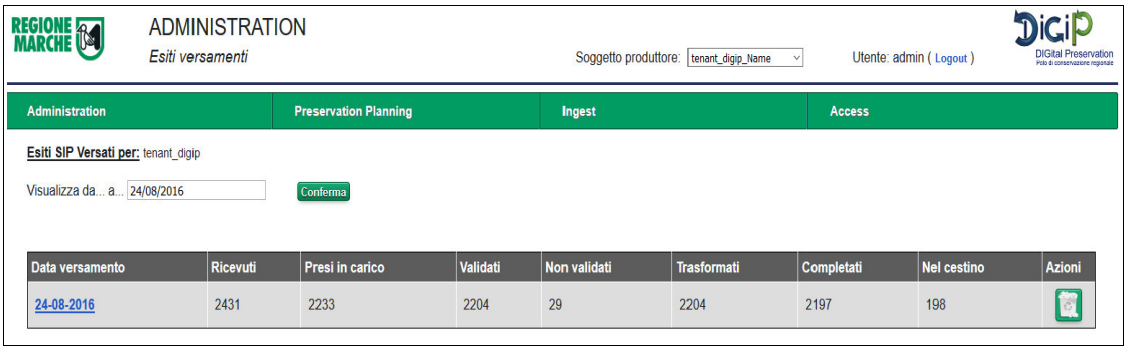


4. **Gestione dati personali:** E' possibile visualizzare direttamente i dettagli dell'utente autenticato al sistema cliccando sul pulsante *Gestione dati personali* . In questa parte inoltre è possibile modificare la sua password.

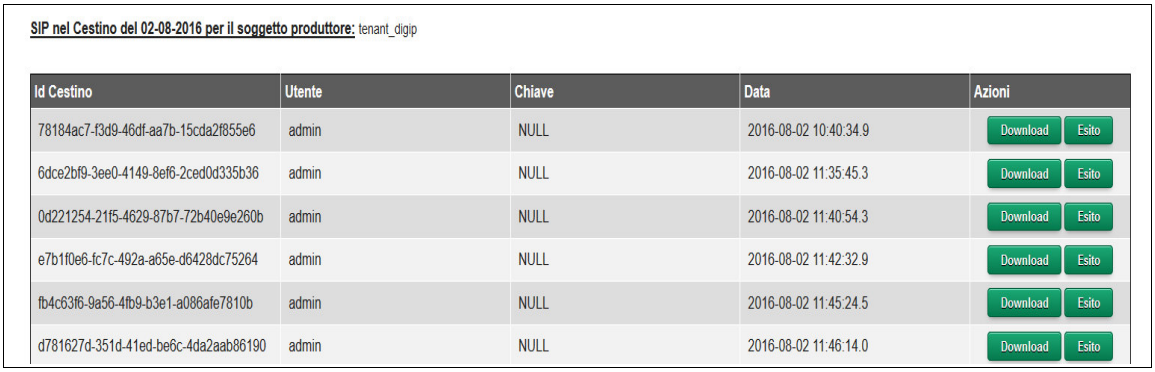
Esiti versamenti

Definizione. La maschera denominata *Esiti versamenti* permette all'utente amministratore di visualizzare, ricercare e monitorare i versamenti effettuati per uno specifico soggetto produttore. Per visualizzare i caricamenti bisogna cliccare il pulsante *Visualizza versamenti* . Si aprirà una nuova schermata dove vengono visualizzati i versamenti del giorno. Per fare una nuova ricerca si può selezionare da calendario la data o il periodo che si desidera. La tabella mostra i versamenti organizzati per data di versamento e i seguenti dettagli:

- Ricevuti: numero di versamenti effettuati dall'ente in quella specifica data. Il produttore trasmette i SIP nei modi definiti nell'accordo formale i quali vengono messi in coda per la validazione di qualità
- Presi In Carico: numero di versamenti formalmente corretti e presi in carico dal sistema
- Validati: rapporto di versamento risultato positivo. Significa che le regole di validazione definite nell'accordo formale risultano rispettate.
- Non validati: rapporto di versamento risultato negativo. Significa che le regole di validazione definite nell'accordo formale non sono rispettate.
- Trasformati: numero di versamenti che hanno subito delle trasformazioni durante il processo di archiviazione. Il sistema, una volta che il SIP è stato positivamente validato, elabora il pacchetto fino alla generazione del corrispondente pacchetto di archiviazione (AIP)
- Completati: numero di pacchetti di archiviazione generati dal corrispondente pacchetto di versamento (SIP);
- Nel cestino: numero di pacchetti di versamento (SIP) ricevuti ma che non sono conformi agli accordi formali concordati tra il Produttore e il Polo di conservazione.



- Azioni: cliccando sull'icona del *Cestino* si possono visualizzare tutti i pacchetti che sono stati scartati in quella determinata data e quindi non sono stati presi in carico dal sistema. La tabella mostra l'utente che ha effettuato il versamento, la chiave cioè il nome del pacchetto versato, la data e due link: *Download* che permette di recuperare il pacchetto zip versato e *Esito* che mostra il codice e il messaggio di errore.



Operazioni:

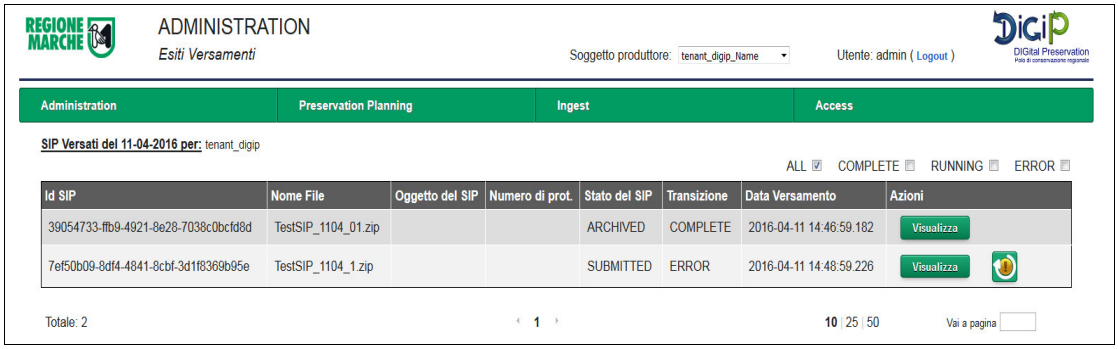
1. **Visualizza Versamenti.** Per visualizzare i versamenti cliccare sulla data versamento. Si aprirà una nuova schermata che mostra in dettaglio l'elenco di tutti i versamenti effettuati in quel giorno e lo stato in cui si trovano:
   - NOT_VALIDATED: Sip che non è stato preso in carica
   - ARCHIVED: Sip archiviato correttamente
   - RUNNING: procedura di archiviazione ancora in corso
   - ERROR: Sip andato in errore e non archiviato correttamente.

   E' possibile filtrare l'elenco dei versamenti per stato del SIP.

   Quando un Sip non è stato archiviato correttamente è possibile ripristinare il versamento. Il processo di ripristino consiste in un riversamento del pacchetto dal passaggio precedente al momento dell'errore. Prima di avviare il processo l'amministratore deve prima identificare quale sia stato il problema che ha generato l'errore. Una volta individuato capire se è

possibile correggere il problema, e in caso affermativo effettuare la modifica. In seguito avviare il ripristino cliccando sull'icona a lato (es. ) .

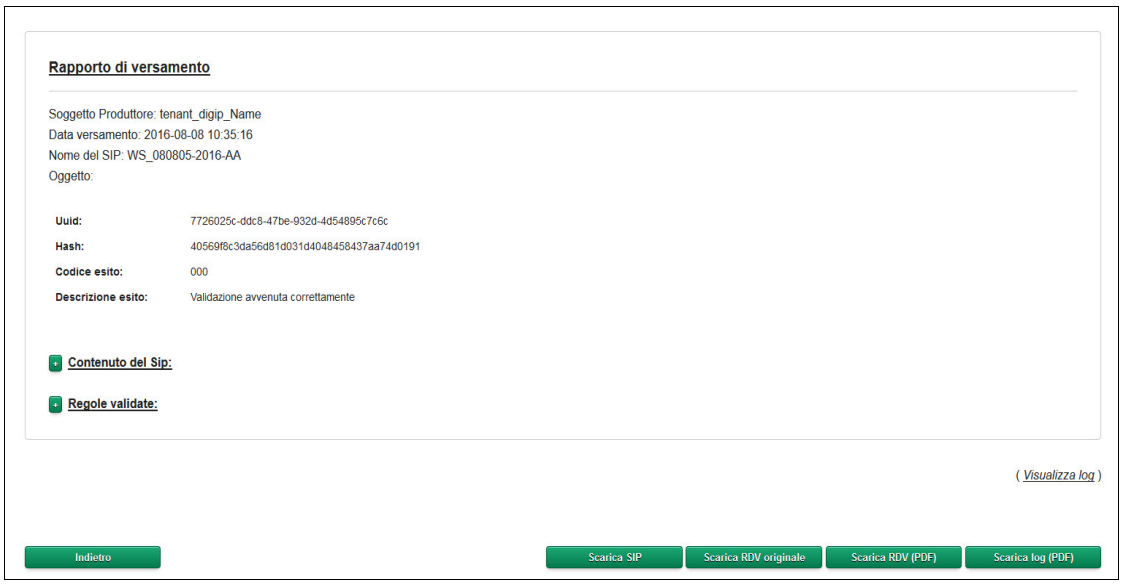
Da questa maschera cliccando sul pulsante *Scarica csv* è possibile scaricare un file csv con l'elenco di tutti i versamenti del giorno.



Premendo il pulsante *Visualizza* viene mostrato il rapporto di versamento dove è specificato in dettaglio l'esito del versamento, il contenuto del pacchetto e l'elenco delle regole validate con i relativi risultati. Cliccando su *Visualizza Log* vengono mostrati i passaggi operativi del sistema.

Da questa maschera è possibile scaricare:

- SIP di partenza, pulsante *Scarica SIP*
- rapporto di versamento (firmato o non firmato a seconda della configurazione definita dal soggetto produttore), pulsante *Scarica RDV originale*
- rapporto di versamento in formato PDF, pulsante *Scarica RDV (PDF)*
- il log in formato PDF, pulsante *Scarica log (PDF)*

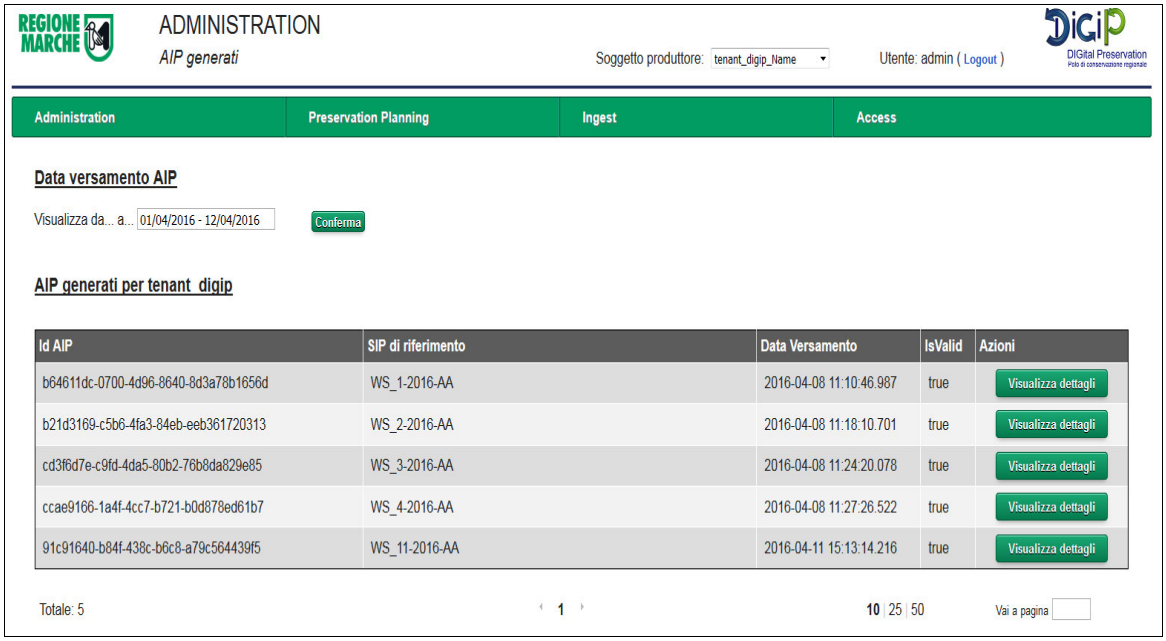


Visualizza AIP

Definizione. La maschera denominata *Visualizza AIP* permette all'utente amministratore di visualizzare, ricercare e scaricare pacchetti di archiviazione (AIP) generati dal processo. I dati sono definiti per soggetto produttore. Per visualizzare un AIP bisogna cliccare il pulsante *Visualizza AIP* .

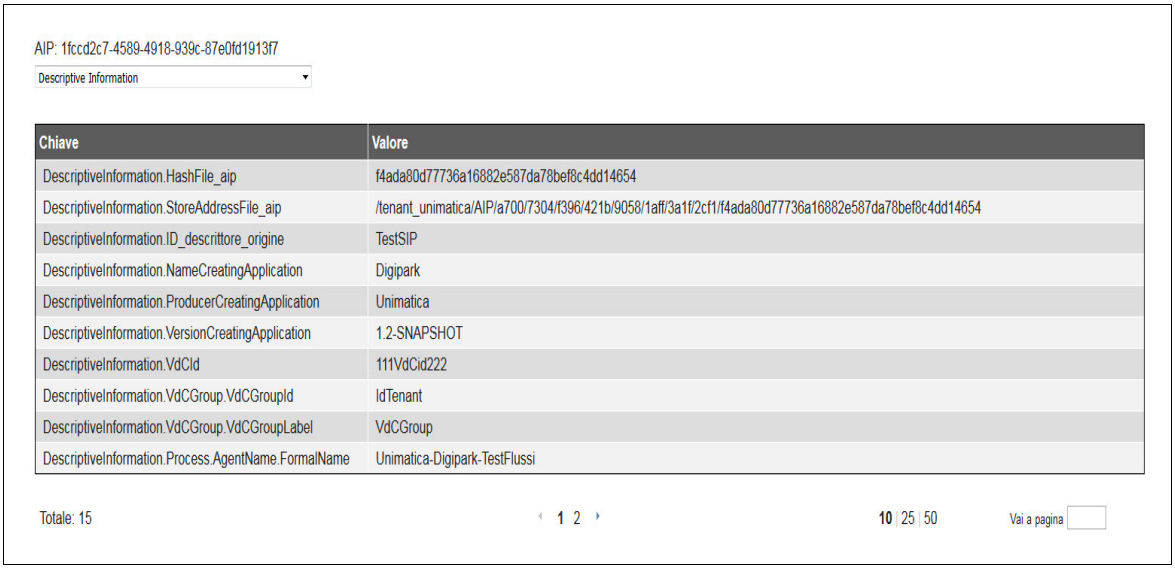
Operazioni:

1. **Visualizza AIP.** Per visualizzare gli AIP creati relativi ad un determinato soggetto produttore cliccare sul pulsante *Visualizza AIP*. Si aprirà una nuova maschera dove sarà possibile fare una ricerca per data versamento del SIP di riferimento. Se presenti, la ricerca mostrerà una tabella con l'elenco degli AIP archiviati: nel dettaglio viene mostrato il suo identificativo univoco, il nome del pacchetto SIP di riferimento, la data del versamento, se l'AIP è ancora valido o è stato modificato. Alla fine è posto un pulsante *Visualizza dettagli*.



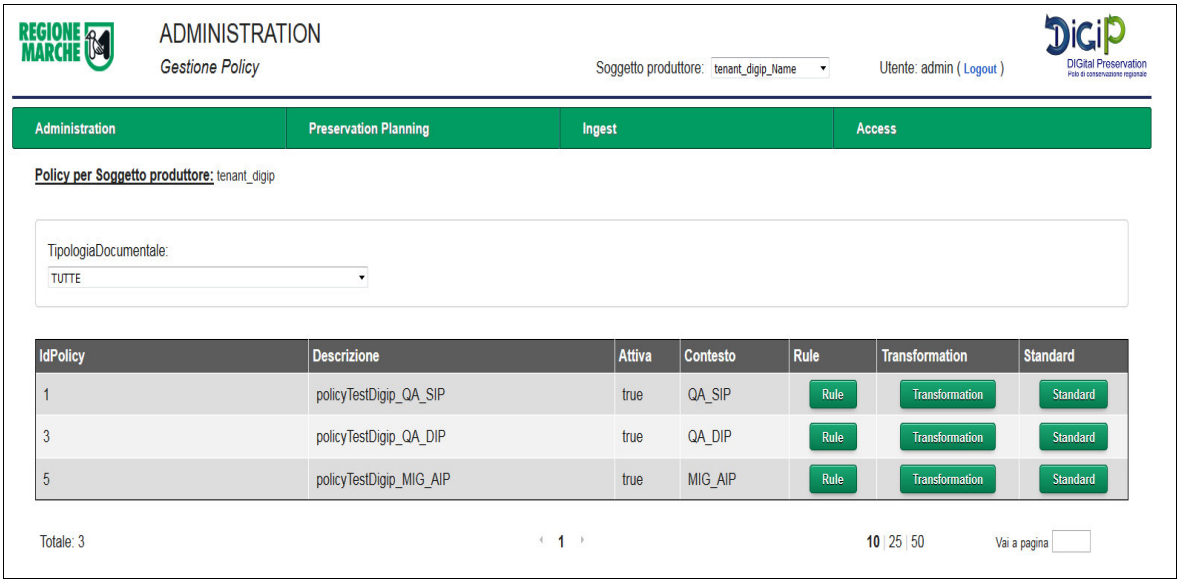
2. **Visualizza dettaglio AIP.** Una volta trovato il pacchetto di archiviazione è possibile visualizzarne i dettagli, nello specifico:
   - i metadati corrispondenti al descrittore AIP, cliccando il pulsante *Visualizza Metadati*
   - l'elenco dei file allegati all'AIP
   - i metadati di ogni file allegato, cliccando il corrispondente pulsante *Visualizza Metadati*
   - il pacchetto AIP (formato .zip), che si può scarica cliccando il pulsante *Scarica AIP*
   - l'elenco degli AIP di riferimento, nel caso in cui siano state effettuate modifiche ai metadati del pacchetto già archiviato. Anche per ciascuno di questi AIP è possibile visualizzare i dettagli cliccando sul pulsante corrispondente.

NOTA: la visualizzazione dei metadati è suddivisa per tipologia (come sono salvati sul database). Sono elencate le tipologie in un menù a tendina e ad ogni selezione viene visualizzata una tabella con i valori di riferimento.



Gestione Policy

Definizione. La maschera denominata *Gestione Policy* permette all'utente amministratore di visualizzare, inserire e modificare le policy applicative. I dati sono definiti per ogni soggetto produttore e per visualizzarli cliccare il rispettivo pulsante *Visualizza Policy*. Si aprirà una nuova schermata dove vengono visualizzate tutte le policy che possono essere filtrate per tipologia documentale, selezionandola da menù a tendina. La tabella descrive le policy, il contesto in cui operano, se sono ancora operative e tre pulsanti che rimandano rispettivamente alle maschere di gestione delle Rule, delle Transformation e degli Standard.



Operazioni:

1. **Creazione Policy.** E' possibile definire una nuova policy premendo il pulsante *Nuova Policy*. Selezionare la tipologia documentale, inserire una descrizione, il contesto operativo e se la

si vuole rendere già operativa scegliere TRUE nella sezione *Attiva.* Una volta terminato cliccare su *Conferma.*

2. **Creazione Rule\Transformation\Standard.** E' possibile definire nuove Rule\Transformation\Standard. Il procedimento è il medesimo per tutte e tre le tipologie. Vediamo nel dettaglio le rule. Cliccare sul pulsante *Nuove Rule* e definire un nome, selezionare il tipo di regola da applicare tra quelle proposte, selezionare un contesto, inserire la regola, se la rule agisce su un tag preciso inserire il nome del tag da controllare e se la si vuole rendere già operativa mettere a true il campo *Attiva*. Una volta terminato cliccare su *Conferma.*

3. **Modifica Policy.** E' possibile modificare una policy direttamente dalla tabella cliccando su i suoi campi. Si può modificare il testo della descrizione, attivare\disattivare la policy e cambiare il contesto selezionandone uno diverso. Per motivi di vincoli sul database non è possibile modificare l'identificativo.

4. **Modifica Rule\Transformation\Standard.** E' possibile modificare Rule\Transformation\Standard già operative. La modifica implica la disattivazione del precedente oggetto e la creazione di uno nuovo versionato e attivato. Il procedimento è il medesimo per tutte e tre le tipologia. Vediamo nel dettaglio le rule. Cliccare sul pulsante *Modifica*, correggere il campo desiderato e premere il pulsante *Conferma*. Tornati alla schermata precedente verranno visualizzate entrambe le rule, la nuova e quella modificata che sarà settata non più attiva (false).

NOTA: Definiamo alcuni campi.

- Contesto di una policy: definisce il processo di riferimento dove deve essere applicata. I contesti sono tre:
  - QA_SIP: che sta per quality assurance SIP, cioè sono tutte quelle policy che vengono applicate ad un SIP quando si vuole generare un AIP.
  - QA_DIP: che sta per quality assurance DIP, cioè sono tutte quelle policy che vengono applicate ad un AIP quando si vuole generare un DIP.

- MIG_AIP: che sta per migrazione AIP, cioè sono tutte quelle policy che vengono applicate ad un AIP quando si sta applicando una migrazione.

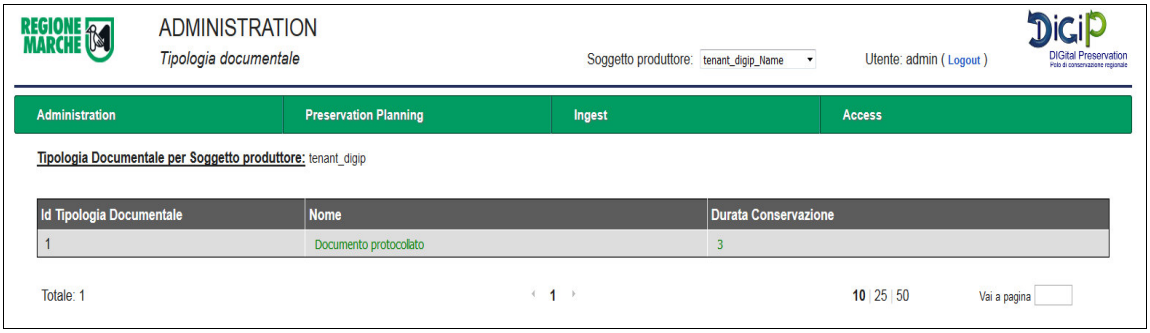
- Contesto di una Rule\Transformation: definisce su quale oggetto del pacchetto Sip è applicata la regola\trasformazione. I contesti sono tre:
  - FILE: la regola\trasformazione agisce sui file allegati dell'information package
  - METADATI: la regola\trasformazione agisce sul file xml di indice dell'information package e sui metadati presenti.
  - CROSS: la regola\trasformazione agisce su tutto l'information package, sui file allegati e sul file xml di indice
- Tipo Rule: definisce la regola che verrà applicata durante il processo. Allo stato attuale le regole sono :
  - XSD: la regola fa un controllo di validazione strutturale dell'indice del pacchetto di versamento. Di base lavora con contesto METADATI. Per definire la regola bisogna copiare il file XSD che si vuole utilizzare.
  - FORMATO_FILE: la regola controlla che i file allegati al pacchetto di versamento abbiano un formato accettato per la conservazione. Di base lavora con contesto FILE. Per definire la regola bisogna inserire le estensioni dei formati che si desidera accettare, separati da uno spazio(esempio .pdf .xml .doc).
  - FORMATO_METADATI: la regola controlla che i nomi dei file definiti all'interno dell'indice del pacchetto di versamento coincidano con il nome dei file allegati e inoltre che il formato sia un formato accettato per la conservazione. Di base lavora con contesto CROSS. Per definire la regola bisogna inserire le estensioni dei formati che si desidera accettare, separati da uno spazio(esempio .pdf .xml .doc).
  - RULE: la regola controlla che uno specifico tag dell'indice del pacchetto di versamento rispetti una determinata regular_expression. Di base lavora con contesto METADATI. E' opportuno con questa regola valorizzare anche il campo *Tag_da_controllare* con il nome specifico del tag presente nel file, su cui agisce la regola. Per definire la regola bisogna inserire la regular expression che si vuole applicare (es. [A-Za-z0-9]).
  - CONTROLLO_HASH: la regola controlla che il valore dell'hash dei file allegati, definito nell'indice del pacchetto di versamento, sia stato calcolato correttamente. Di base lavora con contesto FILE. Per definire la regola bisogna inserire il nome del tag presente nell'indice del pacchetto di versamento che definisce l'hash del file versato (es. HashVersato)
- Tipo Trasformazione: definisce la trasformazione che verrà applicata durante il processo. Allo stato attuale le trasformazioni sono:
  - XSLT: viene applicata al file di indice del pacchetto di versamento una trasformazione xslt, per convertirlo in un formato standard. Di base lavora con contesto METADATI. Per definire la transformation bisogna copiare il file XSLT che si vuole utilizzare.
  - CONVERSION: viene convertito il formato del file in input in un formato richiesto e accettato dalle direttive per la conservazione dei documenti. Di base lavora con entrambi i contesti FILE e CROSS a seconda dei casi d'uso. Per definire la trasformazione bisogna inserire il valore dell'identificativo (primary key) del plugin di conversione da applicare.

- IDENTITY: viene effettuata un trasformazione xslt identica sul file xml di indice del pacchetto di versamento. Di base lavora con contesto METADATI. Per definire la transformation bisogna copiare il file XSLT_identity.
- IDENTITY_FILE: viene effettuata un trasformazione xslt identica sul file allegato al pacchetto di versamento. La trasformazione viene effettuata solo sui file che risultano dello stesso formato definito dalla trasformazione. Di base lavora con contesto FILE. Per definire la trasformazione bisogna inserire il nome per esteso del formato del file da prendere in esame.

  NOTA: è indispensabile che per ogni tipo di file che si vuole versare sia presente una trasformazione *Conversion*, se il file deve essere convertito in un altro formato o *Identity_file,* se il file non deve subire modifiche.

Tipologia Documentale

Definizione. La maschera denominata *Tipologia Documentale* permette all'utente amministratore di visualizzare, inserire e modificare le tipologie documentali applicative. I dati sono definiti per ogni soggetto produttore e per visualizzarli cliccare il rispettivo pulsante *Visualizza*. Si aprirà una nuova schermata dove apparirà una tabella che descrive l'identificativo, il nome e la durata di conservazione dei tipi di documenti presenti.

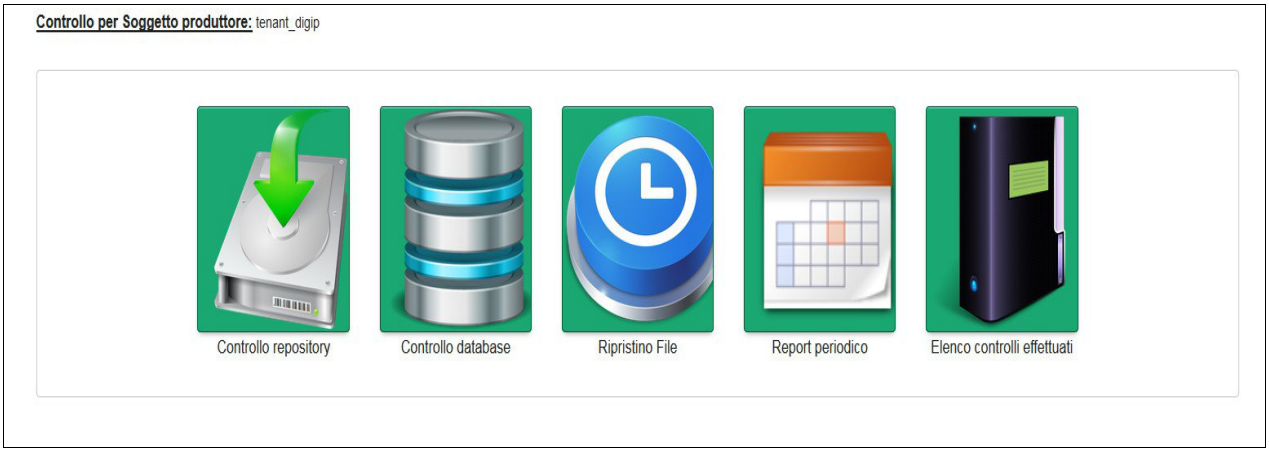


Operazioni:

1. **Creazione.** E' possibile creare una nuova tipologia documentale cliccando sul pulsante *Nuova tipologia documentale*. Inserire il nome del nuovo tipo e la durata di conservazione, definita in anni, dei pacchetti di archiviazione relativi a questa determinata tipologia (valore numerico intero). Una volta terminato premere il pulsante *Conferma.*
2. **Modifica.** E' possibile modificare una tipologia documentale direttamente dalla tabella cliccando su i suoi campi. Si può modificare il testo del nome e cambiare il numero di anni di conservazione dei documenti. Per motivi di vincoli sul database non è possibile modificare l'identificativo.

Pannello di Controllo

Definizione. La maschera denominata *Pannello di controllo* permette all'utente amministratore di avviare processi per il controllo dello stato attuale del sistema. Di seguito l'elenco dei tipi di controlli permessi che possono essere eseguiti sia sullo storage che sul database.

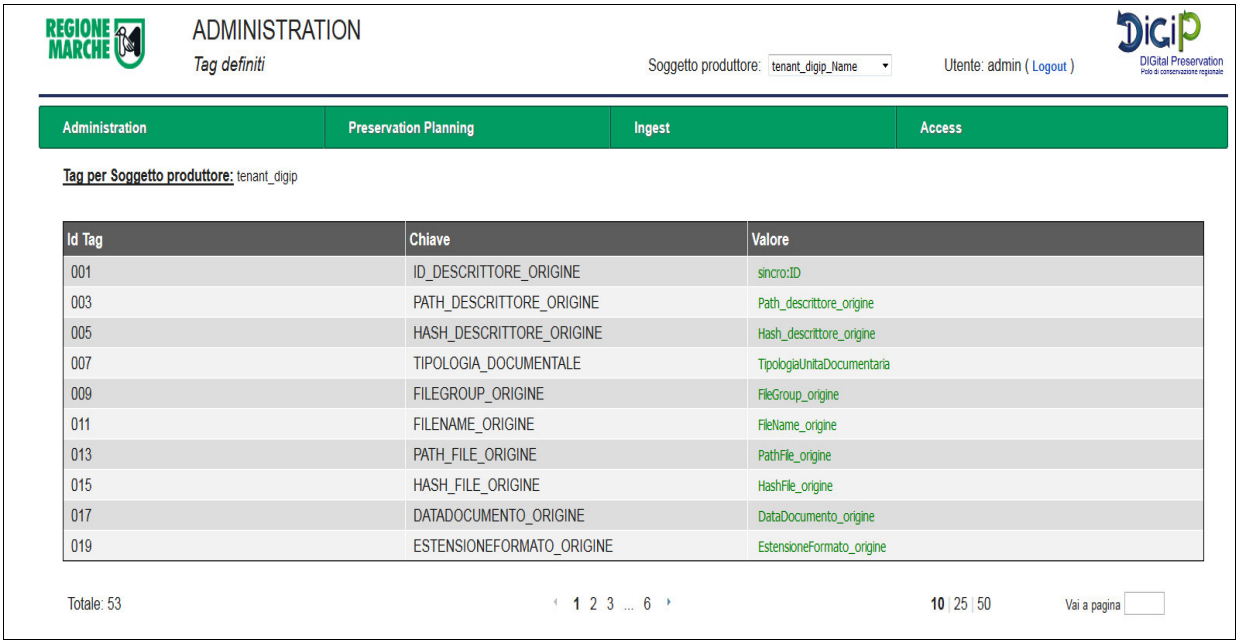


- Controllo repository: avvia processi per il calcolo della dimensione e del numero di file presenti sullo storage e per il controllo dell'integrità (hash corretto) di questi file.
- Controllo database: avvia processi per il calcolo del numero di file presenti sul database, del numero di pacchetti SIP, AIP e DIP caricati e generati.
- Ripristino File: avvia, per ogni file risultato corrotto al controllo dell'integrità, un processo di ripristino del file. Nello specifico se il file appartiene ad un SIP, allora il recupero sarà effettuato a livello sistemistico con l'utilizzo di file backup; se invece appartiene ad un AIP allora viene preso il file originale del SIP di riferimento, applicate le trasformazioni opportune e salvato il file sul repository.
- Report periodico: viene creato un report che riporta per soggetto produttore l'utilizzo del sistema in un preciso periodo di tempo definito dall'amministratore in fase di configurazione. Nella maschera del report periodico sono possibili due azioni: *Download* e *Cancella.* La prima permette di scaricare il report del periodo di riferimento, la seconda invece permette di cancellare definitivamente questo file dalla cartella dove è stato salvato e quindi in futuro non sarà più possibile visualizzarlo.
- Elenco controlli effettuati: la tabella riporta per soggetto produttore l'elenco dei processi avviati in precedenza e i relativi risultati. E' possibile filtrare per tipo di processo.

  NOTE OPERATIVE: Per avviare un processo premere il pulsante *ESEGUI* . Una volta concluso verrà mostrato lo stato del processo e il risultato. I processi di conteggio sono lavori che, a seconda della dimensione del database e del repository possono durare a lungo. Premendo il pulsante *Refresh* si può monitorare e definire concluso il processo attivato. Appena partito il lavoro è possibile anche bloccare il thread premendo il pulsante *STOP* (che appare solo quando un processo è in corso).

Configurazione Tag

Definizione. La maschera denominata *Configurazione Tag* permette all'utente amministratore di visualizzare e modificare i valori dei tag applicativi. I dati sono definiti per ogni soggetto produttore e per visualizzarli bisogna cliccare il rispettivo pulsante *Visualizza*. Si aprirà una nuova schermata dove apparirà una tabella che descrive l'identificativo, la chiave e il valore dei tag utilizzati dal sistema.



Id Tag	Chiave	Valore
001	ID_DESCRITTORE_ORIGINE	sincro:ID
003	PATH_DESCRITTORE_ORIGINE	Path_descrittore_origine
005	HASH_DESCRITTORE_ORIGINE	Hash_descrittore_origine
007	TIPOLOGIA_DOCUMENTALE	TipologiaUnitaDocumentaria
009	FILEGROUP_ORIGINE	FileGroup_origine
011	FILENAME_ORIGINE	FileName_origine
013	PATH_FILE_ORIGINE	PathFile_origine
015	HASH_FILE_ORIGINE	HashFile_origine
017	DATADOCUMENTO_ORIGINE	DataDocumento_origine
019	ESTENSIONEFORMATO_ORIGINE	EstensioneFormato_origine

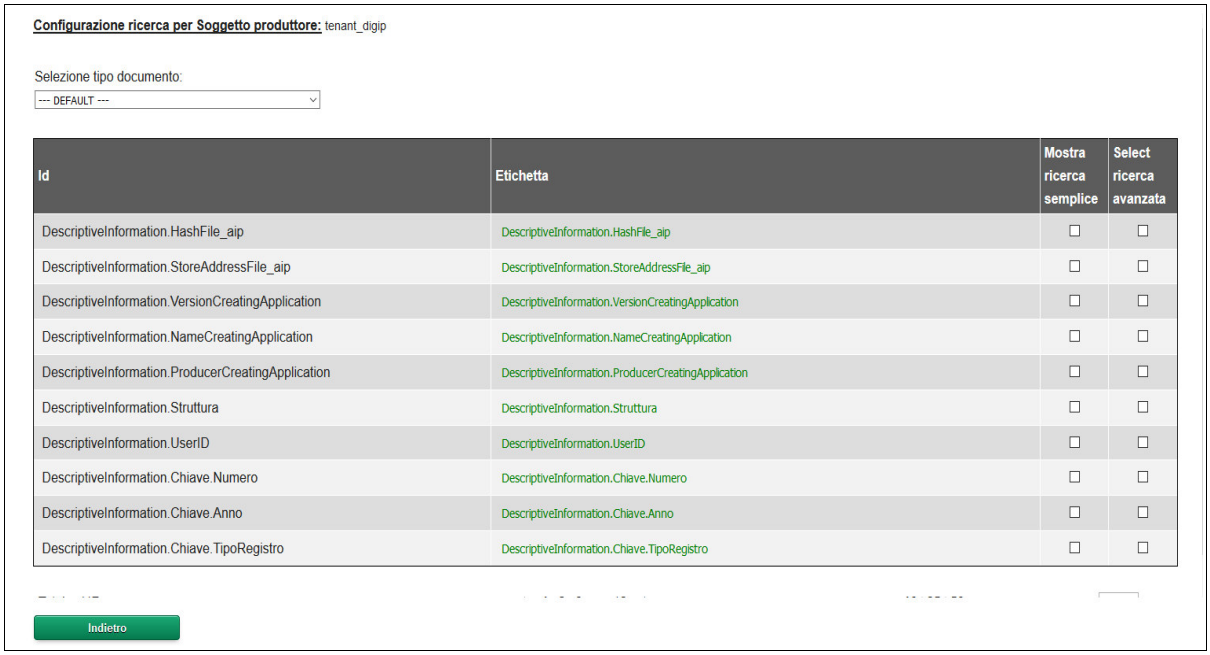
Operazioni:

1. **Creazione.** La creazione è permessa solo a livello sistemistico
2. **Modifica.** E' possibile modificare il valore di un tag direttamente dalla tabella cliccando sul campo. La cella diventerà editabile e quindi si potrà sostituire il nuovo valore al precedente. Per motivi di vincoli sul database non è possibile modificare l'identificativo e per motivi applicativi del processo non è possibile modificare la chiave.

Attenzione: i tag sono elementi fondamentali per tutti i processi applicati dal sistema. La modifica del valore quindi deve essere fatta con cautela e soprattutto riportata anche nei file di trasformazione xslt se presentano il tag in questione.

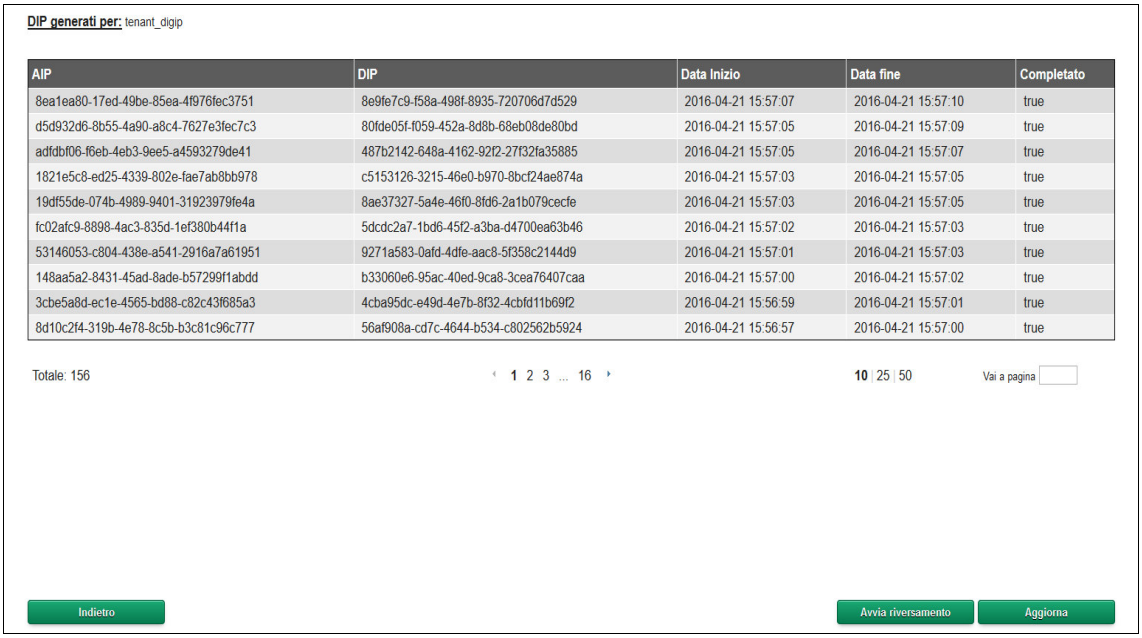
Configurazione ricerca

Definizione. La maschera denominata *Configurazione Ricerca* permette all'utente amministratore di selezionare e definire i tag necessari per la ricerca degli AIP tramite i suoi metadati. L'amministratore, dopo aver selezionato la tipologia documentale di riferimento, potrà scegliere quale informazione relativa al pacchetto utilizzare al momento della ricerca semplice e/o avanzata (vedi dettaglio nella sezione *Access: Ricerca Semplice* e *Ricerca Avanzata*). Inoltre è possibile editare il testo relativo al nome da dare alle etichette, così da rendere la ricerca più chiara e intuitiva per l'utente.



Gestione DIP

Definizione. La maschera denominata *Gestione DIP* permette all'utente amministratore di avviare un processo di riversamento di tutti gli AIP appartenenti ad un preciso soggetto produttore, per la creazione dei DIP corrispondenti. Per visualizzare il processo cliccare sul pulsante *Riversamento* del soggetto produttore corrispondente. Si aprirà una nuova schermata. Per avviare il Riversamento premere il pulsante *Avvia Riversamento*. A seconda del numero di AIP presenti sul database il processo potrebbe essere più o meno lungo. Nella tabella verranno mostrati tutti gli AIP presi in carico e premendo il pulsante *Refresh* si può tenere monitorato il lavoro di generazione DIP. In caso di errore le colonne Data Inizio e Data Fine saranno valorizzate e nella colonna "*Completato*" ci sarà il valore *false*. Se queste colonne non hanno tutte un valore vuol dire che il processo è ancora in corso, quindi premere il pulsante *Refresh* e attendere. Una volta concluso il processo tutti i DIP generati possono essere recuperati nella directory definita dal parametro di configurazione PATH_RIVERSAMENTO, relativo al soggetto produttore su cui si sta lavorando.



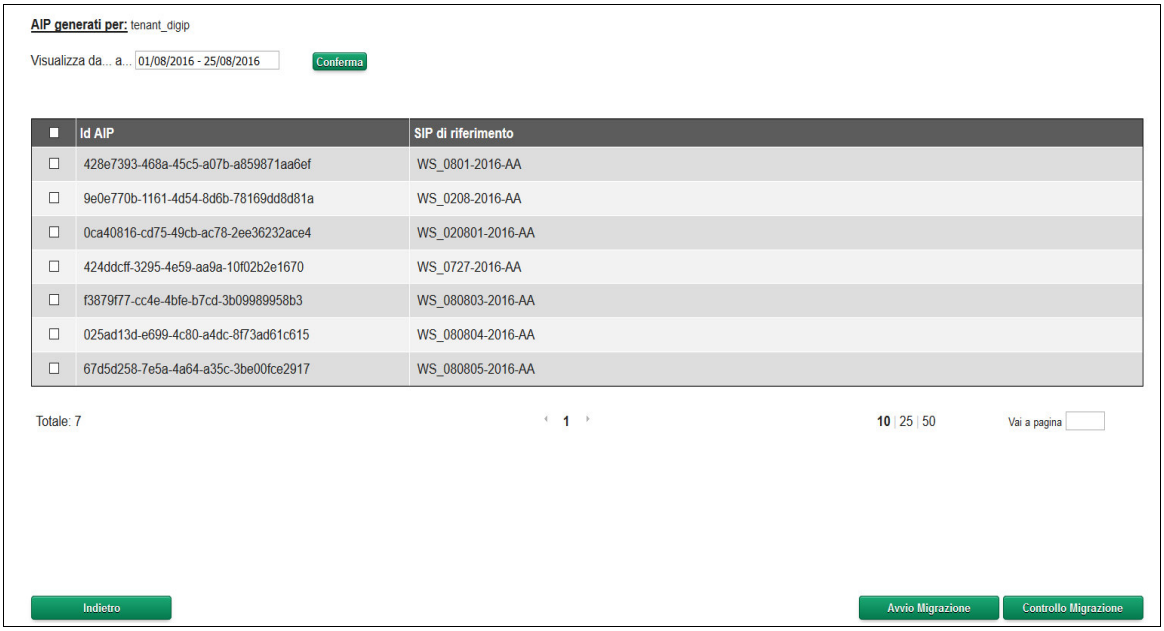
Migrazione AIP

Definizione. La maschera denominata *Migrazione AIP* permette all'utente amministratore di avviare un processo di migrazione di pacchetti di archiviazione (AIP) appartenenti ad un preciso soggetto produttore. La migrazione è un processo che subentra quando a causa di variazioni a livello di politiche di conservazione risulta opportuno modificare elementi già archiviati. Per visualizzare il processo cliccare sul pulsante *Visualizza.*

Operazioni:

1. **Avvio Migrazione.** Il processo di migrazione può essere effettuato o su tutti gli AIP o solo su quelli selezionati dall'utente. Cercare i pacchetti di archiviazione per data versamento. Selezionare solo quelli che si intende migrare e premere il pulsante *Avvio Migrazione*.
2. **Controllo Migrazione.** Premendo il pulsante *Controllo Migrazione* è possibile monitorare il processo appena avviato: lo stato del processo comunica se la migrazione per ciascun AIP è andata a buon fine (COMPLETE), se sta ancora lavorando (RUNNING) o se ci sono stati errori (ERROR). Premendo il pulsante *Refresh* si aggiorna lo stato del processo.

Attenzione: prima di avviare un processo di migrazione è importante definire le trasformazioni che il processo deve effettuare sui pacchetti di archiviazione. Per le modalità di creazione di una nuova transformation si rimanda al paragrafo relativo alla gestione Policy.

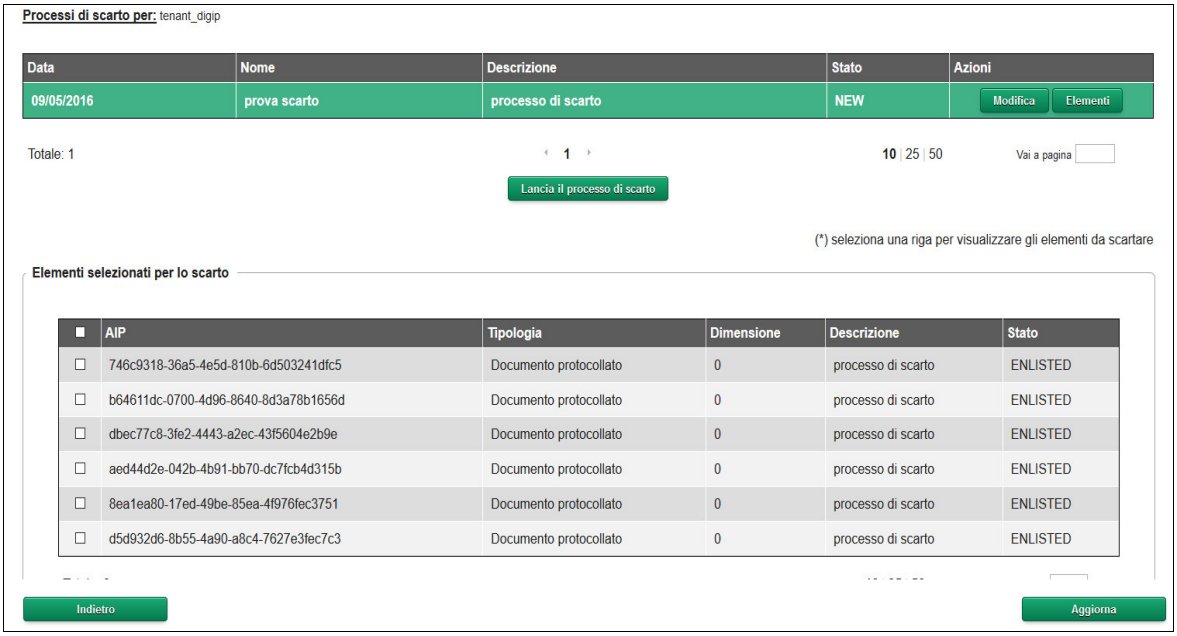


Processo Di Scarto

Definizione. La maschera denominata *Processo di Scarto* permette all'utente amministratore di avviare la cancellazione/scarto degli AIP, appartenenti ad un preciso soggetto produttore, che hanno superato la durata di conservazione (data di scarto). Per visualizzare un processo o eseguirne uno già creato cliccare sul pulsante *Processi*, mentre per crearne uno nuovo premere *Crea Processo*.

Operazioni:

1. **Crea processo:** E' possibile definire un nuovo processo di scarto, per un determinato soggetto produttore, inserendo titolo e descrizione. Cliccando poi sul pulsante *Crea processo* i valori verranno persistiti sul database e verrà dato un identificativo univoco utile al momento dell'esecuzione.
2. **Processi:** si possono visualizzare tutti i processi, la loro data di creazione, nome, descrizione e lo stato in cui si trova (NEW, RUNNING, COMPLETE, ERROR). Inoltre cliccando sul pulsante *Modifica* sarà possibile modificare titolo e descrizione. Cliccando invece *Elementi* apparirà una maschera dove è possibile visualizzare e selezionare gli AIP che hanno una data di scarto inferiore o uguale alla data odierna. Inoltre è possibile selezionare tutti gli AIP che si vogliono effettivamente eliminare dal database. Basta applicare un flag e premere il pulsante *Aggiungi selezionati* , automaticamente i record verranno collegati, tramite una foreign key, all'identificativo del processo che si sta costruendo. Tornando alla schermata precedente e selezionando la riga del processo che si vuole lanciare, apparirà una tabella contenente gli AIP. Questi è ancora possibile toglierli dalla lista di cancellazione selezionandoli e cliccando sul pulsante *Rimuovi dalla lista*. Una volta definito l'elenco degli oggetti da eliminare definitivamente dal database, cliccare sul pulsante *Lancia il processo di scarto*. Nella colonna Stato, si può seguire l'andamento del processo.

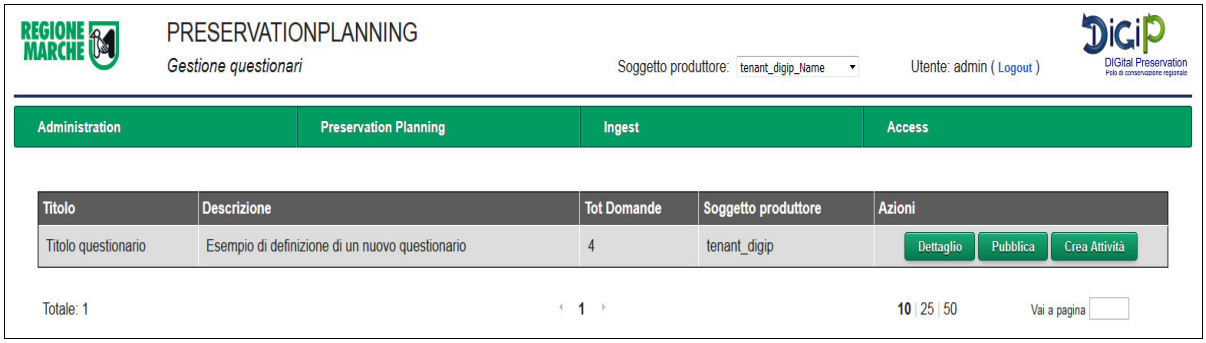


5.3 Area Preservation Planning

Di seguito verranno illustrati tutti i casi d'uso relativi al ruolo di preservation planning. Si precisa che è possibile che un utente non visualizzi tutte le seguenti maschere poichè non gli sono state assegnate quelle specifiche attività.

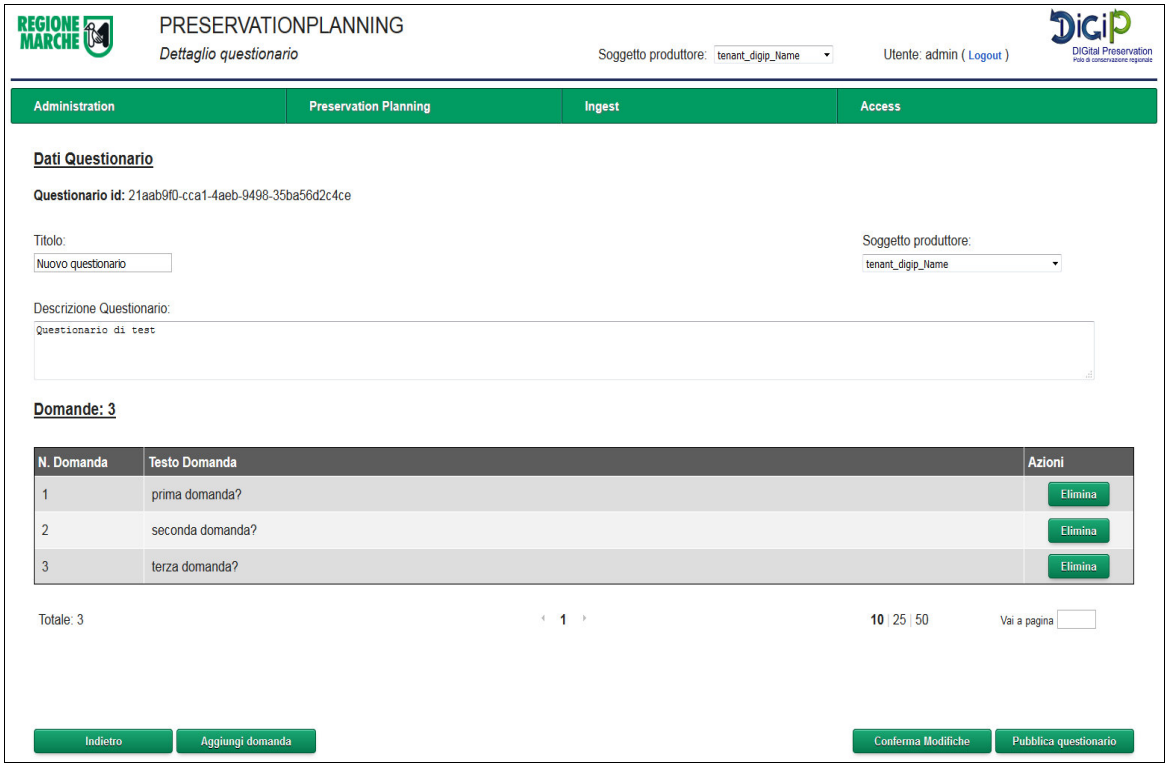
Gestione Questionario

Definizione. La maschera denominata *Gestione Questionario* permette all'utente che ha questo ruolo di creare, modificare e pubblicare questionari da sottoporre agli utenti. Nella tabella sono mostrati tutti i questionari già creati dall'utente.



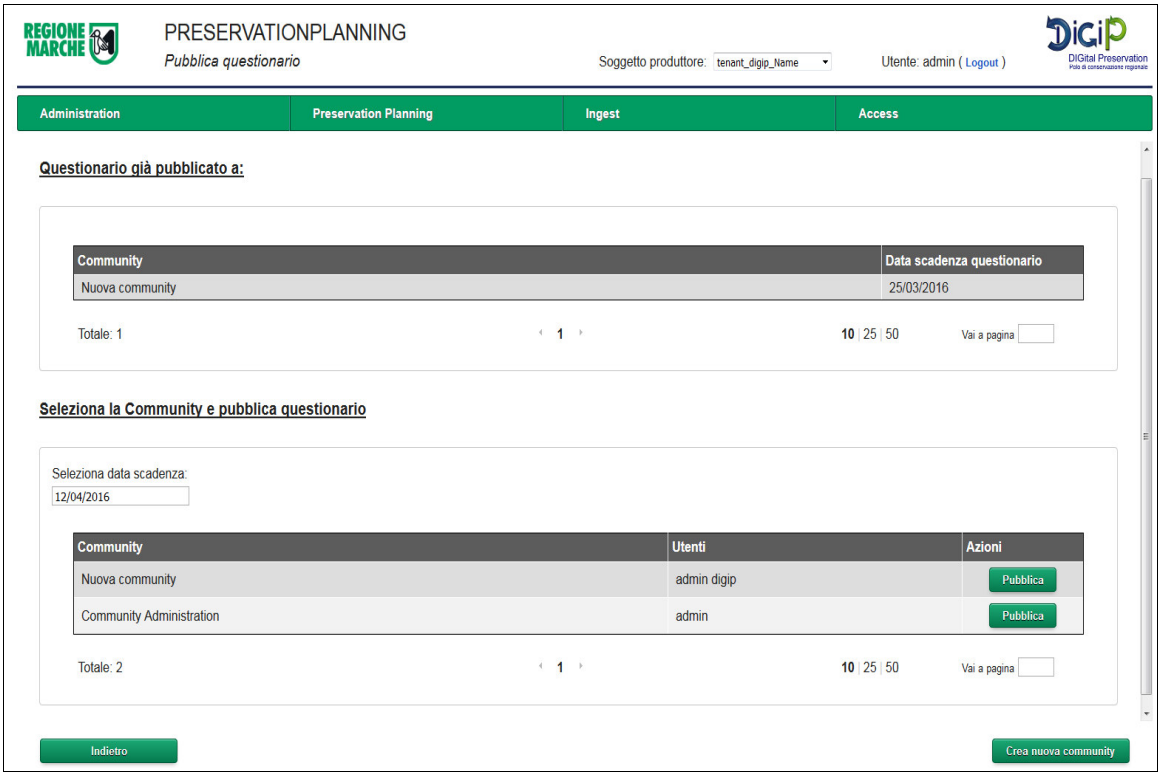
Operazioni:

1. **Crea questionario:** E' possibile definire un nuovo questionario cliccando sul pulsante *Nuovo Questionario*. In questa fase basterà introdurre nell'area di testo predisposta il titolo e una descrizione. Infine selezionare il soggetto produttore di riferimento al quale associarlo e premere *Conferma*. Una volta completati questi passaggi se si torna alla schermata precedente si visualizzerà nella tabella il questionario appena creato.
2. **Visualizza Dettaglio e Modifica:** E' possibile visualizzare i dettagli di un questionario già creato in precedenza cliccando sul pulsante *Dettaglio*. Si aprirà una nuova maschera dove sarà anche possibile modificare i dati inseriti al momento della creazione. Inoltre è possibile creare le domande relative al questionario cliccando sul pulsante *Aggiungi Domanda***.** Una volta definita una domanda subito verrà visualizzata in tabella e il numero aggiornato automaticamente. E' possibile dalla tabella modificare il testo e il numero cliccando sul campo specifico che diventerà editabile. Si precisa che il numero delle domande può essere solamente un campo numerico intero. E' possibile anche eliminare una domanda cliccando sul pulsante corrispondente. Con il pulsante *Conferma* verranno salvate tutte le modifiche effettuate. Cliccando invece sul pulsante *Pubblica questionario* si aprirà direttamente la schermata relativa alla pubblicazione di un questionario, senza passare dal pulsante Pubblica della tabella in schermata principale (di seguito verranno descritti i passaggi). NOTA: una volta che il questionario è già stato pubblicato non è più possibile accedere a questa pagina poiché non si possono più modificare i campi del questionario.



3. **Pubblicare un questionario:** Una volta completata la stesura del questionario è possibile pubblicarlo agli utenti per la compilazione. Per far questo si devi cliccare sul pulsante *Pubblica* . Si aprirà una schermata che mostra: le community (gruppi di utenti) a cui il questionario è già stato pubblicato, la data di scadenza per la compilazione da parte degli utenti e l'elenco delle community relative al soggetto produttore. Da questa schermata si ha anche la possibilità di creare nuove community se non presenti nell'elenco, cliccando il pulsante *crea nuova community* (per i dettagli vedi il paragrafo sotto relativo alle Community). Per pubblicare quindi un questionario bisogna scegliere la o le community a cui lo si vuol render visibile e cliccare il pulsante *Pubblica*. Ogni utente legato alla community scelta riceverà il questionario da compilare.

   NOTA: se un utente fa parte di community differenti e il questionario è stato pubblicato in due momenti diversi, allora gli verrà assegnata la data di scadenza della prima pubblicazione, mentre se viene modificata la data successivamente allora l'utente subisce sempre l'ultima variazione.



4. **Crea Attività:** In base alle risposte date al questionario e dopo una attenta analisi l'utente di preservation planning potrà decidere di creare delle attività che hanno come obiettivo quello di migliorare l'applicativo Digip. Cliccando sul pulsante *Crea Attività* verrà visualizzato per ogni domanda del test il riepilogo del livello di criticità degli argomenti sottoposti. Raffinando la selezione delle domanda si potranno visualizzare e selezionare ulteriormente le risposte date dagli utenti. Infine bisogna definire l'attività descrivendone gli obiettivi e le tempistiche di lavoro.Il procedimento in sintesi è il seguente:

   - ➔ Selezionare le domande che si vogliono prendere in esame, mettendo un flag nel quadratino di riferimento
   - ➔ Premere il pulsante *Raffina selezione*
   - ➔ Scegliere le risposte che andranno a definire l'attività, mettendo un flag nel quadratino di riferimento
   - ➔ Premere il pulsante *Crea attività*
   - ➔ Inserire i campi per completare la creazione di una nuova attività: *Priorità* (campo numerico), *Data Inizio*, *Data Fine* e *Annotazioni* (campo testuale).
   - ➔ Premere il pulsante *Conferma*.

Gestione Attività

Definizione. La maschera denominata *Gestione Attività* permette all'utente che ha ruolo di Preservation Planning di visualizzare e modificare le attività. Le attività sono processi che vengono creati dopo

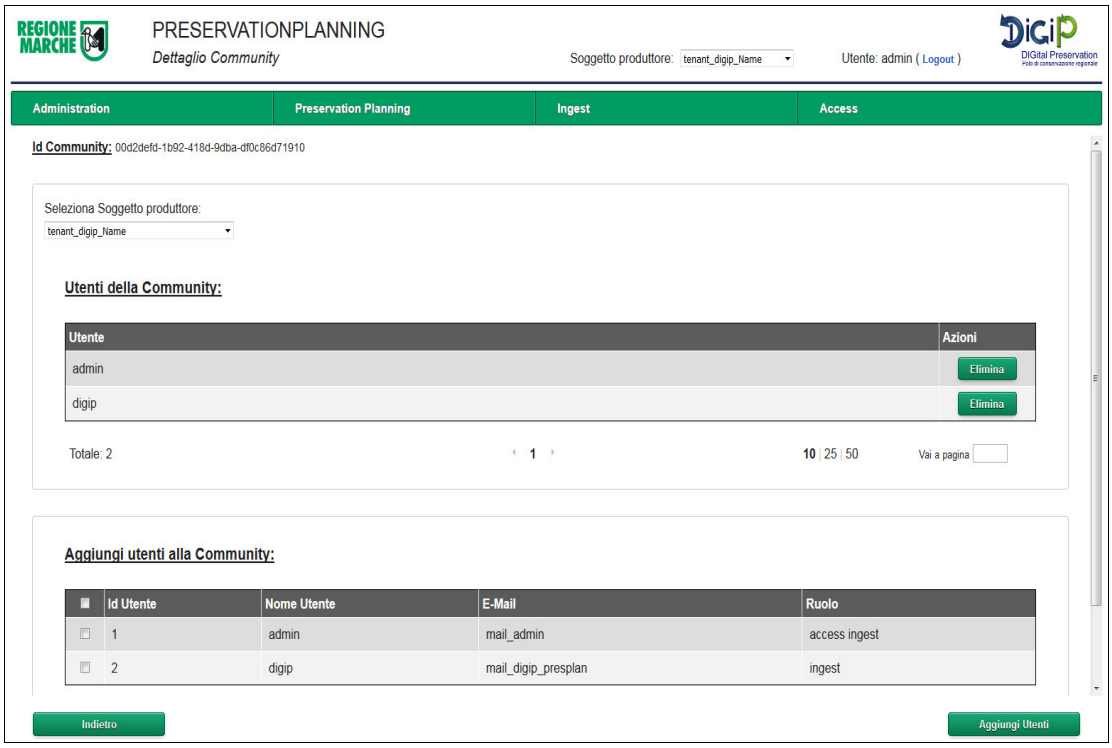
aver preso in esame le risposte date ai questionari: la criticità delle risposte mette in esame problematiche più o meno urgenti da risolvere tramite lavori che denominiamo appunto attività. La tabella elenca quelle già presenti sul database e cliccando sui campi, che diverranno editabili, ne permette la modifica. Per coerenza non sono permesse le modifiche ai campi ID e Data Inizio.

Community

Definizione. La maschera denominata *Community* permette all'utente che ha ruolo di Preservation Planning di visualizzare tutte le community definite in precedenza e di crearne di nuove. La Community è un insieme di utenti appartenenti allo stesso soggetto produttore. Viene utilizzata al momento della pubblicazione di un questionario, quando l'amministratore vuole scegliere a chi spedirlo. Nella tabella vengono elencate tutte quelle presenti con il relativo soggetto produttore di riferimento.

Operazioni:

1. **Crea Community:** Con il pulsante *Nuova Community* è possibile creare una nuova community definendo correttamente tutti i campi e selezionando con un flag opportunamente gli utenti che si desidera ne facciano parte. La community è legata al soggetto produttore che è il medesimo di quello degli utenti, quindi appariranno solo quelli a lui relativi. Una volta terminata la scelta premere il pulsante *Crea Community.*
2. **Visualizza e Modifica Community:** Cliccando il pulsante *Dettaglio* si possono visualizzare tutti i componenti di quella specifica community. E' possibile inoltre eliminare elementi cliccando sul pulsante corrispondente o aggiungerne di nuovi selezionandoli con un flag dalla lista e premendo *Aggiungi Utenti.*



3. **Eliminare Community:** Cliccando il pulsante *Elimina* è possibile eliminare definitivamente una community e tutti i collegamenti di questa ai questionari. Attenzione non verrà cancellato

il collegamento del questionario concreto con l'utente. In pratica se è già stato pubblicato un questionario ad una community, anche dopo la cancellazione di questa, l'utente continuerà a visualizzare il questionario.

Sandbox

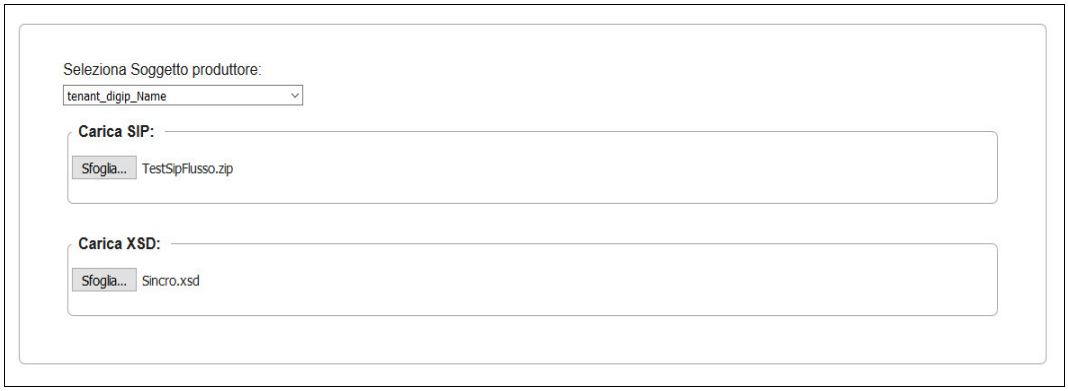
Definizione. La maschera denominata *Sandbox* permette all'utente che ha ruolo di Preservation Planning di lavorare liberamente in uno spazio apposito per verificare le procedure già attive nel sistema e di testare nuove applicazioni con lo scopo di migliorare il sistema. La Sandbox è suddivisa in quattro macro fasi che corrispondono alle fasi del caricamento di un versamento:

- Carica SIP: in questa sezione sarà possibile testare il caricamento di un SIP e la sua corretta struttura.
- RULE: in questa sezione si potranno valutare le regole da applicare al pacchetto SIP, affinché sia definito corretto per l' archiviazione.
- TRANSFORMATION: in questa sezione si possono valutare le trasformazioni da applicare al pacchetto SIP affinchè sia definito corretto per l' archiviazione
- Generazione AIP: in questa sezione è possibile generare il file descrittore dell' AIP.

Alla SandBox è stata associata una directory specifica differente da quella utilizzata per il processo di caricamento SIP, questo per dare la possibilità di fare prove senza intaccare i dati reali. La directory viene definita dal parametro globale $PATH_WORK_SANDBOX. Ogni volta che un utente utilizzerà questo processo, nella directory definita sopra, verrà creata una cartella specifica denominata con l'username dell'utente, questo per permettere l'utilizzo in parallelo del sistema, senza perdite di dati. In ogni pagina poi viene data anche la possibilità di pulire la propria cartella di lavoro cliccando sul pulsante *Pulisci SandBox.*

Operazioni:

1. **Carica SIP:** La maschera permette di:
   - ➔ Scegliere un soggetto produttore con il quale effettuare le prove. La scelta del soggetto produttore comporta che il sistema durante la lavorazione si baserà sulle sue specifiche configurazioni.
   - ➔ Fare l'upload di un pacchetto SIP (file .zip) che sarà l'oggetto di partenza per il quale definire test o nuovi ambiti di applicazione
   - ➔ Fare l'upload di un file xsd di validazione, coerente con le specifiche del soggetto produttore precedentemente scelto
   - ➔ Cliccare il pulsante *Valida SIP* per verificare la corretta struttura del SIP caricato in base al file xsd dato come riferimento.
   - ➔ Una volta avviato e concluso il controllo il sistema risponderà con un link dove si potrà visualizzare il file di esito.



2. **RULE:** La maschera permette di:

   ➔ Scegliere un soggetto produttore con il quale effettuare le prove. La scelta del soggetto produttore comporta che il sistema durante la lavorazione si baserà sulle sue specifiche configurazioni.

   ➔ Fare l'upload di un pacchetto SIP (file .zip) che sarà l'oggetto di partenza per il quale definire test o nuovi ambiti di applicazione.

   ➔ Nella tendina *Rule da applicare* scegliere il tipo di regola che si vuole gestire tra quelle proposte.

   ➔ Nell'area di testo *Inserire Regola* bisogna definire correttamente il profilo della regola scelta, nei seguenti modi:

   - FORMATO_FILE: è una regola che vuole controllare se il formato dei file allegati è un formato accettato per la conservazione. Nella textArea a disposizione bisognerà quindi inserire tutte le estensioni dei file che si ritengono corrette, nella seguente modalità: .ext .ext2 .ext3 ecc.. (esempio: .pdf .xml .txt)
   - FORMATO_METADATI: questa regola vuole controllare se il formato dei file definito all'interno del descrittore del SIP sia lo stesso dei file allegati e se questo formato è accettato per la conservazione. Nella textArea a disposizione bisognerà quindi inserire tutte le estensioni dei file che si ritengono corrette, nella seguente modalità: .ext .ext2 .ext3 ecc.. (esempio: .pdf .xml .txt)
   - RULE: questa rule va a valutare se precisi campi all'interno del descrittore SIP seguano correttamente la regular expression definita dalla regola. In questo caso nella textArea andrà inserita una corretta regular expression come l'esempio seguente: [A-Za-z0-9]. Per questa rule è opportuno riempire anche il *Tag Name* dove inserire il nome preciso del tag nel file descrittore corrispondente al campo che si vuole validare. Per compilare *Inserire TagName* bisogna inserire il nome del tag del file xml descrittore del SIP che identifica il campo che si vuole validare (esempio: sincro:nomeFile).

   ➔ Cliccare il pulsante *Conferma* per procedere.

   ➔ Una volta avviato e concluso il controllo il sistema risponderà con messaggio dove si potrà visualizzare l'esito della regola.

3. **TRANSFORMATION:** La maschera permette di:

   ➔ Scegliere un soggetto produttore con il quale effettuare le prove. La scelta del soggetto produttore comporta che il sistema durante la lavorazione si baserà sulle sue specifiche configurazioni.

   ➔ Fare l'upload di un pacchetto SIP (file .zip) che sarà l'oggetto di partenza per il quale definire test o nuovi ambiti di applicazione.

   ➔ Nella tendina *Trasformazioni da applicare* scegliere il tipo di trasformazione che si vuole gestire tra quelle proposte.

   ➔ Definire correttamente il profilo della trasformazione scelta nel seguente modo:

   - CONVERSION: questo tipo di trasformazione permette di convertire il file allegato del SIP nel formato definito dalla conversion. Selezionare dal menù a tendina il converter che si vuole applicare.
   - XSLT: questa è la classica trasformazione xslt. Serve a organizzare il descrittore del SIP modificandolo in una precisa struttura definita dal file xslt. Nel textArea a disposizione bisognerà quindi copiare e incollare il testo del file xslt di trasformazione che si vuole applicare.

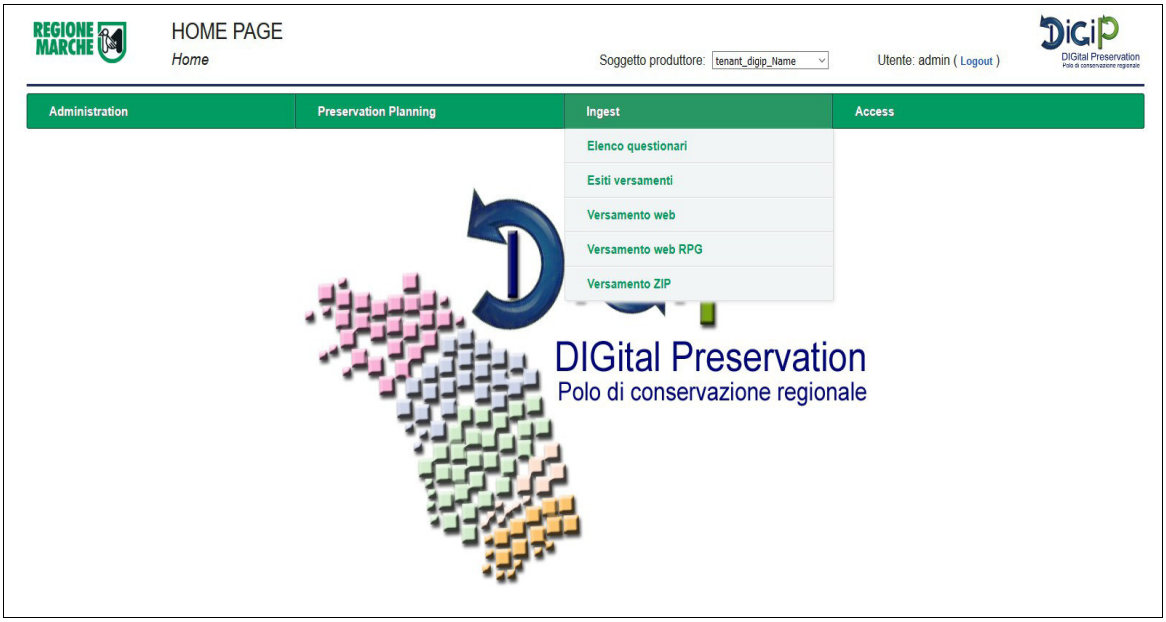
   ➔ Cliccare il pulsante *Conferma* .

   ➔ Una volta avviata e conclusa la procedura il sistema risponderà con messaggio dove si potrà visualizzare l'esito della trasformazione.

4. Generazione AIP: in questa sezione è possibile generare il file descrittore dell' AIP. Il file KIP di partenza è un esempio di come il processo raccoglie tutti i metadati del SIP, dei risultati delle regole e delle trasformazioni e li organizza in un file pronto per essere trasformato nel descrittore AIP. Il file KIP non è modificabile in questo caso, proprio perchè, salvo il valore dei metadati, la struttura è il risultato di molti processi precedenti. Si può invece intervenire sul file xslt, cioè sul file di trasformazione dal KIP all' AIP. Attraverso la sua modifica si possono definire possibili strutture per l'AIP. Dopo aver premuto il pulsante *Conferma* il sistema mostrerà a video il file risultante dalla trasformazione xslt definita.

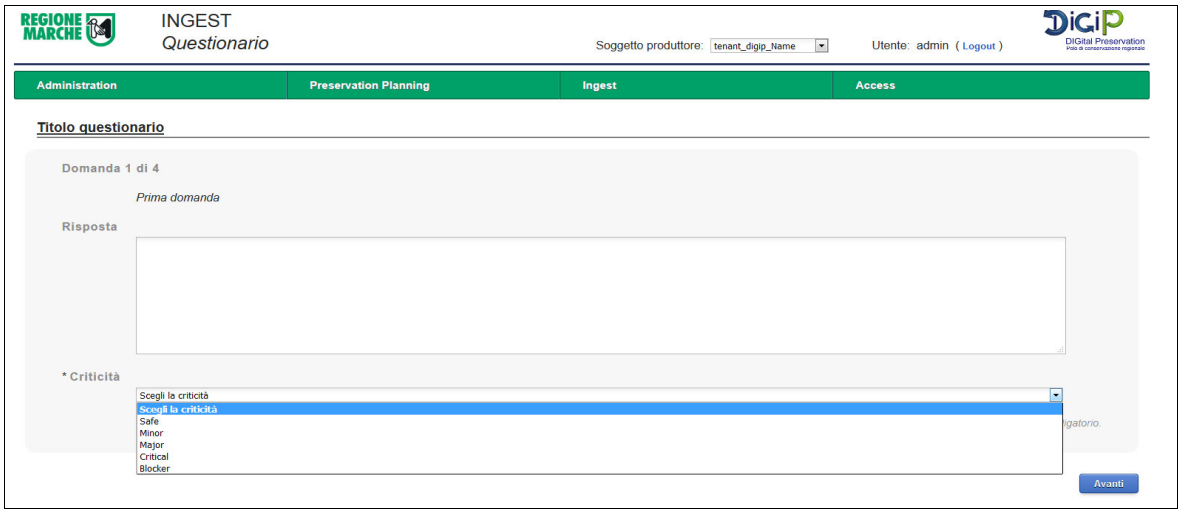
5.4 Area Ingest

Di seguito verranno illustrati tutti i casi d'uso relativi al ruolo di ingest. Si precisa che è possibile che un utente non visualizzi tutte le seguenti maschere poichè non gli sono state assegnate quelle specifiche attività.



Elenco Questionari

Definizione. La maschera denominata *Elenco Questionari* permette all'utente ingest di poter visualizzare l'elenco dei questionari che gli sono stati pubblicati. Per ogni questionario è specificato il titolo, una descrizione sommaria di cosa tratta, il numero di domande a cui rispondere e la data di scadenza, cioè la data ultima entro la quale l'utente può compilare il questionario. Superata questa data non sarà più possibile rispondere alle domande. Cliccando sul pulsante *Visualizza questionario* l'utente può iniziare a visualizzare e a compilare il questionario. La risposta alle domande è suddivisa in risposta e criticità. La criticità è l'unico campo obbligatorio e rappresenta il livello di difficoltà causato dall'argomento del testo della domanda durante l'utilizzo del sistema. Nella casella di testo risposta l'utente può aggiungere informazioni e commenti sul problema in questione che sarà utile al miglioramento del sistema. Con il pulsante *Avanti* si può passare alla domanda successiva e così via. Arrivati all'ultima domanda ci sarà il pulsante *Fine*. Cliccando questo pulsante il questionario verrà chiuso e dichiarato completato. Si può abbandonare e modificare il questionario in qualsiasi momento entro la data di scadenza, le risposte già date vengono mantenute. Una volta però cliccato il pulsante *Fine* non sarà più possibile la modifica ma solo la visualizzazione delle risposte date.



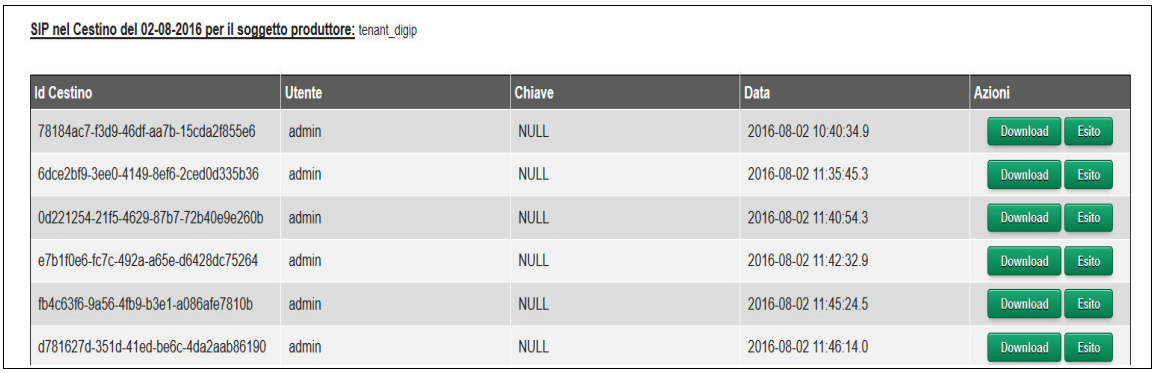
Esiti Versamenti

Definizione. La maschera denominata *Esiti versamenti* permette all'utente ingest di visualizzare, ricercare e monitorare i versamenti effettuati per uno specifico soggetto produttore. Per visualizzare i caricamenti bisogna cliccare il pulsante *Visualizza versamenti*. Si aprirà una nuova schermata dove vengono visualizzati i versamenti del giorno. Per fare una nuova ricerca si può selezionare da calendario la data o il periodo che si desidera visualizzare. La tabella mostra i versamenti organizzati per data di versamento e i seguenti dettagli:

- Ricevuti: numero di versamenti effettuati dall'ente in quella specifica data. Il produttore trasmette i SIP nei modi definiti nell'accordo formale i quali vengono messi in coda per la validazione di qualità
- Presi In Carico: numero di versamenti formalmente corretti e presi in carico dal sistema
- Validati: rapporto di versamento risultato positivo. Significa che le regole di validazione definite nell'accordo formale risultano rispettate.

- Non validati: rapporto di versamento risultato negativo. Significa che le regole di validazione definite nell'accordo formale non sono rispettate.
- Trasformati: numero di versamenti che hanno subito delle trasformazioni durante il processo di archiviazione. Il sistema, una volta che il SIP è stato positivamente validato, elabora il pacchetto fino alla generazione del corrispondente pacchetto di archiviazione (AIP)
- Completati: numero di pacchetti di archiviazione generati dal corrispondente pacchetto di versamento (SIP);
- Nel cestino: numero di pacchetti di versamento (SIP) ricevuti ma che non sono conformi agli accordi formali concordati tra il Produttore e il Polo di conservazione.

- Azioni: cliccando sull'icona del *Cestino* si possono visualizzare tutti i pacchetti che sono stati scartati in quella determinata data e quindi non sono stati presi in carico dal sistema. La tabella mostra l'utente che ha effettuato il versamento, la chiave cioè il nome del pacchetto versato, la data e due link: *Download* che permette di recuperare il pacchetto zip versato e *Esito* che mostra il codice e il messaggio di errore.


SIP nel Cestino del 02-08-2016 per il soggetto produttore: tenant_digip

Id Cestino	Utente	Chiave	Data	Azioni
78184ac7-f3d9-46df-aa7b-15cda2f855e6	admin	NULL	2016-08-02 10:40:34.9	Download Esito
6dce2bf9-3ee0-4149-8ef6-2ced0d335b36	admin	NULL	2016-08-02 11:35:45.3	Download Esito
0d221254-21f5-4629-87b7-72b40e9e260b	admin	NULL	2016-08-02 11:40:54.3	Download Esito
e7b1f0e6-fc7c-492a-a65e-d6428dc75264	admin	NULL	2016-08-02 11:42:32.9	Download Esito
fb4c63f6-9a56-4fb9-b3e1-a086afe7810b	admin	NULL	2016-08-02 11:45:24.5	Download Esito
d781627d-351d-41ed-be6c-4da2aab86190	admin	NULL	2016-08-02 11:46:14.0	Download Esito

Operazioni:

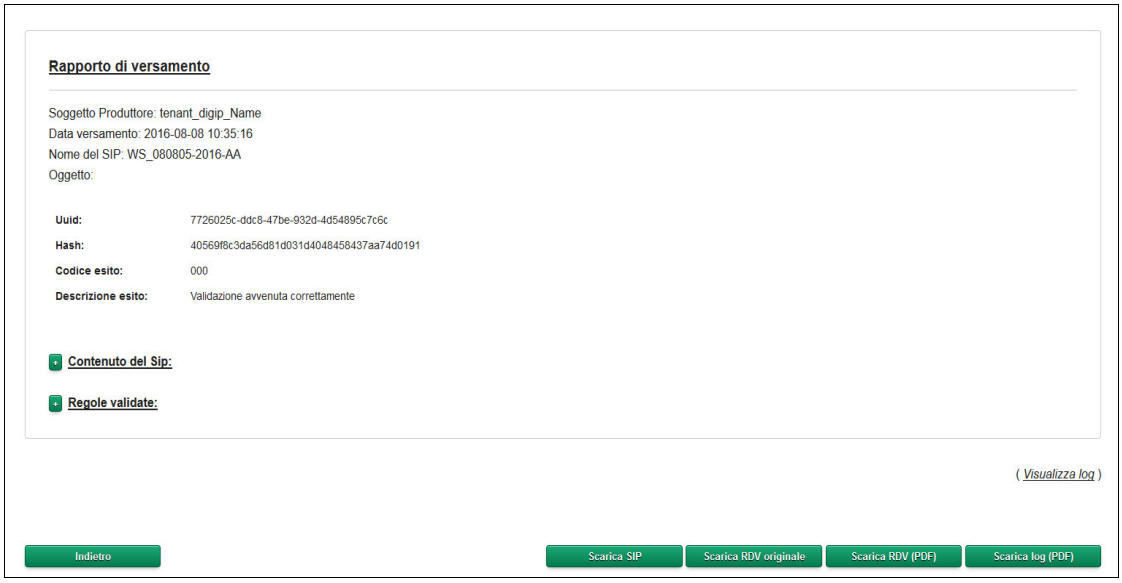
1. **Visualizza Versamenti.** Per visualizzare i versamenti cliccare sulla data versamento. Si aprirà una nuova schermata che mostra in dettaglio l'elenco di tutti i versamenti effettuati in quel giorno e lo stato in cui si trovano:
   - NOT_VALIDATED: Sip che non è stato preso in carica
   - ARCHIVED: Sip archiviato correttamente
   - RUNNING: procedura di archiviazione ancora in corso
   - ERROR: Sip andato in errore e non archiviato correttamente.

   Da questa maschera cliccando sul pulsante *Scarica csv* è possibile scaricare un file csv con l'elenco di tutti i versamenti del giorno.

Premendo il pulsante *Visualizza* viene mostrato il rapporto di versamento dove è specificato in dettaglio l'esito del versamento, il contenuto del pacchetto e l'elenco delle regole validate con i relativi risultati. Cliccando su *Visualizza Log* vengono mostrati i passaggi operativi del sistema.

Da questa maschera è possibile scaricare:

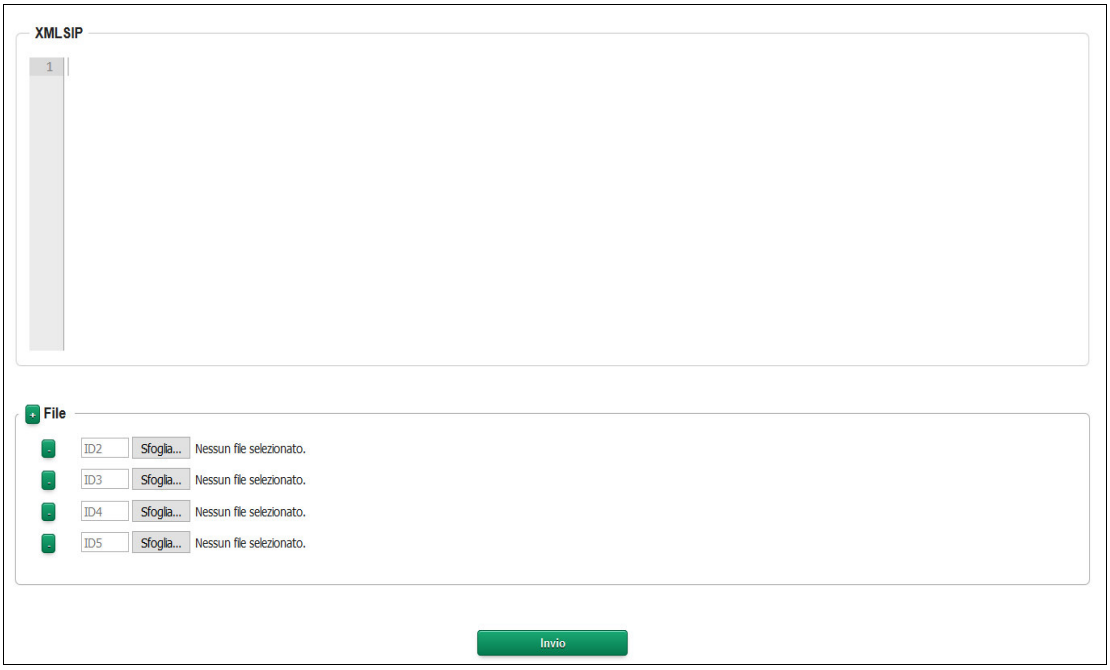
- SIP di partenza, pulsante *Scarica SIP*
- rapporto di versamento (firmato o non firmato a seconda della configurazione definita dal soggetto produttore), pulsante *Scarica RDV originale*
- rapporto di versamento in formato PDF, pulsante *Scarica RDV (PDF)*
- il log in formato PDF, pulsante *Scarica log (PDF)*



Versamento Web

Definizione. La maschera denominata V*ersamento Web* permette all'utente ingest di effettuare uno specifico versamento di un pacchetto SIP via Web. La maschera permette l'inserimento del file di indice descrittore con tutti i metadati e il caricamento dei file allegati nella seguente modalità:

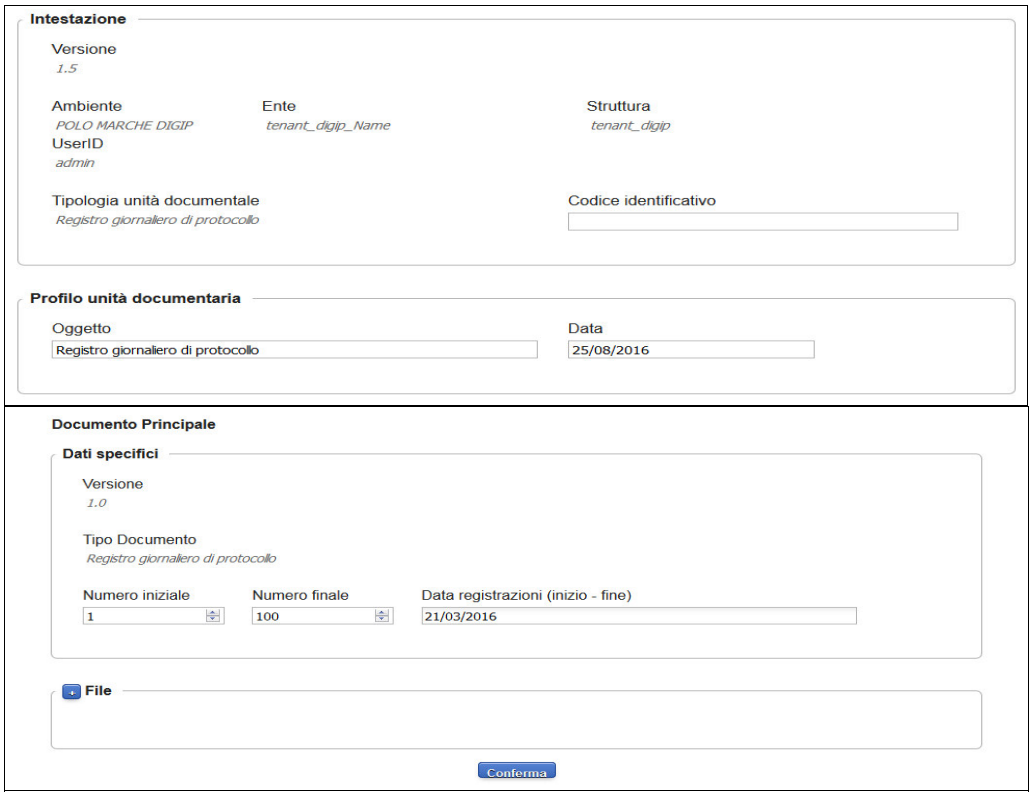
- Scrivere o fare copia e incolla nella casella di testo del file xml descrittore del pacchetto SIP
- Inserire, in relazione a ciascun file da allegare, il valore corrispondente del tag ID presente sull'indice descrittore
- Selezionare e caricare i file allegati cliccando sul pulsante *Sfoglia*.
- Una volta eseguite le operazioni premere il pulsante *Invio* per avviare la procedura di archiviazione. L'utente riceverà un messaggio di esito che può anche scaricare come pdf (pulsante *Scarica RDC (PDF)*). L'utente nella pagina Esiti Versamenti potrà seguire l'andamento del caricamento e recuperare il rapporto di versamento.



Versamento Web RPG

Definizione. La maschera denominata V*ersamento Web RPG* permette all'utente ingest di effettuare uno specifico versamento per i documenti di tipo Registro giornaliero di protocollo. La maschera permette l'inserimento dei metadati e il caricamento dei file nella seguente modalità:

- Inserire nei campi vuoti i corrispondenti valori come riportati nel Disciplinare tecnico, quali:
  - Codice Identificativo: data del documento Registro giornaliero di protocollo (aaaa-mm-gg). Si precisa che questo valore verrà usato per definire il nome del pacchetto SIP.
  - Oggetto: descrivere cosa rappresenta l'Oggetto del documento Registro giornaliero di protocollo (ad es. Registro giornaliero di protocollo dal n. […] al n. […]).
  - Data: data del documento Registro giornaliero di protocollo.
  - Numero iniziale: numero della prima registrazione sul registro giornaliero.
  - Numero finale: numero dell'ultima registrazione sul registro giornaliero.
  - Data registrazioni (inizio – fine): data della prima e dell'ultima registrazione del Registro giornaliero di protocollo.
- Selezionare e caricare il file Registro giornaliero di protocollo cliccando sul pulsante *File* e poi *Sfoglia*.
- Una volta eseguite le operazioni premere il pulsante *Conferma* per versare il Registro giornaliero di protocollo nel sistema di conservazione. L'utente riceverà un messaggio di esito. L'utente nella pagina Esiti Versamenti potrà seguire l'andamento del caricamento e recuperare il rapporto di versamento.



Versamento ZIP

Definizione. La maschera denominata V*ersamento ZIP* permette all'utente ingest di effettuare uno specifico versamento di un pacchetto zip. La maschera permette infatti di fare l'upload del file, premendo il pulsante *Sfoglia*. Questo processo è consentito al solo soggetto produttore che versa via Flusso. Il sistema non fa altro che recuperare il pacchetto zip e salvarlo nella cartella apposita (FTP) configurata per l'Ente al momento dell'attivazione.

Attenzione si precisa che:

- il nome dei pacchetti SIP che si vogliono versare deve essere univoco, salvo nel caso di caricamento di uno precedentemente andato in errore
- si deve mantenere la coerenza tra la descrizione dei file definiti nell'indice e quelli effettivamente allegati.

5.5 Area Access

Di seguito verranno illustrati tutti i casi d'uso relativi al ruolo di access. Si precisa che è possibile che un utente non visualizzi tutte le seguenti maschere poichè non gli sono state assegnate quelle specifiche attività.

Elenco Questionari

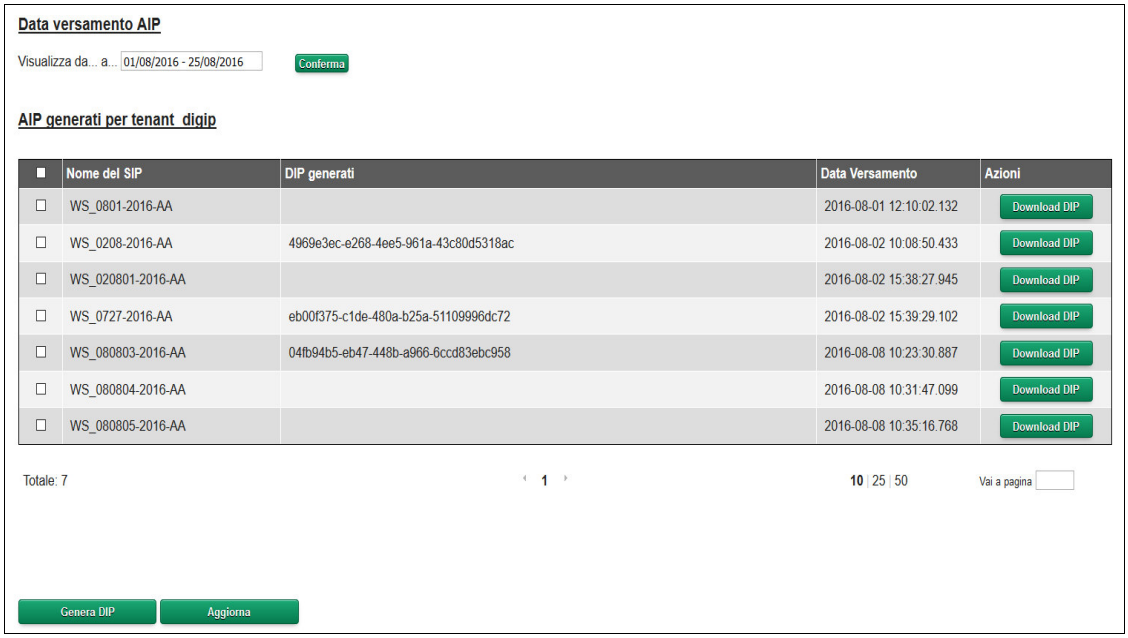
Definizione. La maschera denominata *Elenco Questionari* permette all'utente access di poter visualizzare l'elenco dei questionari che gli sono stati pubblicati. Per ogni questionario è specificato il titolo, una descrizione sommaria di cosa tratta, il numero di domande a cui rispondere e la data di scadenza, cioè la data ultima entro la quale l'utente può compilare il questionario. Superata questa data non sarà più possibile rispondere alle domande. Cliccando sul pulsante *Visualizza questionario* l'utente può iniziare a visualizzare e a compilare il questionario. La risposta alle domande è suddivisa in risposta e criticità. La criticità è l'unico campo obbligatorio e rappresenta il livello di difficoltà causato dall'argomento del testo della domanda durante l'utilizzo del sistema. Nella casella di testo risposta l'utente può aggiungere informazioni e commenti sul problema in questione che saranno utili al miglioramento del sistema. Con il pulsante *Avanti* si può passare alla domanda successiva e così via. Arrivati all'ultima domanda ci sarà il pulsante *Fine*. Cliccando questo pulsante il questionario verrà chiuso e dichiarato completato. Si può abbandonare e modificare il questionario in qualsiasi momento entro la data di scadenza, le risposte già date vengono mantenute. Una volta però cliccato il pulsante *Fine* non sarà più possibile la modifica ma solo la visualizzazione delle risposte date.

Gestione DIP

Definizione. La maschera denominata *Gestione DIP* permette all'utente access di generare e scaricare pacchetti di distribuzione (DIP) a partire dagli AIP, versamenti archiviati. La ricerca degli AIP è fatta per data versamento. Una volta definito il perido la tabella mostrerà l'elenco dei pacchetti presenti sul database. Si precisa che il tutto è vincolato dal soggetto produttore e dal livello di riservatezza dell'utente che effettua la ricerca. Non saranno quindi visibili tutti gli AIP ma solo quelli che di cui l'utente ha accesso.

Operazioni:

1. **Genera DIP:** e' possibile generare DIP selezionando con un flag gli AIP da cui si desidera partire. Terminata la selezione premere il pulsante *Genera DIP.* Una volta che un DIP è creato apparirà in tabella, nella colonna *DIP generati,* il valore del suo dell'identificativo. Con il tasto *Aggiorna* si può mantenere monitorata la procedura di creazione.
2. **Download DIP:** una volta generati i DIP è possibile scaricare i pacchetti (file .zip) premendo il pulsante relativo *Download DIP.*



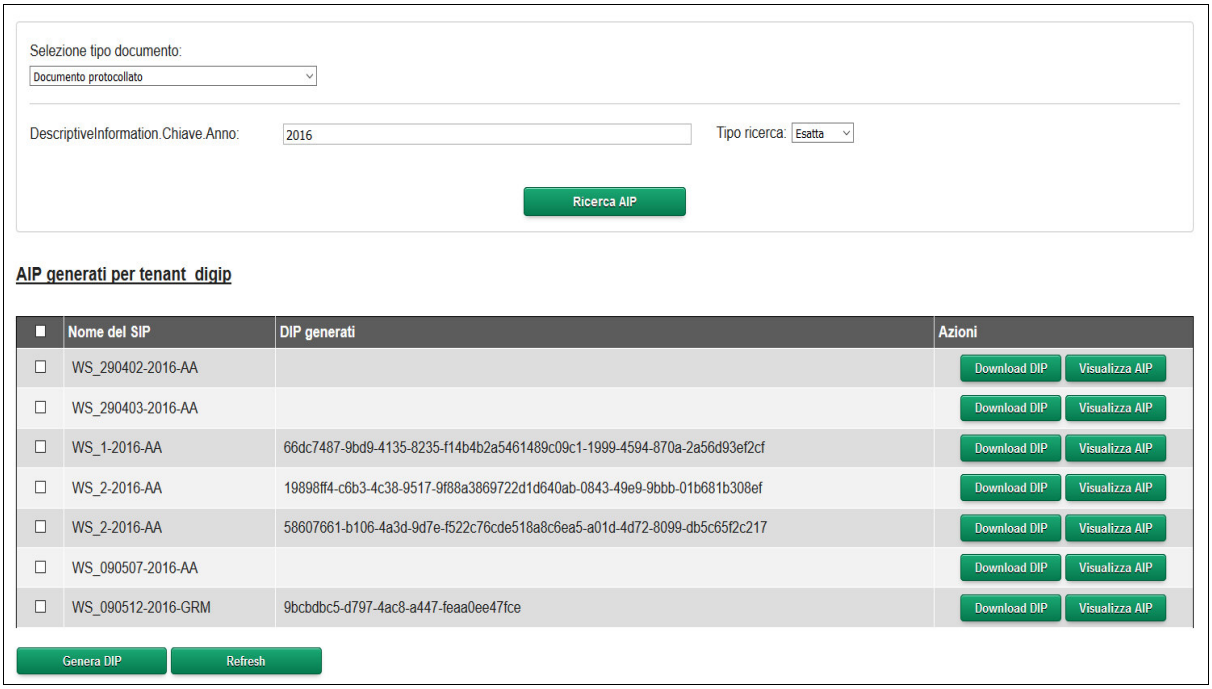
Ricerca semplice

Definizione. La maschera denominata *Ricerca semplice* permette all'utente con questo ruolo di cercare pacchetti AIP tramite i suoi metadati. La ricerca viene filtrata per tipologia documentale. Una volta selezionata vengono mostrati alcuni nomi di metadati: per la precisonione vengono visualizzate le etichette definite dall'amministratore nella maschera *configurazione ricerca.* Inserire nella casella di testo il valore e dal menù a tendina il tipo di ricerca che si vuole effettuare: esatta(=) o contiene(like). Una volta terminato cliccare il pulsante *Ricerca AIP.* Il sistema mostrerà a video gli AIP corrispondenti alle coppie chiave-valore definite.

Una volta trovati i pacchetti sono possibili le seguenti operazioni.

Operazioni:

1. **Genera DIP:** e' possibile generare DIP selezionando con un flag gli AIP da cui si desidera partire. Terminata la selezione premere il pulsante *Genera DIP.* Una volta che un DIP è creato apparirà in tabella, nella colonna *DIP generati,* il valore del suo dell'identificativo. Con il tasto *Refresh* si può mantenere monitorata la procedura di creazione.
2. **Download DIP:** una volta generati i DIP è possibile scaricare i pacchetti (file .zip) premendo il pulsante relativo *Download DIP.*
3. **Visualizza AIP:** cliccando sul pulsante corrispondente è possibile vedere il dettaglio del pacchetto AIP: i file, i metadati dei file e del descrittore suddivisi per tipologia e scaricare lo zip.



Ricerca avanzata

Definizione. La maschera denominata *Ricerca avanzata* permette all'utente con questo ruolo di cercare pacchetti AIP tramite i suoi metadati. La ricerca viene filtrata per tipologia documentale. Una volta selezionata vengono mostrati alcuni nomi di metadati: per la precisonione vengono visualizzate le etichette definite dall'amministratore nella maschera *configurazione ricerca.* Inserire nella casella di testo il valore e dal menù a tendina il tipo di ricerca che si vuole effettuare: esatta(=) o contiene(like). Con il pulsante *Aggiungi* criterio è possibile inserire un nuovo metadato non presente. Una volta terminato cliccare il pulsante *Ricerca AIP.* Il sistema mostrerà a video gli AIP corrispondenti alle coppie chiave-valore definite.

NOTA: gli AIP restituiti sono tutti quelli che soddisfano i parametri di ricerca e soprattutto sono solo quelli che per vincoli di riservatezza l'utente può visualizzare.

Una volta trovati i pacchetti sono possibili le seguenti operazioni.

Operazioni:

1. **Genera DIP:** e' possibile generare DIP selezionando con un flag gli AIP da cui si desidera partire. Terminata la selezione premere il pulsante *Genera DIP.* Una volta che un DIP è creato apparirà in tabella, nella colonna *DIP generati,* il valore del suo dell'identificativo. Con il tasto *Refresh* si può mantenere monitorata la procedura di creazione.
2. **Download DIP:** una volta generati i DIP è possibile scaricare i pacchetti (file .zip) premendo il pulsante relativo *Download DIP.*
3. **Visualizza AIP:** cliccando sul pulsante corrispondente è possibile vedere il dettaglio del pacchetto AIP: i file, i metadati dei file e del descrittore suddivisi per tipologia e scaricare lo zip.

ALLEGATI

ALLEGATO n 1

Di seguito il file XSD che definisce la struttura del Rapporto di Versamento (RDV).

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
 <xs:element name="RapportoDiVersamento">
  <xs:complexType>
   <xs:sequence>
          <xs:element name="SoggettoProduttore" type="xs:string"/>
          <xs:element name="RiferimentoTemporale" type="xs:string"/>
    <xs:element ref="SIP"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="SIP">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Id" type="xs:string"/>
    <xs:element name="Uuid" type="xs:string"/>
    <xs:element name="Hash" type="xs:string"/>
    <xs:element name="CodiceEsitoRegole" type="xs:string"/>
    <xs:element name="DescrizioneEsitoRegole" type="xs:string"/>
    <xs:element ref="File" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element ref="RegoleNonValidate" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element ref="RegoleValidate" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="File">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Id" type="xs:string"/>
    <xs:element name="Uuid" type="xs:string"/>
    <xs:element name="Hash" type="xs:string"/>
    <xs:element ref="VerificaFirma"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="VerificaFirma">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="FileName_origine" type="xs:string"/>
```

```
      <xs:element name="IdentificativoDocumentoFirmato" type="xs:string"/>
      <xs:element name="CodiceVerificaDocumentoFirmato" type="xs:string"/>
      <xs:element name="ValoreVerificaDocumentoFirmato" type="xs:string"/>
      <xs:element name="DescrizioneVerificaDocumentoFirmato" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="RegoleNonValidate">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="PROCESSO" minOccurs="1" maxOccurs="unbounded"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="PROCESSO">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="tipoRule" type="xs:string"/>
    <xs:element name="nomeRule" type="xs:string"/>
    <xs:element name="hashRule" type="xs:string"/>
    <xs:element name="algoritmoHash" type="xs:string"/>
    <xs:element name="codificaHash" type="xs:string"/>
    <xs:element name="esitoRule" type="xs:string"/>
    <xs:element name="messaggio" type="xs:string"/>
    <xs:element name="inizioRegola" type="xs:string"/>
    <xs:element name="fineRegola" type="xs:string"/>
    <xs:element name="dataOra" type="xs:string"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="RegoleValidate">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="PROCESSO" minOccurs="1" maxOccurs="unbounded"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

NOTA: I tag CodiceEsitoRegole e DescrizioneEsitoRegole vengono popolati con valori codificati a seconda della regola in errore. Sono definiti come segue:

Cod_errore	Tipo regola o messaggio
000	Validazione avvenuta correttamente

001	XSD
002	FORMATO_FILE
003	FORMATO_METADATI
004	RULE
005	TRIGGER
006	WORKFLOW
007	CONTROLLO_HASH
111	Fallimenti multipli: vedere dettaglio nelle singole regole

ALLEGATO n 2

Di seguito il file XSD che definisce la struttura della risposta data dal sistema a un versamento via web (versione 1.3)

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
 <xs:complexType name="ECEsitoXSDType">
  <xs:sequence>
   <xs:element name="CodiceEsito" type="ECEsitoPosNegType"/>
   <xs:sequence>
    <xs:element name="ControlloStrutturaXML" type="xs:string" minOccurs="0"/>
    <xs:element name="UnivocitaIDComponenti" type="xs:string" minOccurs="0"/>
    <xs:element name="UnivocitaIDDocumenti" type="xs:string" minOccurs="0"/>
    <xs:element name="CorrispondenzaAllegatiDichiarati" type="ECEsitoPosNegType" minOccurs="0"/>
    <xs:element name="CorrispondenzaAnnessiDichiarati" type="ECEsitoPosNegType" minOccurs="0"/>
    <xs:element name="CorrispondenzaAnnotazioniDichiarate" type="ECEsitoPosNegType" minOccurs="0"/>
   </xs:sequence>
  </xs:sequence>
 </xs:complexType>
 <!-- -->
 <xs:complexType name="ECEsitoXSDAggAllType">
```

```
  <xs:sequence>
   <xs:element name="CodiceEsito" type="ECEsitoPosNegType"/>
   <xs:sequence>
    <xs:element name="ControlloStrutturaXML" type="xs:string" minOccurs="0"/>
    <xs:element name="UnivocitaIDComponenti" type="xs:string" minOccurs="0"/>
   </xs:sequence>
  </xs:sequence>
</xs:complexType>
<!--  -->
<xs:complexType name="ECUnitaDocType">
 <xs:sequence>
  <xs:element name="Versatore" type="SCVersatoreType" minOccurs="0"/>
  <xs:element name="Chiave" type="SCChiaveType" minOccurs="0"/>
  <xs:element name="DataVersamento" type="xs:dateTime" minOccurs="0"/>
  <xs:element name="StatoConservazione" type="ECStatoConsType" minOccurs="0"/>
  <xs:element name="FirmatoDigitalmente" type="xs:boolean" minOccurs="0"/>
  <xs:element name="EsitoUnitaDocumentaria" minOccurs="0">
   <xs:complexType>
    <xs:sequence>
     <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType" minOccurs="0"/>
     <xs:element name="IdentificazioneVersatore" type="xs:string" minOccurs="0"/>
     <xs:element name="UnivocitaChiave" type="ECEsitoPosNegType" minOccurs="0"/>
     <xs:element name="VerificaTipologiaUD" type="ECEsitoPosNegType" minOccurs="0"/>
     <xs:element name="CorrispondenzaDatiSpecifici" type="xs:string" minOccurs="0"/>
     <xs:element name="PresenzaUDCollegate" type="xs:string" minOccurs="0"/>
     <xs:element name="VerificaFirmeUnitaDocumentaria" type="ECEsitoPosNegWarType" minOccurs="0"/>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
  <xs:element name="DocumentoPrincipale" type="ECDocumentoType" minOccurs="0"/>
  <xs:element name="Allegati" minOccurs="0">
   <xs:complexType>
    <xs:sequence>
```

```
        <xs:element name="Allegato" type="ECDocumentoType" maxOccurs="unbounded"/>
       </xs:sequence>
      </xs:complexType>
    </xs:element>
    <xs:element name="Annessi" minOccurs="0">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Annesso" type="ECDocumentoType" maxOccurs="unbounded"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:element name="Annotazioni" minOccurs="0">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Annotazione" type="ECDocumentoType" maxOccurs="unbounded"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
  <!--  -->
  <xs:complexType name="ECUnitaDocAggAllType">
   <xs:sequence>
    <xs:element name="Versatore" type="SCVersatoreType" minOccurs="0"/>
    <xs:element name="Chiave" type="SCChiaveType" minOccurs="0"/>
    <xs:element name="DataVersamento" type="xs:dateTime" minOccurs="0"/>
    <xs:element name="StatoConservazione" type="ECStatoConsType" minOccurs="0"/>
    <xs:element name="FirmatoDigitalmente" type="xs:boolean" minOccurs="0"/>
    <xs:element name="EsitoUnitaDocumentaria" minOccurs="0">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType" minOccurs="0"/>
       <xs:element name="IdentificazioneVersatore" type="xs:string" minOccurs="0"/>
```

```
        <xs:element name="IdentificazioneChiave" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="DocumentoUnivocoInUD" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="VerificaFirmeUnitaDocumentaria" type="ECEsitoPosNegWarType" minOccurs="0"/>
       </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:choice minOccurs="0" maxOccurs="1">
     <xs:element name="Allegato" type="ECDocumentoType" maxOccurs="1" minOccurs="1"/>
     <xs:element name="Annesso" type="ECDocumentoType" maxOccurs="1" minOccurs="1"/>
     <xs:element name="Annotazione" type="ECDocumentoType" maxOccurs="1" minOccurs="1"/>
    </xs:choice>
  </xs:sequence>
 </xs:complexType>
 <!-- -->
 <xs:complexType  name="ECEsitoGeneraleType">
  <xs:sequence>
   <xs:element name="CodiceEsito" type="ECEsitoExtType"/>
   <xs:element name="CodiceErrore" type="xs:string" minOccurs="0"/>
   <xs:element name="MessaggioErrore" type="xs:string" minOccurs="0"/>
  </xs:sequence>
 </xs:complexType>
 <!-- -->
 <xs:complexType name="ECEsitoChiamataWSType">
  <xs:sequence>
   <xs:element name="VersioneWSCorretta" type="ECEsitoPosNegType"/>
   <xs:element name="CredenzialiOperatore" type="ECEsitoPosNegType"/>
   <xs:element name="FileAttesiRicevuti" type="ECEsitoPosNegType"/>
  </xs:sequence>
 </xs:complexType>
 <!-- -->
 <xs:complexType name="ECConfigurazioneType">
  <xs:sequence>
   <xs:element name="TipoConservazione" minOccurs="0">
```

```
      <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
          <xs:enumeration value="SOSTITUTIVA"/>
          <xs:enumeration value="FISCALE"/>
          <xs:enumeration value="MIGRAZIONE"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="SistemaDiMigrazione" type="xs:string" maxOccurs="1" minOccurs="0"/>
    <xs:element name="ForzaAccettazione" type="xs:boolean" minOccurs="0"/>
    <xs:element name="ForzaConservazione" type="xs:boolean" minOccurs="0"/>
    <xs:element name="ForzaCollegamento" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloCrittografico" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloTrust" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloCertificato" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloCRL" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloFormato" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaFirmaSconosciuta" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaFirmaNonConforme" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaFirmaNoDelibera45" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaMarcaSconosciuta" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCrittograficoNegativo" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloTrustNegativo" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCertificatoScaduto" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCertificatoNoValido" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCertificatoNoFirma" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCRLNegativo" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCRLScaduta" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCRLNoValida" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCRLNoScaric" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloFormatoNegativo" type="xs:boolean" minOccurs="0"/>
  </xs:sequence>
 </xs:complexType>
```

```
<!-- -->
<xs:complexType  name="SCVersatoreType">
 <xs:sequence>
  <xs:element name="Ambiente" type="xs:string"/>
  <xs:element name="Ente" type="xs:string"/>
  <xs:element name="Struttura" type="xs:string"/>
  <xs:element name="UserID" type="xs:string"/>
 </xs:sequence>
</xs:complexType>
<!-- -->
<xs:complexType name="SCChiaveType">
 <xs:sequence>
  <xs:element name="Numero" type="xs:token"/>
  <xs:element name="Anno" type="xs:token" nillable="true"/>
  <xs:element name="TipoRegistro" type="xs:token" nillable="true"/>
 </xs:sequence>
</xs:complexType>
<!-- -->
<xs:complexType name="ECDocumentoType">
 <xs:sequence>
  <xs:element name="ChiaveDoc" type="xs:string"/>
  <xs:element name="IDDocumento" type="xs:string" minOccurs="0"/>
  <xs:element name="TipoDocumento" type="xs:string" minOccurs="0"/>
  <xs:element name="FirmatoDigitalmente" type="xs:boolean" minOccurs="0"/>
  <xs:element name="EsitoDocumento">
   <xs:complexType>
    <xs:sequence>
     <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
     <xs:sequence>
      <xs:element name="VerificaTipoDocumento" type="xs:string"/>
      <xs:element name="CorrispondenzaDatiSpecifici" type="xs:string" minOccurs="0"/>
      <xs:element name="CorrispondenzaDatiFiscali" type="xs:string" minOccurs="0"/>
      <xs:element name="NumerazioneFiscale" type="ECEsitoPosNegType" minOccurs="0"/>
```

```
        <xs:element name="VerificaTipoStruttura" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="VerificaFirmeDocumento" type="ECEsitoPosNegWarType" minOccurs="0"/>
        <xs:element name="UnivocitaOrdinePresentazione" type="ECEsitoPosNegType" minOccurs="0"/>
       </xs:sequence>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:element name="Componenti" minOccurs="0">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Componente" type="ECComponenteType" maxOccurs="unbounded"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
  <!--  -->
  <xs:complexType name="ECComponenteType">
   <xs:sequence>
    <xs:element name="OrdinePresentazione" type="xs:positiveInteger" minOccurs="0"/>
    <xs:element name="TipoComponente" type="xs:string" minOccurs="0"/>
    <xs:element name="URN" type="xs:token" minOccurs="0"/>
    <xs:element name="Hash" type="xs:hexBinary" minOccurs="0"/>
    <xs:element name="AlgoritmoHash" type="xs:token" minOccurs="0"/>
    <xs:element name="Encoding" type="xs:token" minOccurs="0"/>
    <xs:element name="FormatoRappresentazione" type="xs:string" minOccurs="0"/>
    <xs:element name="FormatoRappresentazioneEsteso" type="xs:string" minOccurs="0"/>
    <xs:element name="IdoneitaFormato" type="ECEsitoIdonFormatoType" minOccurs="0"/>
    <xs:element name="DimensioneFile" type="xs:nonNegativeInteger" minOccurs="0"/>
    <xs:element name="FirmatoDigitalmente" type="xs:boolean" minOccurs="0"/>
    <xs:element name="EsitoComponente">
     <xs:complexType>
      <xs:sequence>
```

```
      <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
      <xs:sequence>
       <xs:element name="VerificaTipoComponente" type="ECEsitoPosNegType" minOccurs="0"/>
       <xs:element name="CorrispondenzaDatiSpecifici" type="xs:string" minOccurs="0"/>
       <xs:element name="VerificaTipoSupportoComponente" type="xs:string" minOccurs="0"/>
       <xs:element name="VerificaTipoRappresentazione" type="ECEsitoPosNegType" minOccurs="0"/>
       <xs:element name="VerificaSottoComponenteRappresentazione" type="xs:string" minOccurs="0"/>
       <xs:element name="VerificaNomeComponente" type="ECEsitoPosNegType" minOccurs="0"/>
       <xs:element name="VerificaAmmissibilitaFormato" type="ECEsitoPosNegType" minOccurs="0"/>
       <xs:element name="VerificaRiconoscimentoFormato" type="ECEsitoRicFormatoType" minOccurs="0"/>
       <xs:element name="MessaggioRiconoscimentoFormato" type="xs:string" minOccurs="0"/>
       <xs:element name="VerificaRiferimentoUnitaDocumentaria" type="ECEsitoPosNegType" minOccurs="0"/>
       <xs:element name="VerificaFirmeComponente" type="ECEsitoPosNegWarType" minOccurs="0"/>
      </xs:sequence>
     </xs:sequence>
    </xs:complexType>
   </xs:element>
   <xs:element name="Marche" minOccurs="0">
    <xs:complexType>
     <xs:sequence>
      <xs:element name="Marca" type="ECMarcaType" maxOccurs="unbounded"/>
     </xs:sequence>
    </xs:complexType>
   </xs:element>
   <xs:element name="Firmatari" minOccurs="0">
    <xs:complexType>
     <xs:sequence>
      <xs:element name="Firmatario" type="ECFirmatarioType" maxOccurs="unbounded"/>
     </xs:sequence>
    </xs:complexType>
   </xs:element>
   <xs:element name="SottoComponenti" minOccurs="0">
    <xs:complexType>
```

```
      <xs:sequence>
       <xs:element name="SottoComponente" type="ECSottoComponenteType" maxOccurs="unbounded"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
  <!--  -->
  <xs:complexType name="ECMarcaType">
   <xs:sequence>
    <xs:element name="OrdineMarca" type="xs:positiveInteger" minOccurs="0"/>
    <xs:element name="FormatoMarca" type="xs:string" minOccurs="0"/>
    <xs:element name="Timestamp" type="xs:dateTime" minOccurs="0"/>
    <xs:element name="EsitoMarca">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="ControlloConformita" minOccurs="0" type="ECEsitoControlloType"/>
       <xs:element name="VerificaMarca" minOccurs="0">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
          <xs:element name="ControlloCrittografico" minOccurs="0" type="ECEsitoControlloType"/>
          <xs:element name="ControlloCatenaTrusted" minOccurs="0" type="ECEsitoControlloType"/>
          <xs:element name="ControlloCertificato" minOccurs="0" type="ECEsitoControlloType"/>
          <xs:element name="ControlloCRL" minOccurs="0" type="ECEsitoControlloType"/>
         </xs:sequence>
        </xs:complexType>
       </xs:element>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
```

```
<!--  -->
<xs:complexType name="ECFirmatarioType">
 <xs:sequence>
  <xs:element name="OrdineFirma" type="xs:positiveInteger" minOccurs="0"/>
  <xs:element name="CognomeNome" type="xs:string" minOccurs="0"/>
  <xs:element name="FormatoFirma" type="xs:string" minOccurs="0"/>
  <xs:element name="RiferimentoTemporaleUsato" type="xs:dateTime" minOccurs="0"/>
  <xs:element name="TipoRiferimentoTemporaleUsato" type="xs:string" minOccurs="0"/>
  <xs:element name="EsitoFirma">
   <xs:complexType>
    <xs:sequence>
     <xs:element name="ControlloConformita" minOccurs="0" type="ECEsitoControlloType"/>
     <xs:element name="VerificaFirma" minOccurs="0">
      <xs:complexType>
       <xs:sequence>
        <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
        <xs:element name="ControlloCrittografico" minOccurs="0" type="ECEsitoControlloType"/>
        <xs:element name="ControlloCatenaTrusted" minOccurs="0" type="ECEsitoControlloType"/>
        <xs:element name="ControlloCertificato" minOccurs="0" type="ECEsitoControlloType"/>
        <xs:element name="ControlloCRL" minOccurs="0" type="ECEsitoControlloType"/>
       </xs:sequence>
      </xs:complexType>
     </xs:element>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
 </xs:sequence>
</xs:complexType>
<!--  -->
<xs:complexType name="ECSottoComponenteType">
 <xs:sequence>
  <xs:element name="OrdinePresentazione" type="xs:positiveInteger" minOccurs="0"/>
  <xs:element name="TipoComponente" type="xs:string" minOccurs="0"/>
```

```
    <xs:element name="URN" type="xs:token" minOccurs="0"/>
    <xs:element name="Hash" type="xs:hexBinary" minOccurs="0"/>
    <xs:element name="AlgoritmoHash" type="xs:token" minOccurs="0"/>
    <xs:element name="Encoding" type="xs:token" minOccurs="0"/>
    <xs:element name="FormatoRappresentazione" type="xs:string" minOccurs="0"/>
    <xs:element name="FormatoRappresentazioneEsteso" type="xs:string" minOccurs="0"/>
    <xs:element name="IdoneitaFormato" type="ECEsitoIdonFormatoType" minOccurs="0"/>
    <xs:element name="DimensioneFile" type="xs:nonNegativeInteger" minOccurs="0"/>
    <xs:element name="EsitoSottoComponente">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
       <xs:sequence>
        <xs:element name="VerificaTipoComponente" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="CorrispondenzaDatiSpecifici" type="xs:string" minOccurs="0"/>
        <xs:element name="VerificaTipoSupportoComponente" type="xs:string" minOccurs="0"/>
        <xs:element name="VerificaNomeComponente" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="VerificaAmmissibilitaFormato" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="VerificaRiconoscimentoFormato" type="ECEsitoRicFormatoType" minOccurs="0"/>
        <xs:element name="MessaggioRiconoscimentoFormato" type="xs:string" minOccurs="0"/>
        <xs:element name="VerificaRiferimentoUnitaDocumentaria" type="ECEsitoPosNegType" minOccurs="0"/>
       </xs:sequence>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
  <!--  -->
  <xs:simpleType name="ECEsitoExtType">
   <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="POSITIVO"/>
    <xs:enumeration value="NEGATIVO"/>
    <xs:enumeration value="WARNING"/>
```

```
  </xs:restriction>
 </xs:simpleType>
 <!-- -->
 <xs:simpleType name="ECStatoConsType">
  <xs:restriction base="xs:NMTOKEN">
   <xs:enumeration value="IN_ATTESA_SCHED"/>
   <xs:enumeration value="IN_VOLUME_APERTO"/>
   <xs:enumeration value="IN_VOLUME_CHIUSO"/>
   <xs:enumeration value="IN_VOLUME_IN_ERRORE"/>
   <xs:enumeration value="NON_SELEZ_SCHED"/>
  </xs:restriction>
 </xs:simpleType>
 <!-- -->
 <xs:simpleType name="ECEsitoPosNegType">
  <xs:restriction base="xs:NMTOKEN">
   <xs:enumeration value="POSITIVO"/>
   <xs:enumeration value="NEGATIVO"/>
  </xs:restriction>
 </xs:simpleType>
 <!-- -->
 <xs:simpleType name="ECEsitoPosNegWarType">
  <xs:restriction base="xs:NMTOKEN">
   <xs:enumeration value="POSITIVO"/>
   <xs:enumeration value="NEGATIVO"/>
   <xs:enumeration value="WARNING"/>
  </xs:restriction>
 </xs:simpleType>
 <!-- -->
 <xs:simpleType name="ECEsitoRicFormatoType">
  <xs:restriction base="xs:NMTOKEN">
   <xs:enumeration value="POSITIVO"/>
   <xs:enumeration value="NEGATIVO"/>
   <xs:enumeration value="WARNING"/>
```

```
    <xs:enumeration value="DISABILITATO"/>
  </xs:restriction>
 </xs:simpleType>
 <!--  -->
 <xs:simpleType name="ECEsitoIdonFormatoType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="IDONEO"/>
    <xs:enumeration value="GESTITO"/>
    <xs:enumeration value="DEPRECATO"/>
  </xs:restriction>
 </xs:simpleType>
 <!--  -->
 <xs:simpleType name="ECEsitoControlloType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="POSITIVO"/>
    <xs:enumeration value="NEGATIVO"/>
    <xs:enumeration value="WARNING"/>
    <xs:enumeration value="NON_ESEGUITO"/>
    <xs:enumeration value="FORMATO_NON_CONOSCIUTO"/>
    <xs:enumeration value="FORMATO_NON_CONFORME"/>
    <xs:enumeration value="NON_AMMESSO_DELIB_45_CNIPA"/>
    <xs:enumeration value="DISABILITATO"/>
    <xs:enumeration value="NON_NECESSARIO"/>
    <xs:enumeration value="ERRORE"/>
    <xs:enumeration value="CERTIFICATO_ERRATO"/>
    <xs:enumeration value="CERTIFICATO_NON_VALIDO"/>
    <xs:enumeration value="CERTIFICATO_REVOCATO"/>
    <xs:enumeration value="CERTIFICATO_SCADUTO"/>
    <xs:enumeration value="CERTIFICATO_SCADUTO_3_12_2009"/>
    <xs:enumeration value="CRL_NON_SCARICABILE"/>
    <xs:enumeration value="CRL_NON_VALIDA"/>
    <xs:enumeration value="CRL_SCADUTA"/>
  </xs:restriction>
```

```
 </xs:simpleType>
 <!-- -->
<xs:element name="EsitoVersamento">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Versione" type="xs:string" minOccurs="0"/>
    <xs:element name="VersioneXMLChiamata" type="xs:string" minOccurs="0"/>
    <xs:element name="DataVersamento" type="xs:dateTime"/>
    <xs:element name="EsitoGenerale" type="ECEsitoGeneraleType"/>
    <xs:element name="EsitoChiamataWS" type="ECEsitoChiamataWSType"/>
    <xs:element name="EsitoXSD" type="ECEsitoXSDType"/>
    <xs:element name="Configurazione" type="ECConfigurazioneType" minOccurs="0"/>
    <xs:element name="UnitaDocumentaria" type="ECUnitaDocType" minOccurs="0"/>
    <xs:element name="XMLVersamento" type="xs:string" minOccurs="0"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <!-- -->
 <xs:element name="EsitoVersAggAllegati">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Versione" type="xs:string" minOccurs="0"/>
    <xs:element name="VersioneXMLChiamata" type="xs:string" minOccurs="0"/>
    <xs:element name="DataVersamento" type="xs:dateTime"/>
    <xs:element name="EsitoGenerale" type="ECEsitoGeneraleType"/>
    <xs:element name="EsitoChiamataWS" type="ECEsitoChiamataWSType"/>
    <xs:element name="EsitoXSD" type="ECEsitoXSDAggAllType"/>
    <xs:element name="Configurazione" type="ECConfigurazioneType" minOccurs="0"/>
    <xs:element name="UnitaDocumentaria" type="ECUnitaDocAggAllType" minOccurs="0"/>
    <xs:element name="XMLVersamento" type="xs:string" minOccurs="0"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
```

```
</xs:schema>
```

ALLEGATO n 3

Di seguito il file XSD che definisce la struttura della risposta data dal sistema a un versamento con chiamata Rest, effettuato fuori dall'applicativo Digip

(versione 1.4)

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
 <xs:complexType name="ECEsitoXSDType">
  <xs:sequence>
   <xs:element name="CodiceEsito" type="ECEsitoPosNegType"/>
   <xs:sequence>
    <xs:element name="ControlloStrutturaXML" type="xs:string" minOccurs="0"/>
    <xs:element name="UnivocitaIDComponenti" type="xs:string" minOccurs="0"/>
    <xs:element name="UnivocitaIDDocumenti" type="xs:string" minOccurs="0"/>
    <xs:element name="CorrispondenzaAllegatiDichiarati" type="ECEsitoPosNegType" minOccurs="0"/>
    <xs:element name="CorrispondenzaAnnessiDichiarati" type="ECEsitoPosNegType" minOccurs="0"/>
    <xs:element name="CorrispondenzaAnnotazioniDichiarate" type="ECEsitoPosNegType" minOccurs="0"/>
   </xs:sequence>
  </xs:sequence>
 </xs:complexType>
 <!--  -->
 <xs:complexType name="ECEsitoXSDAggAllType">
  <xs:sequence>
   <xs:element name="CodiceEsito" type="ECEsitoPosNegType"/>
   <xs:sequence>
    <xs:element name="ControlloStrutturaXML" type="xs:string" minOccurs="0"/>
    <xs:element name="UnivocitaIDComponenti" type="xs:string" minOccurs="0"/>
   </xs:sequence>
  </xs:sequence>
 </xs:complexType>
```

```
<!-- -->
<xs:complexType name="ECUnitaDocType">
 <xs:sequence>
  <xs:element name="Versatore" type="SCVersatoreType" minOccurs="0"/>
  <xs:element name="Chiave" type="SCChiaveType" minOccurs="0"/>
  <xs:element name="DataVersamento" type="xs:dateTime" minOccurs="0"/>
  <xs:element name="StatoConservazione" type="ECStatoConsType" minOccurs="0"/>
  <xs:element name="FirmatoDigitalmente" type="xs:boolean" minOccurs="0"/>
  <xs:element name="EsitoUnitaDocumentaria" minOccurs="0">
   <xs:complexType>
    <xs:sequence>
     <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType" minOccurs="0"/>
     <xs:element name="IdentificazioneVersatore" type="xs:string" minOccurs="0"/>
     <xs:element name="UnivocitaChiave" type="ECEsitoPosNegType" minOccurs="0"/>
     <xs:element name="VerificaTipologiaUD" type="ECEsitoPosNegType" minOccurs="0"/>
     <xs:element name="CorrispondenzaDatiSpecifici" type="xs:string" minOccurs="0"/>
     <xs:element name="PresenzaUDCollegate" type="xs:string" minOccurs="0"/>
     <xs:element name="VerificaFirmeUnitaDocumentaria" type="ECEsitoPosNegWarType" minOccurs="0"/>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
  <xs:element name="DocumentoPrincipale" type="ECDocumentoType" minOccurs="0"/>
  <xs:element name="Allegati" minOccurs="0">
   <xs:complexType>
    <xs:sequence>
     <xs:element name="Allegato" type="ECDocumentoType" maxOccurs="unbounded"/>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
  <xs:element name="Annessi" minOccurs="0">
   <xs:complexType>
    <xs:sequence>
     <xs:element name="Annesso" type="ECDocumentoType" maxOccurs="unbounded"/>
```

```
      </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:element name="Annotazioni" minOccurs="0">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Annotazione" type="ECDocumentoType" maxOccurs="unbounded"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
  <!-- -->
  <xs:complexType name="ECUnitaDocAggAllType">
   <xs:sequence>
    <xs:element name="Versatore" type="SCVersatoreType" minOccurs="0"/>
    <xs:element name="Chiave" type="SCChiaveType" minOccurs="0"/>
    <xs:element name="DataVersamento" type="xs:dateTime" minOccurs="0"/>
    <xs:element name="StatoConservazione" type="ECStatoConsType" minOccurs="0"/>
    <xs:element name="FirmatoDigitalmente" type="xs:boolean" minOccurs="0"/>
    <xs:element name="EsitoUnitaDocumentaria" minOccurs="0">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType" minOccurs="0"/>
       <xs:element name="IdentificazioneVersatore" type="xs:string" minOccurs="0"/>
       <xs:element name="IdentificazioneChiave" type="ECEsitoPosNegType" minOccurs="0"/>
       <xs:element name="DocumentoUnivocoInUD" type="ECEsitoPosNegType" minOccurs="0"/>
       <xs:element name="VerificaFirmeUnitaDocumentaria" type="ECEsitoPosNegWarType" minOccurs="0"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:choice minOccurs="0" maxOccurs="1">
     <xs:element name="Allegato" type="ECDocumentoType" maxOccurs="1" minOccurs="1"/>
```

```
    <xs:element name="Annesso" type="ECDocumentoType" maxOccurs="1" minOccurs="1"/>
    <xs:element name="Annotazione" type="ECDocumentoType" maxOccurs="1" minOccurs="1"/>
   </xs:choice>
  </xs:sequence>
 </xs:complexType>
 <!-- -->
 <xs:complexType  name="ECEsitoGeneraleType">
  <xs:sequence>
   <xs:element name="CodiceEsito" type="ECEsitoExtType"/>
   <xs:element name="CodiceErrore" type="xs:string" minOccurs="0"/>
   <xs:element name="MessaggioErrore" type="xs:string" minOccurs="0"/>
  </xs:sequence>
 </xs:complexType>
 <!-- -->
 <xs:complexType name="ECEsitoChiamataWSType">
  <xs:sequence>
   <xs:element name="VersioneWSCorretta" type="ECEsitoPosNegType"/>
   <xs:element name="CredenzialiOperatore" type="ECEsitoPosNegType"/>
   <xs:element name="FileAttesiRicevuti" type="ECEsitoPosNegType"/>
  </xs:sequence>
 </xs:complexType>
 <!-- -->
 <xs:complexType name="ECConfigurazioneType">
  <xs:sequence>
   <xs:element name="TipoConservazione" minOccurs="0">
    <xs:simpleType>
     <xs:restriction base="xs:NMTOKEN">
      <xs:enumeration value="SOSTITUTIVA"/>
      <xs:enumeration value="FISCALE"/>
      <xs:enumeration value="MIGRAZIONE"/>
     </xs:restriction>
    </xs:simpleType>
   </xs:element>
```

```
    <xs:element name="SistemaDiMigrazione" type="xs:string" maxOccurs="1" minOccurs="0"/>
    <xs:element name="ForzaAccettazione" type="xs:boolean" minOccurs="0"/>
    <xs:element name="ForzaConservazione" type="xs:boolean" minOccurs="0"/>
    <xs:element name="ForzaCollegamento" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloCrittografico" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloTrust" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloCertificato" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloCRL" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AbilitaControlloFormato" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaFirmaSconosciuta" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaFirmaNonConforme" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaFirmaNoDelibera45" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaMarcaSconosciuta" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCrittograficoNegativo" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloTrustNegativo" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCertificatoScaduto" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCertificatoNoValido" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCertificatoNoFirma" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCRLNegativo" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCRLScaduta" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCRLNoValida" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloCRLNoScaric" type="xs:boolean" minOccurs="0"/>
    <xs:element name="AccettaControlloFormatoNegativo" type="xs:boolean" minOccurs="0"/>
  </xs:sequence>
 </xs:complexType>
 <!--  -->
 <xs:complexType  name="SCVersatoreType">
  <xs:sequence>
    <xs:element name="Ambiente" type="xs:string"/>
    <xs:element name="Ente" type="xs:string"/>
    <xs:element name="Struttura" type="xs:string"/>
    <xs:element name="UserID" type="xs:string"/>
  </xs:sequence>
```

```
</xs:complexType>
<!-- -->
<xs:complexType name="SCChiaveType">
 <xs:sequence>
  <xs:element name="Numero" type="xs:token"/>
  <xs:element name="Anno" type="xs:token" nillable="true"/>
  <xs:element name="TipoRegistro" type="xs:token" nillable="true"/>
 </xs:sequence>
</xs:complexType>
<!-- -->
<xs:complexType name="ECDocumentoType">
 <xs:sequence>
  <xs:element name="ChiaveDoc" type="xs:string"/>
  <xs:element name="IDDocumento" type="xs:string" minOccurs="0"/>
  <xs:element name="TipoDocumento" type="xs:string" minOccurs="0"/>
  <xs:element name="FirmatoDigitalmente" type="xs:boolean" minOccurs="0"/>
  <xs:element name="EsitoDocumento" minOccurs="0">
   <xs:complexType>
    <xs:sequence>
     <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
     <xs:sequence>
      <xs:element name="VerificaTipoDocumento" type="xs:string"/>
      <xs:element name="CorrispondenzaDatiSpecifici" type="xs:string" minOccurs="0"/>
      <xs:element name="CorrispondenzaDatiFiscali" type="xs:string" minOccurs="0"/>
      <xs:element name="NumerazioneFiscale" type="ECEsitoPosNegType" minOccurs="0"/>
      <xs:element name="VerificaTipoStruttura" type="ECEsitoPosNegType" minOccurs="0"/>
      <xs:element name="VerificaFirmeDocumento" type="ECEsitoPosNegWarType" minOccurs="0"/>
      <xs:element name="UnivocitaOrdinePresentazione" type="ECEsitoPosNegType" minOccurs="0"/>
     </xs:sequence>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
  <xs:element name="Componenti" minOccurs="0">
```

```
    <xs:complexType>
     <xs:sequence>
      <xs:element name="Componente" type="ECComponenteType" maxOccurs="unbounded"/>
     </xs:sequence>
    </xs:complexType>
   </xs:element>
  </xs:sequence>
 </xs:complexType>
 <!-- -->
 <xs:complexType name="ECComponenteType">
  <xs:sequence>
   <xs:element name="OrdinePresentazione" type="xs:positiveInteger" minOccurs="0"/>
   <xs:element name="TipoComponente" type="xs:string" minOccurs="0"/>
   <xs:element name="URN" type="xs:token" minOccurs="0"/>
   <xs:element name="Hash" type="xs:hexBinary" minOccurs="0"/>
   <xs:element name="AlgoritmoHash" type="xs:token" minOccurs="0"/>
   <xs:element name="Encoding" type="xs:token" minOccurs="0"/>
   <xs:element name="FormatoRappresentazione" type="xs:string" minOccurs="0"/>
   <xs:element name="FormatoRappresentazioneEsteso" type="xs:string" minOccurs="0"/>
   <xs:element name="IdoneitaFormato" type="ECEsitoIdonFormatoType" minOccurs="0"/>
   <xs:element name="DimensioneFile" type="xs:nonNegativeInteger" minOccurs="0"/>
   <xs:element name="FirmatoDigitalmente" type="xs:boolean" minOccurs="0"/>
   <xs:element name="EsitoComponente">
    <xs:complexType>
     <xs:sequence>
      <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
      <xs:sequence>
       <xs:element name="VerificaTipoComponente" type="ECEsitoPosNegType" minOccurs="0"/>
       <xs:element name="CorrispondenzaDatiSpecifici" type="xs:string" minOccurs="0"/>
       <xs:element name="VerificaTipoSupportoComponente" type="xs:string" minOccurs="0"/>
       <xs:element name="VerificaTipoRappresentazione" type="ECEsitoPosNegType" minOccurs="0"/>
       <xs:element name="VerificaSottoComponenteRappresentazione" type="xs:string" minOccurs="0"/>
       <xs:element name="VerificaNomeComponente" type="ECEsitoPosNegType" minOccurs="0"/>
```

```
        <xs:element name="VerificaAmmissibilitaFormato" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="VerificaRiconoscimentoFormato" type="ECEsitoRicFormatoType" minOccurs="0"/>
        <xs:element name="MessaggioRiconoscimentoFormato" type="xs:string" minOccurs="0"/>
        <xs:element name="VerificaRiferimentoUnitaDocumentaria" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="VerificaFirmeComponente" type="ECEsitoPosNegWarType" minOccurs="0"/>
       </xs:sequence>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:element name="Marche" minOccurs="0">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Marca" type="ECMarcaType" maxOccurs="unbounded"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:element name="Firmatari" minOccurs="0">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="Firmatario" type="ECFirmatarioType" maxOccurs="unbounded"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
    <xs:element name="SottoComponenti" minOccurs="0">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="SottoComponente" type="ECSottoComponenteType" maxOccurs="unbounded"/>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
  <!--  -->
```

```
<xs:complexType name="ECMarcaType">
 <xs:sequence>
  <xs:element name="OrdineMarca" type="xs:positiveInteger" minOccurs="0"/>
  <xs:element name="FormatoMarca" type="xs:string" minOccurs="0"/>
  <xs:element name="Timestamp" type="xs:dateTime" minOccurs="0"/>
  <xs:element name="EsitoMarca">
   <xs:complexType>
    <xs:sequence>
     <xs:element name="ControlloConformita" minOccurs="0" type="ECEsitoControlloType"/>
     <xs:element name="VerificaMarca" minOccurs="0">
      <xs:complexType>
       <xs:sequence>
        <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
        <xs:element name="ControlloCrittografico" minOccurs="0" type="ECEsitoControlloType"/>
        <xs:element name="ControlloCatenaTrusted" minOccurs="0" type="ECEsitoControlloType"/>
        <xs:element name="ControlloCertificato" minOccurs="0" type="ECEsitoControlloType"/>
        <xs:element name="ControlloCRL" minOccurs="0" type="ECEsitoControlloType"/>
       </xs:sequence>
      </xs:complexType>
     </xs:element>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
 </xs:sequence>
</xs:complexType>
<!--  -->
<xs:complexType name="ECFirmatarioType">
 <xs:sequence>
  <xs:element name="OrdineFirma" type="xs:positiveInteger" minOccurs="0"/>
  <xs:element name="CognomeNome" type="xs:string" minOccurs="0"/>
  <xs:element name="FormatoFirma" type="xs:string" minOccurs="0"/>
  <xs:element name="RiferimentoTemporaleUsato" type="xs:dateTime" minOccurs="0"/>
  <xs:element name="TipoRiferimentoTemporaleUsato" type="xs:string" minOccurs="0"/>
```

```
    <xs:element name="EsitoFirma">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="ControlloConformita" minOccurs="0" type="ECEsitoControlloType"/>
       <xs:element name="VerificaFirma" minOccurs="0">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
          <xs:element name="ControlloCrittografico" minOccurs="0" type="ECEsitoControlloType"/>
          <xs:element name="ControlloCatenaTrusted" minOccurs="0" type="ECEsitoControlloType"/>
          <xs:element name="ControlloCertificato" minOccurs="0" type="ECEsitoControlloType"/>
          <xs:element name="ControlloCRL" minOccurs="0" type="ECEsitoControlloType"/>
         </xs:sequence>
        </xs:complexType>
       </xs:element>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
  <!--  -->
  <xs:complexType name="ECSottoComponenteType">
   <xs:sequence>
    <xs:element name="OrdinePresentazione" type="xs:positiveInteger" minOccurs="0"/>
    <xs:element name="TipoComponente" type="xs:string" minOccurs="0"/>
    <xs:element name="URN" type="xs:token" minOccurs="0"/>
    <xs:element name="Hash" type="xs:hexBinary" minOccurs="0"/>
    <xs:element name="AlgoritmoHash" type="xs:token" minOccurs="0"/>
    <xs:element name="Encoding" type="xs:token" minOccurs="0"/>
    <xs:element name="FormatoRappresentazione" type="xs:string" minOccurs="0"/>
    <xs:element name="FormatoRappresentazioneEsteso" type="xs:string" minOccurs="0"/>
    <xs:element name="IdoneitaFormato" type="ECEsitoIdonFormatoType" minOccurs="0"/>
    <xs:element name="DimensioneFile" type="xs:nonNegativeInteger" minOccurs="0"/>
```

```
    <xs:element name="EsitoSottoComponente">
     <xs:complexType>
      <xs:sequence>
       <xs:element name="CodiceEsito" type="ECEsitoPosNegWarType"/>
       <xs:sequence>
        <xs:element name="VerificaTipoComponente" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="CorrispondenzaDatiSpecifici" type="xs:string" minOccurs="0"/>
        <xs:element name="VerificaTipoSupportoComponente" type="xs:string" minOccurs="0"/>
        <xs:element name="VerificaNomeComponente" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="VerificaAmmissibilitaFormato" type="ECEsitoPosNegType" minOccurs="0"/>
        <xs:element name="VerificaRiconoscimentoFormato" type="ECEsitoRicFormatoType" minOccurs="0"/>
        <xs:element name="MessaggioRiconoscimentoFormato" type="xs:string" minOccurs="0"/>
        <xs:element name="VerificaRiferimentoUnitaDocumentaria" type="ECEsitoPosNegType" minOccurs="0"/>
       </xs:sequence>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
  <!-- -->
  <xs:simpleType name="ECEsitoExtType">
   <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="POSITIVO"/>
    <xs:enumeration value="NEGATIVO"/>
    <xs:enumeration value="WARNING"/>
   </xs:restriction>
  </xs:simpleType>
  <!-- -->
  <xs:simpleType name="ECStatoConsType">
   <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="IN_ATTESA_SCHED"/>
    <xs:enumeration value="IN_VOLUME_APERTO"/>
    <xs:enumeration value="IN_VOLUME_CHIUSO"/>
```

```
    <xs:enumeration value="IN_VOLUME_IN_ERRORE"/>
    <xs:enumeration value="NON_SELEZ_SCHED"/>
  </xs:restriction>
</xs:simpleType>
<!--  -->
<xs:simpleType name="ECEsitoPosNegType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="POSITIVO"/>
    <xs:enumeration value="NEGATIVO"/>
  </xs:restriction>
</xs:simpleType>
<!--  -->
<xs:simpleType name="ECEsitoPosNegWarType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="POSITIVO"/>
    <xs:enumeration value="NEGATIVO"/>
    <xs:enumeration value="WARNING"/>
  </xs:restriction>
</xs:simpleType>
<!--  -->
<xs:simpleType name="ECEsitoRicFormatoType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="POSITIVO"/>
    <xs:enumeration value="NEGATIVO"/>
    <xs:enumeration value="WARNING"/>
    <xs:enumeration value="DISABILITATO"/>
  </xs:restriction>
</xs:simpleType>
<!--  -->
<xs:simpleType name="ECEsitoIdonFormatoType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="IDONEO"/>
    <xs:enumeration value="GESTITO"/>
```

```
    <xs:enumeration value="DEPRECATO"/>
  </xs:restriction>
 </xs:simpleType>
 <!--  -->
 <xs:simpleType name="ECEsitoControlloType">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="POSITIVO"/>
    <xs:enumeration value="NEGATIVO"/>
    <xs:enumeration value="WARNING"/>
    <xs:enumeration value="NON_ESEGUITO"/>
    <xs:enumeration value="FORMATO_NON_CONOSCIUTO"/>
    <xs:enumeration value="FORMATO_NON_CONFORME"/>
    <xs:enumeration value="NON_AMMESSO_DELIB_45_CNIPA"/>
    <xs:enumeration value="DISABILITATO"/>
    <xs:enumeration value="NON_NECESSARIO"/>
    <xs:enumeration value="ERRORE"/>
    <xs:enumeration value="CERTIFICATO_ERRATO"/>
    <xs:enumeration value="CERTIFICATO_NON_VALIDO"/>
    <xs:enumeration value="CERTIFICATO_REVOCATO"/>
    <xs:enumeration value="CERTIFICATO_SCADUTO"/>
    <xs:enumeration value="CERTIFICATO_SCADUTO_3_12_2009"/>
    <xs:enumeration value="CRL_NON_SCARICABILE"/>
    <xs:enumeration value="CRL_NON_VALIDA"/>
    <xs:enumeration value="CRL_SCADUTA"/>
  </xs:restriction>
 </xs:simpleType>
 <!--  -->
 <xs:element name="EsitoVersamento">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Versione" type="xs:string" minOccurs="0"/>
    <xs:element name="VersioneXMLChiamata" type="xs:string" minOccurs="0"/>
    <xs:element name="IdSIP" type="xs:string" minOccurs="1" maxOccurs="1"/>
```

```
      <xs:element name="DataVersamento" type="xs:dateTime"/>
      <xs:element name="EsitoGenerale" type="ECEsitoGeneraleType"/>
      <xs:element name="EsitoChiamataWS" type="ECEsitoChiamataWSType"/>
      <xs:element name="EsitoXSD" type="ECEsitoXSDType"/>
      <xs:element name="Configurazione" type="ECConfigurazioneType" minOccurs="0"/>
      <xs:element name="UnitaDocumentaria" type="ECUnitaDocType" minOccurs="0"/>
      <xs:element name="XMLVersamento" type="xs:string" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
 </xs:element>
 <!-- -->
 <xs:element name="EsitoVersAggAllegati">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Versione" type="xs:string" minOccurs="0"/>
    <xs:element name="VersioneXMLChiamata" type="xs:string" minOccurs="0"/>
    <xs:element name="IdSIP" type="xs:string" minOccurs="1" maxOccurs="1"/>
    <xs:element name="DataVersamento" type="xs:dateTime"/>
    <xs:element name="EsitoGenerale" type="ECEsitoGeneraleType"/>
    <xs:element name="EsitoChiamataWS" type="ECEsitoChiamataWSType"/>
    <xs:element name="EsitoXSD" type="ECEsitoXSDAggAllType"/>
    <xs:element name="Configurazione" type="ECConfigurazioneType" minOccurs="0"/>
    <xs:element name="UnitaDocumentaria" type="ECUnitaDocAggAllType" minOccurs="0"/>
    <xs:element name="XMLVersamento" type="xs:string" minOccurs="0"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

REGIONE MARCHE

Manuale per gli utenti

Versamenti WEB-REST

Indice Generale

Introduzione

Il presente documento ha lo scopo di fornire una guida operativa all'utilizzo del sistema di conservazione degli archivi digitali Polo Marche DigiP, per gli utenti appartenenti ad un soggetto produttore (Ente) che negli accordi presi ha stabilito di effettuare versamenti tramite web service.

Premessa

Il processo di conservazione digitale si effettua sui seguenti pacchetti informativi:

- **pacchetto di versamento (SIP):** inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato nel presente Disciplinare e secondo le modalità riportate nel Manuale di conservazione;
- **pacchetto di archiviazione (AIP)**: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione e secondo le modalità riportate nel Manuale di conservazione;
- **pacchetto di distribuzione (DIP)**: pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta secondo le modalità riportate nel Manuale di conservazione.

I pacchetti di versamento (SIP) contengono aggregati logici definiti unità documentarie (UD): queste ultime sono formate da uno o più documenti considerati come un tutto unico e costituiscono le unità elementari di cui si compone l'archivio dell'Ente produttore.

L'Ente produttore sovrintende il processo di conservazione attraverso le seguenti aree funzionali:

- **INGEST**: è l'area funzionale che si occupa della ricezione dei pacchetti di versamento (SIP) trasmessi dall'Ente produttore; verifica l'integrità e la completezza dei pacchetti; mette a disposizione del produttore il Rapporto di Versamento (RdV); genera i pacchetti di archiviazione (AIP). In quest'area inoltre è possibile consultare la lista dei SIP ricevuti dal sistema ed effettuare il download degli stessi.
- **ACCESS**: è l'area funzionale dove si gestisce il flusso di richieste di documenti in uscita e la ricerca da parte dell'Ente produttore. Qui è possibile consultare i documenti archiviati e conservati ed effettuarne il download tramite la generazione de pacchetto di distribuzione (DIP).

Il Rapporto di Versamento (RDV), quale documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dall'Ente produttore, è firmato digitalmente dal Responsabile del servizio di conservazione e protocollato dal Sistema di Protocollo dell'Ente Polo. La segnatura di protocollo così ottenuta rappresenta un valido riferimento temporale opponibile a terzi.

1. ACCESSO AL SISTEMA

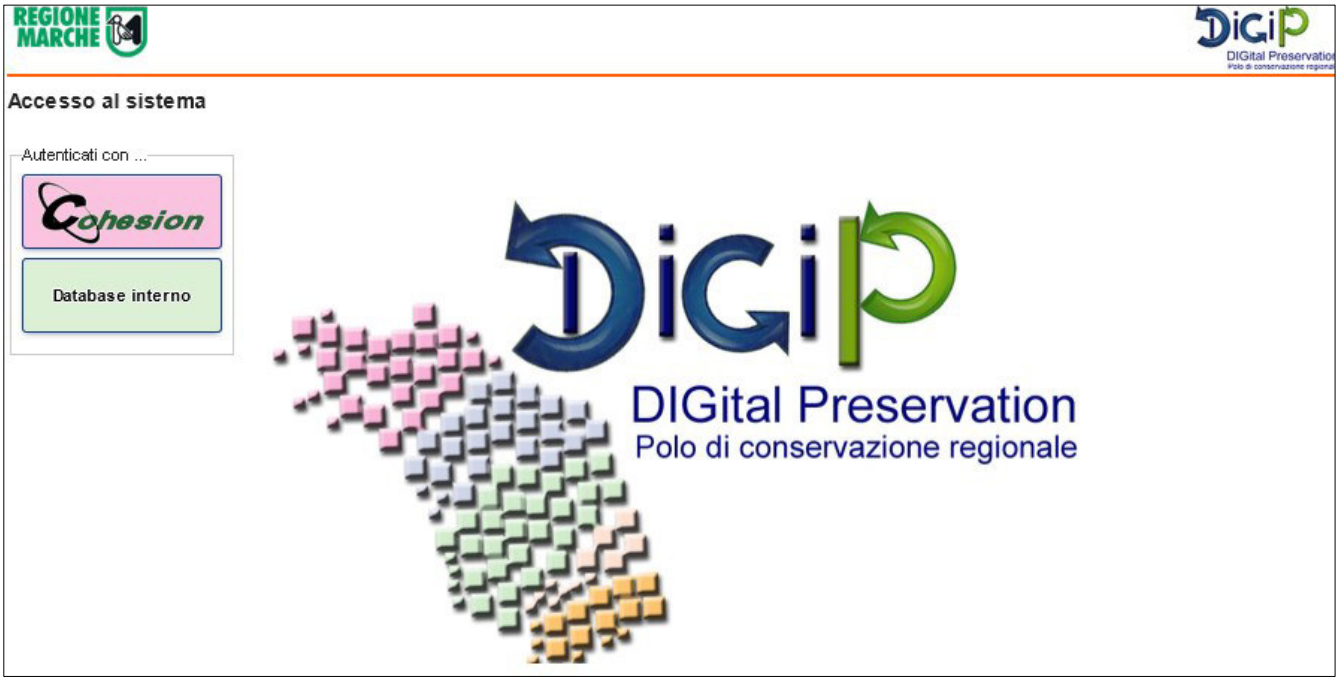
L'accesso all'applicativo DigiP avviene tramite il framework di autenticazione Cohesion, e il processo di autenticazione forte.

Vediamo di seguito i passaggi:

Modalità di accesso:

1. collegarsi all'applicativo DigiP attraverso l'indirizzo comunicato da Marche DigiP

2. l'utente visualizzerà la seguente maschera di Accesso al sistema



3. cliccare sul pulsante Cohesion 

4. l'utente visualizzerà la schermata sotto e dovrà autenticarsi con una delle seguenti modalità: Smart Card, Pin Cohesion, Otp Cohesion

NOTA: una volta autenticati è possibile navigare il sistema ma si precisa che nello specifico è possibile visualizzare solo le maschere relative ai ruoli e casi d'uso assegnati all'utente registrato.

2. Area Ingest

Di seguito verranno illustrati tutti i casi d'uso relativi al ruolo di ingest. Si precisa che è possibile che un utente non visualizzi tutte le seguenti maschere poichè non gli sono state assegnate quelle specifiche attività.

2.1. Esiti Versamenti

Definizione. La maschera denominata *Esiti versamenti* permette all'utente ingest di visualizzare, ricercare e monitorare i versamenti effettuati per uno specifico soggetto produttore.

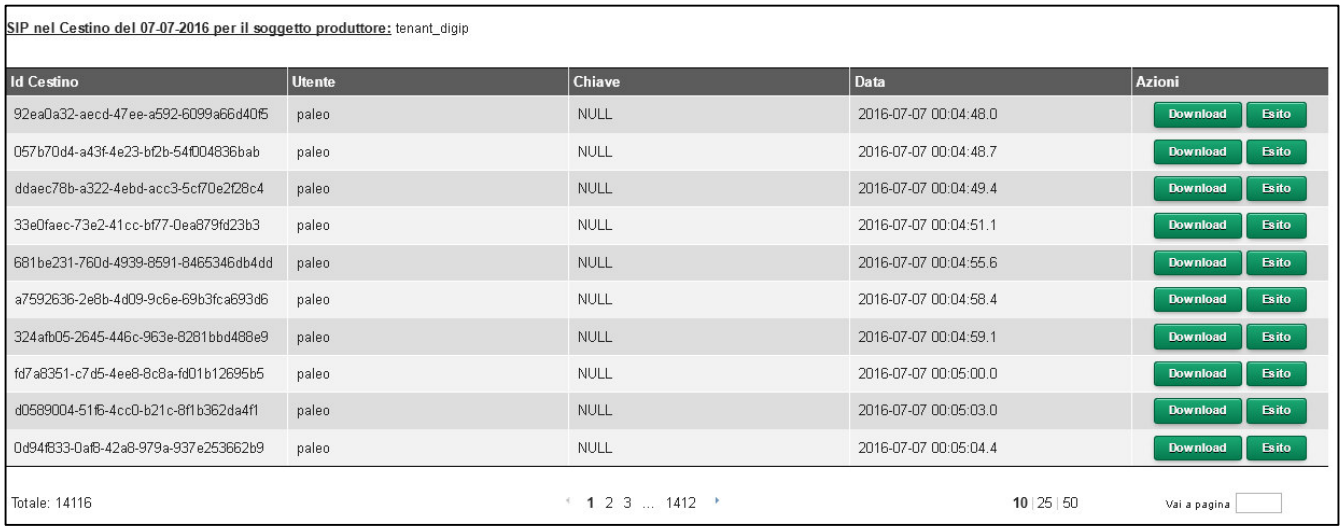
Per visualizzare i caricamenti bisogna cliccare il pulsante *Esiti versamenti*. Si aprirà una nuova schermata dove vengono visualizzati i versamenti del giorno.

Per fare una nuova ricerca si può selezionare da calendario la data o il periodo che si desidera visualizzare.

La tabella mostra i versamenti organizzati per data di versamento e i seguenti dettagli:

- Ricevuti: numero di versamenti effettuati dall'ente in quella specifica data. Il produttore trasmette i SIP nei modi definiti nell'accordo formale i quali vengono messi in coda per la validazione di qualità
- Presi In Carico: numero di versamenti formalmente corretti e presi in carico dal sistema
- Validati: rapporto di versamento risultato positivo. Significa che le regole di validazione definite nell'accordo formale risultano rispettate.
- Non validati: rapporto di versamento risultato negativo. Significa che se le regole di validazione definite nell'accordo formale non sono rispettate.
- Trasformati: numero di versamenti che hanno subito delle trasformazioni durante il processo di archiviazione. Il sistema, una volta che il SIP è stato positivamente validato, elabora il pacchetto fino alla generazione del corrispondente pacchetto di archiviazione (AIP)
- Completati: numero di pacchetti di archiviazione generati dal corrispondente pacchetto di versamento (SIP);
- Nel Cestino: numero di pacchetti di versamento (SIP) Ricevuti ma che non sono conformi alle agli accordi formali concordati tra il Produttore e il Polo di conservazione.

Azioni: cliccando sull'icona del *Cestino* si possono visualizzare tutti i pacchetti che sono stati scartati in quella determinata data e quindi non sono stati presi in carico dal sistema. La tabella mostra l'utente che ha effettuato il versamento, la chiave cioè il nome del pacchetto versato, la data e due link: *Download* che permette di recuperare il pacchetto zip versato e *Esito* che mostra il codice e il messaggio di errore.



SIP nel Cestino del 07-07-2016 per il soggetto produttore: tenant_digip

Id Cestino	Utente	Chiave	Data	Azioni
92ea0a32-aecd-47ee-a592-6099a66d40f5	paleo	NULL	2016-07-07 00:04:48.0	Download Esito
057b70d4-a43f-4e23-bf2b-54f004836bab	paleo	NULL	2016-07-07 00:04:48.7	Download Esito
ddaec78b-a322-4ebd-acc3-5cf70e2f28c4	paleo	NULL	2016-07-07 00:04:49.4	Download Esito
33e0faec-73e2-41cc-bf77-0ea879fd23b3	paleo	NULL	2016-07-07 00:04:51.1	Download Esito
681be231-760d-4939-8591-8465346db4dd	paleo	NULL	2016-07-07 00:04:55.6	Download Esito
a7592636-2e8b-4d09-9c6e-69b3fca693d6	paleo	NULL	2016-07-07 00:04:58.4	Download Esito
324afb05-2645-446c-963e-8281bbd488e9	paleo	NULL	2016-07-07 00:04:59.1	Download Esito
fd7a8351-c7d5-4ee8-8c8a-fd01b12695b5	paleo	NULL	2016-07-07 00:05:00.0	Download Esito
d0589004-51f6-4cc0-b21c-8f1b362da4f1	paleo	NULL	2016-07-07 00:05:03.0	Download Esito
0d94f833-0af8-42a8-979a-937e253662b9	paleo	NULL	2016-07-07 00:05:04.4	Download Esito

Totale: 14116 1 2 3 ... 1412 10 | 25 | 50 Vai a pagina

Operazioni:

Visualizza Versamenti. Per visualizzare i versamenti cliccare sulla data versamento. Si aprirà una nuova schermata che mostra in dettaglio l'elenco di tutti i versamenti effettuati in quel giorno e lo stato in cui si trovano:

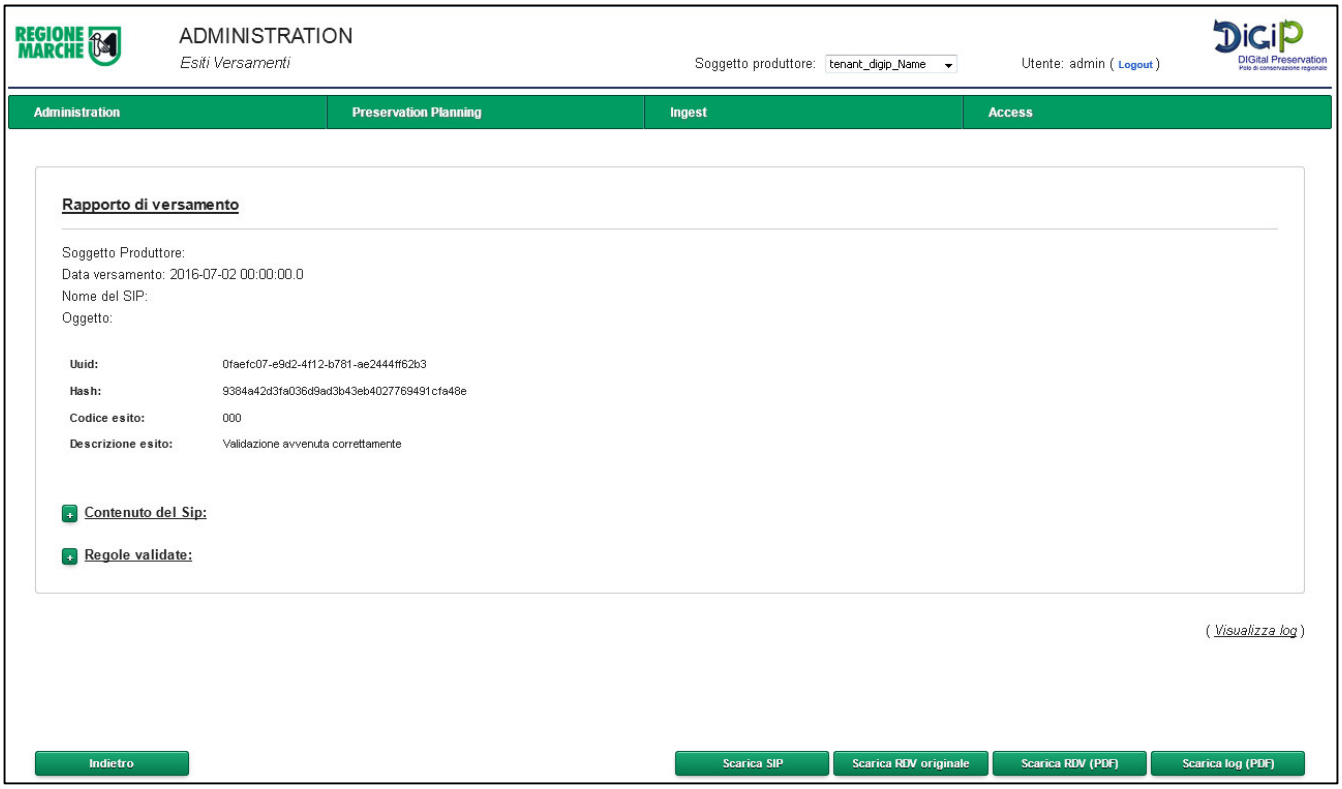
- NOT_VALIDATED: Sip che non è stato preso in carica
- ARCHIVED: Sip archiviato correttamente
- RUNNING: procedura di archiviazione ancora in corso
- ERROR: Sip andato in errore e non archiviato correttamente.

Da questa maschera cliccando sul pulsante *Scarica csv* è possibile scaricare un file csv con l'elenco di tutti i versamenti del giorno.

Premendo il pulsante *Visualizza* viene mostrato il rapporto di versamento dove è specificato in dettaglio l'esito del versamento, il contenuto del pacchetto e l'elenco delle regole validate con i relativi risultati. Cliccando su *Visualizza Log* vengono mostrati i passaggi operativi del sistema.

Da questa maschera è possibile scaricare:

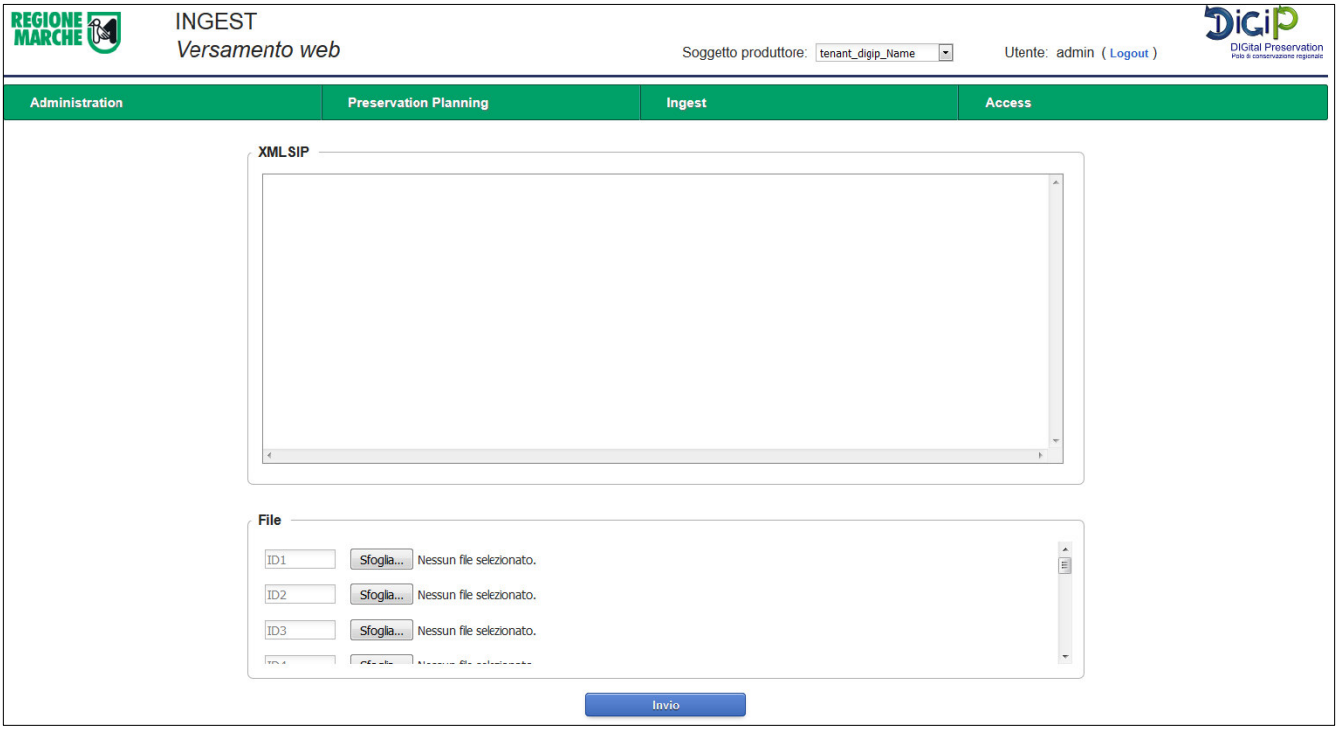
- SIP di partenza, pulsante *Scarica SIP*
- rapporto di versamento (firmato o non firmato a seconda della configurazione definita dal soggetto produttore), pulsante *Scarica RDV originale*
- rapporto di versamento in formato PDF, pulsante *Scarica RDV (PDF)*
- il log in formato PDF, pulsante *Scarica log (PDF)*



2.2. Versamento Web

Definizione. La maschera denominata V*ersamento Web* permette all'utente ingest di effettuare uno specifico versamento di un pacchetto SIP via Web. La maschera permette l'inserimento del file di indice descrittore con tutti i metadati e il caricamento dei file allegati nella seguente modalità:

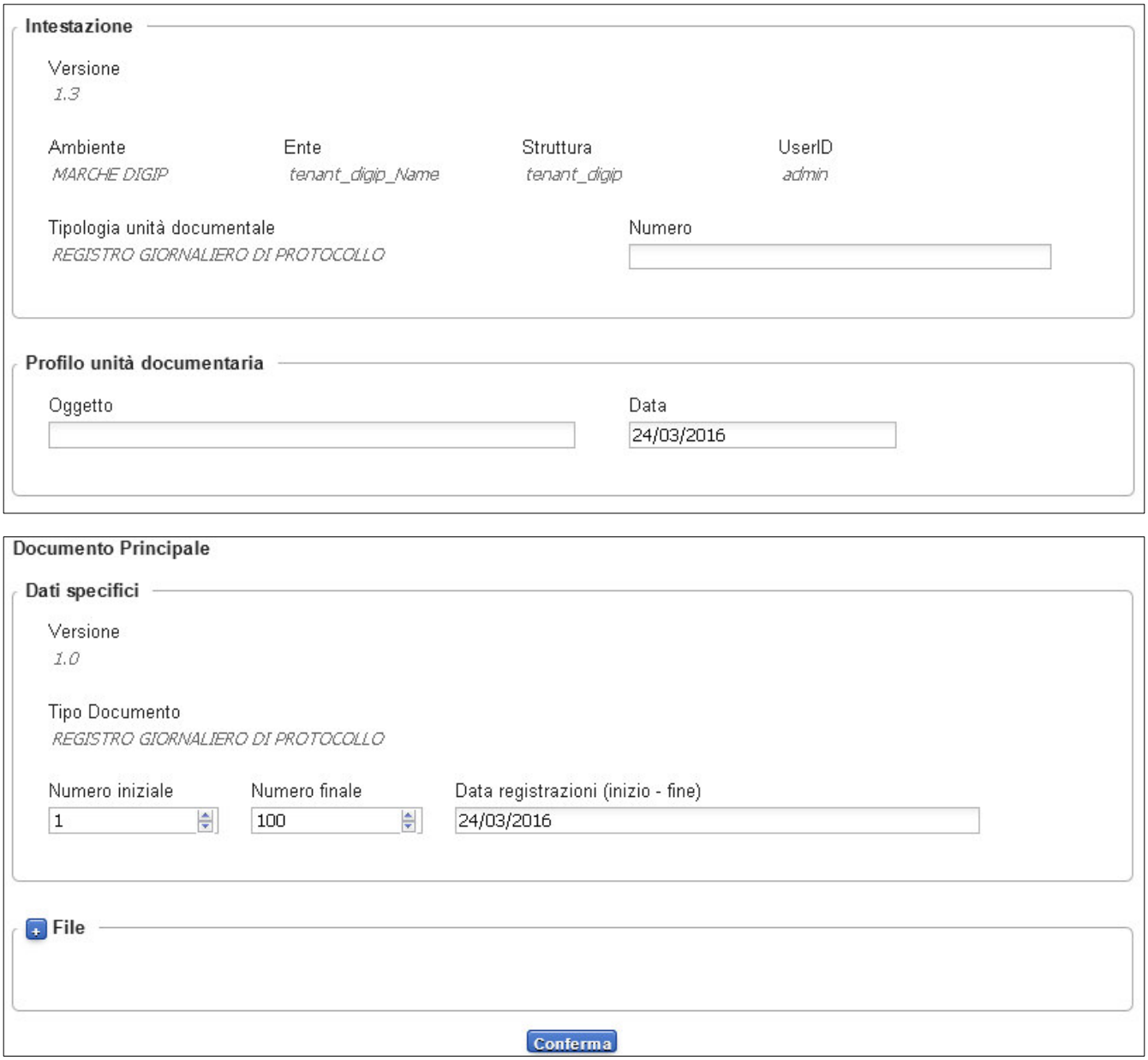
- Scrivere o fare copia e incolla nella casella di testo del file xml descrittore del pacchetto SIP.
- Inserire, in relazione a ciascun file da allegare, il valore corrispondente del tag ID presente sull'indice descrittore
- Selezionare e caricare i file allegati cliccando sul pulsante ***Sfoglia***.
- Una volta eseguite le operazioni premere il pulsante ***Invio*** per avviare la procedura di archiviazione. L'utente riceverà un messaggio di esito. L'utente riceverà un messaggio di esito che può anche scaricare come pdf (pulsante ***Scarica RDC (PDF)***). L'utente nella pagina Esiti Versamenti potrà seguire l'andamento del caricamento e recuperare il rapporto di versamento.



2.3. Versamento Web RPG

Definizione. La maschera denominata V*ersamento Web RPG* permette all'utente ingest di effettuare uno specifico versamento per i documenti di tipo Registro giornaliero di protocollo. La maschera permette l'inserimento dei metadati e il caricamento dei file nella seguente modalità:

- Inserire nei campi vuoti i corrispondenti valori come riportati nel Disciplinare tecnico, quali:
  - **Codice identificativo**: data del documento Registro giornaliero di protocollo (aaaa-mm-gg). Si precisa che questo valore verrà usato per definire il nome del pacchetto SIP.
  - **Oggetto**: descrivere cosa rappresenta l'Oggetto del documento Registro giornaliero di protocollo (ad es. Registro giornaliero di protocollo dal n. […] al n. […]).
  - **Data**: data del documento Registro giornaliero di protocollo.
  - **Numero iniziale**: numero della prima registrazione sul registro giornaliero.
  - **Numero finale**: numero dell'ultima registrazione sul registro giornaliero.
  - **Data registrazioni (inizio – fine)**: data della prima e dell'ultima registrazione del Registro giornaliero di protocollo.
- Selezionare e caricare il file Registro giornaliero di protocollo cliccando sul pulsante *File* e poi *Sfoglia*.
- Una volta eseguite le operazioni premere il pulsante *Conferma* per versare il Registro giornaliero di protocollo nel sistema di conservazione. L'utente riceverà un messaggio di esito. L'utente, nella pagina Esiti Versamenti, potrà seguire l'andamento del caricamento e recuperare il rapporto di versamento.


Intestazione
Versione
1.3
Ambiente
MARCHE DIGIP
Ente
tenant_digip_Name
Struttura
tenant_digip
UserID
admin
Tipologia unità documentale
REGISTRO GIORNALIERO DI PROTOCOLLO
Numero
Profilo unità documentaria
Oggetto
Data
24/03/2016

Documento Principale
Dati specifici
Versione
1.0
Tipo Documento
REGISTRO GIORNALIERO DI PROTOCOLLO
Numero iniziale
1
Numero finale
100
Data registrazioni (inizio - fine)
24/03/2016
File
Conferma

3. Area Access

Di seguito verranno illustrati tutti i casi d'uso relativi al ruolo di access. Si precisa che è possibile che un utente non visualizzi tutte le seguenti maschere poichè non gli sono state assegnate quelle specifiche attività.

3.1. Elenco Questionari

Definizione. La maschera denominata *Elenco Questionari* permette all'utente access di poter visualizzare l'elenco dei questionari che gli sono stati pubblicati. Per ogni questionario è specificato il titolo, una descrizione sommaria di cosa tratta, il numero di domande a cui rispondere e la data di scadenza, cioè la data ultima entro la quale l'utente può compilare il questionario. Superata questa data non sarà più possibile rispondere alle domande.

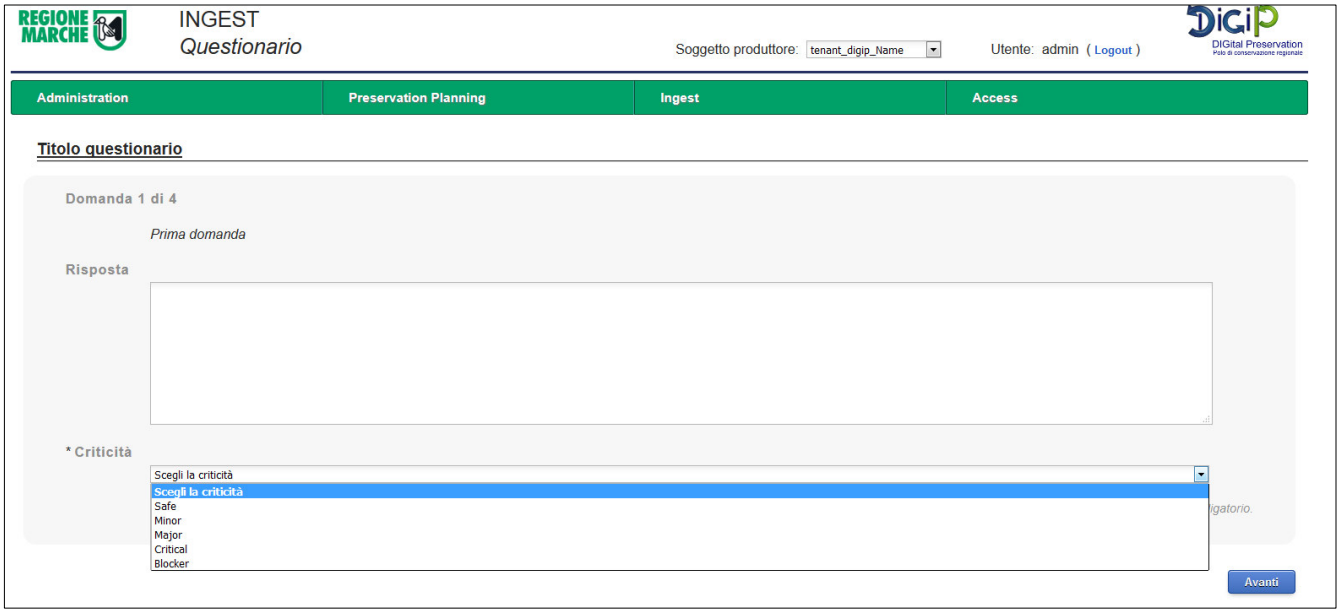
Cliccando sul pulsante *Visualizza questionario* l'utente può iniziare a visualizzare e a compilare il questionario. La risposta alle domande è suddivisa in risposta e criticità. La criticità è l'unico campo obbligatorio e rappresenta il livello di difficoltà causato dall'argomento del testo della domanda durante l'utilizzo del sistema.

Nella casella di testo risposta l'utente può aggiungere informazioni e commenti sul problema in questione che sarà utile al miglioramento del sistema.

Con il pulsante *Avanti* si può passare alla domanda successiva e così via. Arrivati all'ultima domanda ci sarà il pulsante *Fine*. Cliccando questo pulsante il questionario verrà chiuso e dichiarato completato.

Si può abbandonare e modificare il questionario in qualsiasi momento entro la data di scadenza, le risposte già date vengono mantenute.

Una volta però cliccato il pulsante *Fine* non sarà più possibile la modifica ma solo la visualizzazione delle risposte date.



3.2. Gestione DIP

Definizione. La maschera denominata *Gestione DIP* permette all'utente access di generare e scaricare pacchetti di distribuzione (DIP) a partire dagli AIP, versamenti archiviati. La ricerca degli AIP è fatta per data versamento. Una volta definito il perido la tabella mostrerà l'elenco dei pacchetti presenti sul database. Si precisa che il tutto è vincolato dal soggetto produttore e dal livello di riservatezza dell'utente che effettua la ricerca. Non saranno quindi visibili tutti gli AIP ma solo quelli che di cui l'utente ha accesso.

Operazioni:

1. **Genera DIP:** è possibile generare DIP selezionando con un flag gli AIP da cui si desidera partire. Terminata la selezione premere il pulsante *Genera DIP.* Una volta che un DIP è creato apparirà in tabella, nella colonna *DIP generati,* il valore del suo dell'identificativo. Con il tasto *Aggiorna* si può mantenere monitorata la procedura di creazione.
2. **Download DIP:** una volta generati i DIP è possibile scaricare i pacchetti (file .zip) premendo il pulsante relativo *Download DIP.*

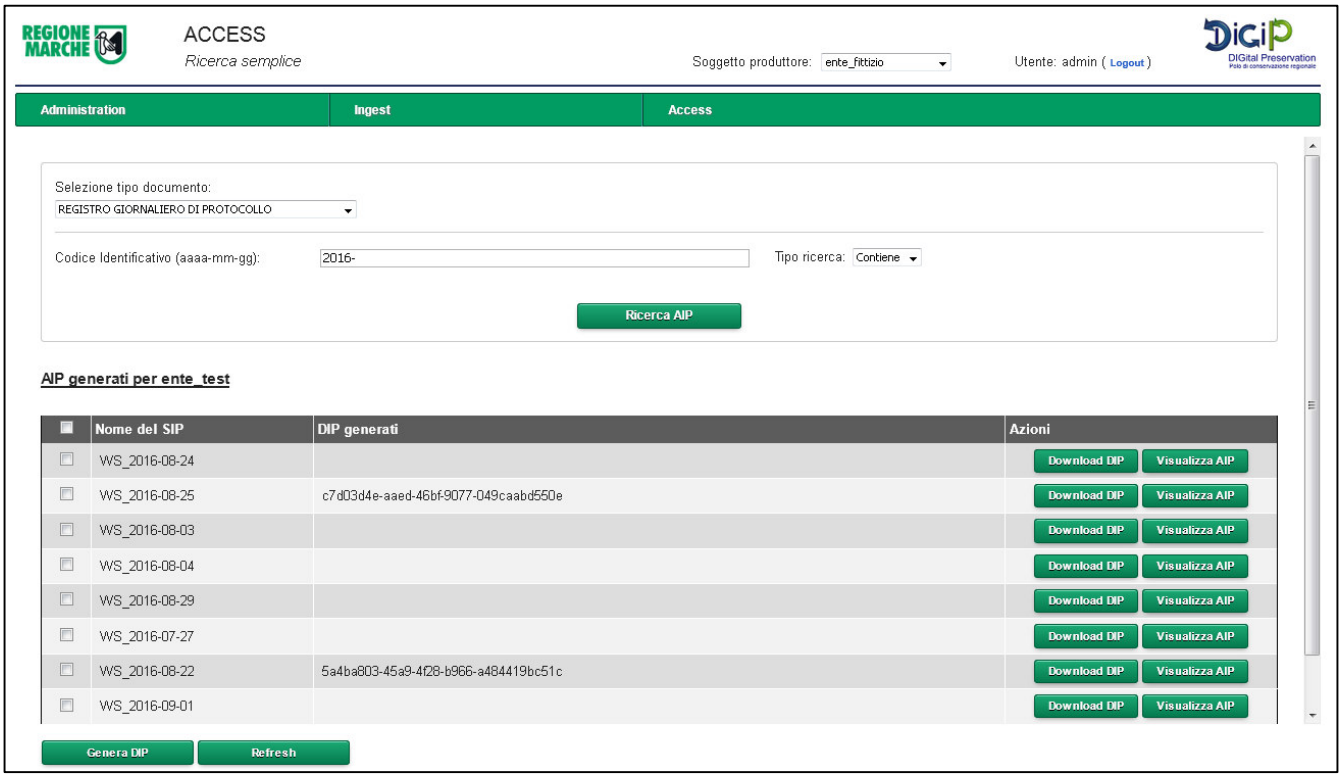
3.3. Ricerca semplice

Definizione. La maschera denominata *Ricerca semplice* permette all'utente con questo ruolo di cercare pacchetti AIP tramite i suoi metadati. La ricerca viene filtrata per tipologia documentale. Una volta selezionata vengono mostrati alcuni nomi di metadati: per la precisione vengono visualizzate le etichette definite dall'amministratore nella maschera *configurazione ricerca.* Inserire nella casella di testo il valore e dal menu a tendina il tipo di ricerca che si vuole effettuare: esatta(=) o contiene(like). Una volta terminato cliccare il pulsante *Ricerca AIP.* Il sistema mostrerà a video gli AIP corrispondenti alle coppie chiave-valore definite.

Una volta trovati i pacchetti sono possibili le seguenti operazioni.

Operazioni:

1. **Genera DIP:** è possibile generare DIP selezionando con un flag gli AIP da cui si desidera partire. Terminata la selezione premere il pulsante *Genera DIP.* Una volta che un DIP è creato apparirà in tabella, nella colonna *DIP generati,* il valore del suo dell'identificativo. Con il tasto *Refresh* si può mantenere monitorata la procedura di creazione.
2. **Download DIP:** una volta generati i DIP è possibile scaricare i pacchetti (file .zip) premendo il pulsante relativo *Download DIP.*
3. **Visualizza AIP:** cliccando sul pulsante corrispondente è possibile vedere il dettaglio del pacchetto AIP: i file, i metadati dei file e del descrittore suddivisi per tipologia e scaricare lo zip.



3.4. Ricerca avanzata

Definizione. La maschera denominata *Ricerca avanzata* permette all'utente con questo ruolo di cercare pacchetti AIP tramite i suoi metadati. La ricerca viene filtrata per tipologia documentale. Una volta selezionata vengono mostrati alcuni nomi di metadati: per la precisione vengono visualizzate le etichette definite dall'amministratore nella maschera *configurazione ricerca.* Inserire nella casella di testo il valore e dal menu a tendina il tipo di ricerca che si vuole effettuare: esatta(=) o contiene(like). Con il pulsante *Aggiungi* criterio è possibile inserire un nuovo metadato non presente. Una volta terminato cliccare il pulsante *Ricerca AIP.* Il sistema mostrerà a video gli AIP corrispondenti alle coppie chiave-valore definite.

NOTA: gli AIP restituiti sono tutti quelli che soddisfano i parametri di ricerca e soprattutto sono solo quelli che per vincoli di riservatezza l'utente può visualizzare.

Una volta trovati i pacchetti sono possibili le seguenti operazioni.

Operazioni:

1. **Genera DIP:** e' possibile generare DIP selezionando con un flag gli AIP da cui si desidera partire. Terminata la selezione premere il pulsante *Genera DIP.* Una volta che un DIP è creato apparirà in tabella, nella colonna *DIP generati,* il valore del suo dell'identificativo. Con il tasto *Refresh* si può mantenere monitorata la procedura di creazione.
2. **Download DIP:** una volta generati i DIP è possibile scaricare i pacchetti (file .zip) premendo il pulsante relativo *Download DIP.*
3. **Visualizza AIP:** cliccando sul pulsante corrispondente è possibile vedere il dettaglio del pacchetto AIP: i file, i metadati dei file e del descrittore suddivisi per tipologia e scaricare lo zip.

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 14

PIANO DI CONSERVAZIONE

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

Premessa

L'art. 68 del DPR 445/2000 prevedeva che ogni amministrazione si dotasse di un «piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti». La normativa quindi, concepisce la selezione come operazione critica di vaglio della documentazione prodotta, funzionale a una migliore conservazione dell'archivio. La selezione non intacca la complessità e l'unitarietà dell'archivio; ma, procedendo all'individuazione dei documenti strumentali e transitori, da destinare allo scarto, vale a dire alla distruzione fisica, evidenzia i nessi fra i documenti essenziali da conservare permanentemente. Perciò l'eliminazione di taluni documenti deve essere preceduta dalla valutazione delle procedure di produzione documentaria, in modo che vengano assicurati la comprensione dell'attività dell'ente produttore e il mantenimento delle attestazioni di diritti.

In merito allo scarto archivistico, è opportuno ricordare che gli enti pubblici – e tra questi l'ATA – devono ottenere per tale intervento l'autorizzazione del Ministero per i beni e le attività culturali, ai sensi dell'art. 21, comma 1, lettera d) del Codice dei beni culturali e del paesaggio (D. lgs. 22 gennaio 2004, n. 42).

La stesura del Piano di conservazione è avvenuta avendo presente quello elaborato dal Gruppo di Lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni del 2005.

Le procedure di scarto

Lo scarto – ma meglio sarebbe usare il termine selezione – di documenti è previsto dal *Codice dei Beni Culturali* (art. 21 comma 1, lettera d; art. 41, comma 3) e rappresenta una delle più delicate attività afferenti alla tutela archivistica. Esso è finalizzato alla migliore preservazione dei documenti che sono stati selezionati per la conservazione per-manente, eliminando masse documentarie non più necessarie per l'attività amministrati-va e sovrabbondanti per la tradizione della memoria storica.

I presupposti per lo scarto sono:

- che la serie archivistica da scartare sia compresa come tale nel piano di conservazione e che siano trascorsi i termini per poter procedere allo scarto;
- che i documenti da scartare non possiedano più alcuna rilevanza sul piano amministrativo e giuridico, che si riferiscano a procedimenti conclusi e non più suscettibili di ulteriori interventi di ordine amministrativo o giurisdizionale;
- che i documenti da scartare siano privi d'interesse ai fini della trasmissione della memoria storica e per la ricerca scientifica.

Recentemente la Direzione generale per gli archivi ha prescritto con proprie circolari (nn. 18, 27 e 33/2008; ma si veda anche la circolare n. 44/2005, relativa agli archivi degli istituti scolastici) che, per procedere allo scarto, occorre avere preliminarmente accertato che delle attività amministrative (o giudiziarie) documentate negli atti di cui si propone lo scarto rimanga comunque traccia essenziale in serie documentarie destinate alla conservazione permanente (ad esempio, a seconda dei casi: protocolli d'ufficio, registri ufficiali di contabilità, rubriche o schedari).

Al termine del lavoro selettivo è fondamentale e necessaria l'approvazione da parte della Soprintendenza archivistica per Umbria e Marche dell'elenco di consistenza contenente il dettaglio della documentazione da scartare, corroborata da debite motivazioni.

Regole generali

- Lo scarto si effettua di norma sui documenti dell'archivio di deposito.
- I termini cronologici indicati devono essere conteggiati dalla chiusura dell'affare.
- L'applicazione del piano di conservazione non può comunque essere automatica, ma si devono valutare caso per caso le eventuali particolarità.
- Lo scarto, se non viene effettuato regolarmente ogni anno e su un archivio organizzato, potrà essere deciso e valutato solo dopo che l'intero complesso archivistico sia stato analizzato e almeno sommariamente riordinato.
- Il Comune non deve scartare i documenti considerati "vitali" (ad esempio quelli che in caso di disastro, sono necessari a ricreare lo stato giuridico dell'ente e la sua situazione legale e finanziaria, a garantire i diritti dei dipendenti e dei cittadini, a soddisfare i suoi obblighi e a proteggere i suoi interessi esterni).
- Lo scarto dei documenti in copia può essere facilmente effettuato qualora sia prevista la conservazione permanente dei documenti in originale e qualora le copie non contengano annotazioni amministrative o visti essenziali per ricostruire il procedimento nella sua correttezza.
- I RPA (Responsabili dei procedimenti Amministrativi), durante la formazione dell'archivio corrente, hanno cura di non inserire nel fascicolo copie superflue di normative o atti repertoriati di carattere generale, facilmente reperibili in un sistema informatico-archivistico ben organizzato.
- Al momento del versamento in deposito i RPA, inoltre, provvedono a togliere dal fascicolo le copie e i documenti, che hanno appunto carattere strumentale e transitorio, utilizzati per espletare il procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad esempio, appunti, promemoria, copie di normativa e documenti di carattere generale).
- Si possono, quindi, scartare in itinere (ovvero nel passaggio dall'archivio corrente all'archivio di deposito):
  - ✓ le copie, purché non contengano annotazioni amministrative o visti essenziali per ricostruire il procedimento nella sua correttezza e nella sua completezza
  - ✓ i documenti strumentali e transitori: ad esempio, le ricevute di pagamento dei servizi a richiesta; le domande di congedo, che non comportino conseguenze sulla carriera del dipendente
  - ✓ le serie che l'ente possiede per conoscenza.
- I tempi di conservazione sono previsti genericamente dal codice civile in materia di prescrizione (libro VI, titolo V); queste indicazioni vanno integrate con la normativa inerente alla tipologia documentale interessata.
- In ogni caso valgono due principi fondamentali: rilevanza e pertinenza della documentazione per il Soggetto Produttore.

Conservazione permanente

Alcune tipologie documentali sono totalmente esenti da scarto. Ecco le principali:

- Decreti
- Contratti, convenzioni e atti rogati
- Registri/Repertori
- Verbali del Consiglio di Amministrazione e di ogni altro organo collegiale
- Regolamenti
- Direttive e Disposizioni Generali
- Repertori generali e particolari
- Manualistica prodotta dal Comune
- Statistiche (esclusi i materiali preparatori)
- Fascicoli del personale
- Bandi di gara e graduatorie
- Verbali di Controlli e visite ispettive
- Pubblicazioni istituzionali
- Convocazioni se non riportate nei verbali
- Corrispondenza istituzionale
- Bilanci
- Inventari di beni mobili e immobili
- Pareri e consulenze legali
- Documenti relativi a contenziosi
- Documentazione di Uffici Tecnici e Urbanistici
- Catasto

Massimario di selezione e scarto o Piano della Conservazione

Il Comune ha adottato il documento del Gruppo di lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni (2005) e lo ha modificato e integrato a seconda delle tipologie documentali da esso prodotte.

titolo/classe	*tipologie documentarie*	*tempo conservazione*
1	***AMMINISTRAZIONE GENERALE***	
1.1	LEGISLAZIONE E CIRCOLARI ESPLICATIVE	
	Pareri chiesti dall'ATA su leggi specifiche	Permanente
	Circolari pervenute: repertorio annuale	Permanente
	Circolari emanate dall'ATA: repertorio annuale	Permanente
1.2	ATTI ISTITUTIVI E REGOLAMENTARI	
	Redazione, modifiche e interpretazioni dello statuto e della convenzione	Permanente, dopo sfoltimento del materiale informativo relativo ad altri Comuni
	Regolamenti emessi dall'ATA: repertorio annuale	Permanente
	Redazione dei regolamenti: un fasc. per ciascun affare	Permanente, previo sfoltimento dei documenti di carattere transitorio
1.3	ARCHIVIO GENERALE	
	Registro di protocollo	Permanente
	Repertorio dei fascicoli	Permanente
	Organizzazione del servizio e dell'attività ordinaria (aggiornamento del manuale di gestione con titolario e piano di conservazione, selezione periodica, riordino, inventariazione, spostamenti e versamenti di materiale, depositi e comodati):	Permanente
	Interventi straordinari (ad esempio, traslochi, restauri, gestione servizi esterni, scelta del software di gestione)	Permanente
	Richieste di accesso per fini amministrativi	1 anno dalla ricollocazione del materiale
	Richieste di informazioni archivistiche e richieste per motivi di studio	Permanente
	Richieste di pubblicazione all'albo pretorio	1 anno
	Registro dell'Albo pretorio	20 anni
	Registri delle spedizioni e delle spese postali	1 anno
	Decreti del Presidente: repertorio	Permanente
	Determinazioni dei dirigenti: repertorio	Permanente
	Deliberazioni dell'Assemblea: repertorio	Permanente
	Verbali delle adunanze dell'Assemblea: repertorio	Permanente
	Verbali degli altri organi collegiali dell'ATA: repertorio	permanente
	Contratti e convenzioni: repertorio	Permanente
1.4	SISTEMA INFORMATIVO	
	Organizzazione del sistema	Permanente
	Statistiche	Permanente, dopo l'eliminazione dei materiali preparatori

1.5	INFORMAZIONI E COMUNICAZIONI AD ENTI E CITTADINI	
	Iniziative specifiche dell'URP: un fasc. per ciascun affare	Permanente, dopo sfoltimento del carteggio di carattere transitorio e strumentale
	Reclami dei cittadini (comunque pervenuti)	Permanente
	Bandi e avvisi a stampa	Permanente
	Materiali preparatori per il sito Web	Permanente
1.6	POLITICA DEL PERSONALE, ORDINAMENTO DEGLI UFFICI E DEI SERVIZI	
	Attribuzione di competenze agli uffici	Permanente
	Organigramma: un fasc. per ciascuna definizione dell'organigramma	Permanente
	Organizzazione degli uffici: un fasc. per ciascun affare	Permanente
	Orari di apertura degli uffici	Permanente
	Materiale preparatorio per le deliberazioni in materia di politica del personale	10 anni
1.7	RELAZIONI CON LE ORGANIZZAZIONI SINDACALI E DI RAPPRESENTANZA DEL PERSONALE	
	Rapporti di carattere generale	Permanente
	Costituzione delle rappresentanze del personale	Permanente
	Verbali della Delegazione trattante per la contrattazione integrativa decentrata	Permanente
1.8	CONTROLLI INTERNI ED ESTERNI	
	Controlli	permanente
1.9	EDITORIA ED ATTIVITA' INFORMATIVO-PROMOZIONALE INTERNA ED ESTERNA	
	Pubblicazioni istituzionali dell'ATA (libri, riviste, inserzioni o altro)	Permanente
	Pubblicazioni istituzionali dell'ATA (materiali preparatori)	2 anni
	Comunicati stampa	Permanente
1.10	CERIMONIALE, ATTIVITA' DI RAPPRESENTANZA, RICONOSCIMENTI	
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente
	Concessione dell'uso del logo: un fascicolo annuale	Permanente
1.11	RAPPORTI ISTITUZIONALI	
1.12	FORME ASSOCIATIVE PER ESERCIZIO DI FUNZIONI E SERVIZI E ADESIONE AD ASSOCIAZIONI	
	Costituzione di enti controllati dall'ATA (comprensivo della nomina dei rappresentanti e dei verbali inviati per approvazione)	Permanente, previo sfoltimento del carteggio di carattere transitorio
	Partecipazione dell'ATA a enti e associazioni (comprensivo della nomina dei rappresentanti)	Permanente, previo sfoltimento del carteggio di carattere transitorio

2	***ORGANI DI GOVERNO, GESTIONE, CONTROLLO, CONSULENZA E GARANZIA***	
2.1	PRESIDENTE	
	Fascicolo personale che dura quanto il mandato	Permanente
2.2	ASSEMBLEA DEGLI ENTI CONVENZIONATI	
	Convocazioni dell'Assemblea e OdG	1 anno (purché riportati nei verbali)
	Interrogazioni e mozioni	Permanente (dopo sfoltimento)
	Bollettino della situazione patrimoniale dei titolari di cariche elettive e di cariche direttive	Permanente
2.3	COMITATO DI COORDINAMENTO	
	Verbali	permanente
2.4	COMMISSARIO STRAORDINARIO	
	Fascicolo personale	Permanente
2.5	DIRETTORE E DIRIGENZA	
	Fascicolo personale	Permanente
2.6	REVISORI DEI CONTI	
	Fascicolo personale	Permanente
2.7	COMMISSARIO 'ad acta'	
	Fascicolo personale	Permanente
2.8	ORGANI DI CONTROLLO INTERNI	
	un fascicolo per ogni organo	Permanente
2.9	ORGANI CONSULTIVI	
	un fascicolo per ogni organo	Permanente
3	***RISORSE UMANE***	
3.0	FASCICOLI DEL PERSONALE	
	Fascicoli personali dei dipendenti e assimilati (quindi anche collaboratori a contratto o a progetto)	Permanente previo sfoltimento da eseguire seguendo la tempistica prevista per le singole classi
3.1	CONCORSI, SELEZIONI, COLLOQUI	
	Criteri generali e normativa per il reclutamento del personale: un fasc. con eventuali sottofascicoli	Permanente
	Procedimenti per il reclutamento del personale: un fasc. per ciascun procedimento (fasc. per affare), con i seguenti sottofascicoli:	
	- bando e manifesto	permanente
	- domande	1 anno dopo la scadenza dei termini per i ricorsi
	- allegati alle domande (ove previsti dal bando)	da restituire dopo la scadenz dei termini per i ricorsi
	- verbali	permanente
	- prove d'esame	1 anno dopo la scadenza dei termini per i ricorsi

	- copie bando restituite all'ATA	1 anno dopo la scadenza dei termini per i ricorsi
	Curricula inviati per richieste di assunzione	2 anni
	Domande di assunzione pervenute senza indizione di concorso o selezione	1 anno
3.2	ASSUNZIONI E CESSAZIONI	
	Criteri generali e normativa per le assunzioni e cessazioni	Permanente
	Determinazioni di assunzione e cessazione dei singoli inserite nei singoli fascicoli personali	Permanente
3.3	COMANDI E DISTACCHI, MOBILITA'	
	Criteri generali e normativa per comandi, distacchi, mobilità	Permanente
	Determinazioni di comandi, distacchi e mobilità inserite nei singoli fascicoli personali	Permanente
3.4	ATTRIBUZIONE DI FUNZIONI, ORDINI DI SERVIZIO E MISSIONI	
	Criteri generali e normativa per le attribuzioni di funzioni, ordini di servizio e missioni	Permanente
	Determinazioni di attribuzione di funzioni inserite nei singoli fascicoli personali	Permanente
	Determinazioni di missioni inserite nei singoli fascicoli personali	10 anni
	Determinazioni di ordini di servizio inserite nei singoli fascicoli PERSONALI	Permanente
	Ordini di servizio collettivi	Permanente
	Autorizzazione allo svolgimento di incarichi esterni	2 anni
3.5	INQUADRAMENTI ED APPLICAZIONE CONTRATTI COLLETTIVI DI LAVORO	
	Criteri generali e normativa per gli inquadramenti e le applicazione dei contratti collettivi di lavoro	Permanente
	Determinazione dei ruoli e contratti collettivi	Permanente
	Determinazioni relative ai singoli dipendenti	Permanente
3.6	RETRIBUZIONI E COMPENSI	
	Criteri generali e normativa per le retribuzioni e compensi	Permanente
	Anagrafe delle prestazioni: schede	5 anni
	Determinazioni inserite nei singoli fascicoli personali	5 anni dalla cessazione dal servizio
	Ruoli degli stipendi: base di dati/ tabulati	Permanente
	Provvedimenti giudiziari di requisizione dello stipendio	5 anni
3.7	TRATTAMENTO FISCALE, CONTRIBUTIVO ED ASSICURATIVO	
	Criteri generali e normativa per gli adempimenti fiscali, contributivi e assicurativi	Permanente

	Trattamento assicurativo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo
	Trattamento contributivo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo
	Trattamento fiscale inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo
	Assicurazione obbligatoria inserita nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo
3.8	TUTELA DELLA SALUTE E SICUREZZA SUL LUOGO DI LAVORO	
	Criteri generali e normativa per la tutela della salute e sicurezza sul luogo di lavoro	Permanente
	Rilevazione dei rischi, ai sensi della 626/94: un fasc. per sede	Tenere l'ultima e scartare la precedente
	Prevenzione infortuni	Permanente
	Registro infortuni	Permanente
	Verbali delle rappresentanze dei lavoratori per la sicurezza	Permanente
	Denuncia di infortunio e pratica relativa, con referti, inserita nei singoli fascicoli personali	Permanente
	Fascicoli relativi alle visite mediche ordinarie (medicina del lavoro	10 anni
3.9	DICHIARAZIONI DI INFERMITA' ED EQUO INDENNIZZO	
	Criteri generali e normativa per le dichiarazioni di infermità	Permanente
	Dichiarazioni di infermità e calcolo dell'indennizzo inserite nel singolo fascicolo personale	Permanente
3.10	INDENNITA' PREMIO DI SERVIZIO E TRATTAMENTO DI FINE RAPPORTO, QUIESCIENZA	
	Criteri generali e normativa per il trattamento di fine rapporto	Permanente
	Trattamento pensionistico e di fine rapporto inserito nel singolo fascicolo personale	Permanente
3.11	SERVIZI AL PERSONALE SU RICHIESTA	
	Criteri generali e normativa per i servizi su richiesta	Permanente
	Domande di servizi su richiesta (mensa, asili nido, colonie estive, soggiorni climatici, etc.)	2 anni
3.12	ORARIO DI LAVORO, PRESENZA ED ASSENZE	
	Criteri generali e normativa per le assenze	Permanente
	Domande e dichiarazioni dei dipendenti sull'orario inserite nel singolo fascicolo personale:	
	- 150 ore	2 anni
	- permessi d'uscita per motivi personali	2 anni
	- permessi per allattamento	2 anni
	- permessi per donazione sangue	2 anni

	- permessi per motivi sindacali	2 anni
	- opzione per orario particolare e part-time	permanente
	Domande e dichiarazioni dei dipendenti sulle assenze (con allegati) inserite nel singolo fascicolo personale:	
	- congedo ordinario	2 anni
	- congedo straordinario per motivi di salute	2 anni
	- congedo straordinario per motivi personali e familiari	alla cessazione del servizio
	- aspettativa per infermità	permanente
	- aspettativa per mandato parlamentare o altre cariche elettive	permanente
	- aspettativa obbligatoria per maternità e puerperio	permanente
	- aspettativa facoltativa per maternità e puerperio	permanente
	- aspettativa per motivi di famiglia	permanente
	- aspettativa sindacale	permanente
	- certificati medici	alla cessazione del servizio
	Referti delle visite di controllo inseriti nel fascicolo personale	alla cessazione del servizio
	fogli firma, cartellini marcatempo, tabulati elettronici di rilevazione presenze	2 anni (in assenza di pendenze disciplinari o giuridiche)
	Rilevazione delle assenze per sciopero:	
	- singole schede	1 anno dopo la redazione dei prospetti riassuntivi
	- prospetti riassuntivi	permanente
3.13	GIUDIZI, RESPONSABILITA' E PROVVEDIMENTI DISCIPLINARI	
	Criteri generali e normativa per i provvedimenti disciplinari	Permanente
	Provvedimenti disciplinari inseriti nel singolo fascicolo personale	Permanente
3.14	FORMAZIONE ED AGGIORNAMENTO PROFESSIONALE	
	Criteri generali e normativa per la formazione e l'aggiornamento professionale	Permanente
	Organizzazione di corsi di formazione e aggiornamento: un fasc. per ciascun corso	Permanente previo sfoltimento dopo 5 anni
	Domande/Invio dei dipendenti a corsi inseriti nel singolo fascicolo personale	Permanente previo sfoltimento dopo 5 anni
3.15	COLLABORATORI ESTERNI	
	Criteri generali e normativa per il trattamento dei collaboratori esterni	Permanente
	Elenco degli incarichi conferiti: repertorio	Permanente
4	***RISORSE FINANZIARIE E PATRIMONIO***	
4.1	BILANCIO PREVENTIVO E PIANO ESECUTIVO DI GESTIONE (PEG)	
	Bilancio preventivo e allegati, tra cui Relazione previsionale e programmatica	Permanente

	PEG: articolato in fascicoli: un fasc. per ogni obiettivo	Permanente, previo sfoltimento
	Carteggio prodotto dai differenti uffici dell'Ente per questioni afferenti alla formazione del bilancio e del PEG	10 anni
4.2	GESTIONE DEL BILANCIO E DEL PEG (CON EVENTUALI VARIAZIONI)	
	Gestione del bilancio: un fascicolo per ciascuna variazione	Permanente, previo sfoltimento
4.3	GESTIONE DELLE ENTRATE: ACCERTAMENTO, RISCOSSIONE, VERSAMENTO	
	Quote dei Comuni per funzionamento ATA. Con sottofascicolo per ciascun Comune.	3 anni dalla riscossione
	Quote dei Comuni per servizio rifiuti. Con sottofascicolo per ciascun Comune.	3 anni dalla riscossione
	Contributi regionali o di altri enti con beneficiario diretto ATA: un fascicolo per ciascun finanziamento	5 anni dalla riscossione
	Contributi regionali o di altri enti con beneficiario diversi: un fascicolo per ciascun finanziamento con un sottofascicolo per ciascun beneficiario	5 anni dalla riscossione
	Contratti di mutuo: un fascicolo per ciascun mutuo	5 anni dall'estinzione del mutuo
	Proventi da affitti e locazioni: un fasc. annuale per ciascun immobile locato	5 anni dal termine del contratto
	Diritti di copia e riscossioni diverse. Un fascicolo per tipologia di versamento	2 anni dal versamento ovvero dal rimborso a seguito di istanza
	Reversali	5 anni
4.4	GESTIONE DELLA SPESA: IMPEGNO, LIQUIDAZIONE, ORDINAZIONE E PAGAMENTO	
	Impegni di spesa (determinazioni dei dirigenti delle UOR): repertorio annuale	5 anni
	Fatture ricevute	10 anni
	Decreti di liquidazione con allegati: repertorio annuale	5 anni
	Mandati di pagamento con allegati inviati alla Tesoreria: repertorio annuale	10 anni dall'approvazione del bilancio purché registrati in scritture contabili di sintesi
	Eventuali copie di mandati	2 anni
4.5	PARTECIPAZIONI FINANZIARIE	
	Gestione delle partecipazioni finanziarie: un fasc. per ciascuna partecipazione	Permanente, previo sfoltimento
4.6	RENDICONTO DELLA GESTIONE; ADEMPIMENTI E VERIFICHE CONTABILI	
	Rendiconto della gestione, articolato in Conto del bilancio, Conto del patrimonio e Conto economico	Permanente
4.7	ADEMPIMENTI FISCALI, CONTRIBUTIVI E ASSICURATIVI	
	Mod. 770	10 anni
	Ricevute dei versamenti (IRPEF, etc.)	10 anni

4.8	BENI IMMOBILI	
	Inventario dei beni immobili: registro o base di dati perenne	Permanente
	Fascicoli dei beni immobili: un fasc. per ciascun bene immobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche, che possono anche essere di competenza di UOR diverse:	
	- acquisizione	permanente
	- manutenzione ordinaria	20 anni
	- gestione	5 anni
	- uso	5 anni
	- alienazione e dismissione	permanente
4.9	BENI MOBILI	
	Inventari dei beni mobili: uno per consegnatario	Permanente
	Fascicoli dei beni mobili: un fasc. per ciascun bene mobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche:	
	- acquisizione	5 anni dalla dismissione
	- manutenzione	5 anni dalla dismissione
	- concessione in uso	5 anni dalla dismissione
	- alienazione e altre forme di dismissione	5 anni dalla dismissione
4.10	ECONOMATO	
	Acquisizione di beni e servizi con cassa economale: un fasc. per ciascun acquisto	5 anni dalla dismissione del bene
	Acquisizione di beni e servizi con tesoreria: un fasc. per ciascun acquisto	5 anni dalla dismissione del bene
	Elenco dei fornitori: repertorio (in forma di base di dati)	Permanente
4.11	TESORERIA	
	Giornale di cassa	Permanente
	Mandati quietanzati, che vengono inviati all'ATA al termine dell'esercizio finanziario: repertorio periodico (mese/anno)	10 anni dall'approvazione del rendiconto
5	***AFFARI LEGALI***	
5.1	CONTENZIOSO	
	Fascicoli di causa	Permanente
5.2	RESPONSABILITA' CIVILE E PATRIMONIALE VERSO TERZI; ASSICURAZIONI	
	Contratti assicurativi: un fascicolo per ciascun contratto	10 anni dalla scadenza
	Richieste e pratiche di risarcimento (fare un sottofascicolo per ciascuna richieste per ciascun contratto)	10 anni
5.3	PARERI E CONSULENZE	
	Pareri e consulenze	Permanente

6	***GESTIONE INTEGRATA DEI RIFIUTI URBANI E ASSIMILATI***	
6.1	PIANIFICAZIONE E STUDI	
	Pianificazione: un fascicolo per ciascuna attività di pianificazione	Permanente, previo sfoltimento
	Studi di fattibilità: un fascicolo per ciascuno studio	Permanente, previo sfoltimento
	Studi diversi: un fascicolo per ciascuno studio	Permanente, previo sfoltimento
	approvazione piani finanziari: un fascicolo annuale con eventuali sottofascicoli per ciascun comune	Permanente, previo sfoltimento
	pareri per conferenze dei servizi: un fascicolo per ciascuna conferenza (si mettono qui anche le convocazioni)	Permanente, previo sfoltimento. Si tiene il parere e i verbali
6.2	GESTIONE SERVIZIO RIFIUTI, TRATTAMENTO, SMALTIMENTO	
	Un fascicolo per ogni affidamento di servizio, con eventuali sottofascicoli	Permanente, previo sfoltimento
6.3	PROGETTI DI SENSIBILIZZAZIONE AMBIENTALE	
	Un fascicolo per ogni progetto, con eventuali sottofascicoli	Permanente, previo sfoltimento
6.4	REALIZZAZIONE OPERE E IMPIANTI	
	Realizzazione di opere pubbliche: un fascicolo per ogni opera, con eventuali sottofascicoli	Permanente. Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Manutenzione ordinaria	5 anni, salvo necessità particolari
	Manutenzione Straordinaria	20 anni, salvo necessità particolari
7	***OGGETTI DIVERSI***	

MANUALE DI GESTIONE DOCUMENTALE

ALLEGATO 15

PIANO PER LA SICUREZZA INFORMATICA

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

INTRODUZIONE

L'ATA ha adottato il Documento programmatico sulla sicurezza (DPS) in base alle disposizioni del disciplinare tecnico on materia di misure minime di sicurezza del codice in materia di protezione dei dati personali (artt. 34-35- e 36 e Allegato B del d.lgs. n. 196 del 30 giugno 2003). Tale documento viene allegato al presente documento per farne parte integrante e sostanziale.

L'ATA ha anche adottato lo studio di fattibilità tecnica funzionale alla redazione del Piano per la continuità operativa e disaster recovery (che si allega al presente documento per farne parte integrante e sostanziale) che verrà redatto nel corso del 2017.

Il presente documento ricomprende pertanto tutte le norme interne in merito alla sicurezza informatica con particolare riguardo al Sistema informatico di gestione documentale ai se dall'art. 4 c.1 lettera c) delle regole tecniche per il protocollo informatico di cui al DPCM 3 dicembre 2013.

Il Piano della sicurezza definisce le attività e gli strumenti da implementare affinché il Sistema di gestione documentale dell'ATA possa garantire che:

- tutti i documenti e le informazioni trattati dall'ATA siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari, nel rispetto del DPS, vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.

A tal fine il Piano della Sicurezza è soggetto a revisione con cadenza almeno biennale.

ACCESSO AL SISTEMA DI GESTIONE DOCUMENTALE DA PARTE DEGLI UTENTI INTERNI ALL'AOO (AREA ORGANIZZATIVA OMOGENEA).

I livelli di autorizzazione di accesso alle funzioni del sistema di gestione documentale sono stabiliti dal Responsabile della gestione documentale (RGD) sulla base del seguente schema:

FUNZIONALITÀ ABILITATE	UTENTI ABILITATI
Definizione delle liste di controllo degli accessi	Responsabile della gestione documentale
Registrazione di protocollo dei documenti in arrivo	Ufficio gestione documentale (Responsabile della gestione documentale e 2 addetti)
Registrazione di protocollo dei documenti in partenza o interni	Tutti gli utenti interni dell'AOO
Classificazione dei documenti	Tutti gli utenti interni dell'AOO abilitati alla protocollazione
Correzione / modifica della classificazione	Ufficio gestione documentale
Assegnazione	Tutti gli utenti interni dell'AOO abilitati alla protocollazione
Fascicolazione dei documenti	Tutti gli utenti interni dell'AOO abilitati alla protocollazione
Protocollazione dei documenti nel registro di emergenza	Ufficio gestione documentale
Consultazione dei documenti	Tutti gli utenti nel limite di quelli a ciascuno assegnati
Aggiornamento anagrafica mittente/destinatario sul Sistema	Ufficio gestione documentale

Come indicato al capitolo 3 del DPS a cui si rimanda l'accesso al Sistema di gestione documentale, da parte degli utenti interni all'AOO, avviene attraverso l'utilizzo di credenziali di autenticazione ed in base a specifici profili di autorizzazione riconosciuti al singolo incaricato:

- **User-ID** per l'identificazione dell'incaricato
- **Password** conosciuta solo dall'incaricato.

Di seguito si riportano sinteticamente alcune delle regole previste dal DPS.

Le credenziali vengono verificate in tempo reale dal sistema di autentificazione che consente l'accesso e memorizza gli accessi della specifica User-id (non la password).

Gli incaricati del trattamento di dati personali, sensibili o giudiziari non possono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento dei dati stessi.

Le credenziali di autenticazione di ciascun operatore vengono consegnate in busta chiusa e sigillata al Responsabile della custodia delle credenziali che coincide con l'Amministratore di Sistema Responsabile dei servizi informatici dell'Ente.

Le password devono essere modificate periodicamente ed ogni tre mesi nel caso di trattamento di dati sensibili o giudiziari.

L'User-Id non può essere assegnato ad altri incaricati neppure in tempi diversi e vengono disattivate nel caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

In caso di prolungata assenza o impedimento del soggetto incaricato del trattamento di dati personali, sensibili o giudiziari e, qualora si renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Responsabile della custodia delle credenziali è autorizzato ad utilizzare le credenziali contenute nella suddetta busta per procedere direttamente o tramite il responsabile del servizio interessato al trattamento, comunicandolo al titolare. Il soggetto titolare delle credenziali provvederà, al momento del proprio rientro in servizio, alla sostituzione della Password, provvedendo all'inserimento della stessa in altra busta sigillata da consegnare al suddetto Responsabile.

Qualora il trattamento dei dati avviene senza l'utilizzo di strumenti elettronici l'incaricato al trattamento deve controllare e custodire gli stessi assicurandosi che a tali documenti non accedano persone prive di autorizzazione.

L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solo previa autorizzazione e le persone ammesse sono identificate e registrate.

SICUREZZA DELLE REGISTRAZIONI DI PROTOCOLLO

Come specificato nel presente Manuale ogni registrazione di protocollo viene memorizzata dal sistema di Gestione documentale unitamente all'identificativo univoco dell'autore che l'ha eseguita e alla data e all'ora della stessa.

Eventuali modifiche, autorizzate come specificato nel presente Manuale, vengono registrate per mezzo di log del sistema che mantengono traccia dell'autore, della modifica effettuata, nonché della data e dell'ora. Il sistema mantiene leggibile la precedente versione per una completa ricostruzione cronologica di ogni registrazione.

Il Sistema non consente la modifica del numero e della data di protocollo: nel caso ciò si rendesse necessario si deve procedere all'annullamento dell'intera registrazione, che rimane comunque tracciata, previa autorizzazione che deve essere indicata nell'operazione di annullamento.

Ogni documento viene registrato al protocollo con un'impronta digitale generata dal Sistema. Al fine di garantire l'immodificabilità delle registrazioni di protocollo il sistema al termine della giornata lavorativa produce il Registro giornaliero delle registrazioni di protocollo in formato digitale. Tale registro sarà trasferito nella giornata successiva al Polo di conservazione documentale della Regione Marche.

SISTEMA INORMATICO DELL'ATA -SICUREZZA LOGICA DEL SISTEMA E BACKUP

La rete informatica (LAN) di ATA Rifiuti si estende su due piani. In ogni piano è presente un armadio di rete che contiene sia gli apparati per la trasmissione dati (switch) che quelli per la fonia (centralino telefonico). I due armadi sono collegati tra loro attraverso un collegamento in rame a 1Gbit/s. La rete supporta connessioni a 1Gbit/s su cavi in rame.

La connessione ad internet è fornita da una connessione wDSL (Hiperlan) con 10/3Mbps Down/Up e banda minima garantita 768/384kbps. Il router Hiperlan – gestito da chi fornisce la connessione – oltre a permettere la connessione ad internet di tutti i personal computer della rete ha anche funzioni minime di firewall. Dall'esterno è possibile accedere alla rete interna attraverso una VPN di tipo PTPP.

Il dominio 'atarifiuti.locale' di tipo Microsoft Active Directory è gestito da uno dei due server presenti nella rete. Il server oltre ad essere controller di domino è anche server DNS e server DHCP.

Il Sistema di gestione documentale e tutti i documenti e dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici mediante l'attivazione dei seguenti strumenti software/hardware:

- Attivazione dell'antivirus costantemente aggiornato. Su ogni personal computer è installato un software antivirus – Trend Micro Business Security - gestito centralmente in modo da ottimizzarne la banda per il download degli aggiornamenti e la gestione delle configurazioni. Il controllo degli aggiornamenti viene eseguito ogni ora.
- Installazione di un firewall hardware e uso di una VPN per il collegamento da remoto.

Le procedure di backup vengono effettuate sul NAS. Il NAS è un QNAP modello TS453A con 4 dischi da 3TB ciascuno in configurazione RAID 6 (questa configurazione è stata preferita al RAID 5 per la doppia ridondanza: il RAID 6 tollera la rottura di 2 dischi senza perdita di dati).

I file creati dagli utenti della rete vengono copiati attraverso un sistema di backup incrementale con uno storico di 2 copie complete a settimana. I dump dei database vengono salvati giornalmente e viene mantenuto uno storico di almeno 5 salvataggi.

I software gestionali usati presso l'ente sono installati su entrambi i server in modo da ripartirne in modo equo il carico. Sono forniti da software house esterne e gestiti dalle stesse attraverso connessioni remote (desktop remoto).

Ad uso del personale interno, è stata creata una rete wireless (1 access point + 2 extender) attraverso la quale è possibile connettersi ad internet ed alle risorse della LAN.

Ai fini della vulnerabilità dei sistemi informativi il sistema di gestione documentale viene tenuto costantemente aggiornato per mezzo dell'installazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Il Backup dei dati contenuti nel sistema di gestione documentale avviene giornalmente in modalità automatica.

Il ripristino dell'accesso ai dati in caso di generico malfunzionamento per danneggiamento degli stessi o degli strumenti elettronici, avviene entro 8 ore lavorative.

TRASMISSIONE E INTERSCAMBIO DI DOCUMENTI

Al fine di evitare la dispersione e la circolazione incontrollata dei documenti e dati, la trasmissione e l'interscambio di documenti e fascicoli informatici all'interno dell'ente avviene esclusivamente per mezzo del sistema di gestione documentale: nessun'altra modalità è consentita.

La trasmissione di documenti informatici al di fuori dell'ente avviene tramite PEC o mediante i meccanismi dell'interoperabilità e della cooperazione applicativa di cui al sistema pubblico di connettività, utilizzando le informazioni contenute della segnatura di protocollo.

I messaggi di posta elettronica certificata prodotti dall'ATA sono compatibili con il protocollo SMTP/MINE definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e smi. Le informazioni relative alla segnatura di protocollo sono strutturate in un file conforme alle specifiche XML, compatibile con un file XML Schema e/o DTD, secondo la normativa vigente.

I documenti registrati sul Sistema di gestione documentale sono conformi ai requisiti e contengono i metadati previsti ai fini della conservazione permanete. Il trasferimento in conservazione avverrà mediante la produzione di pacchetti di versamento, basati su uno schema XML.

SICUREZZA FISICA E INFRASTRUTTURALE DEL SISTEMA

L'ATA si sta dotando di un piano di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio ed il ritorno alla normale operatività sulla scorta dello studio di fattibilità tecnica in allegato.

PIANI FORMATIVI DEL PERSONALE

Ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, l'ente predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- Utilizzo applicativi software per la gestione dei documenti informatici;
- Utilizzo del sistema di gestione documentale;
- Fascicolazione dei documenti informatici;
- Trattamento dei dati personali, sensibili o giudiziari;
- Aggiornamento sui temi suddetti.

MONITORAGGIO PERIODICO DELL'EFFICACIA E DELL'EFFICIENZA DELLE MISURE DI SICUREZZA

I log di sistema sono mantenuti per sei mesi al fine di verificare eventuali violazioni del sistema.

Il responsabile della gestione documentale effettua periodiche verifiche sul corretto funzionamento del sistema di gestione documentale, valutando, anche con controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale.

NORME TRANSITORIE E FINALI

Il presente documento sarà oggetto di integrazione con gli atti che l'ATA adotterà nel corso del 2017 per dare attuazione alle linee guida definite dal DPS, compreso il Piano di continuità operativa.

COPIA DELL'ORIGINALE DI DECRETO DEL PRESIDENTE

n. 36 **del 30.12.2016**

Oggetto: Approvazione dello studio di fattibilità tecnica (SFT), per la successiva redazione del Piano di continuità operativa e del piano di Disaster Recovery, nomina del Responsabile della continuità operativa dell'Ente e costituzione Comitato gestione crisi ai sensi del D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale) e delle correlate regole tecniche e linee guida AGID.

DOCUMENTO ISTRUTTORIO

Oggetto: Approvazione dello studio di fattibilità tecnica (SFT), per la successiva redazione del Piano di continuità operativa e del piano di Disaster Recovery, nomina del Responsabile della continuità operativa dell'Ente e costituzione Comitato gestione crisi ai sensi del D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale) e delle correlate regole tecniche e linee guida AGID.

IL DIRETTORE

RILEVATO che con l'applicazione del Codice dell'Amministrazione Digitale ogni amministrazione pubblica deve garantire la continuità operativa dei sistemi informatici per il corretto svolgimento dei servizi;

ATTESO che necessita quindi predisporre piani di emergenza in grado di assicurare le continuità dei servizi fino al ritorno alla normalità operativa in caso di interruzione del sistema informatico per eventi calamitosi, incendi ecc.;

RICHIAMATE le proprie determinazioni n. 16 del 23/02/2016 con la quale si sono definiti i primi indirizzi per l'implementazione del Sistema di gestione documentale informatizzata, e n. 113 del 9/8/2016 con la quale si è affidato il servizio di assistenza e supporto in materia di sicurezza informatica alla ditta Euristica srl;

PRESO ATTO che la ditta Euristica srl ha svolto il proprio servizio collaborando alla stesura della documentazione necessaria affiancando il personale per una adeguata informazione in materia di Privacy e Continuità Operativa e Disaster Recovery (art. 50 del CAD) e indicando le procedure da seguire per adeguarsi alle prescrizioni della normativa vigente in materia;

RITENUTO a tal fine di approvare lo studio di fattibilità tecnica (SFT) allegato al presente atto per farne parte integrante e sostanziale, redatto in collaborazione con la ditta Euristica, che si sostanzia in un'autovalutazione per individuare le potenziali criticità relative a risorse umane, strutturali, tecnologiche e le misure preventive da adottare oltre al piano di Disaster Recovery per la funzionalità del sistema in siti alternativi per tutta la durata dell'inoperatività della sede;

RILEVATO che tale studio evidenzia la necessità di ottimizzazione del CED primario e l'individuazione di un sito secondario in caso di Disaster Recovery da ultimare entro il 31/12/2017, data entro cui completare il Piano di Continuità operativa e suoi allegati;

PRESO ATTO che l'attuale struttura dell'Ente prevede un unico Dirigente coincidente con il Direttore responsabile delle tre Aree individuate dal Regolamento di Organizzazione approvato con deliberazione dell'Assemblea n. 4 del 09/09/2013 e sono stati individuati i Responsabili dei servizi con determinazione della Direzione n. 19 del 31/12/2013 senza poteri di spesa;

ATTESO quindi che il Responsabile della continuità operativa deve essere necessariamente individuato nel Direttore, dott.ssa Elisabetta Cecchini che sarà affiancata dal Responsabile della sicurezza informatica (Amministratore di Sistema) dott. Matteo Giantomassi;

RITENUTO di costituire il Comitato gestione crisi così composto:
- Responsabile della continuità operativa dott.ssa Elisabetta Cecchini;
- Responsabile della sicurezza informatica (Amministratore di Sistema) dott. Matteo Giantomassi;
- RSPP;

RILEVATO che il Comitato gestione crisi sulla scorta dello Studio di fattibilità tecnica dovrà procedere entro il 31/12/2017 alla redazione del Piano di continuità operativa;

TUTTO CIÒ PREMESSO;

VISTI:
- il DPR 445/2000;
- il D.Lgs. 82/2005 e s.m.i.;
- il D.Lgs. n. 267/2000
- il D.Lgs. n. 165/2001;
- il D.Lgs. n. 150/2009,e ss.mm.ii.;
- il D.L. n. 78/2010 convertito, con modificazioni, dalla L. n. 122/2010;
- il D.L. n. 90/2014 convertito in L. n. 114/2014;
- il D.Lgs. n. 81/2015;
- il vigente Regolamento di organizzazione;
- il parere favorevole riportato in calce, in ordine alla regolarità tecnica di cui all'art. 49 co. 1,del D.Lgs n. 267/2000;

PROPONE

1) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2) Di approvare, ai sensi del D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale), lo studio di fattibilità tecnica (SFT) per la successiva redazione del Piano di continuità operativa e del piano di Disaster Recovery, sulla scorta delle correlate regole tecniche ministeriali e delle linee guida AGID, allegato al presente atto per farne parte integrante e sostanziale;
3) Di nominare Responsabile della continuità operativa dell'Ente ai sensi del D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale) e delle correlate regole tecniche e linee guida Agid il Direttore, dott.ssa Elisabetta Cecchini;

4) Di costituire il Comitato gestione crisi come segue:
   - Responsabile della continuità operativa dott.ssa Elisabetta Cecchini;
   - Responsabile della sicurezza informatica (Amministratore di Sistema) dott. Matteo Giantomassi;
   - RSPP;
5) Di stabilire che il Responsabile della continuità operativa, con il supporto Responsabile della sicurezza informatica (Amministratore di Sistema) e sulla scorta dello Studio di fattibilità tecnica, dovrà procedere entro il 31/12/2017 alla redazione del Piano di continuità operativa;
6) Di dichiarare, riscontrata l'urgenza del caso, immediatamente eseguibile il Decreto di approvazione del presente documento istruttorio, ai sensi dell'art. 134, co. 4 del D.Lgs. 267/2000.

Jesi, 30.12.2016

La Direzione
F.to dott.ssa Elisabetta Cecchini

PARERE DI REGOLARITÀ TECNICA

Ai sensi dell'art. 49, co. 1, del D.Lgs. n. 267/2000, si esprime **parere favorevole** in ordine alla regolarità tecnica del presente atto.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

IL PRESIDENTE

VISTO il documento istruttorio redatto dal Direttore in data 30.12.2016, sopra riportato a formare parte integrante e sostanziale del presente atto, contenente la proposta di approvazione dello studio di fattibilità tecnico;

RITENUTO di condividere la proposta di cui sopra per le motivazioni addotte, che si intendono qui integralmente riportate;

VISTO che il documento istruttorio di cui sopra riporta il prescritto parere di regolarità tecnica;

DECRETA

7) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;

8) Di approvare, ai sensi del D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale), lo studio di fattibilità tecnica (SFT) per la successiva redazione del Piano di continuità operativa e del piano di Disaster Recovery, sulla scorta delle correlate regole tecniche ministeriali e delle linee guida AGID, allegato al presente atto per farne parte integrante e sostanziale;

9) Di nominare Responsabile della continuità operativa dell'Ente ai sensi del D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale) e delle correlate regole tecniche e linee guida Agid il Direttore, dott.ssa Elisabetta Cecchini;

10) Di costituire il Comitato gestione crisi come segue:
    - Responsabile della continuità operativa dott.ssa Elisabetta Cecchini;
    - Responsabile della sicurezza informatica (Amministratore di Sistema) dott. Matteo Giantomassi;
    - RSPP;

11) Di stabilire che il Responsabile della continuità operativa, con il supporto Responsabile della sicurezza informatica (Amministratore di Sistema) e sulla scorta dello Studio di fattibilità tecnica, dovrà procedere entro il 31/12/2017 alla redazione del Piano di continuità operativa;

1) Di dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'articolo 134, co. 4, del D.Lgs. n. 267/2000.

Il Presidente
F.to dott.ssa Liana Serrani

Studio di Fattibilità Tecnica

22/11/2016

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

1 Sommario

1.Introduzione

La continuità dei sistemi informativi rappresenta per le pubbliche amministrazioni, nell'ambito delle politiche generali per la continuità operativa dell'ente, un aspetto necessario all'erogazione dei servizi ai cittadini e imprese e diviene uno strumento utile per assicurare la continuità dei servizi e garantire il corretto svolgimento della vita nel Paese.

Al riguardo e più in particolare il Codice dell'Amministrazione digitale delinea gli obblighi, gli adempimenti e i compiti che spettano alle Pubbliche Amministrazioni, all'Agenzia per l'Italia Digitale e al Ministro per la pubblica amministrazione e l'innovazione, ai fini dell'attuazione della continuità operativa:

1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le p.p.a.a. predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni per il servizio e il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono:

a. il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni.

Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

b. il piano di Disaster Recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

DigitPA [oggi Agenzia per l'Italia Digitale], sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di Disaster Recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi può essere acquisito il parere dell'Agenzia per l'Italia Digitale.

1.1 Obiettivi del Documento

Il presente Studio di Fattibilità Tecnica (SFT) dell'Assemblea Territoriale d'Ambito ATO 2 Ancona (nel seguito anche ATA) viene redatto per poter dare evidenza dei risultati emersi nel percorso di autovalutazione, illustrando tra le altre cose:

• gli eventuali scostamenti tra la soluzione individuata al termine del percorso di autovalutazione e quella effettivamente scelta dalla Amministrazione;

• il percorso e i tempi che si stima siano necessari per adottare la soluzione suggerita al termine del percorso di autovalutazione e per allinearsi a quanto previsto dalle Linee Guida.

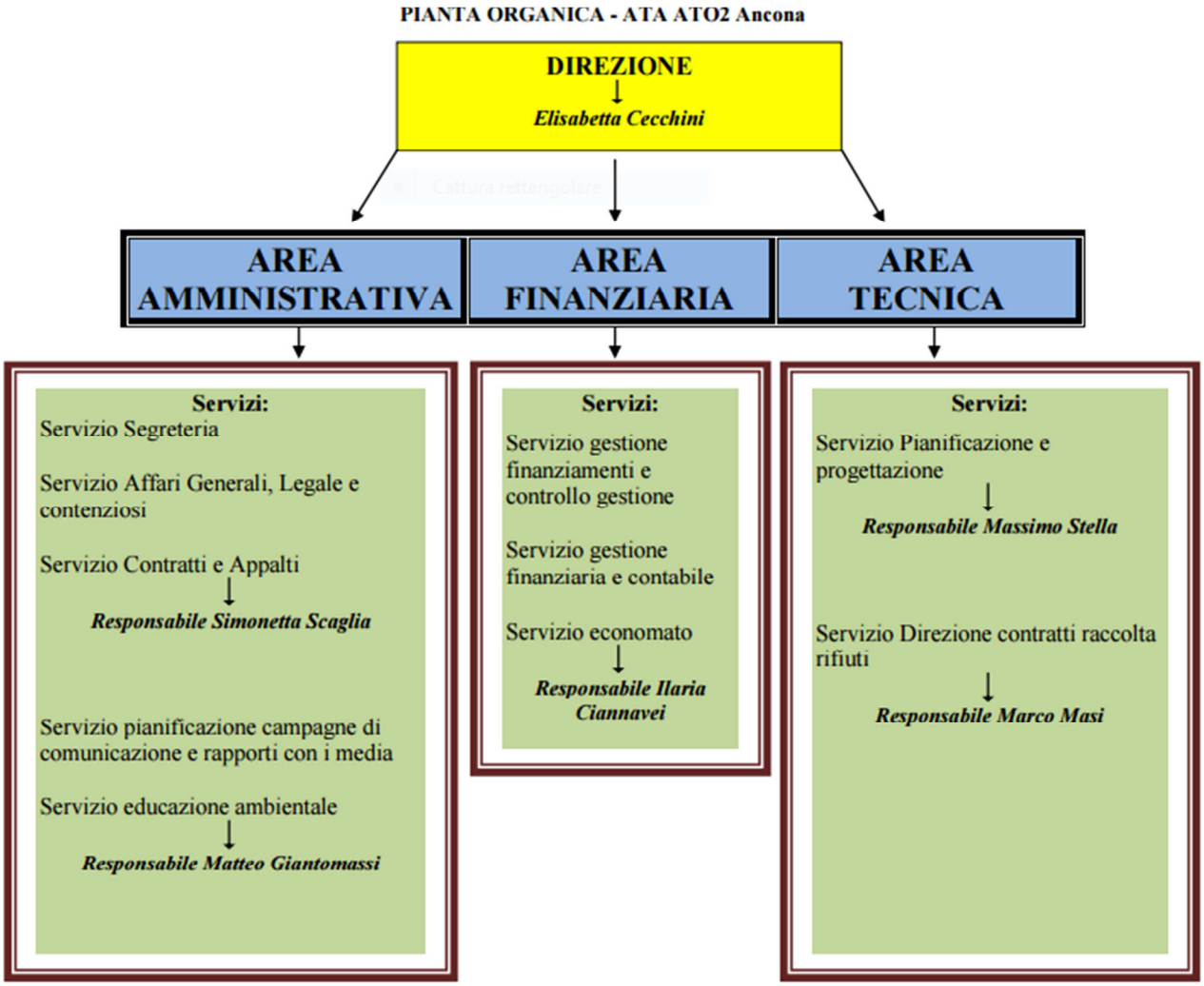
Il documento si prefigge quindi di fornire le informazioni necessarie e propedeutiche alla realizzazione del piano di disaster recovery come parte integrante del più ampio piano di continuità operativa.

2.INFORMAZIONI GENERALI

Nome Amministrazione	Assemblea Territoriale d'Ambito ATO 2 Ancona
Sede centrale(città)	Jesi (Ancona)
Settore di attività	Assemblea Territoriale d'Ambito (Gestione rifiuti)
Responsabile CO/DR	dott.ssa Elisabetta Cecchini
AOO (AreaOrg.Omog.)/ENTE	Ente
Indirizzo PEC per le comunicazioni	atarifiutiancona@pec.it
Data compilazione	22/11/2016
Perimetro di competenza	Tutte le aree dell'Ente

2.1 *Descrizione dell'Amministrazione, organizzazione e funzioni istituzionali*

L'organizzazione viene rappresentata come segue (fonte Organigramma come da sito istituzionale dell'Assemblea Territoriale d'Ambito ATO 2 Ancona)



Il Responsabile della Continuità Operativa per l'Assemblea Territoriale d'Ambito ATO 2 Ancona è la dott.ssa Elisabetta Cecchini.

Di seguito è rappresentata l'articolazione dei servizi e degli uffici, come risulta dal portale istituzionale, area Amministrazione Trasparente, sezione Organizzazione > Organigramma:

GLI UFFICI

Direzione

dott.ssa **Elisabetta Cecchini**
E-mail: cecchini@atarifiuti.an.it

Area Amministrativa

Servizio segreteria - Servizio affari generali, legale e contenziosi - Servizio contratti e appalti
Responsabile
dott.ssa Simonetta Scaglia
E-mail: scaglia@atarifiuti.an.it

Servizio pianificazione campagne di comunicazione e rapporti con i media - Servizio educazione ambientale
Responsabile
dott. Matteo Giantomassi
E-mail: giantomassi@atarifiuti.an.it

Area Finanziaria

Servizio gestione finanziamenti e controllo gestione - Servizio gestione finanziaria e contabile - Servizio economato
Responsabile
dott.ssa Ilaria Ciannavei
E-mail: ciannavei@atarifiuti.an.it

Area Tecnica

Servizio pianificazione e progettazione
Responsabile
ing. Massimo Stella
E-mail: stella@atarifiuti.an.it

Servizio direzione contratti raccolta rifiuti
Responsabile
Marco Masi
E-mail: masi@atarifiuti.an.it

SEDE LEGALE

Assemblea Territoriale d'Ambito
ATO2 - Ancona (ATA)
strada di Passo Varano, 19/A -
60131 Ancona - c/o Provincia di Ancona
C.F.: 93135970429

Sito web: www.atarifiuti.an.it
Pec: atarifiutiancona@pec.it
E-mail: segreteria@atarifiuti.an.it

SEDE OPERATIVA

E-mail: segreteria@atarifiuti.an.it

Viale dell'Industria, 5
60035 Jesi (AN)
Tel: 0731/200969
Fax: 0731/221630

3 L'AMBITO DELLO STUDIO DI FATTIBILITÀ TECNICA

3.1 Servizi Erogati

I Servizi dell'Assemblea Territoriale D'Ambito ATO 2 Ancona (ATA) mappati nel presente SFT sono sinteticamente descritti nell'organigramma di cui al capitolo precedente.

Le caratteristiche, ai fini del presente SFT, dei servizi medesimi, la stima di impatto, gli indici di criticità e i requisiti analizzati ai fini della compilazione del presente SFT sono dettagliati nelle schede allegate al presente documento.

Ai fini della descrizione delle funzioni, si allega il documento di Assetto Organizzativo pubblicato nel portale istituzionale.

3.1.1 Servizi in ambito

Tutti i servizi mappati dall'organigramma sono considerati in ambito.

Classe di Servizi	Servizio	Descrizione Servizio	Tipologia di Utenza
Area Amministrativa	Classe dei Servizi dell'Area Amministrativa	Servizio Segreteria Servizio AAGG, legali e contenziosi Servizio contratti e appalti	Eterogenea
Area Finanziaria	Classe dei Servizi dell'Area Finanziaria	Servizio gestione finanziamenti e controllo di gestione Servizio gestione finanziaria e contabile Servizio economato	Eterogenea
Area Tecnica	Classe dei Servizi dell'Area Tecnica	Servizio pianificazione e progettazione Servizio direzione contratti raccolta rifiuti	Eterogenea

3.1.2 Servizi non in ambito

Non sono previsti servizi esclusi dall'ambito di applicazione del presente SFT.

3.2 Descrizione dettagliata Servizi/Classe di Servizi

Per ogni servizio o classe di servizi che fa parte dell'ambito dello Studio di Fattibilità Tecnica è stata redatta una scheda di autovalutazione, i cui risultati sono riportati negli allegati.

AREA AMMINISTRATIVA

SERVIZIO SEGRETERIA
• Attività ordinaria di segreteria:
- Tenuta del protocollo per la corrispondenza esterna ed interna dell'Ente;
- Cura del centralino;
- Gestione degli archivi;
• Supporto alla Direzione ed alle altre Aree dell'ATA, quali:
- Area Amministrativa, attraverso:
o Predisposizione degli atti e cura dello svolgimento di gare per l'acquisto di quanto necessario per il funzionamento degli uffici;
o Gestione amministrativa del personale, dipendente e assimilato, mediante la tenuta dei libri obbligatori e la verifica delle presenze;
- Area Finanziaria, attraverso:
o Predisposizione di tutti i dati inerenti il personale, dipendente e assimilato, necessari per la gestione del service-paghe;
o Effettuazione di tutte le comunicazioni obbligatorie connesse alla gestione del personale e delle trasmissioni connesse al versamento delle ritenute previdenziali, fiscali e assistenziali;
• Adempimenti necessari all'aggiornamento del Documento programmatico della sicurezza ai sensi del D.Lgs. 196/2003 con la collaborazione dei Responsabili delle altre Aree e Servizi;
• Adempimenti necessari all'aggiornamento del Manuale della sicurezza ai sensi del D. Lgs. 81/2008 e s.m.i. con la collaborazione dei Responsabili delle altre Aree e Servizi;
• Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di regolarità tecnica ex art. 49 D. Lgs. 267/2000.

SERVIZIO AFFARI GENERALI, LEGALE E CONTENZIOSI
• Segreteria dell'Assemblea dell'ATA e predisposizione dei relativi atti;
• Predisposizione delle determinazioni di accertamento di entrata e di impegno di spesa e di qualunque atto amministrativo necessario per la gestione dell'Ente;
• Gestione, nelle attività di propria competenza, delle relazioni con gli organi istituzionali dell'Ente e con Enti e soggetti pubblici e/o privati;
• Cura dell'informazione sugli atti e la possibilità di accesso agli atti da parte degli utenti e di terzi.
• Cura le pubblicazioni nell'Albo Pretorio on-line dei documenti dell'Ente.
• Assistenza giuridica nei confronti degli organi dell'Ente locale in ordine alla conformità dell'azione amministrativa alle leggi, alla Convenzione e ai regolamenti;
• Cura della preparazione e del trasferimento di documenti relativi al contenzioso in atto al legale individuato

dall'Ente;
• Gestione dei processi di analisi, studio, ricerca e approfondimento in merito a problematiche normative, mediante redazione di pareri, relazioni e formulazione di quesiti ai soggetti istituzionalmente preposti;
• Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di regolarità tecnica ex art. 49 D. Lgs. 267/2000;
• Interazione con il Direttore e con tutte le Aree organizzative dell'Ente in merito agli aspetti di carattere legale ovvero giuridico-amministrativo dei vari settori di attività, fornendo pareri e chiarimenti.

SERVIZIO CONTRATTI E APPALTI
• Attivazione delle procedure ad evidenza pubblica, relativamente alla individuazione della procedura più adeguata, alla predisposizione di capitolati di appalto e/o disciplinari (ovvero supporto al personale tecnico incaricato della predisposizione di detti capitolati e/o disciplinari), all'espletamento delle procedure e alle aggiudicazioni;
• Predisposizione degli schemi dei contratti (acquisti in economia, appalti di servizi fornitura e lavori), cura della gestione e della registrazione nel repertorio degli atti dell'Ente, controllo in merito alla regolare esecuzione degli stessi;
• Cura dal punto di vista normativo delle modalità di assunzione e di gestione del personale dell'ATA, comunicazioni alla funzione pubblica degli incarichi conferiti e invio telematico del conto annuale del personale;
• Cura della gestione del Documento programmatico della sicurezza ai sensi del D. Lgs. 196/2003 e di tutti gli adempimenti necessari all'aggiornamento dello stesso;
• Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di regolarità tecnica ex art. 49 D. Lgs. 267/2000.

SERVIZIO PIANIFICAZIONE CAMPAGNE DI COMUNICAZIONE E RAPPORTI CON I MEDIA
· Individuazione e diffusione dell'immagine istituzionale coordinata;
· Pianificazione della comunicazione interna ed esterna e della relativa formazione del personale;
· Pianificazione, ideazione e creazione di piani e campagne di comunicazione integrata e non;
· Attività di monitoraggio degli indici di gradimento e degli effetti delle azioni comunicative e tecniche;
· Progettazione, in collaborazione con le altre aree, di nuovi servizi rivolti al cittadino e/o agli enti convenzionati;
· Organizzazione di eventi istituzionali, informativi e di sensibilizzazione ambientale;
· Ideazione e creazione di materiale informativo cartaceo, informatico e multimediale;
· Assistenza alle attività di comunicazione degli enti convenzionati;
· Individuazione di partnership pubbliche e private nello sviluppo di progetti.
· Organizzazione della raccolta e dell'archiviazione della documentazione inerente l'ATA;
· Rassegna stampa e condivisione delle news internamente alla struttura;
· Cura dei rapporti istituzionali con giornalisti, addetti stampa, amministratori locali e rappresentanti della cultura e della società locale;
· Ideazione e redazione di comunicati e servizi per la stampa, la televisione, la radio ed il web;
· Ideazione e produzione di progetti editoriali propri;
· Produzione di materiale audiovisivo;
· Cura e aggiornamento del sito internet e degli strumenti on-line dell'ATA.
· Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di regolarità tecnica ex art. 49 D. Lgs. 267/2000.

SERVIZIO EDUCAZIONE AMBIENTALE
· Progettazione di campagne educative rivolte agli Istituti scolastici dei Comuni convenzionati;
· Organizzazione ed attuazione di interventi educativi ;
· Ideazione e produzione di materiale didattico rivolto alle istituzioni scolastiche;
· Pianificazione di interventi di educazione e sensibilizzazione ambientale capaci di coinvolgere il tessuto associazionistico e culturale del territorio dell'ATA..
· Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di

regolarità tecnica ex art. 49 D. Lgs. 267/2000.

AREA FINANZIARIA

SERVIZIO GESTIONE FINANZIAMENTI E CONTROLLO GESTIONE
• Espletamento delle procedure di rendicontazione e monitoraggio dei finanziamenti ottenuti dall'ATA;
• Controllo di gestione;
• Supporto ai Comuni in tema di tributo o tariffa rifiuti;
• Verifica dei Piani finanziari predisposti dai gestori del servizio, previsti dalla normativa vigente per il tributo o la tariffa rifiuti da sottoporre all'approvazione dell'Assemblea;
• Verifica dei Piani finanziari predisposti dai gestori degli impianti dell'ATA da sottoporre all'approvazione dell'Assemblea e cura delle autorizzazioni previste dalle norme vigenti in collaborazione con il Serivzio Pianificazione e Progettazione;
• Cura dei rapporti con gli organi istituzionali dell'Ente e con gli altri soggetti pubblici e privati su materie di carattere economico-finanziario;
• Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di regolarità tecnica ex art. 49 D. Lgs. 267/2000.

SERVIZIO GESTIONE FINANZIARIA E CONTABILE
• Ordinaria gestione dell'Ente
- Pareri e visti di regolarità contabile;
- Redazione dei principali documenti contabili, quali Bilancio di previsione ed allegati, Salvaguardia degli equilibri di Bilancio, Rendiconto dell'esercizio finanziario;
- Gestione degli stanziamenti di bilancio, attraverso la gestione del regime delle entrate e delle spese dell'ATA (emissione di reversali e mandati) ed attraverso le variazioni al Bilancio di previsione ed al connesso piano esecutivo di gestione;
- Gestione delle paghe;
- Cura dei rapporti con gli agenti contabili (Economo, Tesoriere, Consegnatario di beni);
• Gestione economico-finanziaria degli appalti e dei contratti;
• Supporto alla Direzione ed alle altre Aree dell'ATA, con particolare riferimento agli aspetti di carattere finanziario;
• Cura dell'aggiornamento del Documento programmatico della sicurezza ai sensi del D. Lgs. 196/2003 per la parte di propria competenza.
• Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di regolarità tecnica ex art. 49 D. Lgs. 267/2000.

SERVIZIO ECONOMATO
• Gestione del Servizio Economato;
• Gestione dei rapporti con i fornitori del Servizio Economato;
• Cura degli aspetti organizzativi e gestionali dell'Ente al fine di mantenere l'efficienza delle attrezzature, la costante disponibilità delle dotazioni dei beni di funzionamento e di tutto il necessario per assicurare la massima efficienza dell'Ente;
• Determinazione dei rimborsi spese per missioni, trasferte e spostamenti per motivi di servizio a favore di dipendenti, collaboratori, amministratori, revisori e consulenti;
• Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di regolarità tecnica ex art. 49 D. Lgs. 267/2000;
• Cura dell'aggiornamento del Documento programmatico della sicurezza ai sensi del D. Lgs. 196/2003 per la parte di propria competenza.

AREA TECNICA

SERVIZIO PIANIFICAZIONE E PROGETTAZIONE
• Cura della predisposizione del Piano d'Ambito e del Piano Straordinario d'Ambito;

• Progettazione di stazioni ecologiche, isole ecologiche e altri strumenti di raccolta dei rifiuti;
• Progettazione impianti di trattamento e recupero rifiuti;
• Controllo della contabilità dei lavori inerenti la realizzazione dell'impiantistica, finalizzato anche all'emissione dei certificati di pagamento dei S.A.L. e alla cura dei rapporti con tutti i soggetti coinvolti;
• Comunicazioni all'Osservatorio dei Lavori Pubblici;
• Gestione tecnica impiantistica;
• Collaborazione con il Servizio Gestione Finanziamenti e Controllo di Gestione nella cura del piano economico-finanziario dell'impianto e determinazione della tariffa di conferimento;
• Determinazione degli standard di prestazione degli impianti e controllo sulla gestione degli stessi;
• Attuazione Piano d'Ambito nei Comuni del territorio della Provincia di Ancona per quanto di competenza;
• Cura dell'aggiornamento del Documento programmatico della sicurezza ai sensi del D. Lgs. 196/2003 per la parte di propria competenza.
• Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di regolarità tecnica ex art. 49 D. Lgs. 267/2000.

SERVIZIO DIREZIONE CONTRATTI RACCOLTA RIFIUTI
• Attuazione Piano d'Ambito nei Comuni del territorio della Provincia di Ancona per quanto di competenza;
• Controllo e monitoraggio dei servizi di raccolta dei rifiuti previsti nel Piano d'Ambito:
- Elaborazione di manuali per il controllo dei servizi previsti nel Piano d'Ambito della raccolta consortile e gestione degli stessi;
- Coordinamento e realizzazione di controlli territoriali sulle modalità di svolgimento del servizio attraverso soggetti interni e/o esterni all'Ente;
- Rapporti con il Servizio pianificazione campagne di comunicazione e rapporti con i media per l'efficiente ed efficace gestione del servizio;
• Rapporti con i gestori del servizio finalizzati alla soluzione di problemi gestionali e più in generale al corretto svolgimento dello stesso;
• Rapporto con il Servizio Pianificazione e Progettazione al fine di garantire la costante integrazione tra raccolta e trattamento, in quanto attività fondamentali del ciclo integrato di gestione dei rifiuti;
• Cura del sistema tariffario relativamente al servizio di raccolta domiciliare dei rifiuti;
• Gestione tecnica di appalti di servizio e contratti;
• Cura dell'aggiornamento del Documento programmatico della sicurezza ai sensi del D. Lgs. 196/2003 per la parte di propria competenza.
• Assistenza informativa ai Comuni interessati dal servizio;
• Gestione dei rapporti con l'utenza:
- Raccolta di tutte le segnalazioni provenienti dagli utenti del territorio consortile;
- Gestione delle problematiche degli utenti derivanti dalle modalità di prestazione del servizio;
- Interazione con il soggetto gestore per la trasmissione delle segnalazioni dell'utenza e per la verifica dell'efficacia della risposta alle problematiche segnalate;
• Controllo e monitoraggio del servizio di raccolta con particolare riferimento alla risoluzione delle problematiche dell'utenza;
• Coordinamento delle attività inerenti la modifica del servizio di raccolta conseguentemente alle richieste dell'utenza;
• Controllo e monitoraggio del conferito degli utenti finalizzato al miglioramento della qualità del materiale raccolto e alla verifica di eventuali violazioni ai regolamenti comunali di igiene urbana (gestione rifiuti);
• Interazione con le altre aree dell'ATA, quali:
- Servizio pianificazione campagne di comunicazione e rapporti con i media per la realizzazione e lo sviluppo di progetti di educazione ambientale e di interventi comunicativi mirati.
• Apposizione, nell'ambito dei settori e dei procedimenti di propria competenza, dei prescritti pareri di regolarità tecnica ex art. 49 D. Lgs. 267/2000.

4 IL RISULTATO DEL PERCORSO DI AUTOVALUTAZIONE sulla scorta delle linee guida AGID

Servizio	Indice complessivo di criticità	Classe di criticità	Soluzione tecnologica (Tier)	RPO da autovalutaz.	RTO da autovalutaz.
Classe dei Servizi dell'Area Amministrativa	4	Media	Tier3	24	24
Classe dei Servizi dell'Area Finanziaria	4	Media	Tier3	24	24
Classe dei Servizi dell'Area Tecnica	4	Media	Tier3	24	24

5 LA SOLUZIONE TECNOLOGICA E TECNICA

5.1 Soluzione adottata o da adottare

Tutti i servizi in ambito sono coperti da una sola soluzione tecnica che fa riferimento alla soluzione tecnologica di tipo Tier3.

Soluzione tecnologica	Servizi/classi di servizi coperti
Tier3	Soluzione tecnica UNICA per tutti i servizi

5.1.1 Sintesi delle soluzioni tecnologiche e tecniche

Soluzione	Tier3/Soluzione Tecnica UNICA
Stato della soluzione	Da adottare
Elenco dei servizi del tier a cui si riferisce questa particolare soluzione	Tutti
Indicare I valori di RPO e RTO obiettivo della soluzione. I valori vanno indicate in ore (0, se immediato)	RTO 24 RPO 24
Gestione infrastruttura IT del/dei sito/i di produzione per i servizi afferenti alla soluzione	Esterna, con fornitore specializzato che sarà opportunamente individuato con procedura ad evidenza pubblica
Gestione della soluzione per il/i sito/i di DR per i servizi afferenti alla soluzione	Esterna. L'ATA intende dotarsi delle risorse elaborative necessarie con metodologia di acquisizione del servizio presso fornitore esterno specializzato, compreso servizio connettività ridondato; in condizioni di emergenza l'ATA può disporre di personale IT presso la sede, sia diretto che esterno
Le caratteristiche della/e soluzione/i di DR sono conformi alle "Linee guida per il DR delle PA"	Le caratteristiche della soluzione tecnica sono conformi a quanto disposto dalle Linee Guida per il DR delle PA nella sua revisione del Novembre 2013
Descrizione dell'organizzazione per la gestione delle emergenze che si intende adottare (per esempio, come indicato nel capitolo 4 delle "Linee guida per il DR delle PA").	L'organizzazione per la gestione delle emergenze, comune per tutti gli scenari previsti, è governata direttamente da personale dell'ATA mediante SLA che comprendono anche livelli di esercizio per emergenze, presso sito di DR localizzato da fornitore specializzato.
Distanza in km prevista tra il sito principale e il sito di DR	Superiore all'ambito comunale, stimata almeno in 50km
Trasferimento dati tra siti: quanti dati vengono trasferiti (GB, TB) relativamente ai servizi afferenti alla soluzione	Totale dei dati previsti in trasferimento espresso in TB in modalità full: Totale giornalieri Gb 50 massimi, Totale settimanali Gb 250 massimi, Totale mensile TB 1 massimo

Trasferimento dati tra siti: indicare se vengono trasferiti dati sensibili e/o giudiziari relativamente ai servizi afferenti alla soluzione	Il trasferimento di dati tra siti potrà comprendere anche quelli di natura sensibile e/o giudiziario
Modalità di trasferimento dati tra siti	Trasmissione online, con banda garantita e con 100% di banda dedicata utilizzata
Tipologia di risorsa elaborativa nel sito Primario	Mista con server virtualizzati su macchine fisiche di proprietà ASSEMBLEA TERRITORIALE D'AMBITO ATO 2
Risorse elaborative previste nel sito secondario	Come al punto precedente, dedicata
Dimensioni dello storage nel sito primario e secondario relativo ai servizi afferenti alla soluzione	TB totali pari a 1
Connettività del sito DR con eventuali sedi periferiche	Da istituire
Numero minimo di PDL per garantire la funzionalità di servizi offerti	Numero minimo di PDL atte a garantire la funzionalità minima in condizione di emergenza pari a 1 per Servizio
Organizzazione per la gestione di eventuali emergenze (ad es. Comitato di Crisi); se non comune con tutte le soluzioni previste, indicarlo	E' prevista la nomina del Comitato di gestione della Crisi e del responsabile della Continuità come previsto dalle Linee Guida del DR per la PA nella revisione del Novembre 2013 e la loro formazione con apposito atto formale (Decreto Presidente)
Condizioni/rischi valutati per dichiarare lo stato di emergenza (Scenari di Crisi) relativamente ai servizi afferenti alla soluzione	Condizioni limite per dichiarare la crisi: Contemporanea indisponibilità dei servizi. Le condizioni formali di dichiarazione /rientro dello stato di crisi sono esplicitate nel Piano di Continuità Operativa e Disaster Recovery in corso di adozione
Piano di Disaster Recovery	Da istituire
Piano di Continuità Operativa	Da istituire

5.2 Riepilogo Servizi, criticità e Soluzione

Nella seguente tabella per ogni servizio/classe di servizi incluso nell'ambito SFT va riportato :

- *Servizio/classe disservizi*
- *Classe criticità, indicata dallo strumento di autovalutazione*
- *Soluzione tecnologica minima, indicata dallo strumento di autovalutazione (i possibili nomi sonoTier1….Tier6)*
- *Soluzione individuata : vanno riportati gli stessi nomi definiti nel paragrafo precedente (ad esempio Tier3/Soluzione Tecnica1, Tier 3/Soluzione Tecnica2)*
- *Soluzione già presente (Indicare SI se la soluzione è già stata realizzata)*

Servizio	Classe di criticità	Soluzione tecnologica minima da autovalutazione	Soluzione individuata	Soluzione già presente
Classe dei Servizi dell'Area Amministrativa	Media	Tier3	Tier3/UNICA	Da realizzare
Classe dei Servizi dell'Area Finanziaria	Media	Tier3	Tier3/UNICA	Da realizzare
Classe dei Servizi dell'Area Tecnica	Media	Tier3	Tier3/UNICA	Da realizzare

5.3 Differenze rispetto all'autovalutazione

Rispetto all'autovalutazione, l'ATA intende adottare una soluzione unica di tipo Tier3 allineando a criteri di protezione e sicurezza come previsti dalle linee guida in materia, e come da risultato dell'autovalutazione medesima.

6 TEMPI E MODALITÀ DI REALIZZAZIONE DELLA SOLUZIONE

Soluzione	Tempi di Realizzazione	Modalità di Realizzazione
Tier3/Soluzione tecnica UNICA	Si prevede la realizzazione entro l'anno 2017	**Prima fase**: ottimizzazione del CED primario
		Seconda fase: individuazione con procedura ad evidenza pubblica del fornitore specializzato per la selezione del sito secondario di DR, ed attivazione delle procedure

Sito primario: Assemblea Territoriale d'Ambito ATO 2 Ancona, sede, CED
Sito secondario di CO/DR: Da individuare, fornitore esterno specializzato in grado di erogare entrambe le modalità (CO e DR)

6.1 Tempi e Modalità Soluzioni Individuate

	Data Disponibilità
Piano CO	Esistente lo spazio individuato per il sito di CO/DR, si prevede di completare la dotazione tecnologica entro il **31/12/2017**. Entro tale data saranno disponibili formalmente il Piano di CO e gli allegati secondo i criteri previsti da AgID, integrati con i documenti predisposti dal fornitore esterno specializzato selezionato con procedura ad evidenza pubblica
Piano DR	Entro il **31/12/2017**. Entro tale data saranno disponibili formalmente il Piano di CO e gli allegati secondo i criteri previsti da AgID, integrati con i documenti predisposti dal fornitore esterno specializzato selezionato con procedura ad evidenza pubblica
Completamento della soluzione effettuato, operatività della soluzione	Entro il **31/12/2017**

6.2 *Vincoli e rischi Soluzione*

Nessun vincolo o rischio segnalabile al momento.

6.3 *Conclusioni ed adeguatezza della Soluzione*

Si ritiene che la soluzione individuata nel presente SFT sia pienamente conforme a quanto disposto dalla normativa in vigore e adeguata al contesto di rischio dell'Assemblea Territoriale d'Ambito ATO 2 Ancona.

Allegati: n. 3 Schede di analisi di rischio per i servizi e descrittori XML

Generale	
Nome Amministrazione	Assemblea Territoriale d'Ambito ATO2 - Ancona (ATA)
Sede centrale (città)	Jesi
Tipologia Ente	Altri enti
Unità Organizzativa	Area Amministrativa
Responsabile Continuità operativa/Disaster recovery	Simonetta Scaglia
AOO (Area Org.Omog.)/ENTE	ENTE
Indirizzo PEC per le comunicazioni	atarifiutiancona@pec.it
Data compilazione	29/09/2016
Codice Fiscale	93135970429

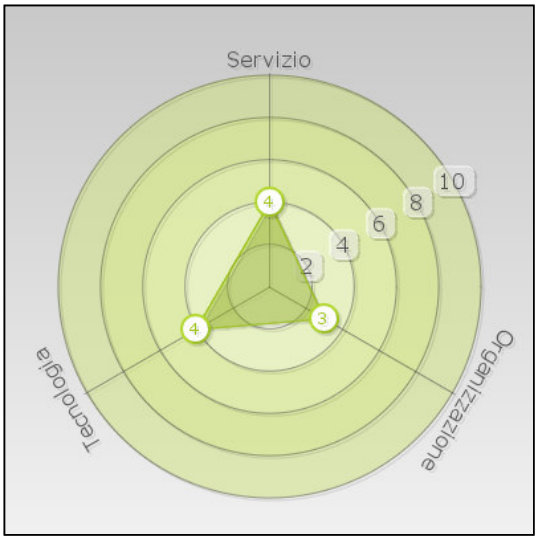
Servizio	
Nome servizio	Classe di servizi Area amministrativa
Tipologia di utenza	eterogenea
Tipo di dati trattati	amministrativi
L'interruzione blocca un altro servizio	sì
Modalità prevalente di interazione con gli utenti	sportello
Giorni alla settimana nei quali viene erogato il servizio	5 giorni su 7
Ore al giorno nelle quali viene erogato il servizio	8 ore al giorno
Sono presenti procedure alternative	sì
E' possibile recuperare la mancata acquisizione dei dati	sì
E' necessario recuperare i dati non acquisiti	sì
L'interruzione determina un immediato disagio agli utenti	sì
Principale danno per l'Amministrazione	inadempienza amministrativa
Livello di danno per l'Amministrazione	alto
Principale tipo di danno per l'utente finale	eterogeneo
Livello di danno per l'utente finale	alto
Tempo massimo tollerabile tra la produzione di un dato e il suo salvataggio	1 giorno
Tempo massimo tollerabile di indisponibilità del servizio	1 giorno

Organizzazione	
Numero di Unità Organizzative	2-5
Numero di sedi	1
Dimensione territoriale	provinciale
Numero dei responsabili privacy	1
Numero degli addetti tramite i quali vengono erogati i servizi	1-10
Numero degli utenti esterni	100.001 o più

Tecnologia	
Presenza di un dipartimento IT	Interno
Numero addetti IT	1-5
Architettura elaborativa	Mista
Architettura applicativa	Mista
Numero di server utilizzati dal servizio	1-3
Numero di postazioni di lavoro	1-10
Numero degli archivi utilizzati dal servizio	1-100
Istanze di DB usate dal servizio	2-5
Dimensione totale dei dati (archivi + istanze DB) usate dal servizio	11-100 Gbyte

Riepilogo degli indici di criticità	
Direttrice	Valori
Servizio	4
Organizzazione	3
Tecnologia	4
Indice Complessivo	4

Valutazione complessiva	
Classe di criticità risultante	Media
Soluzione tecnologica minima	Tier 3



Generale	
Nome Amministrazione	Assemblea Territoriale d'Ambito ATO2 - Ancona (ATA)
Sede centrale (città)	Jesi
Tipologia Ente	Altri enti
Unità Organizzativa	Area Finanziaria
Responsabile Continuità operativa/Disaster recovery	Simonetta Scaglia
AOO (Area Org.Omog.)/ENTE	ENTE
Indirizzo PEC per le comunicazioni	atarifiutiancona@pec.it
Data compilazione	29/09/2016
Codice Fiscale	93135970429

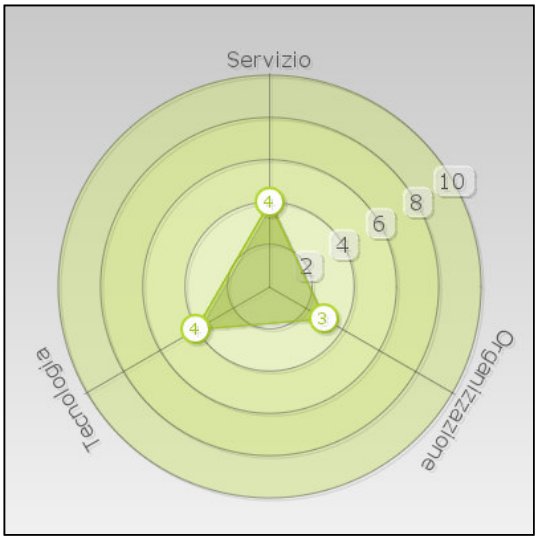
Servizio	
Nome servizio	Classe di servizi Area Finanziaria
Tipologia di utenza	eterogenea
Tipo di dati trattati	amministrativi
L'interruzione blocca un altro servizio	sì
Modalità prevalente di interazione con gli utenti	sportello
Giorni alla settimana nei quali viene erogato il servizio	5 giorni su 7
Ore al giorno nelle quali viene erogato il servizio	8 ore al giorno
Sono presenti procedure alternative	sì
E' possibile recuperare la mancata acquisizione dei dati	sì
E' necessario recuperare i dati non acquisiti	sì
L'interruzione determina un immediato disagio agli utenti	sì
Principale danno per l'Amministrazione	inadempienza amministrativa
Livello di danno per l'Amministrazione	alto
Principale tipo di danno per l'utente finale	economico
Livello di danno per l'utente finale	alto
Tempo massimo tollerabile tra la produzione di un dato e il suo salvataggio	1 giorno
Tempo massimo tollerabile di indisponibilità del servizio	1 giorno

Organizzazione	
Numero di Unità Organizzative	2-5
Numero di sedi	1
Dimensione territoriale	provinciale
Numero dei responsabili privacy	1
Numero degli addetti tramite i quali vengono erogati i servizi	1-10
Numero degli utenti esterni	100.001 o più

Tecnologia	
Presenza di un dipartimento IT	Esterno alla unità responsabile del servizio – Interno alla Amministrazione
Numero addetti IT	1-5
Architettura elaborativa	Mista
Architettura applicativa	Mista
Numero di server utilizzati dal servizio	1-3
Numero di postazioni di lavoro	1-10
Numero degli archivi utilizzati dal servizio	1-100
Istanze di DB usate dal servizio	2-5
Dimensione totale dei dati (archivi + istanze DB) usate dal servizio	11-100 Gbyte

Riepilogo degli indici di criticità	
Direttrice	Valori
Servizio	4
Organizzazione	3
Tecnologia	4
Indice Complessivo	4

Valutazione complessiva	
Classe di criticità risultante	Media
Soluzione tecnologica minima	Tier 3



Generale	
Nome Amministrazione	Assemblea Territoriale d'Ambito ATO2 - Ancona (ATA)
Sede centrale (città)	Jesi
Tipologia Ente	Altri enti
Unità Organizzativa	Area Tecnica
Responsabile Continuità operativa/Disaster recovery	Simonetta Scaglia
AOO (Area Org.Omog.)/ENTE	ENTE
Indirizzo PEC per le comunicazioni	atarifiutiancona@pec.it
Data compilazione	29/09/2016
Codice Fiscale	93135970429

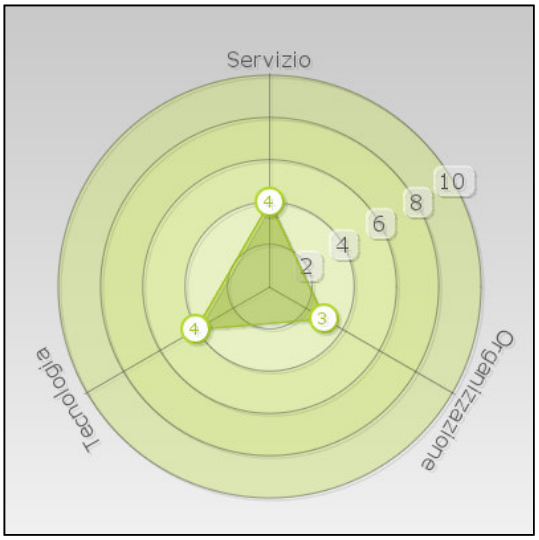
Servizio	
Nome servizio	Classe di servizi Area tecnica
Tipologia di utenza	eterogenea
Tipo di dati trattati	tecnici
L'interruzione blocca un altro servizio	sì
Modalità prevalente di interazione con gli utenti	sportello
Giorni alla settimana nei quali viene erogato il servizio	5 giorni su 7
Ore al giorno nelle quali viene erogato il servizio	8 ore al giorno
Sono presenti procedure alternative	sì
E' possibile recuperare la mancata acquisizione dei dati	sì
E' necessario recuperare i dati non acquisiti	sì
L'interruzione determina un immediato disagio agli utenti	sì
Principale danno per l'Amministrazione	inefficienza amministrativa
Livello di danno per l'Amministrazione	alto
Principale tipo di danno per l'utente finale	eterogeneo
Livello di danno per l'utente finale	alto
Tempo massimo tollerabile tra la produzione di un dato e il suo salvataggio	1 giorno
Tempo massimo tollerabile di indisponibilità del servizio	1 giorno

Organizzazione	
Numero di Unità Organizzative	2-5
Numero di sedi	1
Dimensione territoriale	provinciale
Numero dei responsabili privacy	1
Numero degli addetti tramite i quali vengono erogati i servizi	1-10
Numero degli utenti esterni	100.001 o più

Tecnologia	
Presenza di un dipartimento IT	Esterno alla unità responsabile del servizio – Interno alla Amministrazione
Numero addetti IT	1-5
Architettura elaborativa	Mista
Architettura applicativa	Mista
Numero di server utilizzati dal servizio	1-3
Numero di postazioni di lavoro	1-10
Numero degli archivi utilizzati dal servizio	1-100
Istanze di DB usate dal servizio	2-5
Dimensione totale dei dati (archivi + istanze DB) usate dal servizio	11-100 Gbyte

Riepilogo degli indici di criticità	
Direttrice	Valori
Servizio	4
Organizzazione	3
Tecnologia	4
Indice Complessivo	4

Valutazione complessiva	
Classe di criticità risultante	Media
Soluzione tecnologica minima	Tier 3



CERTIFICATO DI PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che della copia del presente atto è stata disposta la pubblicazione all'Albo pretorio on line in data odierna per 15 giorni interi e consecutivi.

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

CERTIFICATO DI ESEGUITA PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che copia del presente atto è stata affissa all'Albo pretorio on line per 15 giorni interi e consecutivi dal _____ al _____

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

Il presente decreto è divenuto esecutivo il 30.12.2016

☐ Per decorrenza dei termini di cui all'art. 134 del D.Lgs. n. 267/2000.

X Perché dichiarata immediatamente eseguibile ai sensi dell'art. 134, co. 4, del D.Lgs. n. 267/2000.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

CERTIFICATO DI CONFORMITÀ ALL'ORIGINALE

La presente copia, composta di n. 27 pagine, è conforme all'originale conservato in atti e consta altresì di n. 3 allegati.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

COPIA DELL'ORIGINALE DI DECRETO DEL PRESIDENTE

n. 37 **del 30.12.2016**

Oggetto: Approvazione del Documento programmatico sulla sicurezza (DPS) redatto sulla base delle disposizioni previste dagli artt. 34, 35, 36 e dell'Allegato B (disciplinare tecnico in materia di misure minime di sicurezza) del d.lgs. 30 giugno 2003 n. 196 (codice in materia di protezione dei dati personali).

DOCUMENTO ISTRUTTORIO

Oggetto: Approvazione del Documento programmatico sulla sicurezza (DPS) redatto sulla base delle disposizioni previste dagli artt. 34, 35, 36 e dell'Allegato B (disciplinare tecnico in materia di misure minime di sicurezza) del D.Lgs. 30 giugno 2003 n. 196 (codice in materia di protezione dei dati personali).

IL DIRETTORE

RILEVATO che in l'applicazione del Codice in materia di protezione dei dati personali, D.Lgs. 30 giugno 2003 n. 196, ogni amministrazione pubblica deve adottare misure di sicurezza relativamente al trattamento ed alla conservazione dei dati personali che si trova a trattare durante lo svolgimento delle proprie funzioni;

ATTESO che necessita quindi individuare le misure idonee al trattamento e conservazione di tali dati e conseguentemente le misure di sicurezza informatica che si rendono necessarie a tale scopo;

RICHIAMATE le proprie determinazioni n. 16 del 23/02/2016 con la quale si sono definiti i primi indirizzi per l'implementazione del Sistema di gestione documentale informatizzata, e n. 113 del 9/8/2016 con la quale si è affidato il servizio di assistenza e supporto in materia di sicurezza informatica alla ditta Euristica srl;

PRESO ATTO che la ditta Euristica srl ha svolto il proprio servizio collaborando alla stesura della documentazione necessaria affiancando il personale per una adeguata informazione in materia di Privacy e Continuità Operativa e Disaster Recovery (art. 50 del CAD) e indicando le procedure da seguire per adeguarsi alle prescrizioni della normativa vigente in materia;

RITENUTO di approvare il Documento Programmatico sulla Sicurezza (DPS) allegato al presente atto per farne parte integrante e sostanziale, redatto in collaborazione con la ditta Euristica, che consiste sostanzialmente in linee guida che l'ATA dovrà seguire per implementare un idoneo sistema di sicurezza informatica per il trattamento dei dati e dei documenti amministrativi e loro conservazione;

PRESO ATTO che, una volta approvato il DPS, nel corso dell'anno 2017 si dovrà darne attuazione e si dovranno predisporre tutti i documenti di riferimento in esso previsti;

TUTTO CIÒ PREMESSO;

VISTI:
- il D.Lgs. 196/2003;
- il DPR 445/2000;
- il D.Lgs. 82/2005 e s.m.i.;
- il D.Lgs. n. 267/2000
- il D.Lgs. n. 165/2001;
- il D.Lgs. n. 150/2009 e ss.mm.ii.;
- il D.L. n. 78/2010 convertito, con modificazioni, dalla L. n. 122/2010;
- il D.L. n. 90/2014 convertito in L. n. 114/2014;
- il D.Lgs. n. 81/2015;
- il vigente Regolamento di organizzazione;
- il parere favorevole riportato in calce, in ordine alla regolarità tecnica di cui all'art. 49 co. 1, del D.Lgs n. 267/2000;

PROPONE

1) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2) Di approvare, ai sensi del D.Lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali), il Documento Programmatico sulla Sicurezza (DPS), allegato al presente atto per farne parte integrante e sostanziale.
3) Di dare atto che il DPS di cui al precedente punto 2 consiste sostanzialmente in linee guida che l'ATA dovrà seguire per implementare un idoneo sistema di sicurezza informatica per il trattamento dei dati e dei documenti amministrativi e loro conservazione;
4) Di dare atto che il DPS di cui al precedente punto 2 dovrà essere successivamente corredato da tutti i documenti di riferimento in esso previsti, che si dovranno predisporre nel corso dell'anno 2017;
5) Di dare mandato al Direttore con il supporto della struttura di dare attuazione alle linee guida contenute nel DPS di cui al precedente punto 2 entro il 31/12/2017 provvedendo anche alla predisposizione dei documenti ivi previsti sempre entro il 31/12/2017 che dovranno far parte integrante dello stesso;
6) Di trasmettere il presente atto al Responsabile del trattamento dei dati personali, al Responsabile del Trattamento in qualità di Amministratore di Sistema, individuati con il precedente decreto n. 33/2016 e a tutti gli incaricati per il trattamento dei dati personali individuati dal Direttore;
7) Di dichiarare, riscontrata l'urgenza del caso, immediatamente eseguibile il Decreto di approvazione del presente documento istruttorio, ai sensi dell'art. 134, co. 4 del D.Lgs. 267/2000.

Jesi, 30.12.2016

La Direzione
F.to dott.ssa Elisabetta Cecchini

PARERE DI REGOLARITÀ TECNICA

Ai sensi dell'art. 49, co. 1, del D.Lgs. n. 267/2000, si esprime **parere favorevole** in ordine alla regolarità tecnica del presente atto.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

IL PRESIDENTE

VISTO il documento istruttorio redatto dal Direttore in data 30.12.2016, sopra riportato a formare parte integrante e sostanziale del presente atto, contenente la proposta di approvazione Documento Programmatico sulla Sicurezza dell'ente (DPS);

RITENUTO di condividere la proposta di cui sopra per le motivazioni addotte, che si intendono qui integralmente riportate;

VISTO che il documento istruttorio di cui sopra riporta il prescritto parere di regolarità tecnica;

DECRETA

1) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2) Di approvare, ai sensi del D.Lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali), il Documento Programmatico sulla Sicurezza (DPS), allegato al presente atto per farne parte integrante e sostanziale.
3) Di dare atto che il DPS di cui al precedente punto 2 consiste sostanzialmente in linee guida che l'ATA dovrà seguire per implementare un idoneo sistema di sicurezza informatica per il trattamento dei dati e dei documenti amministrativi e loro conservazione;
4) Di dare atto che il DPS di cui al precedente punto 2 dovrà essere successivamente corredato da tutti i documenti di riferimento in esso previsti, che si dovranno predisporre nel corso dell'anno 2017;
5) Di dare mandato al Direttore con il supporto della struttura di dare attuazione alle linee guida contenute nel DPS di cui al precedente punto 2 entro il 31/12/2017 provvedendo anche alla predisposizione dei documenti ivi previsti sempre entro il 31/12/2017 che dovranno far parte integrante dello stesso;
6) Di trasmettere il presente atto al Responsabile del trattamento dei dati personali, al Responsabile del Trattamento in qualità di Amministratore di Sistema, individuati con il precedente decreto n. 33/2016 e a tutti gli incaricati per il trattamento dei dati personali individuati dal Direttore;
7) Di dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'articolo 134, co. 4, del D.Lgs. n. 267/2000.

Il Presidente
F.to dott.ssa Liana Serrani

Documento Programmatico sulla Sicurezza

Redatto in base alle disposizioni del
disciplinare tecnico in materia di misure minime di sicurezza
del codice in materia di protezione dei dati personali

(artt. 34, 35, 36 e Allegato B del d.lgs. 30 giugno 2003, 196)

(Rev. 0 – dicembre 2016)

Assemblea Territoriale
d'Ambito ATO2 - Ancona
www.atarifiuti.an.it

Sede legale:
Strada di Passo Varano, 19/A - 60131 Ancona (AN) - c/o Provincia di Ancona
C.F. 93135970429 Pec: atarifiutiancona@pec.it

Sede operativa:
Viale dell'Industria, 5 - 60035 Jesi (AN)
Tel. 0731.200969 Fax 0731.221630

1. Documento programmatico sulla sicurezza

1.1. Revisione

Indice delle revisioni

Rev	Data	Descrizione	Aggiornamenti
Anno	2016	Prima stesura	Tutte le sezioni del documento

1.2. Scopo del documento e linee guida per la sua composizione

Il presente Documento Programmatico Sulla Sicurezza (di seguito indicato anche come DPS) è redatto per fornire linee guida sulla soddisfazione delle misure minime di sicurezza che debbono essere adottate da questo Ente nel trattamento di dati personali, conformemente a quanto previsto dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)**.

Inoltre costituisce, assieme agli allegati indicati, un valido strumento per la adozione delle misure previste **dall'Art. 31, dall'Art. 34 e dall'Art. 35** dello stesso **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)**.

Nell'ambito del presente documento, sono adottate le seguenti linee guida, che costituiscono gli obiettivi che l'ATA persegue per eseguire una corretta e coerente politica di sicurezza:

Classificazione dei trattamenti
I trattamenti di dati personali devono essere classificati secondo i seguenti principi generali: l'ATA deve riporre assoluta attenzione affinché venga garantita una adeguata protezione ai dati personali e deve individuare le specifiche modalità di trattamento dei dati e i relativi flussi e processi. Si deve procedere, conseguentemente, ad una classificazione, ai fini della sicurezza, rispettando i livelli di protezione dei dati sensibili e strategici in relazione alla operatività del Sistema Informativo.

Classificazione dei dati
I criteri generali di classificazione dei dati dell'ATA ai fini della sicurezza devono valere in linea generale, quindi sia che essi siano originati direttamente, sia che essi siano derivati da terzi. Questo elemento è da considerare attività di primaria importanza in quanto costituisce la "base di conoscenza" su cui si fonda il corretto e sicuro trattamento dei dati.

Criteri di attribuzione di ruoli e responsabilità
I criteri generali di attribuzione di ruoli e responsabilità ai fini della sicurezza devono, in linea generale: individuare i ruoli all'interno dell'ATA ai fini della sicurezza per consentire di fissare le "necessità" di trattamento per ciascun soggetto, determinandone i compiti ed i poteri, in relazione alle diverse tipologie di dati e modalità di trattamento in cui esso è coinvolto, che saranno esercitati previo il controllo di accesso attraverso l'identificazione mediante utente e password.

Sicurezza Fisica
I criteri tecnico–organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per il controllo dell'accesso fisico delle persone nei locali interessati devono, in linea generale: riguardare tutti i dispositivi per il trattamento dei dati, siano essi elettronici che tradizionali, nonché i dati personali, indipendentemente dal supporto su cui essi sono conservati, al fine di essere custoditi in ambienti sicuri. Gli ambienti, sotto il profilo della protezione fisica, saranno distinti in aree a protezione diversificata a seconda delle necessità di protezione dei dati in essere trattati.

Controlli di accesso a dati e processi
I criteri tecnico−organizzativi per il controllo di accesso logico a dati e processi di trattamento dei dati devono, in linea generale: consentire l'abbinamento password - utente per controllare gli accessi alle informazioni, alle applicazioni ed alle attrezzature. Conseguentemente, in tutte le situazioni di trattamento dei dati personali gli incaricati devono essere forniti di identificativo utente e password da utilizzare in combinazione al fine di consentire l'identificazione. Gli incaricati devono essere responsabilizzati per la custodia della password e dell'identificativo utente affidatagli.

Gestione delle password
I criteri tecnico−organizzativi per la gestione delle password di accesso devono, in linea generale: fornire ad ogni operatore che agisce su personal computer sia collegato in rete che non una password, fornita dal responsabile del Sistema Informativo come codice univoco, per l'identificazione dello stesso. Tale codice deve essere conosciuto e custodito dall'operatore a cui è affidato.

Continuità operativa
I criteri tecnico−organizzativi per garantire il ripristino della disponibilità dei dati personali a seguito di distruzione o danneggiamento dei dati stessi o degli strumenti elettronici di trattamento: devono fare riferimento alle analisi dei rischi adottate, in cui sono definiti i criteri generali di massima per la sicurezza dei dati in modo che siano disponibili anche in seguito ad eventi che li distruggano o danneggino.

Outsourcing
I criteri tecnico−organizzativi per garantire l'adozione delle misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno della propria struttura (outsourcing−telelavoro): devono, in base ai vari processi, prevedere eventuali deleghe dall'ATA a organizzazioni esterne. Per tali dati devono essere richieste le giuste assicurazioni affinchè i dati in loro possesso vengano trattati adottando adeguate misure di sicurezza.

Cifratura e segregazione di taluni dati sensibili
I criteri tecnico−organizzativi per la cifratura o per la separazione di alcune categorie di dati personali sensibili, dagli altri dati personali dell'interessato: devono attivarsi indipendentemente dai criteri di archiviazioni e dai formati. Per tutti i dati sensibili suddetti si deve altresì operare separando i processi che riguardano tali dati e cifrando gli stessi dopo la loro elaborazione.

Protezione da programmi maliziosi
I criteri tecnico−organizzativi per la protezione dei dati e dei processi di trattamento da programmi maliziosi (malware) devono, in linea generale: prevedere adeguate protezioni a causa del progresso tecnologico che comporta il progressivo aumento di nuove vulnerabilità e minacce per il sistema informativo; ne consegue che dinamicamente, il sistema informativo deve essere protetto mediante idonei programmi antivirus ed antintrusione con aggiornamento possibilmente automatico.

Riutilizzo dei supporti di memorizzazione
I criteri tecnico−organizzativi per il riutilizzo dei supporti di memorizzazione dei dati (sia per il mantenimento che per il backup) devono, in linea generale: garantire che tutti i supporti che contengono dati sensibili al termine del trattamento devono essere distrutti in modo che non sia consentito il recupero delle informazioni ivi contenute. Nel caso che tali supporti debbano essere riutilizzati preventivamente si deve procedere alla cancellazione in modo permanente ed irrecuperabile delle informazioni ivi contenute. Tale procedura, previa formazione di una copia, deve essere adottata nel caso in cui i supporti contenenti dati personali debbano per qualsiasi ragione essere spostati al di fuori del perimetro dell'Ente o, comunque al di fuori del controllo diretto dell'ATA. E' da evitare l'uso dei dispositivi di memorizzazione rimovibili per lo scambio di dati all'interno dell'ATA: deve essere utilizzato in maniera idonea il sistema informatico e le possibilità di operare in rete.

Criteri e procedure per l'integrità dei dati
I criteri generali per garantire l'integrità dei dati trattati dall'ATA devono, in linea generale: verificare che siano protetti dai rischi, anche accidentali, di distruzione, perdita o modifica non consentita tutti i dati. A tal fine, oltre alle misure di sicurezza preventive, deve essere predisposto un sistema di copiatura al fine di consentire il recupero dei dati. Le copie devono essere le più aggiornate possibile, devono avere la medesima efficacia giuridica degli originali e devono essere trattate e protette con le medesime misure previste per gli originali.

Criteri e procedure per la sicurezza delle trasmissione dati
I criteri generali per garantire l'integrità e la sicurezza delle trasmissioni dei dati da e verso entità esterne devono, in linea generale: provvedere alla massima protezione delle trasmissioni dati in tutti i casi in cui i dati devono essere trasferiti, sia per via elettronica che tradizionale, anche all'interno dell'ATA; devono essere altresì osservate idonee misure di sicurezza al fine di ridurre i rischi di perdita o distruzione, anche accidentale, di intercettazione dei dati, di trattamento comunque non conforme alle finalità di raccolta.

Piano di formazione degli incaricati
Al fine di rendere edotti gli incaricati del trattamento dei rischi individuati, dei modi per prevenire i danni, delle regolamentazioni in materia di sicurezza operanti nell'ATA, deve essere definito un apposito piano di formazione che in termini generali preveda che: l'efficacia delle misure predisposte, poichè subordinata alla collaborazione ed alla effettiva applicazione da parte degli incaricati, deve, con cadenza periodica e, comunque, ogni qualvolta vi siano rilevanti modifiche del piano di sicurezza, prevedere che gli incaricati ed i responsabili siano edotti sulle misure che devono essere adottate e dei rischi che sono stati individuati. L'attività di formazione viene svolta in considerazione delle effettive necessità operative e di conoscenza di ciascun incaricato, responsabile o gruppo.

Revisione della sicurezza
L'efficacia delle misure di sicurezza come specificate nel presente documento, ed in tutta la documentazione che l'ATA dovrà produrre sia in osservanza di obblighi di legge sia per specifiche scelte interne, deve essere verificata periodicamente e comunque almeno una volta l'anno. L'ATA deve perseguire una politica dinamica di gestione della sicurezza e, ne consegue che, ove si manifestasse l'esigenza, il Documento Programmatico della Sicurezza e tutta la documentazione a corredo deve essere sottoposta periodicamente a revisione.

Auditing (verifiche ispettive) della sicurezza
L'efficacia delle misure di sicurezza deve essere verificata periodicamente e comunque almeno una volta l'anno, individuando apposito personale responsabile (interno o esterno all'ATA), con le modalità minime di controllo indicate dall'Allegato B della normativa, ovvero modalità idonee al reale stato di applicazione

1.3. Campo di applicazione

Il Documento Programmatico Sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico Sulla Sicurezza riguarda il trattamento di tutti i dati personali:
- Sensibili
- Giudiziari
- Comuni

Si veda il paragrafo 1.5 per le definizioni di dettaglio.

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali effettuato per mezzo di:
- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il Documento programmatico sulla sicurezza è conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione dell'ATA, poiché approvato e reso noto mediante atti formali dell'ATA.

1.4. Principali riferimenti normativi

- CODICE IN MATERIA DI DATI PERSONALI (Dlgs. n.196 del 30 giugno 2003)
- DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Allegato B al Dlgs. n.196 del 30 giugno 2003)
- LINEE GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI PER FINALITÀ DI PUBBLICAZIONE E DIFFUSIONE DI ATTI E DOCUMENTI DI ENTI LOCALI DELL'APRILE 2007
- PROVV. GEN. GARANTE PRIVACY IN MATERIA DI AMMINISTRATORI DI SISTEMA DEL NOVEMBRE 2008 E SMI
- PROVV. GEN. GARANTE PRIVACY IN MATERIA DI VIDEOSORVEGLIANZA DELL'APRILE 2010 E SMI

- LINEE GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI CONTENUTI ANCHE IN ATTI E DOCUMENTI AMMINISTRATIVI, EFFETTUATO DA SOGGETTI PUBBLICI PER FINALITÀ DI PUBBLICAZIONE E DIFFUSIONE SUL WEB DEL MARZO 2011
- LINEE GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI, CONTENUTI ANCHE IN ATTI E DOCUMENTI AMMINISTRATIVI, EFFETTUATO PER FINALITÀ DI PUBBLICITÀ E TRASPARENZA SUL WEB DA SOGGETTI PUBBLICI E DA ALTRI ENTI OBBLIGATI DEL MAGGIO 2014
- PROVV. GEN. GARANTE PRIVACY IN MATERIA DI MISURE DI SICUREZZA E MODALITÀ DI SCAMBIO DEI DATI PERSONALI TRA AMMINISTRAZIONI PUBBLICHE DEL LUGLIO 2015

1.5. Definizioni

1.5.1. Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

1.5.2. Dato personale

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

1.5.3. Dati sensibili

I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

1.5.4. Dati giudiziari

I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

1.5.5. Titolare

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

1.5.6. Responsabile

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

1.5.7. Incaricati

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

1.5.8. Interessato

La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

1.5.9. Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.5.10. Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.5.11. Dato anonimo

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

1.5.12. Blocco

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

1.5.13. Banca dati

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

1.5.14. Comunicazione elettronica

Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.
Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

1.5.15. Misure minime

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

1.5.16. Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

1.5.17. Autenticazione informatica

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

1.5.18. Credenziali di autenticazione

I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica.

1.5.19. Parola chiave

Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

1.5.20. Profilo di autorizzazione

L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

1.5.21. Sistema di autorizzazione

L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

2. Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali

2.1. Titolare del trattamento dei dati personali

Titolare del trattamento dei dati è l'ASSEMBLEA TERRITORIALE D'AMBITO rappresentato allo scopo dal Presidente in carica pro tempore.

2.1.1. Compiti del titolare del trattamento dei dati personali

In base a quanto stabilito dall'Art. 4, comma 1, lettera f) del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) il *"Titolare del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"*.

Il Titolare del trattamento si impegna ad assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003) tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il Titolare del trattamento decide di affidare il trattamento dei dati in parte all'esterno della struttura, nei modi previsti dagli incarichi specifici che emana direttamente o per tramite dei Responsabili del trattamento dei dati.

Avvalendosi della possibilità prevista dall'Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003), il Titolare del trattamento, per esigenze organizzative, può designare più soggetti Responsabili del trattamento mediante suddivisione di compiti, i quali sono individuati tra i Responsabili dei Servizi poiché questi soggetti, per esperienza, capacità ed affidabilità, forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

I compiti affidati ai Responsabili del trattamento sono analiticamente specificati per iscritto dal Titolare del trattamento. I Responsabili del trattamento effettuano il trattamento attenendosi alle istruzioni impartite dal Titolare del trattamento, con specifici dettagli descritti al paragrafo 2.2.

2.2. Responsabile del trattamento dei dati personali

Il Responsabile del trattamento dei dati personali è il garante dei trattamenti dei dati personali eseguiti nell'ambito delle funzioni dell'ATA. Possono essere nominati dal Titolare del Trattamento Dati con atto proprio, con i compiti definiti nel paragrafo che segue. L'ATA ha previsto la nomina dei nomina Responsabile del Trattamento dati i responsabili delle Aree in cui è organizzata, come indicato nell'organigramma reperibile all'area dell'Amministrazione Trasparente al momento il Direttore risulta l'unico Responsabile delle tre Aree.

2.2.1. Compiti del Responsabile del trattamento di dati personali

Il Responsabile del trattamento di dati personali ha il compito di:

- Nominare gli Incaricati del trattamento dei dati personali (interni ed esterni) limitatamente ai Trattamenti di cui sono responsabili.
- Sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).
- Dare le istruzioni adeguate agli Incaricati del trattamento effettuato con strumenti elettronici.
- Dare le istruzioni adeguate agli Incaricati del trattamento effettuato senza l'ausilio di strumenti elettronici.
- Verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli Incaricati del trattamento dei dati personali.

2.2.2. Nomina dei responsabili del trattamento di dati personali

La nomina di ciascun Responsabile del trattamentodi dati personali è effettuata dal Titolare del trattamento con lettera di incarico in cui sono specificate le responsabilità che gli sono affidate, controfirmata dall'interessato per accettazione.

Nella lettera di nomina debbono essere indicati i Trattamenti di cui è responsabile per quanto attiene alla sicurezza e a quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).

Copia della lettera di nomina accettata è conservata a cura del Titolare del trattamento in luogo sicuro, con apposito affidamento del compito al Responsabile competente per le Risorse Umane.

Il Titolare del trattamento ha informato il Responsabile del trattamento di dati personali delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).

Il Titolare del trattamento rende disponibile al Responsabile del trattamentodi dati personali una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina, unitamente al presente documento, agli allegati descritti e ogni altra documentazione tecnica e/o organizzativa riterrà utile.

La nomina del Responsabile del trattamento di dati personali è a tempo indeterminato, e decade per revoca data dal Titolare del trattamento ovvero per dimissioni o designazione ad altra mansione del Responsabile del trattamento di dati personali.

La nomina del Responsabile del trattamento di dati personali può essere pertanto affidata ad altro soggetto.

2.3. Incarichi particolari

Nell'ambito degli incarichi al trattamento dei dati personali, possono esserne attivati alcuni specifici, descritti nei paragrafi seguenti. Questi incarichi, laddove non specificati, si intendono inclusi nelle nomine a Responsabile del Trattamento, Incaricato al trattamento o Amministratore di Sistema, come meglio specificato nelle singole descrizioni.

2.3.1. Incaricati della custodia delle copie delle credenziali

In conformità a quanto disposto dal punto 10 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003), sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il Titolare del trattamento può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

Il Titolare, o suo delegato, in relazione all'attività svolta, ha individuato, nominato e incaricato per iscritto, un Incaricato della custodia delle copie delle credenziali.

È compito dell'Incaricato della custodia delle copie delle credenziali:

- Autorizzare l'assegnazione e la gestione delle Credenziali di autenticazione per l'accesso ai dati personali degli Incaricati del trattamento, su richiesta del Responsabile dello specifico trattamento, avvalendosi eventualmente del supporto tecnico dell'incaricato della gestione e della manutenzione degli strumenti elettronici, in conformità a quanto disposto dal punto 3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003).
- Istruire gli incaricati del trattamento sull'uso delle componenti riservata delle credenziali di autenticazione, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia, in conformità a quanto disposto dal punto 4 e dal punto 5 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003).

- Assicurare che il Codice per l'identificazione, laddove sia stato già utilizzato, non sia assegnato ad altri Incaricati del trattamento, neppure in tempi diversi, in conformità a quanto disposto dal punto 6 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003).
- Revocare le Credenziali di autenticazione per l'accesso ai dati degli Incaricati del trattamento nel caso di mancato utilizzo per oltre 6 (sei) mesi, in conformità a quanto disposto dal punto 7 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003).
- Revocare tutte le Credenziali di autenticazione non utilizzate in caso di perdita della qualità che consentiva all'Incaricato del trattamento l'accesso ai dati personali, in conformità a quanto disposto dal punto 8 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003).
- Impartire istruzioni agli Incaricati del trattamento per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, in conformità a quanto disposto dal punto 9 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003).

In caso di prolungata assenza o impedimento di un Incaricato del trattamento che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e/o di sicurezza del sistema, l'Incaricato della custodia delle copie delle credenziali, in accordo con il Responsabile dello specifico trattamento di dati personali, assicura la disponibilità di dati o strumenti elettronici operando secondo le seguenti istruzioni:

1. Utilizzando i diritti di "amministratore di sistema", modifica in modo forzoso la componente riservata delle credenziali di autenticazione dell'Incaricato del trattamento dei dati personali assente o impedito ad effettuare il trattamento.
2. Comunica la componente riservata delle credenziali di autenticazione così modificata al Responsabile dello specifico trattamento di dati personali il quale potrà utilizzarla o farla utilizzare ad un altro Incaricato del trattamento dei dati personali designato, solo temporaneamente e per il tempo strettamente indispensabile alle attività di operatività e/o di sicurezza del sistema.
3. Terminata l'assenza o l'impedimento dell'Incaricato del trattamento che aveva reso indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, quest'ultimo dovrà essere informato dell'intervento effettuato e dovrà modificare la propria componente riservata delle credenziali di autenticazione al primo accesso utile al sistema.

In caso di prolungata assenza o impedimento di un Responsabile dello specifico trattamento di dati personali che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e/o di sicurezza del sistema, l'Incaricato della custodia delle copie delle credenziali, in accordo con il Titolare, o suo delegato, assicura la disponibilità di dati o strumenti elettronici operando secondo le seguenti istruzioni:

1. Utilizzando i diritti di "amministratore di sistema", modifica in modo forzoso la componente riservata delle credenziali di autenticazione del Responsabile dello specifico trattamento di dati personali assente o impedito ad effettuare il trattamento.
2. Comunica la componente riservata delle credenziali di autenticazione così modificata al Responsabile della sicurezza di dati personali il quale potrà utilizzarla o farla utilizzare ad un altro Incaricato del trattamento dei dati personali designato, solo temporaneamente e per il tempo strettamente indispensabile alle attività di operatività e/o di sicurezza del sistema.
3. Terminata l'assenza o l'impedimento del Responsabile dello specifico trattamento di dati personali che aveva reso indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, quest'ultimo dovrà essere informato dell'intervento effettuato e dovrà modificare la propria componente riservata delle credenziali di autenticazione al primo accesso utile al sistema.

Qualora si adottino criteri automatici di gestione delle attività appena descritte, il ruolo dell'Incaricato della custodia delle copie delle credenziali può essere assegnato al Responsabile del Sistema Informatico o Amministratore di Sistema. Pertanto, in assenza di una nomina specifica, tale ruolo si intende assegnato all'Amministratore di Sistema dell'ATA.

2.3.2. Incaricati delle copie di sicurezza delle banche dati

In conformità a quanto disposto dal punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il Titolare, o suo delegato, in relazione all'attività svolta, ha individuato, nominato e incaricato per iscritto un Incaricato delle copie di sicurezza delle banche dati.

L'Incaricato delle copie di sicurezza delle banche dati è la persona fisica che ha il compito di sovraintendere alla esecuzione periodica delle copie di sicurezza delle Banche dati personali gestite direttamente presso la struttura

dell'ATA. Per questo, ove non diversamente specificato, per Incaricato delle copie di sicurezza delle banche dati si intende l'incaricato interno all'ATA.

Le Banche dati gestite esternamente all'ATA, in modalità di outsourcing da persona fisica o giuridica (soggetti denominati outsourcer), sono gestite da Incaricati esterni alle copie di sicurezza della banche dati individuati ed incaricati, in forma scritta, dal Responsabile dello specifico trattamento dati che ha competenza di governare sull'operato degli outsourcer suddetti. Tali attività non rientrano, pertanto, tra i compiti specifici dell'Incaricato delle copie di sicurezza delle banche dati qui descritti. Le politiche di gestione delle copie di sicurezza delle banche dati eseguite da Incaricati esterni possono, tuttavia, essere pienamente conformate a quelle descritte per gli Incaricati interni alle copie di sicurezza dei dati; in ogni caso sono approvate dal Responsabile dello specifico trattamento dati cui compete il controllo delle attività dell'outsourcer, il quale può chiedere parere favorevole all'Incaricato delle copie di sicurezza delle banche dati e/o al Responsabile per la sicurezza dei dati personali.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Titolare, o suo delegato, stabilisce, con il supporto tecnico eventuale dell'Incaricato della gestione e della manutenzione degli strumenti elettronici, la periodicità con cui debbono essere effettuate le copie di sicurezza delle Banche di dati trattate.

I criteri possono essere concordati con l'Incaricato della gestione e della manutenzione degli strumenti elettronici in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In conformità a quanto disposto dal punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) la frequenza con cui debbono essere effettuate le copie dei dati personali non deve superare in nessun caso i 7 (sette) giorni dall'ultima copia di sicurezza eseguita.

In particolare, esiste una politica formale di copia delle Banche di dati nella quale sono definite le seguenti specifiche:

- Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up".
- Il numero di "Copie di Back-Up" effettuate ogni volta.
- Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle "Copie di Back-Up".
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le "Copie di Back-Up".
- Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up".

E' compito dell'Incaricato delle copie di sicurezza delle banche dati:

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal Titolare, o suo delegato, .
- Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
- Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.
- Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
- Di segnalare tempestivamente all'Incaricato della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora si adottino criteri automatici di gestione delle attività appena descritte, il ruolo dell'Incaricato delle copie di sicurezza può essere assegnato al Responsabile del Sistema Informatico o Amministratore di Sistema. Pertanto, in assenza di una nomina specifica, tale ruolo si intende assegnato all'Amministratore di Sistema dell'ATA.

2.3.3. Incaricati della custodia delle aree e dei locali

In conformità a quanto disposto dal punto 19.4 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il Titolare, o suo delegato, , può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Incaricati della custodia delle aree e dei locali in cui sono effettuati i trattamenti di dati personali o in cui vengono conservati documenti contenenti dati personali.

Gli Incaricati della custodia delle aree e dei locali debbono:

- Consentire l'accesso alle aree e ai locali di cui debbono assicurare il controllo solo agli Incaricati del trattamento autorizzati.

- Identificare e registrare le persone ammesse, a qualunque titolo, dopo l'orario di chiusura.
- Informare tempestivamente il Titolare, o suo delegato, nel caso in cui si siano riscontrate situazioni anomale.
- Controllare la chiusura dei locali al termine dell'orario.

Qualora il Titolare, o suo delegato, ritenga di non nominare alcun Incaricato della custodia delle aree e dei locali, si intende che sono i singoli Responsabili del Trattamento Dati, ciascuno per la propria competenza, i responsabili della garanzia di custodia di aree e locali.

2.3.4. Incaricati della gestione e della manutenzione degli strumenti elettronici contenti dati

In conformità a quanto disposto dal punto 15, punto 16, punto 17 e punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il Titolare, o suo delegato, in relazione all'attività svolta, ha individuato, nominato e incaricato per iscritto più Incaricati della gestione e della manutenzione degli strumenti elettronici contenenti dati.

Ogni incaricato della gestione e della manutenzione degli strumenti elettronici è persona fisica o giuridica che sovrintende alle risorse messe a disposizione dell'ATA che contengano, in qualunque forma, una o più Banche di dati.

È compito degli Incaricati della gestione e della manutenzione degli strumenti elettronici:

- Attivare per tutti i trattamenti di manutenzione le autorizzazioni di accesso a locali e informazioni, su indicazione del Responsabile del trattamento di dati personali.
- Definire l'attivazione di idonei strumenti per la protezione contro il rischio di accesso abusivo ai dati, danneggiamento anche accidentale degli stessi, ovvero l'interruzione, totale o parziale, o l'alterazione del funzionamento. Questi strumenti debbono essere verificati con cadenza almeno semestrale.
- Informare il Titolare del trattamento dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali contenuti negli strumenti oggetto della manutenzione.

Il Titolare del trattamento o suo delegato nomina uno o più soggetti Incaricati della gestione e della manutenzione degli strumenti elettronici a cui è stato conferito il compito di sovrintendere al buon funzionamento degli strumenti elettronici contenenti dati.

Il Titolare del trattamento do suo delegato informa ciascun Incaricato della gestione e della manutenzione degli strumenti elettronici delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).

La nomina di uno o più Incaricati della gestione e della manutenzione degli strumenti elettronici è effettuata con una lettera di incarico ed è controfirmata per accettazione; copia della lettera di nomina accettata è conservata a cura del Titolare del trattamento dei dati, o da suo delegato, in luogo sicuro.

Il Titolare del trattamento, o suo delegato, rende disponibile a ciascun Incaricato della gestione e della manutenzione degli strumenti elettronici una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina, unitamente al presente documento, agli allegati descritti e ogni altra documentazione tecnica e/o organizzativa riterrà utile.

La nomina dell'Incaricato della gestione e della manutenzione degli strumenti elettronici è a tempo indeterminato, e decade per revoca data dal Titolare del trattamento ovvero per dimissioni o designazione ad altra mansione dell'Incaricato medesimo. La nomina dell'Incaricato può essere pertanto affidata ad altro soggetto.

In assenza di una nomina specifica, tale ruolo si intende assegnato all'Amministratore di Sistema dell'ATA.

2.4. Incaricato del trattamento dei dati personali

2.4.1. Compiti degli incaricati del trattamento dei dati personali

In base a quanto stabilito dall'Art. 30 del Dlgs. n.196 del 30 giugno 2003, le operazioni di trattamento possono essere effettuate solo da Incaricati del trattamento, in questo Ente, che operano sotto la diretta autorità del

Responsabile del trattamento di dati personali cui gli Incaricati fanno riferimento per competenza e mansione, attenendosi alle istruzioni impartite.

In base a quanto definito dall'Art. 4, punto 1, comma h) del Dlgs. n.196 del 30 giugno 2003, gli *"Incaricati del trattamento sono persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal Titolare del trattamento o, se designato, dal Responsabile di uno specifico trattamento di dati personali"*.

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati che contengono i predetti dati personali.
- Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.
- L'Incaricato del trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.
- Ogni Incaricato del trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
- Gli Incaricati del trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
- La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- L'Incaricato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.
- In caso di trattamento di dati sensibili e di dati giudiziari la componente riservata delle credenziali di autenticazione (parola chiave) deve essere modificata almeno ogni tre mesi.
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici , composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;

- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.
- Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

2.4.2. Nomina degli incaricati del trattamento dei dati personali

La nomina di ciascun Incaricato del trattamento dei dati personali è effettuata dal Responsabile del trattamento di dati personali cui l'Incaricato fa riferimento per competenza e mansione, con una lettera di incarico in cui sono specificati i compiti che gli sono stati affidati e che è controfirmata dall'interessato per presa visione.

Copia della lettera di nomina firmata è conservata a cura del Responsabile del trattamento di dati personali in luogo sicuro.

Il Responsabile del trattamento di dati personali ha informato ciascun Incaricato del trattamento dei dati personali delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).

Il Titolare, o suo delegato, rende disponibile a ciascun Incaricato del trattamento dei dati personali una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina, unitamente al presente documento, agli allegati descritti e ogni altra documentazione tecnica e/o organizzativa riterrà utile.

Gli Incaricati del trattamento dei dati personali hanno ricevuto idonee ed analitiche istruzioni scritte, ove applicabile per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli Incaricati del trattamento dei dati personali è assegnata una credenziale di autenticazione.

Agli Incaricati del trattamento dei dati personali è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale di autenticazione e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

La nomina dell'Incaricato del trattamento dei dati personali è a tempo indeterminato, e decade per revoca data dal Titolare del trattamento (o dal Responsabile dello specifico trattamento di dati personali che gli ha affidato l'incarico) ovvero per dimissioni o designazione ad altra mansione dell'Incaricato medesimo.

La nomina dell'Incaricato può essere pertanto affidata ad altro soggetto.

2.5. Amministratore di Sistema

2.5.1. Compiti dell'Amministratore di Sistema

In conformità a quanto disposto dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il Titolare, o suo delegato, ha individuato, nominato e incaricato per iscritto, un Responsabile del sistema informatico e Amministratore di sistema (nel seguito del documento indicato per

semplificazione come Responsabile del sistema informatico), cui è conferito il compito di sovrintendere alle risorse del sistema e di consentirne l'utilizzazione, secondo le seguenti disposizioni:

- Verificare la rispondenza del sistema informatico rispetto alle norme sulla sicurezza emanate dal Garante della Privacy, ed in base alle risultanze provvedere agli adempimenti necessari in relazione alle disposizioni di legge in materia di sicurezza del trattamento dei dati.
- Gestire il sistema informatico, nel quale risiedono le banche dati, in base alle disposizioni del D. Lgs. n. 196/2003, del relativo Allegato B e dei successivi disciplinari tecnici, attenendosi alle disposizioni in esse contenute.
- Collaborare con il Titolare ed i Responsabili degli specifici trattamenti di dati personali al fine di esercitare un doveroso controllo sulle attività effettuate dagli incaricati al trattamento, affinché le azioni svolte siano rispondenti alle norme vigenti.
- Sovrintendere alle attività di salvaguardia degli archivi, individuare eventualmente un preposto alla custodia delle credenziali di autenticazione e provvedere, in collaborazione con il preposto eventualmente individuato alla custodia, affinché siano assegnate le parole chiave di accesso al sistema agli utilizzatori che ne abbiano facoltà.
- Provvedere ad attivare un sistema efficace di gestione giornaliera delle copie di sicurezza degli archivi di dati.
- Predisporre, mediante adeguati strumenti, tutte le misure idonee a limitare danni conseguenti a guasti tecnici, violazione del sistema, virus informatici e quanto altro possa mettere a rischio i dati.
- Curare l'aggiornamento periodico dei programmi antivirus in conformità al disposto dell'Allegato B del D. Lgs. n. 196/2003.
- Verificare la situazione del software installato, sia per una maggiore tutela nei confronti di programmi che potrebbero danneggiare il sistema, sia per dare attuazione al rispetto delle norme sulla tutela dei diritti d'autore. Potrà pertanto emanare eventuali Regolamenti tecnici specifici (denominati policy) nel quale si stabiliscano le norme di comportamento per l'utilizzo dei sistemi (strumenti e programmi) ponendo particolare attenzione ad evitare l'installazione di software non autorizzato (anche se gratuito).
- Assegnare agli utilizzatori dei terminali i codici di autenticazione (codice utente e Password associata) e gestire gli stessi in base ai disposti dell'Allegato B del D. Lgs. n. 196/2003.
- Predisporre ed aggiornare, in collaborazione con il Titolare o i Responsabili degli specifici trattamenti dei dati personali, il sistema di sicurezza in base alle disposizioni degli Artt. 31, 33 e 34 D. Lgs. n. 196/2003.

Sono inoltre compiti dell'Amministratore di Sistema tutti quelli ad esso/i assegnati dal Titolare del Trattamento Dati ai sensi e per gli effetti del Provv. Gen. Dela Garante Privacy Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008(G.U. n. 300 del 24 dicembre 2008), così modificato in base al provvedimento del 25 giugno 2009.

2.5.2. Nomina dell'Amministratore di Sistema

La nomina dell'Amministratore di Sistema è stata effettuata dal Titolare, e sarà oggetto di revisione annualmente come risulta dai documenti allegati al presente DPS, in ottemperanza a quanto ricihiesto dal Provv. Gen. Del Garante Privacy Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), così modificato in base al provvedimento del 25 giugno 2009.
Le attività previste per questo ruolo sono concordate tra Titolare e Amministratore di Sistema secondo le vigenti disposizioni del Garante Privacy, e controllate periodicamente attraverso la checklist annuale allegata al presente documento. Le attività sono altresì rendicontate con la Relazione Annuale sullo Stato del Sistema redatta entro il 15 dicembre di ogni anno.

3. Trattamenti con l'ausilio di strumenti elettronici

3.1. Sistema di autenticazione informatica

3.1.1. Procedura di identificazione

In conformità a quanto disposto dal punto 1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003), poichè il trattamento di dati personali è effettuato con strumenti elettronici, il Titolare, o suo delegato, si assicura che il trattamento sia consentito solamente agli Incaricati del trattamento dei dati personali dotati di Credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti e di autorizzazione relativa.

3.1.2. Identificazione dell'incaricato

In conformità a quanto disposto dal punto 2 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il Titolare, o suo delegato , avvalendosi della collaborazione dell'Incaricato della custodia delle copie delle credenziali e dell'Incaricato della gestione e della manutenzione degli strumenti elettronici (se necessario) si assicura che il trattamento di dati personali, effettuato con strumenti elettronici, è consentito solamente agli Incaricati del trattamento dotati di una Credenziale di autenticazione, costituita da un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.

In conformità a quanto disposto dal punto 3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) ad ogni Incaricato del trattamento possono essere assegnate o associate individualmente una o più Credenziali per l'autenticazione.

3.1.3. Cautele per assicurare la segretezza della componente riservata della credenziale

In conformità a quanto disposto dal punto 4 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) gli incaricati debbono adottare le necessarie cautele per assicurare la segretezza della parola chiave e Custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc.).

Inoltre ogni Incaricato del trattamento è informato e reso edotto che le Credenziali di autenticazione:

- Sono personali
- Devono essere memorizzate
- Non devono essere comunicate a nessuno
- Non devono essere trascritte

3.1.4. Caratteristiche della parola chiave

In conformità a quanto disposto dal punto 5 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) la Componente riservata delle credenziali di autenticazione (parola chiave o password) rispetta i seguenti criteri:

- Non deve contenere nomi comuni
- Non deve contenere nomi di persona
- Deve contenere sia lettere che numeri
- Deve comprendere maiuscole e minuscole
- Deve essere diversa dallo User-Id
- Deve essere lunga almeno 8 caratteri fino al massimo consentito dal sistema di autenticazione
- Non deve essere riconducibile all'incaricato

Possono essere assegnati criteri di caratteristiche della parola chiave in maniera maggiormente restrittiva, qualora il Titolare del Trattamento o suo delegato (tipicamente il Responsabile del Sistema Informatico o Amministratore di Sistema) ritenga di applicare tali canoni per ragioni di idonee misure di sicurezza.

3.1.5. Modalità di richiesta delle credenziali di autenticazione

L'assegnazione delle Credenziali di autenticazione avviene dietro specifica richiesta del Responsabile del trattamento.

La richiesta viene inoltrata al Responsabile del sistema informatico ovvero Amministratore di Sistema in forma scritta (nell'ordine) dal Titolare del Trattamendo dei Dati ovvero dal Responsabile di specifico Trattamento dei Dati ovvero dall figura apicale di riferimento dell'Incaricato al Trattamento al quale si intende fornire credenziali di autenticazione.

Il Responsabile del sistema informatico ovvero l'Amministratore di Sistema provvede:

- A comunicare all'Incaricato del trattamento dei dati personali, nonché a colui che ha eseguito formale richiesta scritta, al momento dell'attivazione, la sua Credenziale di autenticazione
- A comunicare all'Incaricato del trattamento dei dati personali al momento dell'attivazione la sua Componente riservata delle credenziali di autenticazione (parola chiave o password) temporanea, che sarà modificata al primo accesso
- Alla abilitazione dei permessi che consentano all'Incaricato del trattamento dei dati personali di accedere al trattamento che gli è stato affidato
- Ad effettuare le verifiche di corretto accesso
- A conservare copia della richiesta

Il Responsabile del trattamento informa i propri Incaricati del trattamento dei criteri e delle regole che debbono essere osservate per assicurare la segretezza della Componente riservata delle credenziali di autenticazione (parola chiave o password).

Il Responsabile del trattamento che ha effettuato la richiesta fornisce idonee informazioni, anche in forma strutturata, con le quali sono specificati i criteri che debbono essere rispettati per la Componente riservata delle credenziali di autenticazione (parola chiave o password), ovvero distribuisce idoneo Disciplinare Tecnico.

Al primo accesso l'Incaricato del trattamento dovrà modificare la Componente riservata delle credenziali di autenticazione (parola chiave o password) rispettando le regole definite nella lettera di assegnazione delle Credenziali di autenticazione.

È compito del Titolare, o suo delegato, approntare, direttamente o per mezzo di deleghe di compiti specifici, gli strumenti ed i controlli mediante cui verificare il corretto uso delle Credenziali di autenticazione e monitorare e vigilare sui tentativi di accesso non autorizzato.

I tentativi di accesso non autorizzati saranno registrati e dovrà essere data tempestiva comunicazione al Titolare del trattamento.

In caso di smarrimento della Componente riservata delle credenziali di autenticazione (parola chiave o password) il Responsabile dello specifico trattamento dell'incaricato dovrà richedere al Responsabile del sistema informatico una nuova assegnazione.

Il Responsabile del sistema informatico provvederà ad annullare la Componente riservata delle credenziali di autenticazione (parola chiave o password) precedente e ad assegnarne una nuova provvisoria.

Le Credenziali di autenticazione che non sono utilizzate per più di 6 mesi dovranno essere disabilitate d'autorità dal Responsabile del sistema informatico.

Il Responsabile del trattamento devono dare informazione al Titolare, o suo delegato, circa le dimissioni del personale o lo spostamento di mansione per annullare le Credenziali di autenticazione dell'Incaricato del trattamento.

3.1.6. Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico

In conformità a quanto disposto dal punto 9 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) gli Incaricati del trattamento hanno l'obbligo di:

- Non lasciare incustodito il proprio posto di lavoro.
- Di chiudere tutte le applicazioni aperte o meglio ancora di spegnere il sistema informatico in caso di assenza prolungata.
- Di bloccare l'uso della postazione di lavoro, mediante funzionalità specifica del sistema operativo, in caso di breve assenza dal posto di lavoro, attivata manualmente o in forma automatica.

3.1.7. Accesso straordinario

In conformità a quanto disposto dal punto 10 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) gli Incaricati della custodia delle copie delle credenziali, hanno il compito di assicurare la disponibilità dei dati e degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

La custodia delle copie delle Credenziali di autorizzazione è organizzata garantendo la relativa segretezza, adottando criteri di protezione delle credenziali cartacee in cassaforte e adozione di sistemi elettronici di conservazione delle stesso con croteri di sicurezza elevata.

Gli Incaricati della custodia delle copie delle credenziali informano tempestivamente l'Incaricato del trattamento ogni qualvolta sia stato effettuato un tale tipo di intervento.

In conformità a quanto disposto dal punto 11 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

3.2. Sistema di autorizzazione

Il Responsabile del trattamentotrattamento di dati personali ha individuato gli Incaricati del trattamento per ogni tipologia di banca di dati personali trattata.

In conformità a quanto disposto dal punto 12 e dal punto 13 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il tipo di trattamento effettuato da ogni singolo Incaricato del trattamento risulta essere differenziato.

In particolare il Responsabile del trattamento di dati personali autorizza le operazioni di trattamento consentite ad ogni Incaricato del trattamento tra le seguenti:

- Inserire nuove informazioni nella banca di dati personali
- Accedere alle informazioni in visualizzazione e stampa
- Modificare le informazioni esistenti nella banca di dati personali
- Cancellare le informazioni esistenti nella banca di dati personali

In conformità a quanto disposto dal punto 15 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) almeno una volta l'anno e comunque entro il 31 marzo, il Responsabile del trattamento di dati personali aggiorna l'Elenco dei permessi di accesso che sono stati assegnati agli Incaricati del trattamento per ogni tipologia di banca di dati.

In conformità a quanto disposto dal punto 19.2 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. 196 del 30 giugno 2003), tale Elenco deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.3. Altre misure di sicurezza

In considerazione di quanto disposto dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), oltre all'applicazione di altre norme specifiche, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate formalmente dal Titolare, o suo delegato, di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate formalmente dal Titolare, o suo delegato, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione formale del Titolare, o suo delegato, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate formalmente dal Titolare, o suo delegato, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

3.4. Periodicità di revisione del documento programmatico sulla sicurezza

Con periodicità almeno annuale, il Titolare del trattamento di dati sensibili o di dati giudiziari verifica ed aggiorna il Documento programmatico sulla sicurezza contenente idonee informazioni riguardo ai punti 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).

3.5. Elenco dei trattamenti di dati personali

3.5.1. Elenco delle sedi e degli uffici in cui vengono trattati i dati

Al Titolare, o suo delegato, è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati.

In conformità a quanto disposto dal punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) per redigere l'Elenco delle sedi in cui vengono trattati i dati deve essere utilizzato un modulo che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere aggiornato e conservato in luogo sicuro a cura del Titolare, o suo delegato.

3.5.2. Elenco degli archivi dei dati oggetto del trattamento

Al Responsabile dello specifico trattamento di dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.

Ogni banca di dati o archivio deve essere classificato in relazione alle informazioni contenute indicando se si tratta di:

- Dati personali Comuni
- Dati personali Sensibili
- Dati personali Giudiziari

In conformità a quanto disposto dal punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato un modulo che deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.5.3. Elenco dei sistemi di elaborazione per il trattamento

Al Responsabile del sistema informatico è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.

Per ogni sistema deve essere specificato:

- Il nome dell'Incaricato della gestione e della manutenzione
- Il nome dell'incaricato o degli incaricati che lo utilizzano
- Il nome di uno o più Incaricati della custodia delle copie delle credenziali

In conformità a quanto disposto dal punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) per ogni sistema deve essere utilizzato un modulo che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del Responsabile del sistema informatico in luogo sicuro e deve essere trasmesso in copia controllata agli Incaricati della gestione e della manutenzione degli strumenti elettronici di competenza.

3.6. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

3.6.1. Elenco dei soggetti autorizzati al trattamento dei dati

Il Responsabile del trattamentotrattamento di dati personali ha il compito di:

- Nominare gli Incaricati del trattamento dei dati personali (siano essi interni o esterni) limitatamente alle Banche di dati di cui sono responsabili
- Assegnare le Credenziali di autenticazione
- Informare il Responsabile del sistema informatico delle variazioni intervenute nell'assegnazione delle Credenziali di autorizzazione.

Il Responsabile del trattamentotrattamento di dati personali tiene aggiornato ad ogni variazione l'Elenco del personale autorizzato al trattamento dei dati per quanto attiene alle competenze e mansioni specifiche della propria sfera di responsabilità.

Ogni Elenco del personale autorizzato al trattamento dei dati deve essere redatto dal Responsabile del trattamento di dati personali deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del medesimo Responsabile del trattamento di dati personali in luogo sicuro.

Una copia degli Elenchi del personale autorizzato al trattamento dei dati deve essere consegnata all'Incaricato della custodia delle copie delle credenziali.

3.6.2. Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

I Responsabili degli specifici trattamenti di dati personali hanno il compito di verificare ogni anno, entro il 31 marzo, le Credenziali di autenticazione assegnate agli incaricati che afferiscono allo loro sfera di competenza e mansione.

Ogni Responsabile degli specifici trattamenti di dati personali tiene pertanto aggiornato costantemente ogni variazione dell'Elenco del personale autorizzato al trattamento dei dati che afferisce al Responsabile in questione.

Ogni Elenco del personale autorizzato al trattamento dei dati viene redatto e viene allegato al presente Documento Programmatico sulla Sicurezza, e conservato a cura del Responsabile degli specifici trattamenti di dati personali, in luogo sicuro.

Una copia di ogni Elenco del personale autorizzato al trattamento dei dati viene consegnata all'Incaricato della custodia delle copie delle credenziali.

3.6.3. Distribuzione dei compiti e delle responsabilità

In conformità a quanto disposto dal punto 19.2 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. 196 del 30 giugno 2003), il Titolare del trattamento autorizza la struttura di riferimento, definisce i compiti e le relative responsabilità, in relazione ai trattamenti effettuati, e predispone un modulo che deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.7. Analisi dei rischi

3.7.1. Analisi dei rischi hardware

Il Titolare, o suo delegato, anche avvalendosi di consulenti interni o esterni e/o della collaborazione del responsabile del sistema informatico, deve verificare ogni anno:

- La situazione delle apparecchiature hardware installate con cui vengono trattati i dati
- La situazione delle apparecchiature periferiche
- La situazione dei dispositivi di collegamento con le reti pubbliche

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito

Il Responsabile del sistema informatico aggiorna il Report annuale dei rischi hardware.

In conformità a quanto disposto dal punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) l'analisi dei rischi viene allegata al presente Documento Programmatico sulla Sicurezza.

Gli Incaricati della gestione e della manutenzione degli strumenti elettronici nel caso in cui esistano rischi evidenti informano tempestivamente il Titolare, o suo delegato, affinché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.7.2. Analisi dei rischi sui sistemi operativi e sui software installati

Al Titolare, o suo delegato, anche avvalendosi di consulenti interni o esterni e/o della collaborazione del responsabile del sistema informatico, è affidato il compito di verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei software utilizzati.
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti.
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Il Responsabile del sistema informatico aggiorna il Report annuale dei rischi sui software installati.

In conformità a quanto disposto dal punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003), tale analisi dei rischi viene allegata al presente Documento Programmatico sulla Sicurezza.

Gli Incaricati della gestione e della manutenzione degli strumenti elettronici, nel caso in cui esistano rischi evidenti, informano tempestivamente il Titolare, o suo delegato, affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.7.3. Analisi degli altri rischi nel trattamento dei dati

Al Titolare, o suo delegato, anche avvalendosi di consulenti interni o esterni, ed in collaborazione con i Responsabili degli specifici trattamenti di dati personali, è affidato il compito di analizzare eventuali altri rischi connessi al trattamento dei dati tenendo conto in particolare di:

- Rischi connessi al comportamento degli operatori
- Rischi connessi al contesto fisico ed ambientale

Il Titolare, o suo delegato, aggiorna il Report annuale degli altri rischi.

In conformità a quanto disposto dal punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) l'alisi dei rischi suddetta viene allegata al presente Documento Programmatico sulla Sicurezza.

I Responsabili degli specifici trattamenti di dati personali, nel caso in cui esistano rischi evidenti, informano tempestivamente il Titolare, o suo delegato affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.8. Misure da adottare per garantire l'integrità e la disponibilità dei dati

Il Titolare, o suo delegato, anche avvalendosi di consulenti interni o esterni e/o della collaborazione del responsabile del sistema informatico, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le procedure che consentano di garantire l'integrità e la disponibilità dei dati trattati. I criteri sono definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Sono impartite precise istruzioni contenute in un apposito Disciplinare interno da allegare al presente documento.

3.9. Misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

3.9.1. Misure generali

In considerazione di quanto disposto dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Titolare, o suo delegato, o dal Responsabile dello specifico trattamento di dati personali oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Titolare, o suo delegato, o dal Responsabile dello specifico trattamento di dati personali, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Titolare, o suo delegato, o dal Responsabile dello specifico trattamento di dati personali, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal Titolare, o suo delegato, o dal Responsabile dello specifico trattamento di dati personali, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

3.9.2. Procedure per controllare l'accesso ai locali in cui vengono trattati i dati

Sono impartite precise istruzioni contenute nel Disciplinare interno da allegare al presente documento.

3.10. Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare

3.10.1. Trattamenti di dati personali affidati all'esterno della struttura del titolare

Il Titolare, o suo delegato, ha facoltà di decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, eventualmente sentito il parere del Responsabile del trattamento di dati personali e/o del Responsabile del sistema informatico. Tali soggetti esterni possono essere persone fisiche o giuridiche (o comunque altre forme organizzative) che diano garanzia di affidabilità nella gestione di tali trattamenti esterni.

In caso in cui questo avvenga, il Titolare, o suo delegato, , redige ed aggiorna ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, ed indica per ognuno di essi il tipo di trattamento effettuato, specificando:

- I soggetti interessati
- I luoghi dove fisicamente avviene il trattamento dei dati stessi
- I/Il responsabili/e del trattamento di dati personali di riferimento per l'ATA
- La forma documentale che il soggetto esterno alla struttura dell'ATA mette a disposizione per le attività di controllo del proprio operato (a titolo di esempio e non esaustivo, Dichiarazioni di Conformità ai sensi del D.Lgs 196/03, Piano di sicurezza delle informazioni, Documento programmatico sulla sicurezza e simili)

Per l'inventario dei soggetti a cui affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, viene utilizzato un modulo che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e conservato a cura del Titolare, o suo delegato, in luogo sicuro.

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, sia possibile nominare responsabili del trattamento soggetti controllabili dal Titolare del trattamento stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso), gli stessi sono indicati quali Responsabili del trattamento in Out-sourcing, mediante un modulo da compilare specificatamente.

Nel caso in cui siano stati nominati uno o più Responsabili del trattamento in Out-sourcing, in conformità a quanto disposto dal punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il modulo apposito viene allegato al presente Documento Programmatico sulla Sicurezza.

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, non sia possibile nominare i responsabili del trattamento, in quanto soggetti autonomi non controllabili dal titolare del trattamento stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso), sono individuati i Titolari autonomi del trattamento in Out-sourcing, per il quale trattamento, ai sensi dell'art. 28 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003), si intendono autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

Nel caso in cui siano stati nominati uno o più Titolari autonomi del trattamento in Out-sourcing, in conformità a quanto disposto dal punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il modulo compilato viene allegato al presente Documento Programmatico sulla Sicurezza.

3.10.2. Criteri per la scelta di soggetti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare

Il Titolare, o suo delegato, può affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare a quei soggetti terzi che abbiano i requisiti di esperienza, capacità ed affidabilità individuati all'art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003).

Il Titolare a cui è stato affidato il trattamento dei dati all'esterno rilascia una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento ai sensi del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), c.d. Dichiarazione di Conformità, unitamente a rendere sempre

disponibile copia del piano della siurezza dele informazioni e/o copia del Documento programmatico sullo stato della sicurezza.

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, di qualsiasi natura, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE , se il terzo destinatario non è italiano ma risiede in un paese comunitario,

e comunque, in ogni caso, solamente in base alle finalità istituzionali dell'ATA oppure in base a specifica Autorizzazione al Trattamento da parte del Garante.

Se il trattamento concerne dati di natura sensibile, l'ATA fa riferimento alle disposizioni integrative previste dal D.Lgs. 11 maggio 1999 n. 135, pubblicato nella Gazzetta Ufficiale n. 113 del 17 maggio 1999.

Non sono previsti ambiti all'interno dei quali sia attuabile il trasferimento verso soggetti residenti in Paesi extra-Ue.

3.10.3. Nomina del responsabile del trattamento per soggetti esterni alla struttura del Titolare in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Titolare, o suo delegato, si assicura che siano rispettate le norme di sicurezza di un livello almeno non inferiore a quanto stabilito per il trattamento interno.

Il Responsabile del trattamento in Out-sourcing accetta la nomina in forma scritta.

La nomina del Responsabile del trattamento in Out-sourcing è controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare, o suo delegato, in luogo sicuro.

Il Titolare, o suo delegato, informa il Responsabile del trattamento in Out-sourcing, dei compiti che gli sono assegnati in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).

Al momento dell'affidamento dell'incarico il Responsabile del trattamento in Out-sourcing, dichiara di accettare per iscritto almeno le seguenti prescrizioni operative:

- *Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali*
- *Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali*
- *Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.*
- *Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.*
- *Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate, anche senza preavviso*

In conformità a quanto disposto dal punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. 196 del 30 giugno 2003) il modulo suddetto, viene allegato al presente Documento Programmatico sulla Sicurezza.

3.10.4. Nomina del titolare autonomo del trattamento in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Titolare, o suo delegato, si assicura che siano rispettate le norme di sicurezza di un livello almeno non inferiore a quanto stabilito per il trattamento interno.

Il Titolare autonomo del trattamento in Out-sourcing accettare la nomina, secondo il modello di riferimento.

La nomina del Titolare autonomo del trattamento in Out-sourcing viene controfirmata per accettazione e copia della lettera di nomina accettata è conservata a cura del Titolare, o suo delegato, in luogo sicuro.

Il Titolare, o suo delegato, informa il Titolare autonomo del trattamento in Out-sourcing, dei compiti che gli sono assegnati in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).

Al momento dell'affidamento dell'incarico il Titolare autonomo del trattamento in Out-sourcing, dichiara di accettare per iscritto almeno le seguenti prescrizioni operative:

- *Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali*
- *Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali*
- *Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.*
- *Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.*
- *Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate, anche senza preavviso*

In conformità a quanto disposto dal punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. 196 del 30 giugno 2003) il modulo di riferimento, viene allegato al presente Documento Programmatico sulla Sicurezza.

3.11. Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

3.11.1. Protezione contro l'accesso abusivo

In conformità a quanto disposto dal punto 16, punto 17 e punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) al fine di garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso abusivo, il Titolare, o suo delegato, stabilisce, con l'eventuale supporto del Responsabile del sistema informatico e dei Responsabili di specifico trattamento dei dati personali le misure tecniche da adottare in rapporto ad eventuali rischi.

I criteri sono definiti dal Titolare, o suo delegato, in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare, per ogni Sistema interessato sono definite le seguenti specifiche:

- In conformità a quanto disposto dal punto 16 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) individua idonei strumenti per la protezione degli strumenti elettronici contro il rischio di intrusione e dell'azione di programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.
- In conformità a quanto disposto dal punto 17 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) stabilire la frequenza con cui aggiornare i programmi per elaboratore per prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti.
- In conformità a quanto disposto dal punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) individuare come proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso abusivo da parte di chiunque abusivamente si introduce nel sistema informatico o telematico.

Per ogni sistema deve essere utilizzato un modulo che deve essere conservato a cura del Titolare, o suo delegato, in luogo sicuro e deve essere trasmesso in copia controllata all'Incaricato della gestione e della manutenzione degli strumenti elettronici di competenza.

In conformità a quanto disposto dal punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il modulo deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.11.2. Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

Non sono impartite al momento specifiche istruzioni in merito.

3.11.3. Riutilizzo dei supporti rimovibili

Non sono impartite al momento specifiche istruzioni in merito.

3.11.4. Ripristino dell'accesso ai dati in caso di danneggiamento

Si rinvia alla documentazione di aggiornamento ai sensi dell'art. 50bis del Codice di Amministrazione Digitale.

3.12. Trattamenti effettuati da organismi sanitari e esercenti le professioni sanitarie

3.12.1. Cifratura dei dati o separazione dei dati identificativi

Il Titolare, o suo delegato, per i trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale elencati ha stabilito di adottare le seguenti misure di sicurezza come specificato nella tabella che segue in conformità a quanto disposto dal punto 19.8 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003).

3.12.2. Tabella dei trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale

Non applicabile al contesto dell'ATA.

3.13. Misure di tutela e garanzia

3.13.1. Descrizione degli interventi effettuati da soggetti esterni

Nel caso in cui ci si avvalga di soggetti esterni alla propria struttura, per provvedere al controllo del buon funzionamento infrastrutturale, hardware e/o software, degli strumenti elettronici contenenti dati, per eventuale riparazione, aggiornamento o sostituzione, nonché per trattamenti di dati completamente esternalizzati o erogati in outsourcing (da qualunque persona fisica, giuridica ovvero organizzazione), il Responsabile dello specifico trattamento dei dati competente per il controllo di tali attività (ovvero il Titolare, o suo delegato, qualora lo preveda espressamente), deve farsi consegnare puntualmente dal personale che ha effettuato l'intervento tecnico, una dichiarazione scritta con la descrizione dettagliata delle operazioni eseguite che attesti la conformità a quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003). Tale dichiarazione è integrata complessivamente da Dichiarazione di Conformità ai sensi del Disciplinare Tecnico previsto dall'Allegato B della normativa suddetta, e dalla messa a disposizione di copia del Piano di sicurezza delle informazioni.

4. Trattamenti senza l'ausilio di strumenti elettronici

4.1. Nomina e istruzioni agli incaricati

In base a quanto stabilito dall'Art. 30 del Dlgs. n.196 del 30 giugno 2003, le operazioni di trattamento possono essere effettuate solo da Incaricati del trattamento che operano sotto la diretta autorità del Titolare del trattamento o, se designato, del Responsabile del trattamento di dati personali, attenendosi alle istruzioni impartite.

Il Responsabile del trattamento di dati personali deve predisporre per ogni archivio di cui è responsabile l'elenco degli Incaricati del trattamento autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante per l'accesso agli archivi.

In base a quanto stabilito dal punto 28 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), i documenti che contengono dati sensibili o giudiziari debbono essere custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Oltre alle indicazioni generali contenute nel presente capitolo, sono impartite precise istruzioni contenute in Disciplinare interno, allegato al presente documento.

4.2. Norme di sicurezza per gli incaricati del trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici

In base a quanto stabilito dal punto 27 e dal punto 28 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici vengono stabilite le seguenti regole che gli Incaricati del trattamento debbono osservare:

I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.

Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.

L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri.

Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.

I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.

Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.

Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.

Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;

Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.

E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.

Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.

L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.

E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.

Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

4.3. Copie degli atti e dei documenti cartacee

In base a quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), è fatto divieto a chiunque di:

Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Titolare, o suo delegato, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
Sottrarre, cancellare, distruggere senza l'autorizzazione del Titolare, o suo delegato, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
Consegnare a persone non autorizzate dal Titolare, o suo delegato, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

4.4. Controllo degli accessi agli atti cartacei

In base a quanto stabilito dal punto 29 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), l'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato dai soggetti Incaricati della custodia delle aree e dei locali ed è consentito, solo agli Incaricati del trattamento autorizzati dal Responsabile dello specifico trattamento.

Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, debbono essere identificate e registrate.

5. Diritti dell'interessato

5.1. Diritto di accesso ai dati personali

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

5.2. Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:
   a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
   b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
   c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
   d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
   e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
   f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;

g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981, n. 121.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f), provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

5.3. Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

5.4. Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:
a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

6. NORME FINALI

Tutti i documenti che le presenti linee guida individuano quali allegati al DPS dovranno essere redatti ed allegati a cura del Responsabile della sicurezza del rattamento dei dati e/o Amministratore di sistema nel corso del primo anno di vigenza. Successivamente i soggetti competenti ne dovranno curare gli aggiornamenti annuali ed allegarli al DPS.

CERTIFICATO DI PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che della copia del presente atto è stata disposta la pubblicazione all'Albo pretorio on line in data odierna per 15 giorni interi e consecutivi.

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

CERTIFICATO DI ESEGUITA PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che copia del presente atto è stata affissa all'Albo pretorio on line per 15 giorni interi e consecutivi dal _____ al _____

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

Il presente decreto è divenuto esecutivo il 30.12.2016

☐ Per decorrenza dei termini di cui all'art. 134 del D.Lgs. n. 267/2000.

X Perché dichiarata immediatamente eseguibile ai sensi dell'art. 134, co. 4, del D.Lgs. n. 267/2000.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

CERTIFICATO DI CONFORMITÀ ALL'ORIGINALE

La presente copia, composta di n. 39 pagine, è conforme all'originale conservato in atti e consta altresì di n. 1 allegato.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

COPIA DELL'ORIGINALE DI DECRETO DEL PRESIDENTE

n. 33 **del 28.12.2016**

Oggetto: Adempimenti in materia di privacy ai sensi del D.Lgs. 196/2003: nomina del Responsabile del Trattamento dei dati personali e del Responsabile del Trattamento in qualità di Amministratore di Sistema.

DOCUMENTO ISTRUTTORIO

Oggetto: Adempimenti in materia di privacy ai sensi del D.Lgs. 196/2003: nomina del Responsabile del Trattamento dei dati personali e del Responsabile del Trattamento in qualità di Amministratore di Sistema, ed approvazione del Documento programmatico della sicurezza.

IL DIRETTORE

RICHIAMATE le proprie determinazioni n. 16 del 23/02/2016 con la quale si sono definiti i primi indirizzi per l'implementazione del Sistema di gestione documentale informatizzata, e n. 113 del 9/8/2016 con la quale si è affidato il servizio di assistenza e supporto in materia di sicurezza informatica alla ditta Euristica srl;

PRESO ATTO che la ditta Euristica srl ha svolto il proprio servizio collaborando alla stesura della documentazione necessaria affiancando il personale per una adeguata informazione in materia di Privacy e Continuità Operativa e Disaster Recoveri (art. 50 bis del CAD) e indicando le procedure da seguire per adeguarsi alle prescrizioni della normativa vigente in materia;

ATTESO che il Titolare del Trattamento dei dati personali di cui all'art. 4, comma 2, lettera f) del D.Lgs. 196/2003 è Presidente in quanto rappresentante legale dell'Ente e che occorre individuare il Responsabile del Trattamento dei dati personali e il Responsabile del Trattamento in qualità di Amministratore di Sistema oltre che nominare gli incaricati al trattamento dei dati personali;

PRESO ATTO che, data l'organizzazione dell'Ente, il Responsabile del Trattamento dei dati personali debba coincidere con il Direttore, mentre il Responsabile del Trattamento in qualità di Amministratore di Sistema debba essere il responsabile del servizio informatico dell'Ente (entrambe le figure da nominarsi da parte del Presidente) e che sarà cura del Direttore nominare successivamente gli incaricati al trattamento dei dati personali;

VISTI gli allegati moduli da utilizzare per le nomine suddette;

TUTTO CIÒ PREMESSO;

VISTI:
- D.Lgs n.196/2003
- il D.Lgs n. 82/2005
- il DPR n. 445/2000
- il D.Lgs. n. 267/2000;
- il parere favorevole, riportato in calce, in ordine alla regolarità tecnica di cui all'art. 49, co. 1, del D.Lgs. n. 267/2000;

PROPONE

1. Di dare atto che il Titolare del Trattamento dei dati personali di cui all'art4, comma 2, lettera f) del D.Lgs. 196/2003 è il Presidente in quanto rappresentante legale dell'Ente;
2. Di nominare Responsabile del trattamento dei dati personali il Direttore, dott.ssa Elisabetta Cecchini, e Responsabile del Trattamento in qualità di Amministratore di Sistema il dott. Matteo Giantomassi che si occupa del servizio informatico dell'Ente;
3. Di dare atto che il Direttore procederà con la nomina degli altri dipendenti dell'Ente (compresi i lavoratori in somministrazione) quali "incaricati del trattamento dei dati personali";
4. Di approvare i seguenti allegati:
    - Schema atto di nomina di Responsabile del Trattamento dei dati personali
    - Schema atto di nomina di Responsabile del Trattamento in qualità di Amministratore di Sistema;
    - Schema lettera nomina dell'incaricato al trattamento dei dati personali;
    - Schema lettera nomina del responsabile del trattamento dei dati personali in out-sourcing (o incaricato esterno);
5. Di dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'articolo 134, co. 4, del D.Lgs. n. 267/2000.

Jesi, 28 dicembre 2016

La Direzione
F.to dott.ssa Elisabetta Cecchini

PARERE DI REGOLARITÀ TECNICA

Ai sensi dell'art. 49, co. 1, del D.Lgs. n. 267/2000, si esprime **parere favorevole** in ordine alla regolarità tecnica del presente atto.

Jesi, lì 28.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

IL PRESIDENTE

VISTO il documento istruttorio redatto dal Direttore in data 28.12.2016, sopra riportato a formare parte integrante e sostanziale del presente atto, contenente la proposta di nomina del Responsabile del Trattamento dei dati personale e del Responsabile del Trattamento in qualità di Amministratore di Sistema e l'approvazione del Documento programmatico della sicurezza dell'ATA in tema di privacy;

RITENUTO di condividere la proposta di cui sopra per le motivazioni addotte, che si intendono qui integralmente riportate;

DATO ATTO che il documento istruttorio di cui sopra riporta il prescritto parere di regolarità tecnica;

DECRETA

1. Di dare atto che il Titolare del Trattamento dei dati personali di cui all'art4, comma 2, lettera f) del D.Lgs. 196/2003 è il Presidente in quanto rappresentante legale dell'Ente;
2. Di nominare Responsabile del trattamento dei dati personali il Direttore, dott.ssa Elisabetta Cecchini, e Responsabile del Trattamento in qualità di Amministratore di Sistema il dott. Matteo Giantomassi che si occupa del servizio informatico dell'Ente;
3. Di dare atto che il Direttore procederà con la nomina degli altri dipendenti dell'Ente (compresi i lavoratori in somministrazione) quali "incaricati del trattamento dei dati personali";
4. Di approvare i seguenti allegati:
    - Schema atto di nomina di Responsabile del Trattamento dei dati personali
    - Schema atto di nomina di Responsabile del Trattamento in qualità di Amministratore di Sistema;
    - Schema lettera nomina dell'incaricato al trattamento dei dati personali;
    - Schema lettera nomina del responsabile del trattamento dei dati personali in out-sourcing (o incaricato esterno);
5. Di dichiarare, riscontrata l'urgenza del caso, immediatamente eseguibile il presente Decreto, ai sensi dell'art. 134, co. 4 del D.Lgs. n. 267/2000.

Jesi, 28 dicembre 2016

Il Presidente
F.to dott.ssa Liana Serrani

Lettera di nomina del responsabile del trattamento dei dati personali

Al Responsabile del Trattamento di dati personali _____
_____

IL PRESIDENTE

In qualità di rappresentante pro tempore di Assemblea Territoriale d'Ambito ATO 2, Titolare del Trattamento dei Dati ai sensi del dlgs 196/03;

Ai sensi degli art. 29 e 30 del Testo Unico in materia di trattamento dei dati personali D. Lgs. 196/03;

Tenuto conto del ruolo funzionale svolto dalla S.V. nell'ambito di _____;

Considerato che, nell'ambito di tale ruolo, la S.V. sovrintende, con autonomia operativa, alle procedure del trattamento dei dati e garantisce in modo idoneo, per capacità, esperienza ed affidabilità, il pieno rispetto e l'applicazione delle norme previste in materia di trattamento dei dati personali e di individuazione e attuazione delle misure di sicurezza;

NOMINA la S.V.
RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI IN AMBITO DI

_____
_____
_____

In particolare, nel rispetto della normativa indicata nelle premesse, alla S.V. vengono affidate le seguenti responsabilità e compiti :

1. Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
2. Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
3. Redigere ed aggiornare ad ogni variazione l'elenco degli uffici in cui vengono trattati i dati.
4. Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
5. Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
6. Redigere e di aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati.
7. Nominare per ciascun ufficio in cui viene effettuato il trattamento dei dati, un incaricato con il compito di controllare i sistemi, le apparecchiature, e se previsti, i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
8. Definire e verificare periodicamente le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.

9. Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
10. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati della gestione e della manutenzione degli strumenti elettronici.
11. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati della custodia delle copie delle credenziali qualora vi sia più di un incaricato del trattamento.
12. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati delle copie di sicurezza delle banche dati.
13. Custodire e conservare i supporti utilizzati per le copie dei dati.

In funzione dell'incarico conferito, sarà inoltre cura della S.V.:

1. Nominare gli Incaricati del trattamento dei dati personali (interni ed esterni) limitatamente ai Trattamenti di cui sono responsabili.
2. Sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).
3. Dare le istruzioni adeguate agli Incaricati del trattamento effettuato con strumenti elettronici.
4. Dare le istruzioni adeguate agli Incaricati del trattamento effettuato senza l'ausilio di strumenti elettronici.
5. Verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli Incaricati del trattamento dei dati personali.

La S.V. provvederà a diffondere fra gli incaricati il documento programmatico per la sicurezza e contribuirà, sulla base della sua applicazione, alla revisione periodica del documento stesso.

IL PRESIDENTE
Titolare del Trattamento Dati (o suo delegato)

(Data e firma)
_____

IL RESPONSABILE
del Trattamento Dati per presa visione e accettazione

(Data e firma)
_____

Atto di nomina di Responsabile del Trattamento in qualità di Amministratore di Sistema
Provvedimento Generale del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e smi

Il sottoscritto _____ Presidente di Assemblea Territoriale d'Ambito ATO 2, domiciliato allo scopo in via _____, in qualità di Titolare del trattamento di dati personali operati nell'ambito dell'attività istituzionale dell'Ente, con il presente atto

Designa

il Sig. _____(nome, cognome e ruolo svolto se soggetto interno)

oppure

il Sig. _____ della Società (nome, cognome, partita Iva, sede se soggetto esterno)

(possono essere designati anche più Amministratori di Sistema, ciascuno con lettera separata)

Amministratore di Sistema

ai sensi e per gli effetti degli articoli da 31 a 36 del D.Lgs. 30 giugno 2003 n. 196, del Provvedimento Generale del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e s.m.i., nonché in osservanza del Disciplinare Tecnico in materia di misure minime di sicurezza di cui all'allegato B) del medesimo Codice.

L'Amministratore di Sistema viene designato quale figura professionale dedicata a _____

(inserire le mansioni assegnate in dettaglio, ad esempio citando la normativa, oppure il DPS, oppure un eventuale contratto formale tra l'Ente ed il soggetto designato)

Il Sig. _____ nella qualità di Amministratore di Sistema ha il potere e il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione del D.Lgs. 30 giugno 2003 n. 196, con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali.

La designazione del Sig. _____ avviene in ragione del possesso in capo a quest'ultimo/a dei requisiti di capacità tecniche, professionali e di condotta, che si riassumono brevemente in seguito:

(inserire le competenze tecniche ed i titoli di studio)

Specificatamente, l'Amministratore di Sistema sarà tenuto a:

1 - classificare analiticamente le banche dati ed impostare/organizzare un sistema complessivo di trattamento dei dati personali comuni e sensibili che riguardi tutte le operazioni richiamate dall'art. 4, comma 1, lett. a) nessuna esclusa, predisponendo e curando ogni relativa fase applicativa nel rispetto della normativa vigente in materia di protezione dei dati personali;
2 – individuare per iscritto il/i soggetto/i incaricato della custodia delle parole chiave per l'accesso al sistema informativo e vigilare sulla sua attività, se applicabile;

3 – individuare per iscritto gli altri soggetti, diversi dal/dagli incaricato/i della custodia delle parole chiave, che possono avere accesso ad informazioni che concernono le medesime, se applicabile;
4 – impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da **1** a **10** del Disciplinare Tecnico, allegato B) al D.Lgs. 19672003;
5 – impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da **12** a **14** del Disciplinare Tecnico, allegato B) del D.Lgs. 196/2003;
6 - adottare un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste; tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
7 - assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery), anche automatici nonché approntare adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS);
8 – impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedano le modalità di utilizzo dei sistemi di salvataggio dei dati con frequenza almeno settimanale;
9 – adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
10 - organizzare i flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware, la verifica di eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi quali accesso abusivo al sistema informatico o telematico (articolo 615 *ter*), frode informatica (articolo 640 *ter*), danneggiamento di informazioni, dati e programmi informatici (articoli 635 *bis* e *ter*), danneggiamento di sistemi informatici e telematici (articoli 635 *quater* e *quinques*);
11 – predisporre, anche in contraddittorio con il Titolare dei trattamenti, un piano di controlli periodici, da eseguirsi con cadenza almeno semestrale, atti a verificare l'efficacia delle misure di sicurezza adottate;
12 – coadiuvare, se richiesto, il Titolare del trattamento nella predisposizione e/o aggiornamento e/o integrazione del Documento Programmatico sulla Sicurezza (D.P.S.) previsto dal punto 19 del Disciplinare Tecnico, allegato B) del D.Lgs. 196/2003 nonché alla stesura del documento denominato "Disciplinare in Materia di Utilizzo di Strumenti Informatici".

E' compito dell'Amministratore di Sistema monitorare costantemente lo stato di sicurezza di tutti i processi di elaborazione dati di cui sopra, mantenendo aggiornati tutti i supporti hardware e software e, se del caso, comunicando al Titolare tutte le attività da porre in essere al fine di garantire un adeguato livello di sicurezza in proporzione alla tipologia e quantità dei dati personali trattati.

L'operato dell'Amministratore di Sistema sarà oggetto, con cadenza annuale, ad una attività di verifica da parte del Titolare del trattamento, tesa a controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti. L' Amministratore di Sistema avrà cura di inviare ogni anno, entro il 15 Dicembre, una Relazione sullo Stato del Sistema, intestata al Titolare del Trattamento dei Dati, con la quale riepiloga lo stato delle attività eseguite e le eventuali proposte di migliorie suggerite.

Jesi, lì

Il Titolare del trattamento dati …….. L'Amministratore di Sistema

_____ _____

Lettera di nomina dell'incaricato al trattamento dei dati personali

All'Incaricato del Trattamento di dati personali _____
_____

IL Presidente (ovvero se delegato il RESPONSABILE TRATTAMENTO DATI)

In qualità di rappresentante pro tempore di Assemblea Territoriale d'Ambito ATO 2 (ovvero in qualità di Responsabile del Trattamento dei Dati) ai sensi del dlgs 196/03;

Ai sensi degli art. 29 e 30 del Testo Unico in materia di trattamento dei dati personali D. Lgs. 196/03;

Tenuto conto del ruolo funzionale svolto dalla S.V. nell'ambito di _____;

Considerato che, nell'ambito di tale ruolo, la S.V. esegue attività operative di trattamento dei dati;

NOMINA la S.V.
INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI IN AMBITO DI

_____
_____
_____

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati che contengono i predetti dati personali.
- Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.
- L'Incaricato del trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.
- Ogni Incaricato del trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
- Gli Incaricati del trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
- La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- L'Incaricato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.
- In caso di trattamento di dati sensibili e di dati giudiziari la componente riservata delle credenziali di autenticazione (parola chiave) deve essere modificata almeno ogni tre mesi.
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici , composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.
- Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

IL PRESIDENTE
Titolare del Trattamento Dati (o suo delegato)

(Data e firma)
_____

L'INCARICATO
del Trattamento Dati per visione e accettazione

(Data e firma)
_____

Lettera di nomina del responsabile del trattamento dei dati personali in out-sourcing (o incaricato esterno)

Al Responsabile del Trattamento di dati personali in out-sourcing _____
_____

IL PRESIDENTE (ovvero, se delegato, il Responsabile del Trattamento Dati)

In qualità di rappresentante pro tempore di Assemblea Territoriale d'Ambito ATO 2, Titolare del Trattamento dei Dati ai sensi del dlgs 196/03 (ovvero in qualità di Responsabile del Trattamento Dati);

Ai sensi degli art. 29 e 30 del Testo Unico in materia di trattamento dei dati personali D. Lgs. 196/03;

Tenuto conto del ruolo funzionale svolto dalla S.V. nell'ambito di _____;

Considerato che, nell'ambito di tale ruolo, la S.V. sovrintende, con autonomia operativa, alle procedure del trattamento dei dati e garantisce in modo idoneo, per capacità, esperienza ed affidabilità, il pieno rispetto e l'applicazione delle norme previste in materia di trattamento dei dati personali e di individuazione e attuazione delle misure di sicurezza;

NOMINA la S.V.
RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI IN OUT-SOURCING (O INCARICATO ESTERNO)
IN AMBITO DI

_____
_____
_____

In particolare, nel rispetto della normativa indicata nelle premesse, alla S.V. vengono affidate le seguenti responsabilità:

1. Garantire che tutte le misure di sicurezza dei dati riguardanti i dati personali siano applicate.
2. Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
3. Redigere ed aggiornare ad ogni variazione l'elenco degli uffici in cui vengono trattati i dati.
4. Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
5. Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
6. Redigere e di aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati.
7. Nominare per ciascun ufficio in cui viene effettuato il trattamento dei dati, un incaricato con il compito di controllare i sistemi, le apparecchiature, e se previsti, i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
8. Definire e verificare periodicamente le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.
9. Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
10. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati della gestione e della manutenzione degli strumenti elettronici.
11. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati della custodia delle copie delle credenziali qualora vi sia più di un incaricato del trattamento.
12. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati delle copie di sicurezza delle banche dati.
13. Custodire e conservare i supporti utilizzati per le copie dei dati.

In funzione della responsabilità conferita, sarà inoltre cura della S.V.:

1. Nominare gli Incaricati del trattamento dei dati personali limitatamente ai Trattamenti di cui sono responsabili.
2. Sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).
3. Dare le istruzioni adeguate agli Incaricati del trattamento effettuato con strumenti elettronici.
4. Dare le istruzioni adeguate agli Incaricati del trattamento effettuato senza l'ausilio di strumenti elettronici.
5. Verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli Incaricati del trattamento dei dati personali, trasmettendo Dichiarazione di Conformità ed ogni altra documentazione di Sicurezza delle Informazioni idonea a garantire tali condizioni
6. Verificare periodicamente, e comunque almeno annualmente, la sussistenza delle condizioni per la conservazione dei profili dei propri Amministratori di Sistema, trasmettendo documentazione idonea a garantire tali condizioni
7. Individuare le banche dati oggetto del trattamento
    a. Redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.
    b. Classificare in relazione alle informazioni in essa contenute indicando se si tratta di Dati Personali Comuni, Dati Personali Sensibili, Dati Personali Giudiziari
    c. Indicare le finalità e le modalità di trattamento
8. Mantenere un inventario delle sedi e locali ove vengono trattati i dati
    a. Redigere e di aggiornare ad ogni variazione l'elenco delle sedi e i relativi uffici, in cui viene effettuato il trattamento dei dati.
    b. Per ogni ufficio andranno indicati le dotazioni e i dispositivi atti ad evitare l'accesso non autorizzato ai dati o alla loro perdita.
9. Mantenere un Inventario dei sistemi elettronici
    a. Redigere e di aggiornare ad ogni variazione l'elenco dei sistemi elettronici o di elaborazione con cui viene effettuato il trattamento dei dati.

La S.V. provvederà a diffondere fra gli incaricati il documento programmatico per la sicurezza e contribuirà, sulla base della sua applicazione, alla revisione periodica del documento stesso.

IL PRESIDENTE
Titolare del Trattamento Dati (o suo delegato)

(Data e firma)
_____

IL RESPONSABILE
del Trattamento Dati in Out-Sourcing (o incaricato esterno) per visione e accettazione

(Data e firma)
_____

CERTIFICATO DI PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che della copia del presente atto è stata disposta la pubblicazione all'Albo pretorio on line in data odierna per 15 giorni interi e consecutivi.

Jesi, lì 29.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

CERTIFICATO DI ESEGUITA PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che copia del presente atto è stata affissa all'Albo pretorio on line per 15 giorni interi e consecutivi dal _____ al _____

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

Il presente decreto è divenuto esecutivo il 28.12.2016

☐ Per decorrenza dei termini di cui all'art. 134 del D.Lgs. n. 267/2000.

X Perché dichiarata immediatamente eseguibile ai sensi dell'art. 134, co. 4, del D.Lgs. n. 267/2000.

Jesi, lì 28.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

COPIA DELL'ORIGINALE DI DECRETO DEL PRESIDENTE

n. 38 **del 30.12.2016**

Oggetto: Adempimenti in materia di privacy ai sensi del D.Lgs. 196/2003: nomina dell' Incaricato della custodia delle copie delle credenziali e Incaricato delle copie di sicurezza delle banche dati.

DOCUMENTO ISTRUTTORIO

Oggetto: Adempimenti in materia di privacy ai sensi del D.Lgs. 196/2003: nomina dell' Incaricato della custodia delle copie delle credenziali e Incaricato delle copie di sicurezza delle banche dati.

IL DIRETTORE

RICHIAMATE le determinazioni n. 16 del 23/02/2016 con la quale si sono definiti i primi indirizzi per l'implementazione del Sistema di gestione documentale informatizzata, e n. 113 del 9/8/2016 con la quale si è affidato il servizio di assistenza e supporto in materia di sicurezza informatica alla ditta Euristica srl;

PRESO ATTO che la ditta Euristica srl ha svolto il proprio servizio collaborando alla stesura della documentazione necessaria affiancando il personale per una adeguata formazione in materia di Privacy e Continuità Operativa e Disaster Recoveri (art. 50 bis del CAD) e indicando le procedure da seguire per adeguarsi alle prescrizioni della normativa vigente in materia;

RICHIAMATI i Decreti del Presidente n. 33 del 28/12/2016 con il quale sono stati individuati il Titolare ed il Responsabile del Trattamento dei dati personali, il Responsabile del Trattamento in qualità di Amministratore di Sistema e n. 37 con il quale è stato approvato il Documento programmatico della sicurezza (DPS);

DATO ATTO che il DPS detta delle linee guida che l'ATA dovrà seguire per implementare un idoneo sistema di sicurezza informatica per il trattamento dei dati e dei documenti amministrativi e loro conservazione;

PRESO ATTO che nell'Area amministrativa dell'ente è presente il Servizio informatico il cui Responsabile coincide con l'Amministratore di Sistema;

ATTESO che si rende necessario provvedere alla individuazione dell'Incaricato della custodia delle copie delle credenziali e dell' Incaricato delle copie di sicurezza delle banche dati;

RITENUTO che tali figure possano essere ricoperte dal Responsabile del servizio informatico dell'Ente, nonché Amministratore di Sistema, dott. Matteo Giantomassi;

TUTTO CIÒ PREMESSO;

VISTI:
- D.Lgs n.196/2003
- il D.Lgs n. 82/2005
- il DPR n. 445/2000
- il D.Lgs. n. 267/2000;
- il parere favorevole, riportato in calce, in ordine alla regolarità tecnica di cui all'art. 49, co. 1, del D.Lgs. n. 267/2000;

PROPONE

1. Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2. Di dare atto che nell'Area amministrativa dell'ente è presente il Servizio informatico il cui Responsabile coincide con l'Amministratore di Sistema dott. Matteo Giantomassi.
3. Di nominare conseguentemente il dott. Matteo Giantomassi:
   - Incaricato della custodia delle copie delle credenziali di cui al paragrafo 2.3.1. del DPS;
   - Incaricato delle copie di sicurezza delle banche dati di cui al paragrafo 2.3.2. del DPS;
4. Di dare atto che gli Incaricati della gestione e della manutenzione degli strumenti elettronici contenenti dati saranno invece ricercati all'esterno dell'Ente ma saranno coordinati dal Responsabile del Servizio informatico;
5. Di dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'articolo 134, co. 4, del D.Lgs. n. 267/2000.

Jesi, 30 dicembre 2016

La Direzione
F.to dott.ssa Elisabetta Cecchini

PARERE DI REGOLARITÀ TECNICA

Ai sensi dell'art. 49, co. 1, del D.Lgs. n. 267/2000, si esprime **parere favorevole** in ordine alla regolarità tecnica del presente atto.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

IL PRESIDENTE

VISTO il documento istruttorio redatto dal Direttore in data 30.12.2016, sopra riportato a formare parte integrante e sostanziale del presente atto, contenente la proposta di nomina del Responsabile del Trattamento dei dati personale e del Responsabile del Trattamento in qualità di Amministratore di Sistema e l'approvazione del Documento programmatico della sicurezza dell'ATA in tema di privacy;

RITENUTO di condividere la proposta di cui sopra per le motivazioni addotte, che si intendono qui integralmente riportate;

DATO ATTO che il documento istruttorio di cui sopra riporta il prescritto parere di regolarità tecnica;

DECRETA

1. Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2. Di dare atto che nell'Area amministrativa dell'ente è presente il Servizio informatico il cui Responsabile coincide con l'Amministratore di Sistema dott. Matteo Giantomassi.
3. Di nominare conseguentemente il dott. Matteo Giantomassi:
   - Incaricato della custodia delle copie delle credenziali di cui al paragrafo 2.3.1. del DPS;
   - Incaricato delle copie di sicurezza delle banche dati di cui al paragrafo 2.3.2. del DPS;
4. Di dare atto che gli Incaricati della gestione e della manutenzione degli strumenti elettronici contenenti dati saranno invece ricercati all'esterno dell'Ente ma saranno coordinati dal Responsabile del Servizio informatico;
5. Di dichiarare, riscontrata l'urgenza del caso, immediatamente eseguibile il presente Decreto, ai sensi dell'art. 134, co. 4 del D.Lgs. n. 267/2000.

Jesi, 30 dicembre 2016

Il Presidente
F.to dott.ssa Liana Serrani

CERTIFICATO DI PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che della copia del presente atto è stata disposta la pubblicazione all'Albo pretorio on line in data odierna per 15 giorni interi e consecutivi.

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

CERTIFICATO DI ESEGUITA PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che copia del presente atto è stata affissa all'Albo pretorio on line per 15 giorni interi e consecutivi dal _____ al _____

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

Il presente decreto è divenuto esecutivo il 30.12.2016

☐ Per decorrenza dei termini di cui all'art. 134 del D.Lgs. n. 267/2000.

X Perché dichiarata immediatamente eseguibile ai sensi dell'art. 134, co. 4, del D.Lgs. n. 267/2000.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

CERTIFICATO DI CONFORMITÀ ALL'ORIGINALE

La presente copia, composta di n. 5 pagine, è conforme all'originale conservato in atti.

Jesi, lì 30.12.2016

Il Direttore
dott.ssa Elisabetta Cecchini

PARERE DI REGOLARITÀ TECNICA

Ai sensi dell'art. 49, co. 1, del D.Lgs. n. 267/2000, si esprime **parere favorevole** in ordine alla regolarità tecnica del presente atto.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

IL PRESIDENTE

VISTO il documento istruttorio redatto dal Direttore in data 30.12.2016, sopra riportato a formare parte integrante e sostanziale del presente atto, contenente la proposta di approvazione del Manuale di gestione documentale e suoi allegati;

RITENUTO di condividere la proposta di cui sopra per le motivazioni addotte, che si intendono qui integralmente riportate;

VISTO che il documento istruttorio di cui sopra riporta il prescritto parere di regolarità tecnica;

DECRETA

1) Di stabilire che le premesse formano parte integrante e sostanziale del presente atto;
2) Di approvare il Manuale di gestione documentale allegato al presente atto per farne parte integrante e sostanziale, corredato dai seguenti documenti:
   - Allegato 1 Definizioni, norme e regole di riferimento
   - Allegato 2 Area organizzativa omogenea, atto di istituzione del servizio gestione informatica e documentale e atto di nomina del RGD
   - Allegato 3 Modello di carta intestata
   - Allegato 4 Contratto Gestore Posta Elettronica Certificata
   - Allegato 5 Elenco titolari di firma digitale, degli indirizzi di posta elettronica certificata e di posta elettronica dell'Ente
   - Allegato 6 Timbri ed etichette in uso
   - Allegato 7 Modello di Registro di emergenza
   - Allegato 8 Titolario di classificazione
   - Allegato 9 Incaricati al trattamento dei documenti amministrativi
   - Allegato 10 Linee guida per la fascicolazione
   - Allegato 11 Modello di Camicia di fascicolo cartaceo
   - Allegato 12 Convenzione Regione Marche e disciplinare tecnico per il servizio di conservazione sostitutiva
   - Allegato 13 Manuale dei processi per la conservazione digitale
   - Allegato 14 Piano di conservazione
   - Allegato 15 Piano per la sicurezza informatica
3) Di dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'articolo 134, co. 4, del D.Lgs. n. 267/2000.

Il Presidente
F.to dott.ssa Liana Serrani

CERTIFICATO DI PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che della copia del presente atto è stata disposta la pubblicazione all'Albo pretorio on line in data odierna per 15 giorni interi e consecutivi.

Jesi, lì 20.01.2017

Il Direttore
F.to dott.ssa Elisabetta Cecchini

CERTIFICATO DI ESEGUITA PUBBLICAZIONE

Ai sensi dell'art. 124 del D.Lgs. n. 267/2000, si certifica che copia del presente atto è stata affissa all'Albo pretorio on line per 15 giorni interi e consecutivi dal _____ al _____

Jesi, lì

Il Direttore
dott.ssa Elisabetta Cecchini

Il presente decreto è divenuto esecutivo il 30.12.2016

☐ Per decorrenza dei termini di cui all'art. 134 del D.Lgs. n. 267/2000.

X Perché dichiarata immediatamente eseguibile ai sensi dell'art. 134, co. 4, del D.Lgs. n. 267/2000.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini

CERTIFICATO DI CONFORMITÀ ALL'ORIGINALE

La presente copia, composta di n. 422 pagine, è conforme all'originale conservato in atti e consta altresì di n. 16 allegati.

Jesi, lì 30.12.2016

Il Direttore
F.to dott.ssa Elisabetta Cecchini