PA Digitale s.p.a.
Via Leonardo Da Vinci, 13
26854 PIEVE FISSIRAGA (LO)
Tel. 0371-5935.11 Fax 0371-5935.440
Registro Imprese di Lodi,
C.F e P.IVA n° 06628860964
C.C.I.A.A. Di Lodi R.E.A. N° 1464686
Capitale Sociale 1.100.000,00 Euro I.V.

ISO 9001:2008

PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE

padigitale.it E.mail: amministrazione@padigitale.it
PEC: protocollo.pec.padigitalespa@legalmail.it

CDN
CONSERVAZIONE DIGITALE A NORMA

Manuale

del sistema di conservazione

digitale dei documenti informatici

Sede Legale: Via Leonardo Da Vinci, 13
26854 Pieve Fissiraga (LODI)
Numero Iscrizione R.I. di Lodi, Codice fiscale
e Part. IVA: 06628860964
C.C.I.A.A. di Lodi R.E.A. 1464686
Capitale Sociale 1.100.000 € I.V.

Manuale del sistema di Conservazione

EMISSIONE DEL DOCUMENTO:

Azione	Data	Nominativo	Funzione
Redazione	6 ottobre 2014	Simone Pezzini	Responsabile della funzione archivistica di conservazione
Verifica	6 ottobre 2014	Simone Pezzini	Responsabile della funzione archivistica di conservazione
Approvazione	6 ottobre 2014	Fabrizio Toninelli	Responsabile del Servizio di Conservazione

LISTA DI DISTRIBUZIONE INTERNA:

Nominativo	Ente di appartenenza (Produttore/Conservatore)	Riferimenti
Fabrizio Toninelli	Conservatore	Responsabile del servizio di conservazione
Simone Pezzini	Conservatore	Responsabile della funzione archivistica di conservazione
Roberto Ghidini	Conservatore	Responsabile della sicurezza dei sistemi per la conservazione, Responsabile dei sistemi informativi per la conservazione
Nicolò Formenti	Conservatore	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
Roberto Lavesi	Conservatore	Responsabile del trattamento dei dati
Referente Cliente per il servizio di conservazione	Produttore	Cliente

Manuale del sistema di Conservazione

Questa pagina è lasciata intenzionalmente bianca

Manuale del sistema di Conservazione

Sommario

Manuale del sistema di Conservazione

Manuale del sistema di Conservazione

Manuale del sistema di Conservazione

1. Allegati

1. Documenti rilevanti ai fini delle disposizioni tributarie: Elenco tipi documento
2. Specifiche pacchetto di versamento, descrittore evidenze e pacchetto di invio file
3. Specifiche rapporto di versamento
4. Specifiche pacchetti per funzioni ausiliarie (ad esempio invio dei documenti, richieste di annullamento, richieste di documenti, richieste dei rapporti di versamento, ecc.)
5. Specifiche descrittore XML per file EML

Manuale del sistema di Conservazione

2. Versioni del documento

Versione/Release n°:	1.00	**Data Versione/Release:**	03.04.2013
Descrizione modifiche:	rilascio prima versione		
Motivazioni:	==		

Versione/Release n°:	1.01	**Data Versione/Release:**	08.04.2013
Descrizione modifiche:	Aggiornamento dei riferimenti normativi		
Motivazioni:	**Adeguamento**		

Versione/Release n°:	1.02	**Data Versione/Release:**	24.06.2013
Descrizione modifiche:	Aggiornamento del capitolo 5 – Riferimenti tecnici		
Motivazioni:	**Emanazione del D.P.C.M. del 22.03.2013**		

Versione/Release n°:	1.03	**Data Versione/Release:**	08.04.2014
Descrizione modifiche:	Aggiornamento nuovi riferimenti normativi, tecnici, standard e a documenti di prassi Aggiornamento Aggiornamento capitolo 5 Aggiornamento capitolo 11 Aggiornamento capitolo 17.2		
Motivazioni:	**Recepimento nuovi riferimenti normativi, tecnici, standard e a documenti di prassi:** - UNI/TS 11465/1 - Sicurezza nella conservazione dei dati – Parte 1: Requisiti per la realizzazione e la Gestione - UNI/TS 11465/3 - Sicurezza nella conservazione dei dati – Completamento italiano - ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione (adeguamento alla vers. 2012) - D.P.C.M. del 03/12/2013 – "Regole tecniche in materia di sistema di conservazione" - D.P.C.M. del 03/12/2013 – "Regole tecniche per il protocollo informatico" - DECRETO 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche - Circolare MEF del 31 marzo 2014 n. 1/DF - circolare interpretativa del DECRETO 3 aprile 2013, n. 55		

Versione/Release n°:	2.00	**Data Versione/Release:**	01.07.2014
Descrizione modifiche:	Aggiornamento e coordinamento generale del testo ai nuovi riferimenti normativi Aggiornato il capitolo 4 - Riferimenti normativi e di prassi Aggiornato il capitolo 8.1 - Responsabile del servizio di conservazione Aggiornato il capitolo 11 - Struttura organizzativa del sistema di conservazione Soppresso il capitolo 15.3 - Comunicazione alle Agenzie fiscali dell'impronta relativa ai documenti informatici rilevanti ai fini tributari Aggiornamento del capitolo		
Motivazioni:	Coordinamento del testo a seguito della emanazione: - del DM- MEF del 17.06.2014 in sostituzione del DM 23.01.2004; - della Circolare Agenzia delle Entrate del 24 giugno 2014 n. 18/E;		

Versione/Release n°:	2.01	**Data Versione/Release:**	06.10.2014
Descrizione modifiche:	Inserito nel frontespizio informazioni su EMISSIONE DEL DOCUMENTO e LISTA DI DISTRIBUZIONE INTERNA Revisione del documento con eliminazione riferimenti contrattuali Aggiornato il capitolo 4 - Riferimenti normativi e di prassi Aggiornato il capitolo 5 - Riferimenti tecnici Aggiornato il capitolo 8 - Revisione del testo Aggiornato il capitolo 9.3 - Aggiunto paragrafo 9.3.4 su gestione change management e relative verifiche Aggiornato il capitolo 11 – Nella tabella "Descrizione delle fasi del processo di conservazione" aggiunte le seguenti fasi: Fase 1 – Attivazione del servizio, Fase 15 – Chiusura del servizio		
Motivazioni:	Revisione per requisiti accreditamento AgID.		

3. Scopo del documento

Il presente documento è il **Manuale del sistema di conservazione** (di seguito per brevità chiamato anche "***Manuale***") e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione dei processi, in particolare le modalità di versamento, archiviazione e distribuzione, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione digitale di documenti informatici.

Con il presente *Manuale* si fa riferimento alla versione corrente del presente documento.

In particolare, nel presente *Manuale* sono riportati:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
c) la descrizione delle tipologie dei documenti informatici sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento e della descrizione dei controlli effettuati su ciascuno specifico formato adottato;
e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
i) la descrizione delle procedure per la produzione di duplicati o copie;
j) i tempi entro i quali le diverse tipologie di documenti informatici devono essere oggetto di scarto/cancellazione;
k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
l) le normative in vigore nei luoghi dove sono conservati i documenti.

Il *Manuale* recepisce le disposizioni di cui al D.Lgs. 7 marzo 2005, n. 82, e s.m.i. (Codice dell'amministrazione digitale), di seguito per brevità chiamato anche "Codice" o "CAD", oltre alle indicazioni riportate nei provvedimenti di legge o di prassi richiamati nel capitolo "***Riferimenti normativi e di prassi***" nonché i provvedimenti di natura tecnica richiamati nel capitolo "***Riferimenti tecnici***".

3.1 Versione del Manuale

Questo documento è pubblicato sul sito Web di descrizione del Servizio (http://www.cdan.it/) nella apposita area riservata ai Clienti ed è quindi consultabile telematicamente. Il documento è pubblicato in formato PDF sottoscritto con firma digitale del Responsabile del servizio di Conservazione in modo tale da assicurarne l'integrità e l'autenticità. Vengono mantenute in linea tutte le versioni e, per ogni versione, è riportata la data di entrata in vigore.

Come versione corrente del Manuale si intenderà esclusivamente la versione in formato elettronico disponibile sul sito Web di PA Digitale. Il codice interno di questo documento è riportato sul frontespizio.

Il Cliente è tenuto a leggere con la massima attenzione il presente Manuale predisposto da PA Digitale.

Il Cliente in qualità di unico Responsabile della conservazione approva e fa propri i contenuti del presente Manuale di conservazione.

Per una più agevole e scorrevole lettura del presente Manuale si raccomanda la consultazione del capitolo dedicato alle definizioni, abbreviazioni e termini tecnici.

4. Riferimenti normativi e di prassi

- **Codice civile** - R.D. del 16 marzo 1942 n. 262;
- **Legge del 7 agosto 1990, n.241 e s.m.i.** – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **DPR 28 dicembre 2000, n. 445**, e successive modificazioni - "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" o "TUDA";
- **DPR 11 febbraio 2005, n. 68** - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- **Decreto legislativo 30 giugno 2003, n. 196**, e successive modificazioni, recante "Codice in materia di protezione dei dati personali";
- **Decreto legislativo 22 gennaio 2004, n. 42**, e successive modificazioni, recante "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137";
- **Decreto legislativo 7 marzo 2005, n. 82**, e successive modificazioni - "Codice dell'amministrazione digitale" o "CAD";
- **Circolare n. 5/d Agenzia delle dogane del 25 gennaio 2005** - D.M. 23/1/2004 recante "modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto".
- **Circolare dell'Agenzia delle Entrate n. 45/E del 19 ottobre 2005** - Decreto legislativo 20 febbraio 2004, n. 52; attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA;
- **Circolare dell'Agenzia delle Entrate n. 36/E del 6 dicembre 2006** - Decreto ministeriale 23 gennaio 2004; Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto;
- **Risoluzione Agenzia delle entrate n. 298 del 18 ottobre 2007** - Istanza di interpello, articolo 11 legge 27 luglio 2002, n. 212, - Conservazione su supporti informatici delle copie delle dichiarazioni da parte dei CAF - Adempimenti correlati e termine per l'invio dell'impronta dell'archivio informatico;
- **Risoluzione n. 349 Agenzia delle entrate del 28 novembre 2007** - IVA - biglietto di trasporto elettronico - articolo 1 del decreto ministeriale 30 giugno 1992 Istanza di interpello -ART.11, legge 27 luglio 2000, n. 212;
- **Risoluzione n. 67/E Agenzia delle entrate del 28 febbraio 2008** - Articoli 21 e 39 del d.P.R. 26 ottobre 1972, n.633, D.M. 23 gennaio 2004, conservazione sostitutiva dei documenti rilevanti ai fini delle disposizioni tributarie- obblighi del vettore o dello spedizioniere. Messa a disposizione delle fatture tramite strumenti elettronici;
- **Risoluzione n.85/E Agenzia delle entrate del 11 marzo 2008** - Conservazione sostitutiva delle distinte meccanografiche di fatturazione;
- **DM 09 luglio 2008** - Modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio;
- **Risoluzione n. 354/E Agenzia delle entrate del 8 agosto 2008** - Interpello – ALFA Ass.ne prof.le dott. comm. e avv. – Articolo 3, comma 9-bis, del D.P.R. n. 322 del 1998 – Incaricati della trasmissione delle dichiarazioni – Conservazione delle copie delle dichiarazioni – Obbligo di sottoscrizione da parte del contribuente delle copie conservate dall'incaricato su supporti informatici;
- **Circolare 20/2008 - Ministero del lavoro, della salute e delle politiche sociali del 21/08/2008** - Libro Unico del Lavoro e attività ispettiva – articoli 39 e 40 del decreto legge n. 112 del 2008: prime istruzioni operative al personale ispettivo;
- **Regolamento ISVAP n. 27 del 14 ottobre 2008** -Tenuta dei registri assicurativi;
- **Provvedimento Agenzia delle entrate del 25 ottobre 2010** - Provvedimento attuativo della comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'articolo 5 del decreto 23 gennaio 2004;
- **Decreto legge del 06 dicembre 11 , n. 201** - Estratto Art.40, comma 4 - Libro Unico del Lavoro;
- **Decreto legge 24 gennaio 2012, n. 1** - Estratto – Dematerializzazione Contrassegni Assicurativi;
- **Circolare n. 5/E Agenzia delle entrate del 29 febbraio 2012** - Quesiti riguardanti la comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'articolo 5 del decreto 23 gennaio 2004 e del provvedimento del Direttore dell'Agenzia delle Entrate del 25 ottobre 2010;
- **Circolare MEF del 31 marzo 2014 n. 1/DF** – circolare interpretativa del DECRETO 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1,

commi da 209 a 213, della legge 24 dicembre 2007, n. 244.

- **Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto – articolo 21, comma 5, del decreto legislativo n. 82/2005. (Ministero dell'economia e delle finanze) – in vigore dal 27.06.2014;
- **Circolare Agenzia delle Entrate del 24 giugno 2014 n. 18/E** - OGGETTO: IVA. Ulteriori istruzioni in tema di fatturazione.

5. Riferimenti tecnici

- **D.P.C.M. del 31 ottobre 2000** - Regole tecniche per il protocollo informatico;
- **Decreto 02 novembre 2005 – Ministero per l'innovazione e le tecnologie** - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata;
- **D.P.C.M. 22 Febbraio 2013** - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali;
- **DECRETO 3 aprile 2013, n. 55 -** Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.
- **D.P.C.M. 03 Dicembre 2013** - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
- **D.P.C.M. 03 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 del 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.

6. Standard e specifiche tecniche

Di seguito si riporta l'elenco degli standard a cui PA Digitale ha fatto riferimento per il sistema di conservazione.

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
- **ISO/IEC 27001:2005,** Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System).
- **ETSI TS 101 533-1** 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.
- **UNI/TS 11465/1 -** Sicurezza nella conservazione dei dati – Parte 1: Requisiti per la realizzazione e la Gestione
- **UNI/TS 11465/3 -** Sicurezza nella conservazione dei dati – Completamento italiano
- **ETSI TR 101 533-2** 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** S-Recupero degli Oggetti digitali.
- **ISO 15836:2003** Information and documentation - The Dublin Core metadata element set, Sistema di metadati del Dublin Core.
- **ISO 19005:2005** Definizione standard PDF/A
- **MOREQ** Requisiti modello per la gestione dei record elettronici.
- **ITU-T X.509** Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. Definisce lo standard per i certificate utilizzati nella firma digitale.
- **ETSI TS 101 733 CAdES specification** – CMS Advanced Electronic Signature. Definizione dello standard per i file P7M.
- **RFC3161** Standard per la marca temporale.
- **FIPS 180-3** Secure Hash Standard. Contiene le specifiche per il calcolo dei valori di hash SHA256.

7. Definizioni, abbreviazioni e termini tecnici

7.1 Definizioni

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale, i termini e le espressioni sotto elencate avranno il significato descritto nelle definizioni in esso riportate. Qualora le definizioni adottate dalla normativa di riferimento non fossero riportate nell'elenco che segue, si rimanda ai testi in vigore per la loro consultazione.

I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.

Ai fini della fruizione del Servizio di conservazione digitale dei documenti informatici descritto nel presente *Manuale*, valgono ad ogni effetto le seguenti definizioni:

Accesso: operazione che consente a chi ne ha diritto di prendere visione dei documenti informatici conservati;

Accreditamento: riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza, ad un soggetto pubblico o privato che svolge attività di conservazione o di certificazione del processo di conservazione;

Agente di Alterazione: sono agenti di alterazione le macro, i codici eseguibili nascosti, le formule di foglio di lavoro nascoste o difficili da individuare, sequenze di caratteri nascoste all'interno dei dati le quali sono ignorate dall'applicazione originalmente prevista per la presentazione, che però possono essere riconosciute quando i dati vengano elaborati con altre applicazioni;

Aggregazione documentale informatica: raccolta 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: complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività;

Archivio informatico: archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico;

Area organizzativa omogenea: 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 D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;

Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico: dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico;

Autenticità: 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;

Base di dati: collezione di dati registrati e correlati tra loro;

Certificatore accreditato: soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dell'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza;

Ciclo di gestione: arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo;

Chiusura del pacchetto di archiviazione: operazione consistente nella sottoscrizione del pacchetto di archiviazione con firma digitale apposta da un Firmatario Delegato di PA Digitale e apposizione di una validazione temporale con marca temporale alla relativa impronta;

Classificazione: attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati;

Cliente: è il produttore, unico e legittimo titolare degli oggetti/dati/documenti depositati in conservazione;

Codice o CAD: decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni;

Codice eseguibile: insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici;

Conservatore accreditato: soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale o da un certificatore accreditato, il possesso dei requisiti del livello più elevato, in termini di qualità e di

sicurezza;

Conservazione: insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel Manuale di conservazione;

Contrassegno a stampa: contrassegno generato elettronicamente, apposto a stampa sulla copia analogica di un documento amministrativo informatico per verificarne provenienza e conformità all'originale;

Contratto: è il Contratto per l'affidamento del servizio di conservazione digitale di documenti informatici perfezionato tra PA Digitale ed il Cliente che regola gli aspetti generali dell'erogazione del Servizio di conservazione digitale dei documenti informatici del Cliente;

Coordinatore della Gestione Documentale: responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 e s.m.i. nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee;

Copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

Copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

Copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

Copia di sicurezza: copia di backup degli archivi del sistema di conservazione;

Descrittore evidenze: vedi pacchetto informativo;

Destinatario: identifica il soggetto/sistema al quale il documento informatico è indirizzato;

DIRT: documenti informatici rilevanti ai fini delle disposizioni tributarie;

Documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

Documento analogico originale: documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

Documento originale unico: è quel documento analogico il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta, anche presso terzi e che non soddisfa, dunque, alcuna delle condizioni elencate nella definizione di "Documento analogico originale";

Documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

Duplicato Informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso supporto o su supporti diversi, della medesima sequenza di valori binari del documento originario;

Duplicazione dei documenti informatici: produzione di duplicati informatici;

Esibizione: operazione che consente di visualizzare un documento conservato e di ottenerne copia;

Estratto per riassunto: documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici;

Evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;

Fascicolo informatico: raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo, nell'ambito della pubblica amministrazione. Per i soggetti privati è da considerarsi fascicolo informatico ogni aggregazione documentale, comunque formata, funzionale all'erogazione di uno specifico servizio o prestazione;

File di chiusura: insieme di metadati, su cui è apposta la firma digitale e marca temporale, in grado di fornire prova dell'integrità di un insieme di documenti informatici, ad esso associati, la cui conservazione decorre dal momento di apposizione della marca temporale;

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 titolare 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;

Fruibilità di un dato: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;

Firmatario delegato: Responsabile del servizio di conservazione o Persona formalmente delegata ad apporre la propria firma digitale sui File di Chiusura per conto di PA Digitale; questa persona può essere interna o esterna a PA Digitale, laddove è giuridicamente

possibile;

Formato: modalità di rappresentazione del documento informatico mediante codifica binaria; comunemente è identificato attraverso l'estensione del file e/o il tipo MIME;

Fornitore esterno: organizzazione che fornisce a PA Digitale servizi relativi al suo sistema di conservazione dei documenti;

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;

Funzionalità interoperative: le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;

Funzionalità minima: la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;

Funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una sequenza di bit (impronta) in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti;

Generazione automatica di documento informatico: formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni;

Identificativo univoco: sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione;

Immodificabilità: caratteristica che rende la rappresentazione del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso;

Impronta: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;

Insieme minimo di metadati del documento informatico: complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta;

Integrità: insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato;

Interoperabilità: capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi;

Leggibilità: insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti;

Log di sistema: registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati;

Manuale di gestione: strumento che descrive il sistema di gestione informatica dei documenti;

Memorizzazione: processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici;

Marca temporale: evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una *Time Stamping Authority*;

Metadati: insieme di dati associati a 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;

Normativa regolante la conservazione digitale di documenti informatici: si intende: il D.lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione Digitale "CAD") e i relativi decreti attuativi, le regole tecniche e aggiungendo, per il documento informatico a rilevanza tributaria, le disposizioni di cui al DMEF 17 giugno 2014 e s.m.i., il DPR 26 ottobre 1972 n. 633 e s.m.i., il DPR 29 settembre 1973 n. 600 e s.m.i., i provvedimenti interpretativi emessi dagli organi competenti;

Originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

Pacchetto di archiviazione: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e le modalità riportate nel *Manuale* di conservazione;

Pacchetto di distribuzione: pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta;

Pacchetto di invio documenti: pacchetto informativo utilizzato per inviare i documenti fisici al sistema di conservazione a seguito dell'avvenuta accettazione di un pacchetto di versamento;

Pacchetto di versamento: pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel *Manuale* di conservazione;

Pacchetto informativo: contenitore che racchiude uno o più oggetti da conservare (documenti informatici, documenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare;

Piano della sicurezza del sistema di conservazione: documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza;

Piano della sicurezza del sistema di gestione informatica dei documenti: documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza;

Piano di conservazione: strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;

Piano generale della sicurezza: documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza;

Presa in carico: accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal *Manuale* di conservazione;

Processo di conservazione: insieme delle attività finalizzate alla conservazione dei documenti informatici;

Processo/servizio di marcatura temporale: è il processo/servizio che associa in modo affidabile un'informazione e un particolare momento, al fine di stabilire prove attendibili che indicano il momento in cui l'informazione esisteva;

Produttore: persona fisica o giuridica responsabile del contenuto del pacchetto di versamento identificato, nel caso di pubblica amministrazione, nella figura del responsabile della gestione documentale;

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;

Rapporto di conferma: attestazione dell'avvenuta ricezione di un pacchetto di versamento in attesa della ricezione dei documenti in esso descritti;

Registrazione informatica: insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente;

Registro particolare: registro informatico specializzato per tipologia o per oggetto; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;

Registro di protocollo: registro informatico della corrispondenza 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;

Repertorio informatico: registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche che trattano il procedimento, ordinati secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica;

Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: dirigente o funzionario, comunque 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;

Responsabile della conservazione: è il Cliente, nella persona fisica dallo stesso formalmente incaricata quale responsabile dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici depositati in conservazione nell'ambito della fornitura del servizio fornito da PA Digitale;

Responsabile del Servizio di conservazione: è PA Digitale che opererà attraverso uno o più persone fisiche formalmente incaricate all'esecuzione dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici nell'ambito della fornitura del servizio di conservazione ai propri clienti;

Responsabile del trattamento dei dati: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

Responsabile della sicurezza: soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza;

Riferimento temporale: informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento;

Scarto: operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse culturale;

Servizio di conservazione dei documenti: è il Servizio di conservazione dei documenti informatici fornito da PA Digitale che risponde all'esigenza di avere i documenti informatici del Cliente conservati nel rispetto della normativa vigente; è il Servizio a cui sono affidati i documenti informatici del Cliente per essere conservati in modo elettronico per uno specifico periodo di tempo concordato con il Produttore;

Sistema di classificazione: strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata;

Sistema di conservazione: insieme di hardware, software, politiche, procedure, linee guida, regolamenti interni, infrastrutture fisiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti del Cliente almeno per il periodo di tempo concordato con il Produttore. Detto sistema tratta i documenti informatici in conservazione in pacchetti informativi che si distinguono in: pacchetti di versamento, pacchetti di archiviazione e pacchetti di distribuzione;

Sistema di gestione informatica dei documenti: nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.; per i privati è il sistema che consente la tenuta di un documento informatico;

Staticità: caratteristica che indica l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione;

Transazione informatica: particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati;

Testo unico: decreto del Presidente della Repubbli

ca 28 dicembre 2000, n. 445, e successive modificazioni;

Titolare del trattamento[1]**:** 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;

Ufficio utente: riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico;

Utente: persona, ente o 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;

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.

Versamento agli archivi di stato: operazione con cui il responsabile della conservazione di un'amministrazione statale effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali;

7.2 Abbreviazioni e termini tecnici

Agenzia per L'Italia Digitale (già DigitPA): Ente pubblico non economico, con competenza nel settore delle tecnologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione. L'Ente, che ha ereditato le funzioni di DigitPA che, a sua volta, ha ereditato le funzioni del CNIPA, opera secondo le direttive per l'attuazione delle politiche e sotto la vigilanza del Ministro per la pubblica amministrazione e l'innovazione, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale;

ASP - Application Service Provider: Fornitore di Servizi Applicativi;

CAD: Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni - "Codice dell'amministrazione digitale";

CA - Certificatore Accreditato: soggetto autorizzato dall'Agenzia per l'Italia Digitale che garantisce l'identità dei soggetti che utilizzano la firma digitale;

[1] Art. 4, lett. f), D.Lgs. 196/2003;

CC - Common Criteria: Criteri per la valutazione della sicurezza nei sistemi informatici, con riconoscimento internazionale in quanto evoluzione dei criteri europei (ITSEC), statunitensi (Federal Criteria), e canadesi (Canadian Criteria);

C.M. - Circolare Ministeriale;

CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione: creato con l'articolo 176 del DL 196/03, il CNIPA ha incorporato le strutture e le funzioni dell'AIPA e del Centro Tecnico della RUPA ed è stato quindi sostituito da DigitPA e quindi dall'AgID - Agenzia per l'Italia Digitale;

D.LGS. - Decreto Legislativo;

D.M. - Decreto Ministeriale;

DNS – Domain Name System: Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet: Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http://www.telecomitalia.it)/ in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3).

D.P.C.M.: Decreto del Presidente del Consiglio dei Ministri;

D.P.R.: Decreto Presidente della Repubblica;

DPS: Documento Programmatico per la Sicurezza;

ETSI: European Telecommunications Standards Institute;

Internet Data Center o IDC: il centro servizi che ospita e gestisce l'insieme delle risorse hardware, il software di base, l'applicativo necessario a consentire l'utilizzo dei prodotti, dei software e delle procedure informatiche di proprietà del PA Digitale, nonché i documenti informatici del Cliente;

HSM - Hardware Security Module: dispositivi hardware dedicati per la sicurezza crittografica e la gestione delle chiavi in grado di garantire un elevato livello di protezione;

HTTP (Hypertext Transfer Protocol): Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web;

HTTPS (Secure Hypertext Transfer Protocol): Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifratura dei dati trasmessi durante la consultazione di siti e pagine Internet. Corrisponde ad un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL;

ICT - Information and Communication Technology: Tecnologia dell'Informazione e delle Telecomunicazioni. Il dipartimento che gestisce i sistemi informatici e telematici;

INTERNET: Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere informazioni da luoghi diversi. Lo sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW);

ISO – International Organization for Standardization: Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei sistemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO;

ITSEC – Information Technology Security Evaluation Criteria: Criteri europei per la valutazione della sicurezza nei sistemi informatici;

MEF: Ministero dell'Economia e delle Finanze;

NTP – Network Time Protocol: Protocollo per la sincronizzazione del tempo;

OID – Object IDentifier: Sequenza numerica univoca che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO;

PU: Pubblico Ufficiale

PIN – Personal Identification Number: Codice di sicurezza riservato che permette l'identificazione del soggetto abbinato ad un dispositivo fisico. Permette ad esempio l'attivazione delle funzioni del dispositivo di firma;

POP – Point of Presence: Punto di accesso alla rete internet;

PSCD - Prestatore di Servizi di Conservazione dei Dati: nella fattispecie, PA Digitale;

SSL – Secure Socket Layer: Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica;

SLA - Service Level Agreement: strumenti contrattuali che definiscono le metriche di servizio (es. qualità di servizio) che devono essere rispettate da un fornitore di servizi nei confronti dei propri clienti;

TSA - Time Stamping Authority;

TSS - Time Stamping Service;

TUDA - DPR 28 dicembre 2000, n. 445, e successive modificazioni - "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";

URL – Uniform Resource Locator: Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http:, ftp:, file:, telnet:, news:) specifica il protocollo di accesso all'oggetto;

XML - Extensible Markup Language;

WWW – World Wide Web: insieme di risorse interconnesse da hyperlink accessibili tramite Internet.

8. Dati di identificazione

8.1 Responsabile del servizio di conservazione

Il Cliente è il Titolare dei documenti informatici posti in conservazione e, attraverso il proprio Responsabile della Conservazione, definisce e attua le politiche complessive del sistema di conservazione governandone quindi la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo esplicitato nel presente *Manuale*.

Il suddetto Responsabile della conservazione, sotto la propria responsabilità, ha affidato a **PA Digitale**, quale **prestatore del servizio di conservazione digitale dei documenti informatici**, il servizio di conservazione digitale dei documenti informatici del Cliente avendogli riconosciuto una specifica competenza ed esperienza in relazione alle attività ad esso delegate.

In particolare, PA Digitale, ai fini dell'erogazione del servizio di conservazione, svolge le attività ad essa delegate dal Cliente come in dettaglio riportate nel documento di delega denominato "***Nomina del responsabile del servizio di conservazione***".

Il Cliente ha altresì nominato PA Digitale quale **Responsabile esterno del trattamento dei dati** come previsto dal Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 e s.m.i.).

Pertanto, i ruoli di Produttore, Titolare del trattamento e di Responsabile della conservazione sono ricoperti dal Cliente, mentre i ruoli di Responsabile del servizio di conservazione e Responsabile esterno del trattamento dei dati sono ricoperti da PA Digitale.

Ciò premesso, ai fini dell'esecuzione del Servizio di conservazione dei documenti informatici del Cliente, la società:

PADIGITALE Spa
Sede Legale: Via Leonardo Da Vinci, 13
26854 Pieve Fissiraga (LODI)
Numero Iscrizione R.I. di Lodi, Codice fiscale e Part. IVA: 06628860964
C.C.I.A.A. di Lodi N° R.E.A.: 1464686
N° Telefono (centralino): +39 0371-5935.11
N° FAX: +39 0371-5935.440
e-mail PEC: **protocollo.pec.padigitalespa@legamail.it**
Legale rappresentante: Fabrizio Toninelli, Amministratore Unico
Sito web generale (informativo): **www.padigitale.it**
Sito web del servizio di conservazione: **cs.urbi.it**

in qualità di fornitore del servizio di conservazione, è **delegata** allo svolgimento delle attività specificatamente indicate nel documento di "***Nomina del responsabile del servizio di conservazione***".

Come si dirà in seguito, il sistema di conservazione digitale dei documenti informatici opera secondo modelli organizzativi esplicitamente definiti dal Cliente che garantiscono la sua distinzione logica e fisica dal sistema di gestione documentale che resta sotto la completa responsabilità del Cliente medesimo.

La conservazione dei documenti viene pertanto svolta al di fuori della struttura organizzativa del Cliente.

PA Digitale espleterà, attraverso i propri incaricati e nei limiti della delega ricevuta, tutte le attività e le funzioni inerenti il processo di conservazione.

In particolare, PA Digitale, attraverso il proprio Responsabile del Servizio di Conservazione pro tempore o altri soggetti da questi formalmente delegati, indicati nel loro complesso come **Firmatari delegati**, appositamente dotati di certificati qualificati emessi secondo la normativa vigente in tema di firma digitale, provvederà ad apporre la firma digitale e la marca temporale, ove previsto dalla legge, dai regolamenti tecnici e/o dal presente *Manuale*.

Si precisa che, nel contesto del presente documento, i certificati qualificati di firma di PA Digitale o dei suoi Firmatari delegati, sono utilizzati come uno strumento per dimostrare l'integrità di un insieme di dati o documenti informatici, a prescindere che il documento informatico sia firmato dal Cliente al momento della sua accettazione nel sistema di conservazione. Tale firma, anche in base alla legislazione vigente, non costituisce pertanto sottoscrizione del contenuto dei documenti conservati, del cui contenuto la PA Digitale non è in alcun modo responsabile.

PA Digitale, per le attività finalizzate alla conservazione digitale dei documenti informatici ad essa delegate, si avvale di personale appartenente alla propria struttura, dotato di idonea conoscenza, esperienza, capacità e affidabilità, formalmente incaricato a svolgere ciascuna specifica funzione.

8.2 Dati identificativi della Certification Authority (C.A.)

I Certificatori accreditati sono soggetti pubblici o privati che emettono certificati qualificati conformi alle Direttive europea 1999/93/CE e alla normativa nazionale in materia. Devono aver richiesto e ottenuto il riconoscimento del possesso dei requisiti più elevati in termini di qualità e di sicurezza mediante la procedura di accreditamento prevista dal CAD.

I certificati di firma digitale utilizzati dal processo di Conservazione nonché le marche temporali sono rilasciate dai seguenti soggetti:

Ragione sociale	Indirizzo della sede legale	Altri dati
Aruba Posta Elettronica Certificata S.p.A.	Via Sergio Ramelli, 8 – 52100 Arezzo IT	N° REA : 145843 N° iscrizione al Registro delle imprese: 01879020517 N° Partita IVA : 01879020517 N° Telefono (centralino) : +39 0575 0500 N° FAX : +39 0575 862022 e-mail PEC: direzione.ca@arubapec.it

Si precisa che i certificati di supporto alla firma sono usati solo per firmare documenti e dati riferiti al contesto del presente documento.

8.3 Dati identificativi dei documenti informatici da trattare

I documenti informatici da sottoporre a conservazione fanno riferimento alle diverse tipologie e classi documentali in dettaglio definite nell'apposito allegato "ELENCO DEI DOCUMENTI INFORMATICI SOTTOPOSTI A CONSERVAZIONE", i cui attributi devono essere conformi agli standard riportati al capitolo 12 del presente *Manuale*.

8.4 Luogo di conservazione dei documenti informatici

L'IDC dove sono memorizzati i documenti informatici del Cliente è localizzato fisicamente in Italia.
L'IDC potrà essere situato presso uno o più fornitori esterni comunque situati in Italia rispetto ai quali PA Digitale si assume piena responsabilità circa la conformità alla legge italiana dei servizi forniti.

8.5 Obblighi connessi al trattamento dei dati personali

8.5.1 Tutela e diritti degli interessati

In materia di trattamento dei dati personali PA Digitale garantisce la tutela degli interessati in ottemperanza a quanto disposto del D.Lgs. 196/2003 e s.m.i. In particolare, agli interessati sono fornite le informative di cui all'art. 13 del richiamato provvedimento. Nella suddetta informativa il Cliente è informato sui diritti di accesso ai dati personali ed altri diritti (art. 7, D.Lgs. 196/2003 e s.m.i.).

8.5.2 Modalità del trattamento

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Specifiche misure di sicurezza, come descritte nel presente *Manuale* sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

8.5.3 Finalità del trattamento

Erogazione del servizio di conservazione digitale dei documenti informatici:
I dati raccolti sono utilizzati per l'attivazione del Servizio di conservazione digitale dei documenti informatici.
PA Digitale utilizzerà i dati raccolti per lo svolgimento dell'attività connessa e/o derivante dal Servizio di conservazione digitale dei documenti informatici del Cliente.

Scopi di natura commerciale:
PA Digitale potrà utilizzare le coordinate di posta elettronica fornite dal Produttore per inviare comunicazioni relative a prodotti e/o servizi analoghi a quelli acquistati dal Cliente salva in ogni caso la possibilità dell'interessato di opporsi a tale trattamento.

Altre forme di utilizzo dei dati:
Per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e la difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati, i documenti informatici ed i dati forniti a PA Digitale potranno essere comunicati a soggetti pubblici, quali forze dell'ordine, Autorità pubbliche e autorità Giudiziaria per lo svolgimento delle attività di loro competenza.

8.5.4 Sicurezza dei dati

Come previsto dalle norme vigenti in materia, PA Digitale adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo: i rischi di distruzione o perdita, anche accidentale, dei documenti informatici, di danneggiamento delle risorse hardware su cui i documenti informatici sono registrati ed i locali ove i medesimi vengono custoditi; l'accesso non autorizzato ai documenti stessi; i trattamenti non consentiti dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate assicurano:

a) l'integrità dei documenti informatici, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;

b) la disponibilità dei dati e dei documenti informatici da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei documenti informatici, evitando la perdita o la riduzione dei dati anche accidentale utilizzando un sistema di backup;

c) la riservatezza dei documenti informatici da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.

9. Modello di funzionamento del sistema di conservazione

9.1 Descrizione del servizio

L'obiettivo ed il compito di PA Digitale è quello di conservare i documenti informatici del Cliente con sistemi coerenti alla normativa regolante la conservazione digitale dei documenti informatici.

In particolare, il servizio di conservazione digitale di PA Digitale soddisfa le seguenti funzioni d'uso:
- salvaguardia dell'integrità dei documenti informatici conservati mediante apposizione della firma digitale al pacchetto di archiviazione. Nel suddetto pacchetto di archiviazione è presente, fra l'altro, l'impronta di ogni singolo documento sottoposto a conservazione;
- prolungamento della validità del documento mediante apposizione della marca temporale al pacchetto di archiviazione;
- accesso diretto tramite interfaccia Web ai documenti informatici conservati;
- semplicità di invio e versamento dei documenti informatici da sottoporre a conservazione;
- totale sicurezza nella trasmissione dei documenti informatici da sottoporre a conservazione.

Il sistema di conservazione opera secondo un modello organizzativo che garantisce la sua distinzione logica dal sistema di gestione documentale, qualora esistente presso il Cliente.

In particolare, la conservazione è svolta affidando a PA Digitale il ruolo ed i compiti fissati nel documento di nomina a Responsabile del servizio di conservazione.

A tal fine, PA Digitale ed il Cliente hanno adottato il presente *Manuale* ove sono illustrati dettagliatamente l'organizzazione, i soggetti coinvolti ed i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione dei processi, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione ed alla verifica del funzionamento, nel tempo, del sistema di conservazione.

9.2 Obblighi del Cliente

Il processo di conservazione impone al Cliente l'istituzione di un'organizzazione interna idonea, che garantisca la piena osservanza delle disposizioni normative in tema di gestione documentale[2] e delle procedure da osservare per la corretta produzione/formazione/emissione e sottoscrizione dei documenti informatici destinati alla conservazione digitale in conformità alle regole tecniche di cui all'art. 71 del CAD ed a quanto stabilito dal presente *Manuale*.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla conservazione digitale dei documenti informatici che dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro affinché esso venga svolto secondo i principi stabiliti dalla normativa regolante la conservazione digitale dei documenti informatici.

Il Cliente, quindi, all'interno della propria struttura organizzativa, dovrà aver definito:
a) le procedure propedeutiche alla conservazione digitale a lungo termine dei documenti informatici;
b) le funzioni e le attività delegate, con particolare attenzione alla verifica della congruità e continuità dei processi di produzione/formazione/emissione dei documenti informatici destinati alla conservazione digitale a lungo termine;
c) la gestione delle responsabilità derivanti dalle funzioni ed attività delegate;
d) la documentazione delle deleghe ed il relativo mantenimento;
e) le misure organizzative e tecniche idonee ad evitare danno ad altri.

Il Cliente deve attenersi scrupolosamente alle regole previste dal presente *Manuale e nei documenti ad esso allegati.*

Il Cliente deve altresì prendere visione del presente *Manuale* prima di inoltrare i pacchetti di versamento e/o qualsiasi altra richiesta a PA Digitale.

9.3 Obblighi di PA Digitale

PA Digitale, limitatamente alle attività ad essa delegate, è responsabile verso il Cliente per l'adempimento degli obblighi discendenti dall'espletamento delle attività previste dalla normativa vigente in materia di conservazione digitale di documenti informatici.

[2] Vedi, a puro titolo di esempio, il DPR 28.12.2000, n. 445, il DPCM 3.12.2013 sul protocollo informatico, ove applicabili;

In particolare, PA Digitale, ai fini dell'erogazione del Servizio, svolge le attività ad essa delegate dal Cliente come in dettaglio riportate nel documento di "*Nomina del Responsabile del Servizio di Conservazione*", nei modi e nei termini specificati nel presente *Manuale* e negli allegati ad esso relativi.

Pertanto è obbligo di PA Digitale conservare digitalmente i documenti informatici del Cliente allo scopo di assicurare, dalla presa in carico e fino all'eventuale cancellazione, la loro conservazione a norma, garantendone, tramite l'adozione di regole, procedure e tecnologie, le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il Sistema di conservazione di PA Digitale è in grado di esibire tutti i documenti informatici in esso conservati in qualsiasi momento del periodo di conservazione; a tal fine, PA Digitale ha in essere procedure adeguate a soddisfare, senza indebiti ritardi, le richieste di accesso, esibizione o consegna dei documenti conservati, effettuate dai soggetti debitamente autorizzati.

Oltre alla restituzione dei documenti informatici trasferiti e conservati presso PA Digitale, viene garantita anche la restituzione delle relative evidenze informatiche che comprovano la corretta conservazione degli stessi, fornendo gli elementi necessari per valutare la loro autenticità e validità giuridica.

Non rientra fra i Servizi offerti da PA Digitale la conservazione di documenti analogici.

9.3.1 Compiti organizzativi

PA Digitale provvede alla realizzazione di una base di dati relativa ai documenti informatici che il Cliente versa in conservazione, gestita secondo i principi di sicurezza illustrati nel presente *Manuale* attuati adottando procedure di tracciabilità tali da garantire la corretta conservazione, l'accessibilità a ogni singolo documento e la sua esibizione.

PA Digitale si occupa altresì di definire:

a) le caratteristiche ed i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare e organizzare gli stessi in modo da garantire la corretta conservazione e la sicurezza dei dati, anche al fine di poterli prontamente produrre, ove necessario;
b) le procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l'esecuzione operativa di conservazione.
c) le procedure informatiche ed organizzative per la corretta tenuta dei supporti su cui vengono memorizzati i documenti informatici oggetto di conservazione.
d) le procedure informatiche ed organizzative atte ad esibire la documentazione conservata, in caso di richieste formulate da chi ne abbia titolo.

PA Digitale si occupa di redigere e sottoporre a revisione il presente *Manuale*. Il Cliente si dovrà dotare di un proprio Manuale della Conservazione costituito dalla descrizione di componenti, processi ed organizzazione propri, integrato e completato, se ritenuto necessario, dal presente *Manuale*.

9.3.2 Compiti di manutenzione e controllo

PA Digitale provvede a:

- mantenere un registro cronologico del software dei programmi in uso nelle eventuali diverse versioni succedute nel tempo ed un registro cronologico degli eventi di gestione del sistema di conservazione;
- implementare specifici controlli di sistema per individuare e prevenire l'azione di software che possano alterare i programmi ed i dati;
- verificare la corretta funzionalità del sistema e dei programmi in gestione;
- analizzare e valutare periodicamente la registrazione degli eventi rilevanti ai fini della sicurezza (analisi del log di sistema);
- definire e documentare le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- mantenere e gestire i dispositivi di firma in conformità con le procedure stabilite dal certificatore qualificato che ha rilasciato i relativi certificati;
- verificare la validità delle marche temporali utilizzate dal sistema di conservazione.

9.3.3 Compiti operativi

PA Digitale effettua le seguenti attività:

- supervisione dell'intero sistema di conservazione digitale, verificando accuratamente i processi di apposizione delle firme digitali, dei riferimenti temporali e delle marche temporali, in modo che la procedura rispetti la normativa, assicurandosi che tutto il processo si realizzi secondo le procedure descritte nel presente *Manuale*;
- sincronizzazione dell'ora di sistema di tutti i sistemi utilizzati, verifica e controllo della sincronizzazione del clock di sistema per

consentire registrazioni accurate e comparabili tra loro;
- mantenimento della documentazione descrittiva del processo di conservazione aggiornata nel corso del tempo.

9.3.4 Compiti di change management e relative verifiche

PA Digitale effettua le seguenti attività:
- verificare periodicamente la continua conformità del sistema alle norme e agli standard di riferimento;
- gestire il cambiamento, ossia tutte le attività che possono portare ad un cambiamento del sistema, mantenendo l'aderenza a normativa e standard di riferimento. Esempi di tipologie cambiamenti possono essere:
  - infrastrutturali, al fine di garantire l'operatività e fruibilità del servizio;
  - tecnologici, al fine di garantire l'adeguamento tecnologico della soluzione realizzata;
  - adeguamento al processo di business dettato da un cambiamento della norma e/o degli standard previsti.
- di aggiornamento e reingegnerizzazione delle procedure, qualora gli eventi di cui sopra impattino sui processi definiti e descritti nel presente manuale.

9.4 Modello di funzionamento

Il servizio di conservazione digitale dei documenti informatici è erogato e sviluppato per rispondere alle esigenze di qualsiasi soggetto che abbia l'esigenza di conservare documenti informatici come imprese, professionisti, associazioni, Pubblica Amministrazione centrale e locale. Il servizio permette di conservare i documenti informatici del Cliente, garantendone l'integrità e la validità legale nel tempo nonché la loro "esibizione a norma".

Come già fatto osservare, il sistema di conservazione opera secondo i modelli organizzativi esplicitamente concordati con il Cliente.

Pertanto, la conservazione non viene svolta all'interno della struttura organizzativa del Cliente (soggetto titolare dei documenti informatici da conservare), ma è affidata a PA Digitale, che espleterà le attività per le quali ha ricevuto formale delega, nei limiti della stessa e per le quali opera in modo autonomo e ne è responsabile.

La sequenza di attività che vanno dalla fase propedeutica alla formazione dei documenti informatici alla fase di conservazione degli stessi è di seguito schematicamente rappresentata:

sistemi	fase	Descrizione e MACRO FASI del processo di conservazione	Attività a carico di:	
			Cliente	PA Digitale
Sistema di gestione documentale del Cliente	1	Produzione/formazione/emissione dei documenti informatici e contestuale generazione e associazione dei relativi metadati	X	
	2	Produzione del pacchetto di versamento[3]	X	
	3	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi dei relativi metadati **N.b. È necessario che il cliente mantenga una copia dei documenti inviati in conservazione almeno fino alla ricezione della notifica di avvenuta conservazione.**	X	
Sistema di conservazione digitale dei documenti informatici	4	Acquisizione da parte del sistema di conservazione del pacchetto di versamento prodotto dal Cliente per la sua presa in carico		X
	5	Verifica che il pacchetto di versamento ed i documenti informatici in esso descritti siano coerenti e conformi alle prescrizioni di cui al *Manuale*		X
	6	Eventuale rifiuto del pacchetto di versamento o dei documenti informatici, nel caso in cui le verifiche di cui alla fase 5 abbiano evidenziato delle anomalie		X
	7	Generazione, anche in modo automatico, del rapporto di versamento relativo a ciascun pacchetto di versamento		X
	8	Invio al Cliente del rapporto di versamento		X
	9	Preparazione e gestione del pacchetto di archiviazione		X

[3] Per la dettagliata descrizione del pacchetto di versamento si rimanda a quanto precisato nel capitolo 13 del presente Manuale.

	10	"Chiusura" del pacchetto di archiviazione mediante sottoscrizione con firma digitale di PA Digitale e apposizione di marca temporale		X
	11	Richieste di esibizione dei documenti informatici conservati	X	
	12	Preparazione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente con tutti gli elementi necessari a garantire l'integrità e l'autenticità degli stessi		X
	13	Richiesta del Cliente di duplicati informatici	X	
	14	Produzione di duplicati informatici su richiesta del Cliente		X

Dal prospetto di cui sopra emerge chiaramente come ogni singola fase del processo è propedeutica alle altre.
In ogni caso, prima di dare corso al processo di conservazione, il Cliente e PA Digitale dovranno definire come configurare il servizio in base alle specifiche esigenze del Cliente concordando le modalità di gestione e fruizione oltre alla quantità e tipologia di documenti da conservare.

9.5 Descrizione delle architetture e delle infrastrutture utilizzate

9.5.1 Infrastruttura informatica data center

Il Data Center dal quale sono erogati i servizi si trova sul territorio nazionale ed è conforme ai requisiti della normativa ISO/IEC 27001:2005.

9.5.2 Infrastruttura di sistema

L'architettura della Server Farm è basata su componenti le cui principali caratteristiche sono:
- affidabilità delle singole componenti scelte;
- ridondanza fisica di tutti i componenti HW;
- ridondanza dei componenti SW di sistema e networking.

La disponibilità dell'infrastruttura presenta un uptime del 99.95%, garantita a diversi livelli sia grazie alle scelte architetturali che alle tecnologie utilizzate.

9.5.3 Sottosistema di virtualizzazione

L'infrastruttura si basa su Cloud Server HA configurati con le seguenti tecnologie di alta affidabilità:
- Vmotion: consente di migrare real time le VM tra host fisico ad un altro cluster;
- Storage Vmotion: rilocazione di VM fra datastore senza interruzione del servizio;
- High Availability: in caso di failure di un host virtualizzatore o della VM.

Inoltre l'infrastruttura fisica ha le seguenti caratteristiche di alta affidabilità:
- i server fisici sono raggruppati in cluster ridondati N+1;
- il fault di un server comporta la rilocazione delle risorse sugli altri due nodi del cluster;
- i server fisici utilizzati sono di classe Enterprise multiprocessore;
- le schede di rete e gli apparati di rete sono ridondati;
- switch e schede HBA FC sono ridontati e configurati in bilanciamento;
- gli storage box sono di livello enteprise ad alimentatori ridondati, controller ridondati, dischi in configurazione RAID, porte fc ridondate ed in bilanciamento vs gli switch della SAN;
- switch e pattern FC della SAN sono ridontati sia livello edge che core, con realizzazione dual fabric.

9.5.4 Sottosistema storage

Per eliminare ogni rischio di interruzione del servizio dovuto a guasti HW, tutti i dischi delle VM e dei dati sono memorizzati esclusivamente su SAN ad alte prestazioni dedicate al servizio.
La configurazione della SAN garantisce assenza di Single Point of Failure, tutti i sistemi sono in costante monitoraggio che garantisce tempi di sostituzione componenti hw senza completo fermo del sistema.
Le garanzie:
- alta affidabilità dei componenti fisici, tutti i componenti sono ridontati, cioè disco in RAID5 + hot-spare, SAN dual-fabric ecc.
- scalabilità verticale ed orizzontale dell'infrastruttura che è in grado di supportare richieste di workload e di spazio addizionale evitando situazioni di overbooking.

9.5.5 Sottosistema di backup

Implementazioni di backup esistono per tutti i layer dell'infrastruttura, lato server come switch FC per la SAN ed apparati di networking.

Le risorse degli apparati di salvataggio e stoccaggio dati, quali tape library o storage dedicati al backup, sono implementate seguendo la crescita delle dimensioni dei dati da salvare.
Backup applicativi e di dati, sono effettuati con granularità giornaliera e retention settimanale con software IBM Tivoli Storage.
Il sistema dispone di una procedura di disaster recovery con RPO di 1gg ed RTO minimo di 1gg e massimo di 3gg.
Il Data Center dal quale viene erogato il servizio di Disaster Recovery è situato sul territorio nazionale ed è conforme ai requisiti della normativa ISO/IEC 27001:2005

9.5.6 Sottosistema di networking

L'infrastruttura di rete è basata su scalabilità e flessibilità, al fine dell'erogazione dei servizi applicativi.
Il modello architetturale verte su un impiego massivo della virtualizzazione dei servizi di rete, con una suddivisione logica a più livelli del contesto.

Dal punto di vista fisico la rete è :
- completamente ridondata;
- strutturata in blocchi con un livello di accesso separato per isolare i contesti applicativi e gestionali;
- utilizza reti ethernet ad 1Gb per gli host con backbone a 10Gb
- banda internet ampliabile in base all'utilizzo, anche temporaneamente

9.5.7 Sottosistemi firewall e componenti di sicurezza

L'architettura di sicurezza e firewall è implementata utilizzando due cluster firewall in alta affidabilità: per la gestione dell'accesso internet e per la gestione della rete interna (VLAN).
Ogni cluster FW è altresì composto da due unità fisiche di FW in alta affidabilità.
I server applicativi utilizzano VLAN per ottenere una separazione del livello database da quello applicativo, al fine di elevare la sicurezza di gestione dei documenti e di ridurre al minimo il rischio di compromissione dei sistemi in caso di attacco.
L'infrastruttura dispone di sonde IPS (Intrusion Prevention System) che garantiscono una protezione perimetrale da attacchi, per esempio di tipo DDOS (Distributed Denial of Service).
La sicurezza di accesso ai componenti del sistema è garantita attraverso l'uso di password a criptazione forte.
L'accesso da parte di PA Digitale Spa ai sistemi per scopi di amministrazione avviene attraverso connessioni autenticate attraverso username/password e certificati digitali.

9.6 Misure di sicurezza adottate

9.6.1 Ubicazione data center

L'IDC acquisisce risorse di banda da diversi carriers, per avere la massima affidabilità contando su linee completamente ridontate e carriers anch'esso ridondati.
Il Data Center dal quale sono erogati i servizi si trova sul territorio nazionale ed è conforme ai requisiti della normativa ISO/IEC 27001:2005.

Il Data Center dispone di una connessione ad Internet attraverso linee multiple per una capacità complessiva di alcuni Gbit/s e sono dotati di sistemi di condizionamento, gruppi di continuità, generatori elettrici, sistemi antincendio e monitoraggio attivo 24x7. Il Data Center è connesso alla rete tramite linee ridondate ad elevata capacità, in grado di garantire la massima disponibilità ed affidabilità.

In particolare :

- Il Data Center risiede in un caveaux blindato.
- Sorveglianza armata h24 dell'intero complesso.
- Sorveglianza elettronica contro l'intrusione, l'incendio e anomalie ambientali critiche.
- Sistemi automatici di videocontrollo per ciascun piano (ai sensi T.U. Sulla privacy).
- Sistema ridondante di controllo del clima delle sale macchine con allarmi locali e remoti su valori critici.
- Sistema di alimentazione ridondante per ogni fila di armadi con prese e spine di sicurezza antistrappo e antifuoco.
- Impianto di sicurezza dell'alimentazione mediante impianto di terra certificato conforme L.626 e separazione galvanica delle sorgenti.
- Sistema anticendio a gas con sensori a soffitto e a pavimento a saturazione ambientale. Bombole dedicate per ogni piano, impianto ridondato e separato.
- Doppie porte antincendio per piano con dispositivo automatico di chiusura.
- Condizionamento statico dell'alimentazione dei tramite Gruppi di continuita' statici online.

- Gruppo elettrogeno diesel per erogazione continuata di eletricità in mancanza della rete.

E' assicurata la sorveglianza dei locali 365/7/24 con personale proprio o esterno autorizzato o con sistemi di monitoraggio remotizzato.
Tutti gli accessi alle areee di datacenter sono sottoposti ad identificazione e registrazione accessi basato su badge e finger print.

10. Soggetti coinvolti, ruoli, funzioni, obblighi e responsabilità

Ai fini del servizio di conservazione digitale dei documenti informatici, si individuano i seguenti ruoli principali:

Ruolo	Organizzazione di appartenenza
Produttore	Cliente
Responsabile della conservazione (RdC)	Cliente
Referenti del Cliente	Cliente
Responsabile del servizio di conservazione	PA Digitale
Utente	Cliente/Terzi autorizzati

Il Produttore è il Cliente e le eventuali persone fisiche dallo stesso incaricate della produzione/formazione/emissione e sottoscrizione dei documenti informatici da depositare in conservazione.

Il Cliente è il soggetto titolare e responsabile a tutti gli effetti dei documenti che devono essere sottoposti al processo di conservazione digitale; è l'unico responsabile del contenuto del pacchetto di versamento, trasmette tale pacchetto al sistema di conservazione secondo i modi, nei termini ed in conformità a quanto stabilito nel presente *Manuale*.

Il Responsabile della conservazione è il Cliente, nella persona fisica dallo stesso individuata. Il Responsabile della conservazione è colui che ha definito le politiche complessive del sistema di conservazione esplicitate nel presente *Manuale* e che si occupa di darne relativa attuazione; governa la gestione dei processi di formazione dei documenti informatici con piena responsabilità, in relazione al modello organizzativo adottato.

Il Responsabile della conservazione agisce in osservanza degli obblighi previsti dalla normativa regolante la conservazione digitale di documenti informatici vigente, cura e vigila affinché i compiti riportati nel presente *Manuale* siano correttamente svolti da PA Digitale.

Referente/i del Cliente è/sono le persone fisiche che il Cliente indica a PA Digitale quali punti di riferimento tecnico ed organizzativo per gli aspetti che riguardano le comunicazioni relative all'erogazione del servizio di conservazione.

Ai fini dello svolgimento del servizio di conservazione, il Cliente con specifica delega ha nominato **Responsabile del servizio di conservazione** digitale dei propri documenti informatici, PA Digitale.

PA Digitale, quale **Responsabile del servizio di conservazione** digitale dei documenti informatici del Cliente, agisce nei limiti della delega ad essa conferita e nell'osservanza degli obblighi ivi previsti nonché nel rispetto della normativa regolante la conservazione digitale di documenti informatici e delle presenti prescrizioni; in particolare, essa agirà attraverso persone fisiche dalla stessa formalmente incaricate.

L'attività di PA Digitale riguarda la sola conservazione digitale dei documenti informatici del Cliente, senza alcuna responsabilità e possibilità di intervento ed accesso al contenuto degli stessi.

A carico di PA Digitale, 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 a cura e carico del Cliente.

Il Responsabile del servizio di conservazione opererà altresì nell'osservanza di quanto stabilito nel presente *Manuale*, al quale, se necessario, è sin da ora autorizzato ad apportare le modifiche, le integrazioni e gli aggiornamenti ritenuti necessari e/o conseguenti al mutato contesto tecnico-giuridico della normativa regolante la conservazione digitale di documenti informatici.

PA Digitale, nell'ambito del suo ruolo di Responsabile del servizio di conservazione designato dal Cliente, non deve e non può accedere e/o sottoporre ad alcun trattamento il contenuto dei documenti informatici ricevuti in conservazione.
Il Responsabile del servizio di conservazione digitale non è responsabile in alcun modo del contenuto dei documenti informatici.

L'utente è il soggetto che richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste nel presente *Manuale*.

Come già anticipato, il processo di conservazione impone al Cliente l'istituzione di una struttura ed una organizzazione interna, coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza alle disposizioni normative di riferimento e di quanto previsto dal presente *Manuale*.

A tale scopo, in base alle specifiche necessità, il Cliente deve, sia dal punto di vista dell'impostazione operativa delle attività propedeutiche alla conservazione digitale dei propri documenti informatici sia dal punto di vista della scelta delle risorse coinvolte nel processo, organizzare il lavoro all'interno della propria organizzazione affinché esso venga svolto secondo i principi stabiliti dalla normativa in materia nonché dalle specifiche regole tecniche.

Tutto il personale di PA Digitale è stato assunto nel rispetto di politiche rigorose volte ad accertarne, tra l'altro, l'alto grado di professionalità nonché i requisiti morali e di onorabilità.

11. Struttura organizzativa del sistema di conservazione

Qui di seguito si da conto della struttura organizzativa del processo di conservazione adottato evidenziando, nel contempo, le funzioni, le responsabilità e gli obblighi dei diversi soggetti che intervengono nel suddetto processo.
Come precisato nel precedente capitolo 9, il processo di conservazione prevede una serie di attività che implicano il concorso di numerosi soggetti, a differenti livelli e con diverse responsabilità.

Qui di seguito vengono dettagliate per singola attività i diversi compiti e responsabilità delle figure preposte alla gestione e controllo del sistema di conservazione.

Il personale addetto al servizio di conservazione, prevede, le seguenti **figure responsabili di processo**:

1. Responsabile del servizio di conservazione;
2. Responsabile della funzione archivistica di conservazione;
3. Responsabile del trattamento dei dati personali;
4. Responsabile della sicurezza dei sistemi per la conservazione;
5. Responsabile dei sistemi informativi per la conservazione;
6. Responsabile dello sviluppo e della manutenzione del sistema di conservazione;

Per ciascuna delle figure sopra elencate si riportano le **attività associate ad ogni ruolo**:

1. **Responsabile del servizio di conservazione**
   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 al Cliente; 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.

2. **Responsabile della funzione archivistica di conservazione**
   Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, 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; collaborazione col Cliente 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.

3. **Responsabile del trattamento dei dati personali**
   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.

4. **Responsabile della sicurezza dei sistemi per la conservazione**
   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.

5. **Responsabile dei sistemi informativi per la conservazione**
   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.

6. **Responsabile dello sviluppo e della manutenzione del sistema di conservazione**
   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 manutenzione del sistema di conservazione; interfaccia col Cliente 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.

Le funzioni sopra elencate possono avvalersi, per lo svolgimento delle attività ad esse attribuite, di addetti ed operatori formalmente incaricati.

Qui di seguito sono riportati i dati dei soggetti che nel tempo hanno assunto particolari funzioni e responsabilità con riferimento al sistema di conservazione.

Ruoli e responsabilità

Cognome	Nome	Ruolo	Responsabilità	Data nomina (gg/mm/aaaa)	Data cessazione (gg/mm/aaaa)
Toninelli	Fabrizio	Responsabile del servizio di conservazione (RSC)	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 al Cliente; 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.	29/03/2013	
Pezzini	Simone	Responsabile della funzione archivistica di conservazione (RFAC)	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte del Cliente, 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; collaborazione col Cliente 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.	10/04/2014	
Lavesi	Roberto	Responsabile del trattamento dei dati personali (RTDP)	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.	29/03/2013	
Ghidini	Roberto	Responsabile della sicurezza dei sistemi per la conservazione (RSSC)	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.	29/03/2013	
Ghidini	Roberto	Responsabile dei sistemi informativi per la conservazione (RSIC)	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.	29/03/2013	
Formenti	Nicolò	Responsabile dello sviluppo e della manutenzione del sistema di conservazione (RSSC)	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 manutenzione del sistema di conservazione; interfaccia col Cliente 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	29/03/2013	

			nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.		

Di seguito sono indicati i compiti, le responsabilità e le funzioni di firma in relazione alle diverse fasi del processo di conservazione digitale.

Fasi del processo	Descrizione delle fasi del processo di conservazione		COMPITI	RESPONSABILITA'	FIRMA
FASE 1	**Attivazione del servizio di conservazione**				
	Descrizione sintetica	A seguito della sottoscrizione del contratto da parte del cliente, comprendente la nomina a responsabile del servizio di conservazione e la nomina a responsabile esterno privacy, viene configurato il sistema e attivato un nuovo contesto per fornire il servizio di conservazione a norma in relazione alle diverse classi documentali oggetto di conservazione.	**SC**	**RSC, RSIC, RTDP**	**==**
FASE 2	**Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico**				
	Descrizione sintetica	Il sistema di conservazione riceve i pacchetti di versamento unicamente tramite chiamate web ad un indirizzo specifico soggetto ad autenticazione. Il processo di acquisizione è descritto nel dettaglio nel capitolo 13	**SC**	**RSIC**	**==**
FASE 3	**Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione**				
	Descrizione sintetica	Ciascun pacchetto di versamento ricevuto dal sistema di conservazione viene esaminato al fine di verificarne la coerenza con la configurazione e le impostazioni del sistema stesso. Il dettaglio dei controlli effettuati viene specificato nel capitolo 13	**SC**	**RSIC**	**==**
FASE 4	**Preparazione del rapporto di conferma**				
	Descrizione sintetica	Per ciascun pacchetto di versamento il sistema di conservazione predispone un rapporto di conferma che riepiloga i dati elaborati e che riporta gli eventuali errori riscontrati.	**SC**	**RSIC**	**==**
FASE 5	**Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o non conformità**				
	Descrizione sintetica	I pacchetti di versamento che non rispettano i requisiti della FASE 3 vengono rifiutati dal sistema di conservazione che non accetta nemmeno i relativi documenti. In questo caso il dettaglio degli errori viene riportato all'interno del rapporto di conferma.	**SC**	**RSIC**	**==**
FASE 6	**Ricezione dei documenti**				
	Descrizione sintetica	Per ciascun pacchetto di versamento accettato correttamente il sistema di conservazione attende l'invio dei relativi documenti.	**SC**	**RSIC**	**==**
FASE 7	**Verifica dei documenti**				
	Descrizione sintetica	Tutti i documenti ricevuti vengono esaminati al fine di determinare la conformità con quanto dichiarato nel pacchetto di versamento, con le specifiche del formato utilizzato e con quanto definito nel presente Manuale. I documenti che non superano tutti questi controlli vengono rifiutati dal sistema di conservazione.	**SC**	**RSIC**	**==**
FASE 8	**Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte**				
	Descrizione sintetica	Ciascun pacchetto di versamento ricevuto viene elaborato dal sistema al fine di verificare la conformità con la configurazione e le impostazioni del sistema di conservazione. Tutti i dati elaborati sono riportati all'interno del rapporto di versamento. Il rapporto di versamento viene reso disponibile solamente a seguito della corretta ricezione ed elaborazione di tutti i documenti del singolo pacchetto di versamento.	**SC**	**RSIC**	**==**
FASE 9	**Sottoscrizione del rapporto di versamento con firma digitale apposta da PA Digitale**				
	Descrizione sintetica	Il rapporto di versamento viene reso disponibile tramite richiesta ad un apposito indirizzo web soggetto ad autenticazione. Il rapporto di versamento viene sottoscritto automaticamente dal sistema mediante l'apposizione della firma digitale di PA Digitale.	**SC**	**RSIC**	**RSC**
FASE 10	**Preparazione e gestione del pacchetto di archiviazione (c.d. File di chiusura)**				
	Descrizione sintetica	La struttura dell'indice del pacchetto di archiviazione fa riferimento allo standard "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali", (c.d. SInCRO). E' la norma UNI 11386 dell'ottobre 2010.	**SC**	**RSIC**	**==**

		La norma definisce la struttura dell'insieme di dati a supporto del processo di conservazione; in particolare, la norma individua gli elementi informativi necessari alla creazione dell'indice di conservazione (il cosiddetto "**file di chiusura**") e descrivendone sia la semantica sia l'articolazione per mezzo del linguaggio formale XML. L'obiettivo della norma è quello di utilizzare una struttura-dati condivisa al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, grazie all'adozione dello Schema XML appositamente elaborato. Tale norma, pertanto, rappresenta lo standard nazionale adottato da PA Digitale nella formazione della struttura dell'indice del pacchetto di archiviazione. Per ciascun pacchetto di versamento ricevuto ed elaborato correttamente dal sistema di conservazione unitamente ai documenti in esso descritti, viene creato un corrispondente pacchetto di archiviazione.			
FASE 11	**Sottoscrizione del pacchetto di archiviazione con firma digitale apposta da PA Digitale e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del pacchetto di archiviazione"**				
	Descrizione sintetica	Entro i termini definiti nella configurazione di ciascuna classe documentale, il sistema provvede automaticamente alla generazione dei pacchetti di archiviazione secondo la modalità definita nella FASE 10. Sui pacchetti così generati, sempre in modalità completamente automatica, il sistema appone la firma digitale del Responsabile del servizio di conservazione e, sul pacchetto di archiviazione firmato, una marca temporale.	**SC**	**RSIC**	**RSC**
FASE 12	**Preparazione e sottoscrizione con firma digitale del Responsabile del servizio di conservazione del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente**				
	Descrizione sintetica	Ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione è coincidente con i pacchetti di archiviazione. Il pacchetto di distribuzione viene creato on-demand e si caratterizza per la possibilità di avere al suo interno anche i documenti. Le modalità di creazione e le tipologie dei pacchetti di distribuzione sono descritte nel dettaglio nel capitolo 16.	**SC**	**RSSC**	**RSC**
FASE 13	**Produzione di duplicati informatici o di copie informatiche effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico**				
	Descrizione sintetica	L'architettura completamente web del sistema di conservazione facilita notevolmente le operazioni di recupero dei documenti. Tali operazioni portano alla produzione di duplicati informatici. La descrizione dettagliata della modalità di produzione dei duplicati è riportata nel capitolo 19. La produzione di copie si rende necessaria solamente a seguito di obsolescenza tecnologica di un formato accettato in conservazione e determina, quale diretta conseguenza, l'avvio di una procedura di riversamento sostitutivo. Il dettaglio di tale procedura è descritto nel capitolo 19	**SC**	**RSSC**	**RSC**
FASE 14	**Eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso**				
	Descrizione sintetica	Premesso che nel caso degli archivi pubblici o privati, che rivestono interesse storico-artistico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero per i beni e le attività culturali rilasciata al Cliente secondo quanto previsto dalla normativa vigente in materia, il sistema di conservazione provvederà alla cancellazione dei pacchetti di archiviazione, dei descrittori evidenze e dei documenti allo scadere del termine di cancellazione, dietro specifica richiesta del Cliente. Eventualmente potrà essere fornita copia di tali dati al Cliente come servizio aggiuntivo.	**SC**	**RFAC RTDP**	**==**
FASE 15	**Eventuale chiusura del servizio di conservazione**				
	Descrizione sintetica	Qualora il cliente decidesse di non rinnovare il servizio di conservazione con PA Digitale, al termine di validità del contratto PA Digitale rende disponibili tutti i documenti conservati ed i relativi metadati, scaricabili dal cliente tramite la generazione dei pacchetti di distribuzione. Le modalità di creazione e le tipologie dei pacchetti di distribuzione sono descritte nel dettaglio nel capitolo 16. Trascorso un numero di giorni concordato con il Cliente al momento dell'attivazione del servizio, PA Digitale, sulla scorta di quanto previsto dal Dlgs 196/2003, rimuove dal sistema tutti i documenti informatici del Cliente ed i relativi metadati.	**SC**	**RSC, RSSC**	**RSC**

Legenda:
- **RSIC** - responsabile dei sistemi informativi per la conservazione
- **RSSC** - responsabile dello sviluppo e della manutenzione del sistema di conservazione

- **RFAC** - responsabile della funzione archivistica di conservazione
- **RTDP** - responsabile privacy
- **RSC** - responsabile del servizio di conservazione
- **SC** - **Sistema di conservazione**

12. Descrizione delle tipologie dei documenti sottoposti a conservazione

In questo capitolo viene resa la descrizione delle tipologie di documenti informatici sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni.

Il servizio di conservazione digitale dei documenti informatici non riguarda la conservazione di documenti analogici di alcun tipo e genere.

Prima dell'attivazione del servizio il Cliente esplicita la tipologia di documenti che intende sottoporre a conservazione mediante il servizio offerto da PA Digitale.

Per ogni formato definito viene individuato anche il **software necessario per la visualizzazione** del documento informatico.

PA Digitale configura sul servizio un profilo di conservazione per ogni tipologia/classe di documenti su indicazione del Cliente, classificato come omogeneo in base ai dati da utilizzare per l'indicizzazione ed i termini di conservazione.

Il Cliente è tenuto a depositare in conservazione esclusivamente documenti informatici appartenenti alle tipologie/classi concordate con il Conservatore.

Ogni variazione di formato di documento e di software associato per la visualizzazione oppure dei dati utilizzati per l'indicizzazione deve essere preventivamente concordato con PA Digitale e configurato sul servizio.

12.1 Tipologie dei documenti informatici sottoposti a conservazione

Il sistema di conservazione digitale dei documenti informatici è impostato per accettare le seguenti tipologie di documenti informatici;
- documenti amministrativi;
- documenti rilevanti ai fini tributari;
- altri documenti in genere

Le diverse tipologie di documenti sono prodotti/formati/emessi a cura e sotto l'esclusiva responsabilità del Cliente mediante una delle seguenti principali modalità:
a) redazione tramite l'utilizzo di appositi strumenti software;
b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari;
d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Al fine di garantire l'identificazione certa del soggetto che ha formato il documento, i documenti informatici posti in conservazione saranno in genere sottoscritti con firma digitale del Cliente e dovranno essere identificati in modo univoco e persistente.

Qualora il Cliente intendesse depositare in conservazione **documenti informatici non sottoscritti** con firma digitale, la paternità degli stessi sarà comunque attribuita al Cliente medesimo mediante la sottoscrizione con firma digitale, da parte di quest'ultimo, del pacchetto di versamento e l'associazione allo stesso di un riferimento temporale nei modi stabiliti al successivo capitolo 13 del presente Manuale.

La suddetta possibilità di depositare in conservazione documenti informatici non sottoscritti deve necessariamente essere preventivamente dichiarata, per ogni classe/tipo di documento.

12.2 Copie informatiche di documenti analogici originali unici

Come noto, l'art. 22 del CAD stabilisce che:
a) (comma 2) le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da

altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.

b) (comma 3) le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

Pertanto, alla luce di quanto sopra, il Cliente qualora intendesse depositare in conservazione copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico è tenuto, a propria cura e spese, a predisporre quanto necessario per ottemperare a quanto previsto dalle richiamate disposizioni.

In particolare, sarà cura e carico del Cliente:

a) produrre la copia per immagine su supporto informatico del documento analogico mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto;

successivamente:

b) (ai fini di quanto stabilito dall'articolo 22, co. 3, del CAD), dovrà sottoscrivere con firma digitale la copia per immagine del documento analogico;

oppure

c) laddove richiesto dalla natura dell'attività, (art. 22, comma 2, del CAD), dovrà inserire nel documento informatico contenente la copia per immagine, l'attestazione di conformità all'originale analogico. Il documento informatico così formato dovrà poi essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata di pubblico ufficiale a ciò autorizzato.

Si tenga presente che l'attestazione di conformità delle copie per immagine su supporto informatico di uno o più documenti analogici, effettuata per raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia, può essere prodotta, sempre a cura e carico del Cliente, come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Tale documento informatico separato dovrà essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

In sostanza, in questi casi il Cliente dovrà alternativamente depositare in conservazione:

- la copia per immagine su supporto informatico dell'originale analogico contenente l'attestazione di conformità all'originale analogico debitamente sottoscritto come sopra riportato;

oppure

- le copie per immagine su supporto informatico unitamente all'attestazione di conformità prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni singola copia per immagine, debitamente sottoscritto come sopra riportato.

12.3 Formati gestiti

Come noto, la leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.

Il formato di un documento informatico è la convenzione usata per rappresentare il contenuto informativo mediante una sequenza di byte.

Nel presente capitolo vengono fornite le indicazioni sui formati dei documenti informatici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con la conservazione digitale a lungo termine. Infatti, una possibile soluzione al problema dell'obsolescenza, che porta all'impossibilità di interpretare correttamente formati non più supportati al fine di renderli visualizzabili, è quella di selezionare formati standard.

E' comunque opportuno premettere che per la natura stessa dell'argomento di cui trattasi, questa parte del *Manuale* potrà subire periodici aggiornamenti sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati.

12.3.1 Caratteristiche generali dei formati

PA Digitale raccomanda un insieme di formati che sono stati dalla stessa valutati in funzione di alcune caratteristiche quali:

	caratteristica	descrizione della caratteristica
1	**APERTURA**	Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia

		interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente. Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti. In quest'ultimo caso tuttavia si confida che quest'ultimi garantiscono l'adeguatezza e la completezza delle specifiche stesse. In relazione a questo aspetto, PA Digitale ha privilegiato formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS.
2	**SICUREZZA**	La sicurezza di un formato dipende da due elementi: - il grado di modificabilità del contenuto del file; - la capacità di essere immune dall'inserimento di codice maligno.
3	**PORTABILITÀ**	Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto si ottiene mediante l'impiego fedele di standard documentati e accessibili e dalla loro diffusione sul mercato.
4	**FUNZIONALITÀ**	Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione del Cliente per la formazione e gestione del documento informatico.
5	**SUPPORTO ALLO SVILUPPO**	Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
6	**DIFFUSIONE**	La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

12.3.2 Formati per la conservazione

Oltre al soddisfacimento delle caratteristiche suddette, nella scelta dei formati idonei alla conservazione, PA Digitale è stata estremamente attenta affinché i formati stessi fossero capaci a far assumere al documento le fondamentali caratteristiche di immodificabilità e staticità.

Pertanto, alla luce delle suddette considerazioni, **i formati adottati e consigliati da PA Digitale** per la conservazione delle diverse tipologie di documenti informatici sono le seguenti:

Formato	**Descrizione**	
PDF/A	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. Questo formato è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.
	Sviluppato da	Adobe Systems - http://www.adobe.com/
	Estensione	.pdf
	Tipo MIME	Application/pdf
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 19005-1:2005 (vesr. PDF 1.4)
	Altre caratteristiche	assenza di collegamenti esterni
		assenza di codici eseguibili
		assenza di contenuti crittografati
		il file risulta indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo
		Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A
		Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.
	Software necessario alla visualizzazione	Adobe Reader

Formato	**Descrizione**
XML	Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio: SVG usato nella

Manuale del sistema di Conservazione

	descrizione di immagini vettoriali, XBRL usato nella comunicazione di dati finanziari, ebXML usato nel commercio elettronico, SOAP utilizzato nello scambio dei messaggi tra Web Service	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Contenuto di evidenze informatiche, dei pacchetti di versamento, archiviazione e distribuzione, ecc.
	Sviluppato da	W3C
	Estensione	.xml
	Tipo MIME	Application/xml Text/xml
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da W3C – http://www.w3.org/XML/
	Altre caratteristiche	è un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	Microsoft Internet Explorer / Firefox / Google Chrome

Formato	**Descrizione**	
EML	Electronic Mail Message (EML) è un formato di testo che definisce la sintassi di messaggi di posta elettronica scambiati tra utenti	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Messaggi di posta elettronica e PEC
	Sviluppato da	Internet Engineering Task Force (IETF)
	Estensione	.eml
	Tipo MIME	Message/rfc2822
	Formato aperto	SI
	Specifiche tecniche	Pubblicate da IETF - http://www.ietf.org/rfc/rfc2822.txt
	Altre caratteristiche	è un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione	La maggior parte dei client di posta elettronica supportano la visualizzazione di file eml

Per quanto concerne il formato degli allegati al messaggio di posta elettronica, valgono le indicazioni di cui sopra.

I formati XML ed EML sono accettati solamente per le classi documentali di tipo "PEC".

Pertanto, alla luce di quanto sopra esposto, **i formati accettati in conservazione**, salvo quanto diversamente richiesto dal Cliente, **sono esclusivamente quelli richiamati nel presente capitolo**.

A prescindere dai formati consigliati dal presente manuale, il Cliente è tenuto a depositare in conservazione esclusivamente documenti informatici privi di qualsiasi Agente di alterazione.

Pertanto, i documenti informatici depositati in conservazione NON dovranno contenere, a titolo meramente indicativo e non esaustivo, né macroistruzioni corrispondenti in comandi interni che, al verificarsi di determinati eventi, possono generare automaticamente modifiche o variazione dei dati contenuti nel documento, né codici eseguibili corrispondenti in istruzioni, non sempre visibili all'utente, che consentono all'elaboratore di modificare il contenuto del documento informatico.

12.3.3 Identificazione

L'associazione del documento informatico al suo formato può avvenire, attraverso varie modalità, tra cui le più impiegate sono:

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].doc identifica un formato

sviluppato dalla Microsoft;

2. il magic number: i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 identifica i file immagine di tipo .jpeg;
3. verifica della corrispondenza tra il tipo MIME ricavato dall'estensione del file ed il tipo MIME ricavato dal magic number;

Per identificare il formato dei files posti in conservazione occorre procede all'analisi di ogni singolo documento informatico contenuto all'interno dei pacchetti di versamento. PA Digitale procede come segue:

1	**Fase di IDENTIFICAZIONE**	In questa fase viene ricevuto il pacchetto di versamento che contiene le indicazioni relative a ciascun documento ed in particolare al nome completo del file ed alla sua estensione. Viene verificata la corrispondenza tra l'estensione dichiarata ed il nome del file.
2	**Fase di RICEZIONE**	In questa fase i documenti descritti nei pacchetti di versamento vengono ricevuti nel sistema di conservazione e viene effettuato un primo controllo basato sui metodi di cui ai precedenti punti 1, 2 e 3, ossia estensione del file, magic number e corrispondenza dei mime type.
3	**Fase di VALIDAZIONE**	In questa fase saranno effettuati dei test aggiuntivi per verificare se il formato identificato è corretto secondo gli standard stabiliti nel presente *Manuale* e se rispetta le specifiche del formato. Questi test sono effettuati utilizzando apposite librerie in grado di trattare lo specifico formato.

12.3.4 Verifica della leggibilità dei documenti informatici

Per assicurare la leggibilità dei documenti informatici PA Digitale potrà adottare una delle seguenti misure:

a) conservare in sicurezza, per tutto il tempo in cui il documento informatico è mantenuto nel suo formato originale, il software necessario all'esibizione del dato. Dove necessario, PA Digitale dovrà avere la disponibilità anche del relativo hardware così come di qualsiasi altro dispositivo richiesto per la presentazione dei documenti informatici. Questo obiettivo può essere raggiunto acquisendo o conservando in proprio l'hardware e i dispositivi, come anche assicurandosene l'utilizzo presso fornitori esterni;
b) conservare le specifiche del formato del documento informatico, garantendo che esisteranno applicazioni software in grado di esibire i documenti nei formati ammessi. Questo secondo modo può essere utilizzato solo se le specifiche del formato in questione sono disponibili.

Il Cliente dovrà dotarsi del software e dell'hardware necessario all'esibizione dei documenti informatici prodotti/formati/emessi nei formati ammessi e condivisi.

PA Digitare, dal canto suo, deve avere in essere procedure idonee a verificare l'effettiva leggibilità dei documenti informatici conservati; tali procedure sono eseguite a intervalli idonei a garantire l'individuazione tempestiva di un degrado nella leggibilità, almeno come previsto dalla normativa regolante la conservazione digitale di documenti informatici.

Esempi di "degrado" sono:

a) il danneggiamento del supporto usato per la memorizzazione del dato;
b) l'alterazione di alcuni bit del dato.

Il controllo di leggibilità eseguito da PA Digitale è di due tipologie:

a. **controllo di leggibilità:** consiste nel verificare che i singoli bit degli oggetti siano tutti correttamente leggibili. Questo fornisce garanzia del buono stato del supporto di memorizzazione.
b. **controllo di integrità:** consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema. Questo fornisce una ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

La combinazione dei due tipi di controllo descritti non fornisce però garanzia di poter visualizzare correttamente il documento e che lo stesso sia effettivamente intellegibile dall'uomo.

Infatti questa garanzia non può essere fornita senza entrare nel merito del documento stesso. La garanzia della corretta visualizzazione del documento è d'altro canto garantita dalla scelta del formato PDF/A per i documenti conservati. Questo formato possiede infatti la caratteristica intrinseca di fornire leggibilità a lungo termine oltre all'ulteriore garanzia di essere basato su specifiche pubbliche (ISO 19005-2005).

Pertanto, il Cliente, preso atto che depositare in conservazione documenti informatici in formati diversi da quelli indicati nel presente capitolo potrebbe pregiudicare la corretta visualizzazione dei documenti medesimi nonché il loro contenuto semantico, se ne assume ogni responsabilità.

12.3.5 Migrazione dei formati

Particolarmente delicata è l'operazione di migrazione dei formati, operazione, questa, che potrà essere necessaria nei casi di obsolescenza dei formati.

Il problema che si pone è quello di capire se il contenuto del file di partenza e di arrivo è rimasto inalterato. In altre parole è necessario capire se le *significant properties* si sono conservate.

E' necessario quindi impostare dei test di controllo che, inevitabilmente dovranno essere automatici. Sulla base dello specifico formato divenuto obsoleto e sulla base del nuovo formato di destinazione scelto per l'operazione di migrazione verranno scelti quanti e quali controlli sul buon esito della conversione inserire.

Le specifiche dei formati di partenza e di destinazione saranno decisive e determinanti per l'individuazione dei controlli da attuare.

12.4 Metadati da associare alle diverse tipologie di documenti

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento informatico, escluse quelle che costituiscono il contenuto del documento stesso.

I metadati riguardano principalmente, ma non esclusivamente, i modi, i tempi ed i soggetti coinvolti nel processo della formazione del documento informatico, della sua gestione e della sua conservazione.

Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento.

I metadati che seguono devono essere associati al documento dal Cliente prima del versamento in conservazione.

I metadati forniti dal Cliente restano di proprietà del Cliente medesimo.

I metadati, seppur chiaramente associati al documento informatico, possono essere gestiti indipendentemente dallo stesso.

In relazione ai diversi tipi di documenti informatici posti in conservazione, è previsto un "**set minimo**" di metadati come specificato nel capoverso seguente.

Oltre al set minimo di metadati, il Cliente potrà associare al documento informatico eventuali ulteriori metadati c.d. "*extrainfo*" che, al pari del set minimo di metadati, saranno oggetto di indicizzazione da parte del sistema. I metadati *extrainfo* dovranno essere puntualmente individuati.

12.4.1 Metadati minimi da associare a qualsiasi documento informatico

I metadati che seguono, devono, essere associati ad ogni documento informatico, a prescindere dalla specializzazione che questo assume (amministrativo, fiscale, ecc.).

Al documento informatico immodificabile, il Cliente dovrà associare i metadati che sono stati generati durante la sua formazione.

L'insieme minimo dei metadati è costituito da:
1. l'identificativo univoco e persistente;
2. il riferimento temporale (data di chiusura);
3. l'oggetto;
4. il soggetto che ha formato il documento (nome, cognome, CF)
5. l'eventuale destinatario, (nome, cognome, CF).

come meglio di seguito definiti:

01			
Informazione	**Valori Ammessi**	**Tipo dato**	**Xsd**

Identificativo univoco e persistente	Come da sistema di identificazione formalmente definito.	Alfanumerico 20 caratteri	<xs:attribute name="IDDocumento" type="xs:string" use="required"/>
Definizione			
Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione. Dublin Core raccomanda di identificare il documento per mezzo di una sequenza di caratteri alfabetici o numerici secondo un sistema di identificazione formalmente definito. Esempi di tali sistemi di identificazione includono l'Uniform Resource Identifier (URI), il Digital Object Identifier (DOI) e l'International Standard Book Number (ISBN)			

02

Informazione	Valori Ammessi	Tipo dato	xsd
Data di chiusura	Data	Data formato gg/mm/aaaa	<xs:element name="datachiusura" type="xs:date"/>
Definizione			
La data di chiusura di un documento, indica il momento nel quale il documento informatico è reso immodificabile.			

03

Informazione	Valori Ammessi	Tipo dato	xsd
Oggetto	Testo libero	Alfanumerico 100 caratteri	<xs:element name="oggettodocumento" type="xs:string />
Definizione			
Oggetto, metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura. Dublic Core prevede l'analoga proprietà "Description" che può includere ma non è limitata solo a: un riassunto analitico, un indice, un riferimento al contenuto di una rappresentazione grafica o un testo libero del contenuto.			

04

Informazione	Valori Ammessi	Tipo dato	xsd
Soggetto che ha formato il documento (Produttore)	nome: Testo libero	Alfanumerico 40 caratteri	<xs:element name="soggettoproduttore"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence> </xs:complexType> </xs:element>
	cognome: testo libero	Alfanumerico 40 caratteri	
	Codice fiscale: Codice Fiscale	Alfanumerico 16 caratteri	
Definizione			
Il soggetto che ha l'autorità e la competenza a produrre il documento informatico.			

05

Informazione	Valori Ammessi	Tipo dato	xsd
Destinatario	nome: Testo libero	Alfanumerico 40 caratteri	<xs:element name="destinatario"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element name="cognome" type="xs:string"/> <xs:element name="codicefiscale" type="xs:string"/> </xs:sequence>

	cognome: testo libero	Alfanumerico 40 caratteri	</xs:complexType> </xs:element>
	Codice fiscale: Codice Fiscale	Alfanumerico 16 caratteri	
Definizione			
Il soggetto che ha l'autorità e la competenza a ricevere il documento informatico.			

12.4.2 Metadati minimi del documento informatico amministrativo

Come noto, le pubbliche amministrazioni, ai sensi dell'articolo 40, comma 1, del CAD, formano gli originali dei propri documenti amministrativi informatici attraverso gli strumenti informatici riportati nel *Manuale* di gestione.

Detto documento amministrativo informatico, di cui all'art 23-ter del CAD, formato mediante una delle modalità di cui all'articolo 3, comma 1, del CAD, è identificato e trattato nel sistema di gestione informatica dei documenti del Cliente.

Pertanto, al documento amministrativo informatico, il Cliente deve associare, oltre ai metadati di cui al punto 12.4.1, anche l'insieme minimo dei metadati di cui all'articolo 53 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i..

Nello specifico, quindi, oltre ai metadati di cui al punto 12.4.1, al documento amministrativo informatico il Cliente dovrà associare i seguenti ulteriori metadati:

1. numero di protocollo del documento;
2. data di registrazione di protocollo;
3. mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti;
4. oggetto del documento;
5. data e protocollo del documento ricevuto, se disponibile;
6. l'impronta del documento informatico;

come meglio di seguito definiti:

01

Informazione	Valori Ammessi	Tipo dato	Xsd
numero di protocollo del documento	Come da sistema di protocollo del Cliente	Numerico	<xs:element name="numeroProtocollo" type="xs:int/>
Definizione			
Numero di Protocollo del documento ai sensi del D.P.R. 28 dicembre 2000, n. 445 (nel caso di conservazione di PEC (EML) è il numero di protocollo con cui è stata protocollate la PEC)			

02

Informazione	Valori Ammessi	Tipo dato	xsd
data di registrazione di protocollo	Data	Data formato gg/mm/aaaa	<xs:element name="dataProtocollo" type="xs:date"/>
Definizione			
Data di Protocollo del documento ai sensi del D.P.R. 28 dicembre 2000, n. 445			

03

Informazione	Valori Ammessi	Tipo dato	xsd
mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti	Testo Libero	Alfanumerico 255 caratteri	<xs:element name="soggettoMittenteProtocollo" type="xs:string /> <xs:element

			name="soggettoDestinatarioProtocollo" type="xs:string />
Definizione			
Mittente per i documenti ricevuti o il destinatario o i destinatari per i documenti spediti			

04

Informazione	Valori Ammessi	Tipo dato	xsd
Oggetto del documento	Testo libero	Alfanumerico 2000 caratteri	<xs:element name="oggettoProtocollo" type="xs:string />
Definizione			
Oggetto del Protocollo del documento ai sensi del D.P.R. 28 dicembre 2000, n. 445			

05

Informazione	Valori Ammessi	Tipo dato	xsd
data e protocollo del documento ricevuto, (se disponibile)	Come da sistema di protocollo del Cliente	Numerico	<xs:element name="numeroProtocolloRicevuto" type="xs:int/>
	Data	Data formato gg/mm/aaaa	<xs:element name="dataProtocolloRicevuto" type="xs:date"/>
Definizione			
Data e Numero di Protocollo assegnati dal mittente al documento informatico ricevuto			

06

Informazione	Valori Ammessi	Tipo dato	xsd
l'impronta del documento informatico	Hash documento	SHA-256	<xs:element name="hashDocumentoProtocollo" type="xs:string />
Definizione			
SHA-256 del documento informatico			

Oltre al set minimo di metadati, il Cliente potrà associare al documento amministrativo informatico eventuali ulteriori metadati c.d. "extrainfo" che, al pari del set minimo di metadati, saranno oggetto di indicizzazione da parte del sistema. I metadati extrainfo dovranno essere puntualmente individuati.

12.4.3 Metadati minimi del documento informatico avente rilevanza tributaria

Anche sulla scorta di quanto disposto dall'art. 3, del decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004, devono essere consentite le funzioni di ricerca e di estrazione delle informazioni dagli archivi contenenti documenti informatici rilevanti ai fini delle disposizioni tributarie in relazione ai metadati di seguito riportati:

1. cognome;
2. nome;
3. denominazione;
4. codice fiscale;
5. partita Iva;
6. data documento;
7. periodo d'imposta di riferimento;
8. tipo documento (vedi Allegato 1 "*Documenti rilevanti ai fini delle disposizioni tributarie: Elenco tipi documento*";

come meglio di seguito definiti:

01

Informazione	Valori Ammessi	Tipo dato	xsd
Cognome	Testo libero	Alfanumerico da 1 a 60 caratteri	<xsd:simpleType> <xsd:restriction base="xsd:string"> <xsd:minLength value="1"/> <xsd:maxLength value="60"/>

Manuale del sistema di Conservazione

			</xsd:restriction> </xsd:simpleType>

Definizione

Cognome del soggetto in caso di persona giuridica

02

Informazione	Valori Ammessi	Tipo dato	xsd
nome	Testo libero	Alfanumerico da 1 a 30 caratteri	<xsd:simpleType> <xsd:restriction base="xsd:string"> <xsd:minLength value="1"/> <xsd:maxLength value="30"/> </xsd:restriction> </xsd:simpleType>

Definizione

Nome del soggetto in caso di persona fisica

03

Informazione	Valori Ammessi	Tipo dato	xsd
denominazione	Testo libero	Alfanumerico da 1 a 60 caratteri	<xsd:simpleType> <xsd:restriction base="xsd:string"> <xsd:minLength value="1"/> <xsd:maxLength value="60"/> </xsd:restriction> </xsd:simpleType>

Definizione

Denominazione in caso di persona giuridica

04

Informazione	Valori Ammessi	Tipo dato	xsd
Codice fiscale	Testo formattato secondo le regole previste per il codice fiscale	Alfanumerico di 16 caratteri	<xsd:simpleType> <xsd:restriction base="xsd:string"> <xsd:pattern value="([A-Z]{6}\d{2}[A-Z][0-9A-Z]{2}[A-Z][0-9A-Z]{3}[A-Z])"/> </xsd:restriction> </xsd:simpleType>

Definizione

Codice fiscale del soggetto in caso di persona fisica

05

Informazione	Valori Ammessi	Tipo dato	xsd
Partita IVA	Numeri interi secondo le regole previste per la partita IVA	Sequenza di 11 numeri	<xsd:simpleType> <xsd:restriction base="xsd:string"> <xsd:pattern value="(\d{11})"/> </xsd:restriction> </xsd:simpleType>

Definizione

Partita iva in caso di persona giuridica

06

Informazione	Valori Ammessi	Tipo dato	xsd
Data documento	Data	Data formato gg/mm/aaaa	<xs:simpleType name="DataItaliana"> <xs:restriction base="xs:string"> <xs:pattern value="(((0[1-9] | [12][0-9] | 3[01])([-])(0[13578] | 10 | 12)([-])(\d{4})) | (([0][1-9] | [12][0-9] | 30)([-])(0[469] | 11)([-])(\d{4})) | ((0[1-9] | 1[0-9] | 2[0-8])([-

			])(02)([-])(\d{4})) | ((29)([-])(02)([-])([02468][048]00)) | ((29)([-])(02)([-])([13579][26]00)) | ((29)([-])(02)([-])([0-9][0-9][0][48])) | ((29)([-])(02)([-])([0-9][0-9][2468][048])) | ((29)([-])(02)([-])([0-9][0-9][13579][26])))"/> </xs:restriction> </xs:simpleType>
Definizione			
Data del documento			

07			
Informazione	**Valori Ammessi**	**Tipo dato**	**xsd**
Periodo d'imposta di riferimento	Da Data a Data	Data formato da gg/mm/aaaa a gg/mm/aaaa	<xs:simpleType name="DataItaliana"> <xs:restriction base="xs:string"> <xs:pattern value="(((0[1-9] | [12][0-9] | 3[01])([-])(0[13578] | 10 | 12)([-])(\d{4})) | (([0][1-9] | [12][0-9] | 30)([-])(0[469] | 11)([-])(\d{4})) | ((0[1-9] | 1[0-9] | 2[0-8])([-])(02)([-])(\d{4})) | ((29)([-])(02)([-])([02468][048]00)) | ((29)([-])(02)([-])([13579][26]00)) | ((29)([-])(02)([-])([0-9][0-9][0][48])) | ((29)([-])(02)([-])([0-9][0-9][2468][048])) | ((29)([-])(02)([-])([0-9][0-9][13579][26])))"/> </xs:restriction> </xs:simpleType>
Definizione			
Periodo di imposta di appartenenza del documento			

08			
Informazione	**Valori Ammessi**	**Tipo dato**	**xsd**
Tipo documento	Identificativo univoco del tipo di documento di appartenenza	Valore numerico compreso da 1 e 999999999999	<xsd:simpleType> <xsd:restriction base="xsd:integer"> <xsd:minInclusive value="1"/> <xsd:maxInclusive value="999999999999"/> </xsd:restriction> </xsd:simpleType>
Definizione			
Identificativo del tipo di documento di appartenenza			

Può succedere che, con riferimento alle diverse classi di documenti rilevanti ai fini delle disposizioni tributarie non sarà sempre possibile avere a disposizione tutti i metadati sopra riportati. In questi casi, in relazione ad ogni classe documentale-dovranno essere specificati i metadati minimi che dovranno essere forniti dal Cliente a corredo della classe/tipo dei documenti depositati in conservazione.

Oltre al set minimo di metadati, il Cliente potrà associare al documento amministrativo informatico eventuali ulteriori metadati c.d. "extrainfo" che, al pari del set minimo di metadati, saranno oggetto di indicizzazione da parte del sistema. I metadati extrainfo dovranno essere puntualmente individuati.

12.5 Modalità di assolvimento dell'imposta di bollo sui documenti posti in conservazione

Il Cliente è tenuto al pagamento dell'imposta di bollo eventualmente dovuta sui documenti depositati in conservazione.

Pertanto, il versamento dell'imposta dovuta dovrà essere effettuata dal Cliente nei termini previsti dall'art. 6 del DMEF 17 giugno 2014 e nei modi di cui all'art. 17 del D.Lgs. 9 luglio 1997, n. 241 e loro successive modificazioni e/o integrazioni.

Tutti i relativi e conseguenti obblighi, adempimenti e formalità per l'assolvimento dell'imposta di bollo sui documenti informatici posti in conservazione sono ad esclusivo onere e carico del Cliente, il quale dovrà attenersi alle disposizioni di legge ed ai documenti di prassi emanati ed emanandi.

Allo stesso modo, sono ad esclusivo onere e carico del Cliente tutte le comunicazioni da presentare al competente Ufficio delle entrate in forza di quanto stabilito dalla normativa regolante la conservazione digitale di documenti informatici.

13. Descrizione dei pacchetti di versamento e predisposizione del rapporto di versamento

In questo capitolo viene resa la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento nonché la descrizione della predisposizione del relativo rapporto di versamento.

Come già anticipato in altre parti del presente *Manuale*, unico responsabile del contenuto del pacchetto di versamento è il Cliente (Produttore), che deve formarlo, sottoscriverlo con firma digitale (ove previsto) e trasmetterlo al sistema di conservazione secondo le modalità operative di versamento definite nel presente *Manuale*.

Il Cliente è sempre tenuto a firmare il pacchetto di versamento con propria firma digitale.

La firma del pacchetto di versamento si considera regolarmente effettuata sottoscrivendo il "descrittore evidenze" con firma digitale in corso di validità.

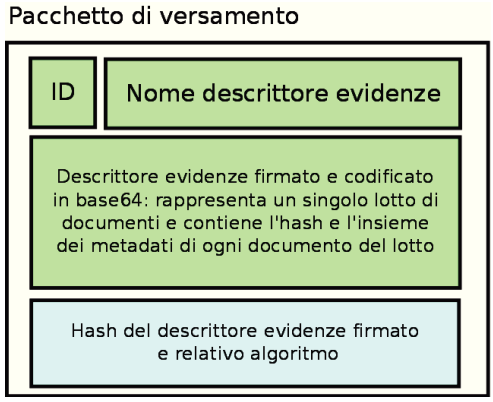
13.1 Modalità di presa in carico di uno o più pacchetti di versamento

La ricezione e presa in carico di un pacchetto di versamento segue uno schema logico di funzionamento che si articola in due fasi distinte:

1. la prima fase consiste nella ricezione del pacchetto di versamento
2. la seconda fase consiste nella ricezione dei documenti informatici descritti nel pacchetto di versamento

13.1.1 Ricezione del pacchetto di versamento

La struttura di un singolo pacchetto di versamento è la seguente:



Come illustrato nello schema, i pacchetti di versamento sono costituiti da un descrittore evidenze firmato e codificato in base64, dal relativo hash con indicazione dell'algoritmo utilizzato, dal nome del descrittore evidenze e dal relativo identificativo. Il descrittore evidenze è un pacchetto informativo che contiene la descrizione completa di un singolo lotto di documenti informatici.

E' richiesto un pacchetto di versamento distinto per ciascun lotto di documenti informatici omogenei inviato (documenti omogenei, ossia aventi la stessa classe documentale).

La funzione di ricezione dei pacchetti di versamento nel sistema di conservazione effettua i seguenti controlli:

- viene verificato che sia ricevuto un solo pacchetto di versamento per ciascuna chiamata in modo tale da garantire una granularità fine di controllo e di dettaglio degli errori e quindi, in caso di problemi, il rifiuto di un numero minore di documenti informatici;
- viene verificato che l'oggetto ricevuto sia effettivamente un pacchetto di versamento andando a verificare la corrispondenza con lo schema XSD specifico;

- viene verificato che il pacchetto di versamento ricevuto sia correttamente elaborabile andando ad estrarre dallo stesso tutte le informazioni disponibili;
- viene verificato che l'hash del descrittore evidenze contenuto nel pacchetto di versamento sia corrispondente all'hash dichiarato all'interno del medesimo pacchetto al fine di avere garanzia che tutta la trasmissione sia avvenuta correttamente e che il descrittore evidenze non sia corrotto;
- viene verificato che il nome del descrittore evidenze abbia estensione P7M;
- viene verificato che il descrittore evidenze sia effettivamente un documento firmato;
- viene verificato che tutte le firme apposte al descrittore evidenze siano valide. In particolare, per ciascun firmatario presente sono eseguiti i seguenti controlli:
  a) viene controllato l'algoritmo utilizzato per la firma;
  b) viene controllato che la chiave pubblica del firmatario possa gestire correttamente e confermare la firma;
  c) viene controllata l'integrità della firma;
  d) viene controllata la validità temporale del certificato;
  e) viene controllato che ci siano le informazioni sul firmatario (serialNumber e SubjectX500Principal);
  f) viene controllato che sia presente la data/ora di firma;
  g) viene controllato che la data e ora di firma sia contenuta in un momento di validità del certificato;
  h) viene controllata l'integrità del documento firmato;
  i) vengono controllate le CRL e CSL (liste di revoca e liste di sospensione);
- viene verificato che il descrittore evidenze sia corrispondente alle relative specifiche XSD;
- viene verificato che il descrittore evidenze sia correttamente elaborabile andando ad estrarre tutte le informazioni in esso contenute e che tutte le informazioni minime richieste siano effettivamente presenti;
- viene verificato che l'utente sia abilitato all'elaborazione del descrittore evidenze;
- viene verificato che l'utente sia abilitato all'invio dei descrittori evidenze;
- viene verificato che la classe documentale dichiarata nel descrittore evidenze abbia un corrispondente univoco nel sistema di conservazione;
- viene verificato che l'identificativo specificato nel descrittore evidenze non sia già presente nel sistema di conservazione;
- viene verificato che non sia già presente nel sistema di conservazione un descrittore evidenze relativo allo stesso periodo temporale ed alla stessa classe documentale;
- viene verificato che il periodo temporale a cui si riferisce il descrittore evidenze non sia sovrapposto ad altri descrittori evidenze già presenti nel sistema di conservazione per la stessa classe documentale;
- viene verificato che il descrittore evidenze abbia il timestamp di firma;
- viene inoltre controllato che per ciascun documento dichiarato e descritto all'interno del descrittore evidenze:
  a) tutti i metadati minimi obbligatori siano presenti e nel formato corretto;
  b) l'estensione del documento sia tra quelle ammesse per il tipo documento;
  c) il formato dichiarato sia corrispondente all'estensione del nome file.

La struttura del descrittore evidenze è specificata nell'Allegato 2. E' opportuno notare che tra le informazioni che devono essere presenti si trova anche la data limite entro cui il pacchetto di versamento deve essere chiuso in conservazione tramite firma digitale del Responsabile del servizio di conservazione e apposizione di una marca temporale.

Tutti i pacchetti di versamento che non superano anche uno solo dei controlli indicati **vengono rifiutati** dal sistema e salvati come ricezioni fallite. In entrambi i casi viene restituito al mittente un rapporto di conferma che riporta un riepilogo dei dati elaborati e l'indicazione di eventuali errori. Il rapporto contiene una dicitura specifica che indica che il rapporto di versamento sarà reso disponibile solamente nel momento in cui tutti i documenti saranno stati ricevuti, controllati e validati correttamente dal sistema di conservazione.

Il rapporto di conferma restituito a seguito dell'invio del pacchetto di versamento contiene, per ciascun documento dichiarato nel

pacchetto stesso, un identificativo che dovrà essere utilizzato in fase di invio del documento al sistema di conservazione.

13.1.2 Ricezione documenti associati ad un pacchetto di versamento

A seguito della corretta ricezione di un pacchetto di versamento il sistema di conservazione è pronto per la ricezione dei documenti informatici descritti nel pacchetto stesso. Tali documenti dovranno essere inviati singolarmente al fine di ridurre i possibili problemi legati al trasferimento degli stessi sulla rete internet.

La tecnica utilizzata per la ricezione dei documenti informatici utilizza la stessa logica del pacchetto di versamento: essa prevede infatti un pacchetto di invio documenti, ossia un oggetto che contiene al suo interno il documento codificato in base64, il relativo hash con indicazione dell'algoritmo utilizzato e l'identificativo univoco specifico del documento che è stato comunicato dal sistema di conservazione a seguito dell'invio del pacchetto di versamento. Quest'ultimo dato è particolarmente importante in quanto permette di associare il documento informatico ricevuto al corretto pacchetto di versamento.

La funzione di ricezione dei documenti informatici nel sistema di conservazione effettua i seguenti controlli:

- viene verificato che sia ricevuto un solo pacchetto di invio documenti per ciascuna chiamata in modo tale da garantire una granularità fine di controllo e di dettaglio degli errori;
- viene verificato che l'oggetto ricevuto sia effettivamente un pacchetto di invio documenti andando a verificare la corrispondenza con lo schema XSD specifico;
- viene verificato che il pacchetto di invio documenti ricevuto sia correttamente elaborabile andando ad estrarre dallo stesso tutte le informazioni disponibili;
- viene verificato che l'hash del documento informatico contenuto nel pacchetto di invio documenti sia corrispondente all'hash dichiarato all'interno del medesimo pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata;
- viene verificato che il documento informatico ricevuto sia effettivamente un documento che era atteso ossia indicato in un precedente pacchetto di versamento ricevuto, elaborato ed accettato correttamente;
- viene verificato che il lotto a cui appartiene il documento informatico sia un lotto ancora valido (non annullato);
- viene verificato che l'hash del documento informatico ricevuto sia corrispondente all'hash atteso per quel particolare documento, ossia all'hash dichiarato all'interno del pacchetto di versamento;
- viene verificato che il formato del documento informatico sia effettivamente valido e corrispondente a quanto dichiarato nel pacchetto di versamento. In tal caso i controlli eseguiti variano in funzione del formato atteso per ciascuno specifico documento. Di seguito sono elencati i controlli eseguiti per ciascun formato trattato dal sistema di conservazione di PA Digitale

  Per i file PDF/A

  - Viene controllato il magic number per verificare che il documento sia effettivamente un PDF;
  - Viene controllato che il documento contenga i metadati XMP;
  - Viene controllato che i metadati XMP siano conformi con lo standard RDF;
  - Viene controllato che sia presente la dichiarazione di conformità allo standard PDF/A-1b o PDF/A-1a all'interno dei metadati XMP.

  Per i file P7M

  - Vengono ripetuti i controlli sulle firme indicati nel paragrafo precedente.

  Per i file XML

  - Viene verificato il rispetto dello schema XSD definito per i descrittori dei file EML. Tale verifica viene applicata solamente alle classi documentali definite come PEC in quanto nelle altre tipologie di classi documenti il formato XML non è ammesso.

  Per i file EML

  Come per i file XML, tale verifica viene applicata solamente alle classi documentali definite come PEC in quanto le uniche in cui il formato EML è ammesso.

  - Viene controllata la presenza del mittente;
  - Viene controllata la presenza del destinatario;

- Viene controllata la presenza della data;
- Viene controllata la presenza di almeno un elemento tra oggetto, corpo ed allegati;
- Viene effettuata una validazione del file EML tramite apposita libreria di verifica.

Per i file in formati diversi da quelli sopra indicati

- Premesso che i formati diversi da quelli sopra indicati non sono ufficialmente supportati e che potrebbero essere i più diversi ed imprevedibili, non è possibile implementare controlli specifici e dettagliati. In questi casi, i controlli saranno effettuati esclusivamente sulla base del mime type ricavato dal nome del file in fase di ricezione del descrittore evidenze che viene confrontato con quello ottenuto dal file stesso.

In relazione a ciascun documento informatico infine:

- viene verificato che non sia già presente nel sistema di conservazione;
- viene verificato che il salvataggio avvenga correttamente all'interno del sistema di conservazione.

Tutti i documenti informatici che non superano anche uno solo dei precedenti controlli **vengono rifiutati**. In questo caso non viene salvata alcuna informazione sul sistema di conservazione ed il documento non conforme viene immediatamente eliminato. La tecnologia dell'invio singolo di ciascun documento informatico consente di evitare, in tali situazioni di errore, il reinvio di tutti i documenti del lotto permettendo di ripetere l'invio per il solo documento che ha generato l'errore.

Quando tutti i documenti di un pacchetto di versamento vengono ricevuti correttamente viene reso disponibile il rapporto di versamento sottoscritto con firma digitale.

Tale rapporto viene anche inviato via email, unitamente al relativo descrittore evidenze, all'indirizzo specificato nella configurazione.

13.2 Predisposizione dei rapporti di versamento

Il sistema di conservazione predispone, per ciascun pacchetto di versamento, un **rapporto di versamento** che viene firmato da PA Digitale. Lo schema del rapporto di versamento è illustrato nell'allegato 3.

In particolare il rapporto di versamento contiene un riepilogo dei dati ricevuti fornendo particolare evidenza ai metadati, che vengono riorganizzati e distinti in funzione della loro caratteristica di obbligatorietà. Inoltre il rapporto di versamento riporta anche l'indicazione degli identificativi che il sistema di conservazione assegna a ciascun documento. I medesimi identificativi sono contenuti anche nel rapporto di conferma e sono indispensabili per procedere all'invio dei documenti stessi al sistema di conservazione a seguito dell'accettazione di un pacchetto di versamento. E' bene notare che il rapporto di versamento viene reso disponibile solamente a seguito della completa e corretta ricezione di tutti i documenti descritti nel pacchetto di versamento.

E' opportuno inoltre ribadire una distinzione tra rapporto di conferma e rapporto di versamento. Il primo viene infatti restituito in tempo reale alla ricezione di un pacchetto di versamento e contiene l'indicazione degli identificativi univoci associati a ciascun documento. Il secondo invece, pur essendo fisicamente molto simile al primo, viene reso disponibile solamente a seguito della ricezione di tutti i documenti ed è inoltre firmato dal Responsabile del servizio di conservazione ed inviato via email ad un indirizzo specifico indicato nella configurazione del sistema di conservazione.

Nel caso in cui siano rilevati degli errori in fase di elaborazione del pacchetto di versamento, quest'ultimo viene memorizzato unitamente al rapporto di conferma restituito come risposta e contenente il dettaglio delle anomalie riscontrate. In questo caso il rapporto di versamento non viene generato e la mail di conferma non viene spedita.

E' necessario che il cliente mantenga una copia dei documenti inviati in conservazione almeno fino alla ricezione della notifica di avvenuta conservazione.

14. Descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione

In questo capitolo viene resa la descrizione del processo di conservazione nonché il trattamento dei pacchetti di archiviazione.

Utilizzo della firma digitale

Il sistema di conservazione a lungo termine ha, fra le altre, la prerogativa di conservare l'autenticità dei documenti in esso contenuti.

La preservazione della suddetta autenticità non può però basarsi *tout court* sulla firma digitale in quanto quest'ultima:
- ha una validità slegata dall'architettura e dalla struttura del sistema di conservazione;
- ha una validità limitata nel tempo e pari al certificato emesso dalla CA;
- vede la propria sicurezza legata ad algoritmi soggetti ad obsolescenza tecnologica.

E' pertanto fondamentale che il sistema di conservazione a lungo termine verifichi la validità ed il valore delle firme digitali apposte dal Cliente sui documenti informatici oggetto di conservazione.

A tale fine, il Cliente dovrà accertarsi che le firme digitali apposte sui documenti informatici inviati in conservazione:

a) siano valide al momento di sottoscrizione del documento informatico;

b) e mantengano piena validità sino al termine ultimo convenuto con PA Digitale per la "chiusura" del pacchetto di archiviazione.

Con la sottoscrizione dei pacchetti di archiviazione PA Digitale non sottoscrive il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto della normativa regolante la conservazione digitale di documenti informatici.

14.1 Processo di conservazione

Il processo di conservazione si articola nelle seguenti fasi:

FASE 1	Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico	
	Descrizione sintetica	Il sistema di conservazione riceve i pacchetti di versamento unicamente tramite chiamate web ad un indirizzo specifico soggetto ad autenticazione. Il processo di acquisizione è descritto nel dettaglio nel capitolo 13.

FASE 2	Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale di conservazione e con i formati di conservazione	
	Descrizione sintetica	Ciascun pacchetto di versamento ricevuto dal sistema di conservazione viene esaminato al fine di verificarne la coerenza con la configurazione e le impostazioni del sistema stesso. Il dettaglio dei controlli effettuati viene specificato nel capitolo 13

FASE 3	Preparazione del rapporto di conferma	
	Descrizione sintetica	Per ciascun pacchetto di versamento il sistema di conservazione predispone un rapporto di conferma che riepiloga i dati elaborati e che riporta gli eventuali errori riscontrati.

FASE 4	Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o non conformità	
	Descrizione sintetica	I pacchetti di versamento che non rispettano i requisiti della FASE 2 vengono rifiutati dal sistema di conservazione che non accetta nemmeno i relativi documenti. In questo caso il dettaglio degli errori viene riportato all'interno del rapporto di conferma.

FASE 5	Ricezione dei documenti	
	Descrizione sintetica	Per ciascun pacchetto di versamento accettato correttamente il sistema di conservazione attende l'invio dei relativi documenti.

FASE 6	Verifica dei documenti	
	Descrizione sintetica	Tutti i documenti ricevuti vengono esaminati al fine di determinare la conformità con quanto dichiarato nel pacchetto di versamento, con le specifiche del formato utilizzato e con quanto definito nel presente Manuale. I

	documenti che non superano tutti questi controlli vengono rifiutati dal sistema di conservazione.

FASE 7	**Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte**
Descrizione sintetica	Ciascun pacchetto di versamento ricevuto viene elaborato dal sistema al fine di verificare la conformità con la configurazione e le impostazioni del sistema di conservazione. Tutti i dati elaborati sono riportati all'interno del rapporto di versamento. Il rapporto di versamento viene reso disponibile solamente a seguito della corretta ricezione ed elaborazione di tutti i documenti del singolo pacchetto di versamento.

FASE 8	**Sottoscrizione del rapporto di versamento con firma digitale apposta da PA Digitale**
Descrizione sintetica	Il rapporto di versamento viene reso disponibile tramite richiesta ad un apposito indirizzo web soggetto ad autenticazione. Il rapporto di versamento viene sottoscritto automaticamente dal sistema mediante l'apposizione della firma digitale di PA Digitale.

FASE 9	**Preparazione e gestione del pacchetto di archiviazione (c.d. File di chiusura)**
Descrizione sintetica	La struttura dell'indice del pacchetto di archiviazione fa riferimento allo standard "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali", (c.d. SInCRO). E' la norma UNI 11386 dell'ottobre 2010. La norma definisce la struttura dell'insieme di dati a supporto del processo di conservazione; in particolare, la norma individua gli elementi informativi necessari alla creazione dell'indice di conservazione (il cosiddetto "**file di chiusura**") e descrivendone sia la semantica sia l'articolazione per mezzo del linguaggio formale XML. L'obiettivo della norma è quello di utilizzare una struttura-dati condivisa al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, grazie all'adozione dello Schema XML appositamente elaborato. Tale norma, pertanto, rappresenta lo standard nazionale adottato da PA Digitale nella formazione della struttura dell'indice del pacchetto di archiviazione. Per ciascun pacchetto di versamento ricevuto ed elaborato correttamente dal sistema di conservazione unitamente ai documenti in esso descritti, viene creato un corrispondente pacchetto di archiviazione.

FASE 10	**Sottoscrizione del pacchetto di archiviazione con firma digitale apposta da PA Digitale e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del pacchetto di archiviazione"**
Descrizione sintetica	Entro i termini definiti nella configurazione di ciascuna classe documentale, il sistema provvede automaticamente alla generazione dei pacchetti di archiviazione secondo la modalità definita nella FASE 9. Sui pacchetti così generati, sempre in modalità completamente automatica, il sistema appone la firma digitale di PA Digitale e, sul pacchetto di archiviazione firmato, una marca temporale.

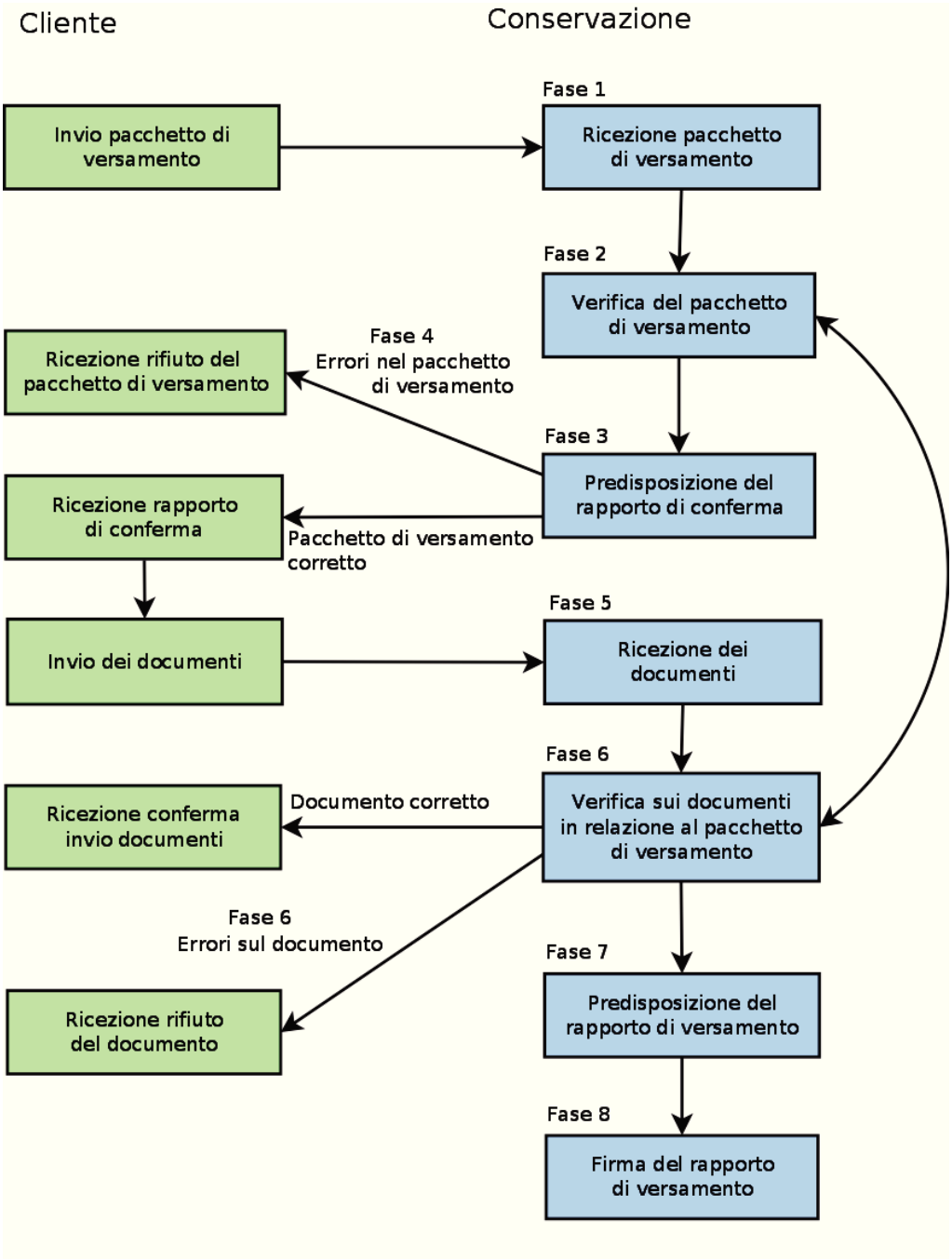
FASE 11	**Preparazione e sottoscrizione con firma digitale di PA Digitale del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente**
Descrizione sintetica	Ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione è coincidente con i pacchetti di archiviazione. Il pacchetto di distribuzione viene creato on-demand e si caratterizza per la possibilità di avere al suo interno anche i documenti. Le modalità di creazione e le tipologie dei pacchetti di distribuzione sono descritte nel dettaglio nel capitolo 16.

FASE 12	**Produzione di duplicati informatici effettuati su richiesta del Cliente in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico**
Descrizione sintetica	L'architettura completamente web del sistema di conservazione facilita notevolmente le operazioni di recupero dei documenti. Tali operazioni portano alla produzione di duplicati informatici. La descrizione dettagliata della modalità di produzione dei duplicati è riportata nel capitolo 19.1. La produzione di copie si rende necessaria solamente a seguito di obsolescenza tecnologica di un formato accettato in conservazione e determina, quale diretta conseguenza, l'avvio di una procedura di riversamento sostitutivo. Il dettaglio di tale procedura è descritto nel capitolo 19.2.

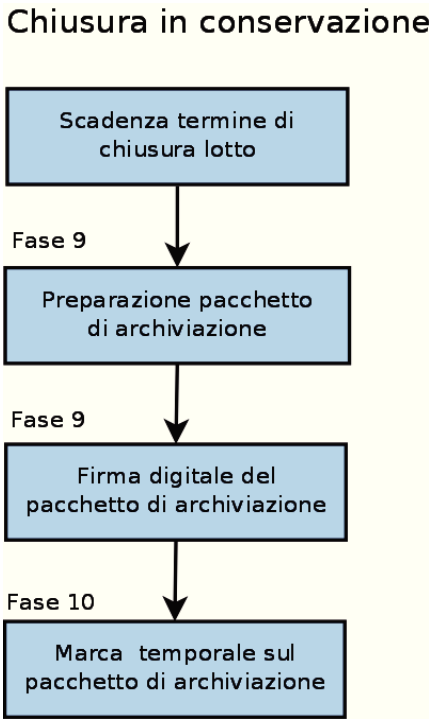
FASE 13	**Eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso**
Descrizione sintetica	Premesso che nel caso degli archivi pubblici o privati, che rivestono interesse storico-artistico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero per i beni e le attività culturali rilasciata al Cliente secondo quanto previsto dalla normativa vigente in materia, il sistema di conservazione provvederà alla cancellazione dei pacchetti di archiviazione, dei descrittori evidenze e dei documenti allo scadere del termine di cancellazione stabilito dal Cliente. Eventualmente potrà essere fornita copia di tali dati al Cliente come servizio aggiuntivo.

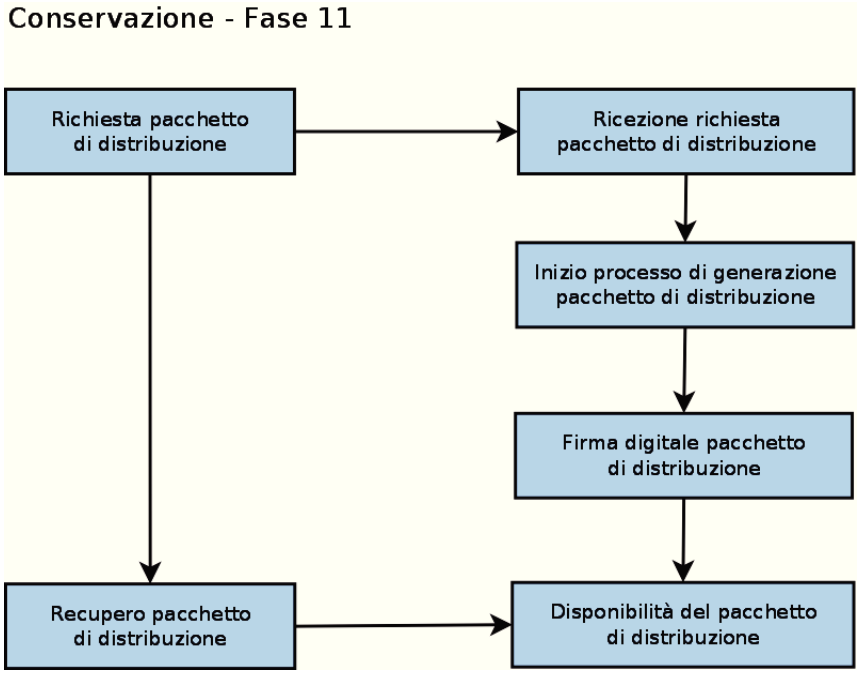
Manuale del sistema di Conservazione

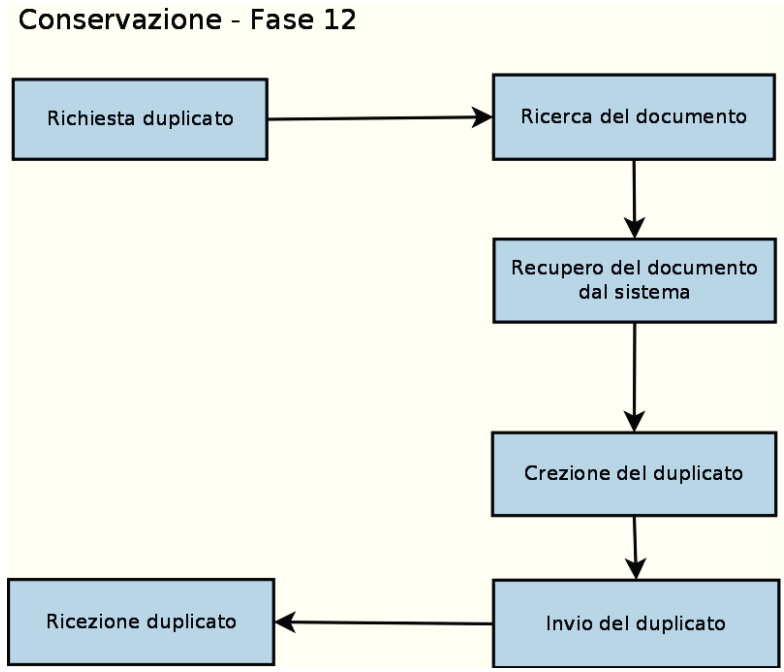
Con la seguente rappresentazione grafica del processo di conservazione sopra delineato nelle sue principali fasi, si fornisce una descrizione chiara ed intuitiva utile per una migliore comprensione dei flussi di attività:



Manuale del sistema di Conservazione







14.2 Trattamento dei pacchetti di archiviazione.

Come accennato al paragrafo precedente, al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, la struttura dell'indice del pacchetto di archiviazione viene realizzata da PA Digitale in conformità con quanto previsto dallo standard "*Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali*", (c.d. SInCRO), ossia dalla norma UNI 11386 dell'ottobre 2010.

I pacchetti di archiviazione generati dal sistema di conservazione vengono trattati al solo scopo di soddisfare i requisiti della conservazione digitale dei documenti ed al soddisfacimento delle richieste di produzione di pacchetti di distribuzione e di esibizione.

Il soddisfacimento dei requisiti della conservazione digitale implica che i pacchetti di archiviazione vengano firmati digitalmente dal responsabile del sistema di conservazione o da un suo delegato e marcati temporalmente per assicurarne la validità nel corso del tempo.

La produzione di pacchetti di distribuzione o l'esibizione di pacchetti di archiviazione comporta invece la produzione di duplicati degli stessi che sono successivamente utilizzati nei processi. Il pacchetto di archiviazione memorizzato all'interno del sistema non subisce più alcuna modifica successiva alla firma digitale e all'apposizione della marca temporale.

14.3 Evidenze di secondo livello

Il sistema di conservazione implementa la funzionalità di chiusura di secondo livello.

Con tale termine si intende un meccanismo di raggruppamento di tutti i pacchetti di archiviazione relativi ad un certo periodo temporale. Questo periodo temporale può essere o il periodo a cui fanno riferimento i documenti (tendenzialmente l'anno solare) oppure, limitatamente ai documenti fiscali, il periodo di imposta.

Tutti i pacchetti di archiviazione che ricadono nel periodo come sopra definito vengono fusi in un unico ulteriore pacchetto di archiviazione di secondo livello, che contiene tutti i riferimenti ai pacchetti di archiviazione di origine, ossia di primo livello.

Questa funzionalità consente di avere una unica entità interoperabile per ciascun tipo di documento per ciascun periodo facilitando le operazioni di gestione massiva dei documenti che si rendessero necessarie.

Il mantenimento della validità legale nel tempo dei documenti potrà a questo punto avvenire tramite aggiornamento della marca temporale apposta su tale pacchetto di archiviazione di secondo livello.

La creazione delle evidenze di secondo livello avviene dopo un configurabile numero di mesi successivi alla chiusura dell'ultimo pacchetto di archiviazione di primo livello appartenente al periodo come sopra definito.

14.4 Chiusura anticipata (in corso d'anno) del pacchetto di archiviazione.

In caso di accessi, verifiche ed ispezioni in corso d'anno, il sistema consente, dietro specifica richiesta del Cliente, l'anticipata chiusura del pacchetto di archiviazione rispetto ai tempi programmati.

15. Documenti rilevanti ai fini delle disposizioni tributarie

15.1 Caratteristiche dei documenti rilevanti ai fini delle disposizioni tributarie

In considerazione di quanto previsto dall'art. 21, co. 5, del CAD[4], i documenti informatici rilevanti ai fini delle disposizioni tributarie (di seguito, per brevità chiamati anche "**DIRT**") sono conservati nel rispetto di quanto previsto dalle disposizioni in materia, attualmente riconducibili al Decreto del 17 giugno 2014 del Ministero dell'Economia e delle Finanze e successive modificazioni ed integrazioni.

Il Cliente, pertanto, è tenuto a conoscere le disposizioni relative alla normativa regolante la conservazione digitale di documenti informatici in vigore ed a controllare l'esattezza dei risultati ottenuti con l'utilizzo del Servizio di conservazione fornito da PA Digitale.

Formazione, emissione e trasmissione dei documenti fiscalmente rilevanti

Ai fini tributari, la formazione, l'emissione, la trasmissione, la copia, la duplicazione, la riproduzione, l'esibizione, la validazione temporale e la sottoscrizione dei documenti informatici, deve avvenire a cura del Cliente nel rispetto delle regole tecniche adottate ai sensi dell'art. 71 del decreto legislativo 7 marzo 2005, n. 82, e dell'art. 21, comma 3, del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633, in materia di fatturazione elettronica.

Immodificabilità, integrità, autenticità e leggibilità dei documenti fiscalmente rilevanti

I documenti informatici rilevanti ai fini tributari devono avere le caratteristiche dell'immodificabilità, dell'integrità, dell'autenticità e della leggibilità, e devono essere utilizzati i formati previsti dal decreto legislativo 7 marzo 2005, n. 82 e dai decreti emanati ai sensi dell'art. 71 del predetto decreto legislativo nonché quelli individuati nel presente Manuale. Detti formati devono essere idonei a garantire l'integrità, l'accesso e la leggibilità nel tempo del documento informatico.

Pertanto, tutti i DIRT che vengono versati in conservazione devono essere statici ed immodificabili, ossia privi di qualsiasi agente di alterazione.

Il Cliente dovrà assicurarsi e garantire che i DIRT che versa in conservazione abbiano le suddette caratteristiche sin dalla loro formazione e, in ogni caso, prima che siano depositati nel sistema di conservazione.

A tale fine, i DIRT, salvo diverso e circostanziato accordo col Responsabile del servizio di conservazione, devono essere prodotti nel formato PDF/A in conformità a quanto previsto nel capitolo 12 del presente *Manuale*.

Ordine cronologico e non soluzione di continuità per periodo di imposta

Posto che l'art. 3 del Decreto MEF 17.06.2014 stabilisce che i documenti informatici sono conservati in modo tale che siano rispettate le norme del codice civile, le disposizioni del codice dell'amministrazione digitale e delle relative regole tecniche e le altre norme tributarie riguardanti la corretta tenuta della contabilità, il Cliente deve farsi carico di versare in conservazione i propri documenti informatici assicurando, ove necessario e/o previsto dalle norme e/o dai principi contabili nazionali, l'ordine cronologico dei medesimi e senza che vi sia soluzione di continuità in relazione a ciascun periodo d'imposta o anno solare.

In altre parole, gli obblighi richiamati dall'art. 3 del DM 17.06.2014, essendo riferibili a norme riguardanti la corretta tenuta della contabilità, sono posti a completo ed esclusivo carico del Cliente.

Ciò comporta che il Cliente, nell'eseguire il versamento in conservazione dei DIRT, dovrà rispettare le regole di corretta tenuta della contabilità e procedere secondo regole uniformi, nell'ambito del medesimo periodo d'imposta o anno solare.

Funzioni di ricerca
PA Digitale non fornisce, in fase di formazione dei documenti, alcuna funzionalità di indicizzazione degli stessi che, quindi, è posta ad esclusivo carico e sotto la responsabilità del Cliente che dovrà associare ad ogni documento versato in conservazione i corrispondenti metadati.

[4] Art. 21, co. 5 del CAD: "Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.";

Pertanto, è il Sistema di Gestione documentale del Cliente che deve assicurare l'indicizzazione dei DIRT in merito al formato, allo stato, alle caratteristiche (fiscali) di ogni singolo DIRT ed ai metadati "minimi" previsti dal Decreto MEF del 17 giugno 2014 (nome, cognome, denominazione, codice fiscale, partita IVA, data e associazioni logiche di questi) e dal presente *Manuale* nel capitolo 12.

Per sfruttare appieno le potenzialità del processo di conservazione dei DIRT non è sufficiente attenersi alle regole tecniche previste dalla norma, ma è necessario che il Cliente si attenga scrupolosamente ad un progettato ciclo di gestione dei DIRT, con il fine di predisporli ed organizzarli sin dalla loro formazione in modo tale da massimizzare la facilità del loro reperimento, prestando particolare attenzione alla fase di classificazione ed organizzazione. Dal puntuale svolgimento di quanto sopra dipende la facilità del loro reperimento.

A tale fine, è necessario che, in relazione ad ogni classe documentale, il Cliente associ ad ogni DIRT i metadati previsti dal presente *Manuale* necessari per adempiere agli obblighi imposti dalle disposizioni in materia.

Il sistema di conservazione garantisce, come riportato nel capitolo 16, le necessarie funzioni di ricerca dei DIRT conservati sulla scorta dei metadati ad essi associati.

Classificazione dei DIRT secondo aggregazioni per "Tipo documento"
Il Sistema di Gestione documentale del Cliente, oltre ad assicurare il formato, l'indicizzazione, l'apposizione del riferimento temporale, la sottoscrizione con firma digitale di ogni DIRT dallo stesso prodotto, deve provvedere altresì alla classificazione per tipologia di documento in conformità a quanto previsto dall'Allegato 1 al presente Manuale.

15.1.1 Modalità di assolvimento dell'imposta di bollo sui DIRT

Come precisato nel precedente capitolo 12, l'imposta di bollo nonché tutti gli obblighi e le formalità per l'assolvimento dell'imposta sui DIRT, qualora dovuta, sono ad esclusivo onere e carico del Cliente, il quale dovrà attenersi alle disposizioni di legge (art. 6, del DMEF del 17 giugno 2014) ed ai documenti di prassi emanati ed emanandi.

15.2 Trattamento dei pacchetti di archiviazione contenenti documenti rilevanti ai fini delle disposizioni tributarie

Il processo di conservazione dei DIRT è effettuato nel rispetto delle regole di cui al DMEF del 17 giugno 2014 e successive modificazioni ed integrazioni.

Nello specifico, il processo di conservazione, prende avvio con il versamento in conservazione del pacchetto di versamento prodotto dal Cliente e termina (ergo, "*viene chiuso in conservazione*") termina con l'apposizione di una marca temporale sul pacchetto di archiviazione.

Con riferimento ai DIRT, il processo di conservazione, in forza di quanto stabilito dall'art. 3 del DMEF del 17 giugno 2014, è effettuato entro il termine previsto dall'art. 7, comma 4-ter, del decreto-legge 10 giugno 1994, n. 357, convertito con modificazioni dalla legge 4 agosto 1994, n. 489 e s.m.i..

Pertanto, il Cliente dovrà provvedere a trasmettere a PA Digitale il pacchetto di versamento, contenente i DIRT da sottoporre a conservazione, rigorosamente entro i termini stabiliti; tale termine è necessario a PA Digitale per "chiudere" in conservazione il pacchetto di archiviazione entro i termini perentori previsti dalla legge.

16. Processo di esibizione e di esportazione dal sistema di conservazione e produzione del pacchetto di distribuzione

In questo capitolo vengono illustrate le modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione.

16.1 Modalità di svolgimento del processo di esibizione

L'esibizione dei documenti conservati può avvenire secondo due modalità:

1. Esibizione dal sistema di conservazione;
2. Esibizione dal sistema Urbi.

16.1.1 Esibizione dal sistema di conservazione

Una apposita funzione permette di effettuare la ricerca del documento di cui è richiesta l'esibizione sulla base della classe documentale, del nome del documento, del periodo di appartenenza inteso come anno, della data del documento e del valore di tutti i metadati che sono stati definiti per la classe documentale specifica.

Una volta individuato il documento informatico di interesse apposite funzioni consentono di scaricare dal sistema di conservazione il documento stesso, il pacchetto di archiviazione, il pacchetto di archiviazione firmato e la marca temporale apposta sul pacchetto di archiviazione firmato. Sono inoltre disponibili anche il pacchetto di versamento, il descrittore evidenze firmato in esso contenuto, il descrittore evidenze estratto dalla busta di firma ed il rapporto di versamento legato al pacchetto di versamento.

Una funzione di verifica permette di controllare rapidamente che l'hash calcolato sul documento informatico sia effettivamente corrispondente all'hash memorizzato nel sistema ed utilizzato per il pacchetto di archiviazione.

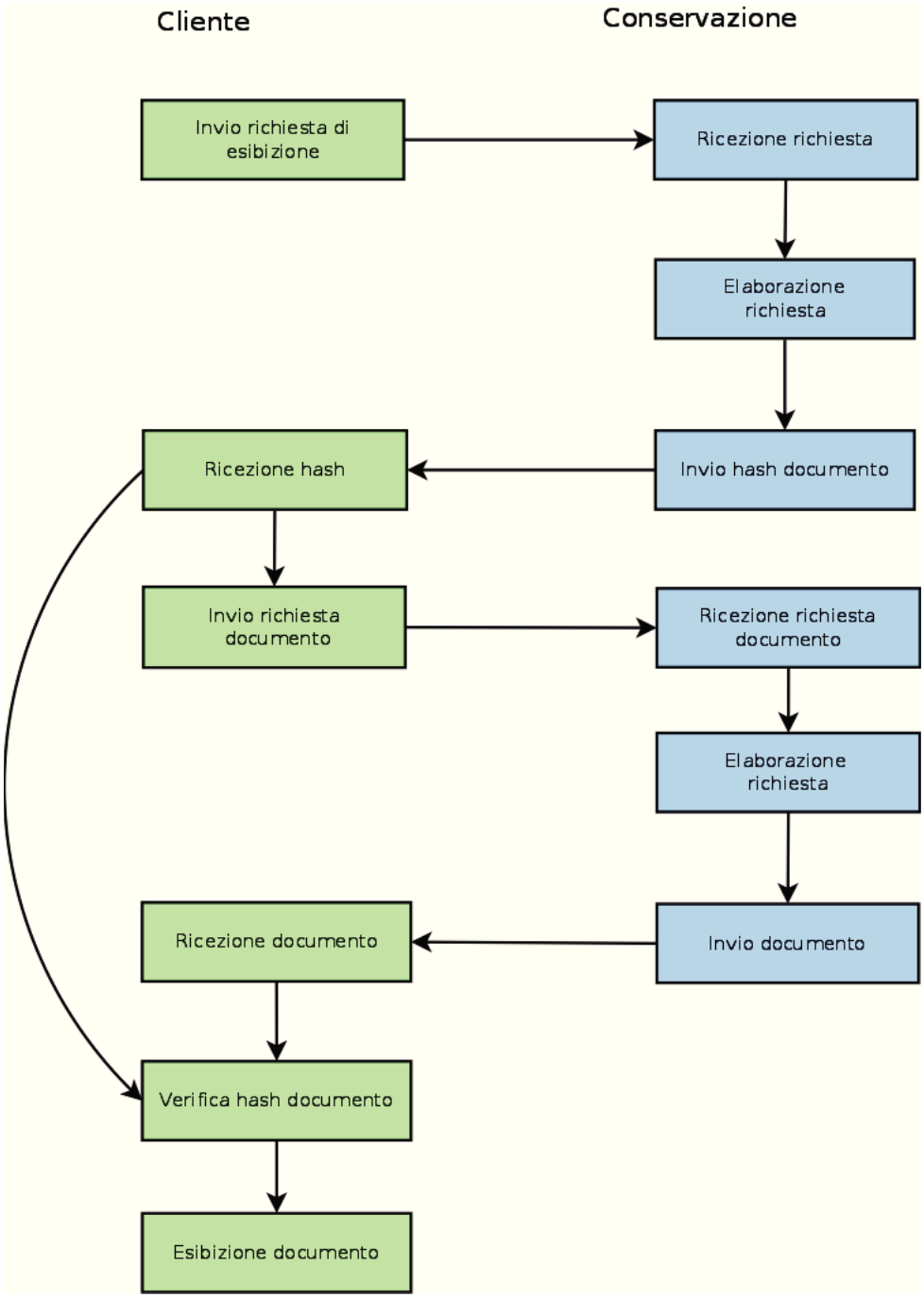
16.1.2 Esibizione dal sistema Urbi

Anche nel caso di ambiente Urbi apposite funzioni di ricerca messe a disposizione dal sistema documentale o dallo specifico applicativo, permettono di individuare il documento informatico di interesse. Il sistema permetterà quindi di scaricare il documento conservato, il pacchetto di archiviazione, il pacchetto di archiviazione firmato e la marca temporale.

Questa operazione di scaricamento avviene tramite un processo composto da due fasi in cui nella prima fase Urbi richiede il documento al sistema di conservazione che risponde riportando l'hash del documento ed il nome dello stesso, nella seconda fase Urbi richiede il documento fisico al sistema di conservazione che risponde inviando il file effettivo. Urbi calcola quindi l'hash sul documento ricevuto e verifica che sia effettivamente corrispondente con quello atteso ricevuto in precedenza.

Lo schema seguente illustra questa procedura:

Manuale del sistema di Conservazione



Una apposita funzione consente inoltre di effettuare la comparazione, per ogni documento, tra gli hash memorizzati nel database del sistema documentale, calcolati sui documenti informatici memorizzati sul sistema documentale, memorizzati sul database del sistema di conservazione, calcolati sui documenti informatici memorizzati all'interno del sistema di conservazione. Questo controllo incrociato consente di avere la certezza dell'integrità sul documento in quanto viene verificata la corrispondenza tra il documento informatico nel sistema Urbi ed il documento informatico nel sistema di conservazione sia in termini di file che in termini di hash memorizzati nel sistema ed associati al file stesso.

16.2 Esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;

16.2.1 Tipologie di pacchetti di distribuzione

La produzione dei pacchetti di distribuzione può avvenire tramite richiesta pervenuta dal sistema Urbi, oppure tramite avvio della procedura direttamente dal sistema di conservazione.

I pacchetti di distribuzione richiedibili possono essere di differenti tipologie sulla base delle specifiche esigenze.

In particolare sono disponibili:

a) il pacchetto di distribuzione non firmato e senza documenti informatici;

b) il pacchetto di distribuzione **firmato** e senza documenti informatici;

c) il pacchetto di distribuzione non firmato con documenti informatici;

d) il pacchetto di distribuzione **firmato** con documenti informatici;

e) il pacchetto di distribuzione non firmato con un singolo specifico documento informatico;

f) il pacchetto di distribuzione **firmato** con un singolo documento informatico.

Come previsto dall'art. 7, co. 1 lett. d) del DPCM 3.12.2013, nei casi di cui ai precedenti punti sub b), d) ed f) PA Digitale genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata.

All'interno di ciascun pacchetto di distribuzione sono sempre contenuti:

- il pacchetto di archiviazione;
- il pacchetto di archiviazione firmato da PA Digitale;
- la marca temporale;
- i documenti informatici (ove previsto).

Tutti i pacchetti di distribuzione sono costruiti come file zip e l'eventuale firma sul pacchetto è apposta da PA Digitale.

Ove non specificato la generazione di ciascun pacchetto di distribuzione corrisponde sempre al rispettivo pacchetto di archiviazione e pacchetto di versamento.

16.2.2 Richiesta pacchetti di distribuzione tramite Urbi

La richiesta dei pacchetti di distribuzione tramite Urbi prevede come prima fase la ricerca del documento informatico di interesse tramite le apposite funzioni messe a disposizione dell'utente dal sistema Urbi.

Individuato con certezza il documento informatico, una procedura consente di effettuare una richiesta di produzione di pacchetti di distribuzione.

In funzione della configurazione del sistema di conservazione e del tipo di pacchetto richiesto, il pacchetto stesso potrebbe essere generato in tempo reale e restituito immediatamente all'utente Urbi, oppure in alternativa potrebbe essere avviato un processo per la generazione del pacchetto. In tal caso il personale addetto alla gestione del sistema di conservazione viene avvisato della richiesta inoltrata e non appena il processo di generazione si sarà concluso provvederà ad avvisare l'utente Urbi ed a rendere disponibile il pacchetto per lo scaricamento.

Nel caso di pacchetti resi disponibili immediatamente la comunicazione avviene secondo la logica della doppia chiamata al sistema di conservazione descritta nei paragrafi precedenti che garantisce la correttezza della comunicazione.

I pacchetti di distribuzione che vengono generati e restituiti in tempo reale alle richieste provenienti dal sistema Urbi vengono successivamente eliminati dal sistema di conservazione.

16.2.3 Richiesta pacchetti di distribuzione da sistema di conservazione

Anche nel caso di richiesta di pacchetti di distribuzione dal sistema di conservazione la fase iniziale è l'individuazione del documento informatico di interesse tramite le apposite funzioni di ricerca.

Una volta trovato il documento vengono rese disponibili funzionalità che consentono di avviare i processi di generazione dei pacchetti di distribuzione della tipologia richiesta. In questa situazione i risultati dei processi di generazione vengono resi disponibili per il download direttamente dal sistema di conservazione stesso nel quale resteranno memorizzati per successivi utilizzi.

Nel caso di pacchetti di distribuzione richiesti dal sistema di conservazione stesso non è disponibile la tipologia di pacchetti di distribuzione che non prevede al suo interno i documenti informatici.

17. Descrizione del sistema di conservazione

In questo capitolo viene descritto il sistema di conservazione, comprensivo di tutte le sue componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime

17.1 Descrizione del sistema di conservazione

Il sistema di conservazione assicura, dalla presa in carico dal produttore e fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, dei seguenti oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità:

a. **documenti informatici** con i metadati ad essi associati di cui al punto 12.4.1 del presente *Manuale*;
b. **documenti amministrativi informatici** con i metadati ad essi associati di cui al punto 12.4.2 del presente *Manuale*;
c. **documenti informatici rilevanti ai fini delle disposizioni tributarie** con i metadati ad essi associati di cui al punto 12.4.3 del presente *Manuale*;

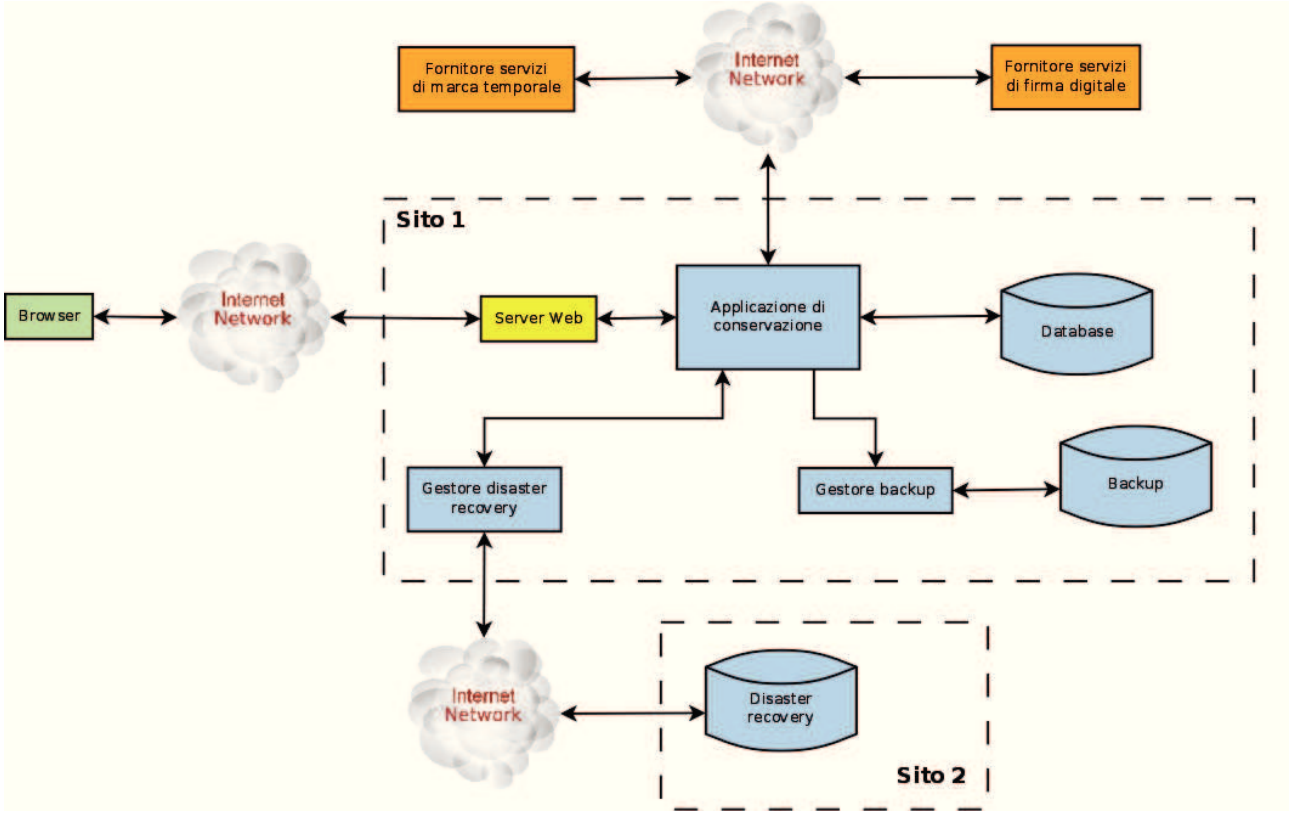
17.2 Componenti tecnologiche del sistema di conservazione

Il sistema di conservazione ha una architettura tecnologica costituita dai seguenti blocchi funzionali:

1. **Il browser dell'utente che utilizza il servizio di conservazione:** è il componente primario ed essenziale per interagire con il sistema. E' considerato browser anche il sistema Urbi che si interfaccia per l'esecuzione delle operazioni automatizzate.
2. **Server web:** è il server che ospita ed esegue l'applicazione, che si occupa della gestione degli accessi, del controllo del traffico, del filtraggio di eventuali richieste anomale, del controllo delle prestazioni, ecc.
3. **Applicazione di conservazione e database:** è il programma di conservazione digitale che sfrutta un database per la memorizzazione delle informazioni.
4. **Fornitore servizi di firma digitale:** è l'ente certificato con cui è stata effettuata l'integrazione al fine di ottenere la possibilità di apporre automaticamente le firme digitali.
5. **Fornitore servizi di marca temporale:** è l'ente certificato cui è stata effettuata l'integrazione al fine di ottenere la possibilità di apporre automaticamente le marche temporali.
6. **Gestore bakcup:** è il sistema automatico di salvataggio periodico dei dati del sistema di conservazione al fine di garantire la salvaguardia delle informazioni.
7. **Gestore disaster recovery:** è il sistema automatico di salvataggio periodico dei dati del sistema di conservazione in un sito differente da quello primario. Questo permette di avere garanzie di integrità dei dati anche in caso di eventi catastrofici che investano il sito primario.
8. **Rete internet:** è la rete che permette l'accesso al sistema di conservazione e che consente l'interconnessione tra loro delle diverse componenti.

Manuale del sistema di Conservazione

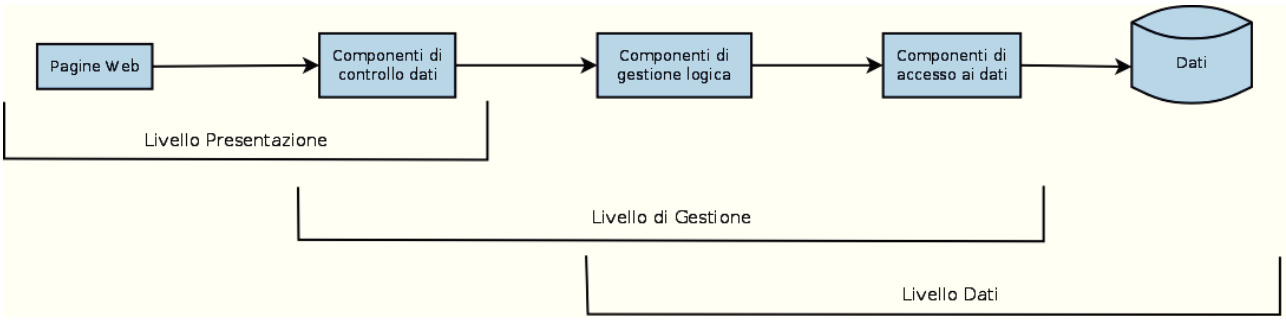
Il legame e le interazioni tra i componenti descritti sono illustrati nello schema seguente:



Manuale del sistema di Conservazione

17.3 Componenti fisiche e logiche del sistema di conservazione

La strutturazione logica dell'applicativo di conservazione prevede la presenza una architettura a tre livelli illustrata nel diagramma seguente:



- Il **livello di presentazione** costituisce l'interfaccia tramite la quale l'utente, o il sistema Urbi, è in grado di interagire con il sistema di conservazione.
- Il **livello di gestione** si occupa di definire e gestire tutte le logiche di funzionamento del sistema.
- Il **livello dati** è invece responsabile dell'accesso fisico ai dati del sistema.

17.4 Procedure di gestione e di evoluzione delle componenti del sistema di conservazione

L'evoluzione del sistema di conservazione viene gestita sotto tre differenti punti di vista:

a. **evoluzione dell'applicazione di conservazione:** il software di gestione della conservazione subisce continue evoluzioni volte all'implementazione di nuove funzionalità, al miglioramento di funzioni esistenti, al miglioramento dell'usabilità, al miglioramento delle prestazioni ed anche alla risoluzione di eventuali anomalie. L'evoluzione della conservazione prevede anche il monitoraggio degli sviluppi effettuati sulle librerie utilizzate e l'aggiornamento delle stesse in caso di problemi di sicurezza o di significativi miglioramenti sulle funzionalità o sulle prestazioni.

b. **evoluzione del software di sistema**: i server su cui è ospitato l'applicativo di conservazione, gli application server e tutti i componenti si sistema utilizzati dall'applicativo, sono costantemente aggiornati per mantenere alti livelli di sicurezza.

c. **evoluzione dell'hardware:** i server sono costantemente controllati anche dal punto di vista dell'hardware. Questo implica attività di monitoraggio delle condizioni fisiche dei server e dei loro componenti per l'individuazione di eventuali condizioni di fault. Il monitoraggio riguarda inoltre il carico di lavoro a cui i server sono sottoposti. Nel caso in cui fossero raggiunti livelli di allerta, viene pianificata una espansione dell'hardware che è resa possibile dall'architettura fortemente scalabile implementata.

d. Periodicamente vengono valutate le statistiche di sfruttamento ed utilizzo delle risorse e viene valutata l'adeguatezza del sistema definendo gli eventuali interventi che si rendessero necessari a garantire un buon livello di prestazioni ed affidabilità.

18. Procedure di monitoraggio della funzionalità del sistema di conservazione

In questo capitolo si riporta la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie.

Le funzionalità di controllo del buon funzionamento possono essere riassunte nei seguenti punti che saranno descritti in dettaglio nel successivo paragrafo:

- Funzioni di monitoraggio complessivo sulle operazioni pianificate
- Sistema di log ed errori
- Invio di email
- Sistema di tracciamento con revisioni
- Controllo dei server

18.1 Procedure di monitoraggio della funzionalità del sistema di conservazione

PA Digitale assicura la verifica periodica del funzionamento, nel tempo, del sistema di conservazione.

Il controllo della buona funzionalità del sistema di conservazione avviene tramite apposite funzionalità di monitoraggio del software. Esse mostrano l'esito delle operazioni automatiche eseguite sul sistema di conservazione come la generazione dei pacchetti di archiviazione, la chiusura dei pacchetti di archiviazione e la verifica dell'integrità degli archivi.

Unitamente all'esito delle predette operazioni vengono controllati anche i log delle operazioni medesime al fine di avere maggiore certezza di quanto effettivamente eseguito dal sistema di conservazione. Tutte queste informazioni sono controllate per ciascun singolo cliente.

La funzione di monitoraggio permette inoltre di controllare anche gli eventuali errori che si dovessero verificare. A questo proposito il meccanismo di gestione prevede che tutti gli errori siano memorizzati a livello di singolo cliente in modo tale da avere un controllo fine del processo e di isolare meglio eventuali problemi legati ai dati. Il monitoraggio consente quindi di visualizzare questi errori. Errori che determinano anche l'invio di email informative circa l'errore stesso ad indirizzi specifici dedicati e definiti nella configurazione del sistema. Nel caso in cui l'errore sia talmente grave da non poter essere memorizzato riferito al singolo cliente, viene comunque memorizzato in un secondo livello di gestione errori che è comune a tutti i clienti ed in tal caso l'email informativa viene spedita ad un indirizzo anch'esso comune a tutti i clienti e deputato alla gestione dell'intero sistema.

Il monitoraggio avviene inoltre anche a livello di processi di elaborazione sul sistema di conservazione. Questo permette di individuare eventuali casi di processi bloccati che potrebbero inficiare il funzionamento del sistema stesso.

Un ultimo controllo del buon funzionamento del sistema può avvenire tramite il monitoraggio delle tracciature che vengono effettuate a livello di database. Tutte le operazioni eseguite determinano infatti la creazione di apposite revisioni che registrano tutte le modifiche intervenute sul sistema permettendo eventualmente di ripristinare i dati a seguito di situazioni anomale.

Il controllo del buon funzionamento del sistema di conservazione avviene infine anche controllando il buon funzionamento fisico degli apparati hardware nonché del software di base dei server che ospitano il servizio. Questo comporta anche il controllo dei file di log dei server che ospitano l'applicativo di conservazione.

La verifica di buona funzionalità può avvenire anche a livello utente. Infatti è previsto l'invio di email informative a seguito delle operazioni di generazione automatica dei pacchetti di archiviazione e di ricezione dei pacchetti di versamento.

18.2 Verifiche sull'integrità degli archivi

PA Digitale assicura la verifica periodica, **con cadenza non superiore all'anno**, dell'integrità degli archivi e della leggibilità degli stessi; assicura, inoltre, agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Il sistema di conservazione esegue periodicamente ed automaticamente le operazioni di controllo dell'integrità degli archivi. Tali operazioni vengono eseguite solo su una certa percentuale dell'archivio che viene definita nella configurazione del sistema di conservazione.

Questa percentuale di controllo viene applicata a livello di descrittore evidenze, documenti, pacchetti di archiviazione, pacchetti di archiviazione firmati e marche temporali e per ciascuna di queste categorie la scelta degli oggetti da controllare avviene

casualmente fino al raggiungimento della percentuale configurata.

Il controllo eseguito è di due tipologie:

- **controllo di leggibilità:** consiste nel verificare che i singoli bit degli oggetti siano tutti correttamente leggibili. Questo fornisce garanzia del buono stato del supporto di memorizzazione.
- **controllo di integrità:** consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema. Questo fornisce una ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

La combinazione dei due tipi di controllo descritti non fornisce però garanzia di poter visualizzare correttamente il documento e che lo stesso sia effettivamente intellegibile dall'uomo.

Infatti questa garanzia non può essere fornita senza entrare nel merito del documento stesso. La garanzia della corretta visualizzazione del documento è d'altro canto garantita dalla scelta del formato PDF/A per i documenti conservati. Questo formato possiede infatti la caratteristica intrinseca di fornire leggibilità a lungo termine oltre all'ulteriore garanzia di essere basato su specifiche pubbliche (ISO 19005-2005).

18.2.1 Pianificazione delle verifiche periodiche da effettuare

Il controllo periodico dell'integrità degli archivi avviene con una frequenza che è liberamente configurabile da uno a sessanta mesi a partire dalla data di avvio del servizio di conservazione. Anche la percentuale di oggetti dell'archivio da verificare può essere definita liberamente in un range che varia tra l'uno ed il cinquanta per cento del totale.

18.2.2 Mantenimento della firma per il periodo di conservazione

Il sistema di conservazione si avvale di un fornitore terzo (Certificatore accreditato) per le attività di firma digitale e di marcatura temporale. Questo fornitore garantisce che gli elaboratori che offrono il servizio di marcatura temporale e di firma digitale sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali. Non è infatti consentito l'accesso e la permanenza di una sola persona. I locali ove si svolgono le procedure di firma e marca sono dotati di sofisticati impianti di allarme, telecamere, microfoni, rilevatori di movimento (che si attivano soltanto quando nessuna persona vi è presente), al fine di controllare ogni movimento all'interno degli stessi.

Sicurezza fisica
Il sistema di validazione temporale si basa su dei server web di Front-end che gestiscono le transazioni con i client, l'autenticazione, l'accounting e l'archiviazione delle marche temporali e dei server di Back-end che si occupano della creazione delle marche temporali e della gestione degli apparati di acquisizione e sincronizzazione del riferimento temporale. I server del sistema di validazione temporale sono ospitati in sale tecniche ad accesso controllato attraverso badge e/o fattore biometrico. Solo il personale autorizzato può accedere a tali sale. Questi ambienti, inoltre, sono protetti da allagamenti ed incendi mediante appositi presidi (sensori, spruzzatori, condizionamento, etc) e gli elaboratori sono alimentati con linea elettrica preferenziale, sorretta da gruppo di continuità.

Sicurezza logica
I server di Front-end e di Back-end del sistema di firma digitale e marcatura temporale dialogano tra loro attraverso protocolli di comunicazioni sicuri e possono essere attivati solo da operatori autorizzati. In particolare, i server di Back-end firmano le marche temporali mediante un dispositivo crittografico hardware (o "dispositivo di firma") di altissima qualità e sicurezza. L'algoritmo di sottoscrizione utilizzato è RSA con chiave di lunghezza 2048 bit ed usata esclusivamente a scopo di marcatura temporale. La coppia di chiavi RSA è generata all'interno del dispositivo di firma. La chiave privata della coppia è usata all'interno del dispositivo di firma. Il dispositivo di firma può essere attivato solo da un operatore appositamente autorizzato e dotato della necessaria parola-chiave.

18.3 Soluzioni adottate in caso di anomalie

Il sistema di conservazione è strutturato in modo tale da eseguire la maggior parte delle attività in modo automatico, senza necessità di un presidio umano, e con misure atte a ridurre al minimo il possibile insorgere di situazione di anomalia. In tali situazioni, che possono comunque verificarsi, PA Digitale è in grado di intervenire con le figure idonee a risolvere il problema riscontrato.

La procedura adottata prevede una prima analisi della situazione da parte dell'assistenza clienti del post vendita che cerca, insieme al cliente, di individuare il problema, possibilmente riuscendo a riprodurre l'anomalia sui sistemi di test di PA Digitale.

Individuata l'anomalia, questa viene inoltrata agli analisti del reparto di produzione che effettuano controlli più approfonditi, andando ad analizzare i dati forniti e studiando una possibile soluzione che viene successivamente affidata agli sviluppatori. Questi ultimi

procedono all'implementazione delle opportune correzioni che risolvano il problema, comunicando quindi al post vendita i dati di quanto realizzato e che saranno poi comunicati al cliente.

Nel caso in cui sia PA Digitale stessa ad individuare situazioni anomale la procedura seguita sarà la medesima, ossia analisi, implementazione e rilascio della correzione.

19. Procedure per la produzione di duplicati o copie

In questo capitolo vengono descritte le procedure adottate per la produzione di duplicati o copie.

19.1 Produzione di duplicati

La produzione di duplicati informatici dei documenti conservati può avvenire a seguito di una richiesta proveniente dall'ambiente Urbi oppure da una richiesta effettuata direttamente all'interno del sistema di conservazione.

In entrambe le situazioni, il passo iniziale consiste nella ricerca del documento informatico di interesse sfruttando le funzionalità messe a disposizione sia dal sistema di conservazione che dal sistema Urbi. Individuato il documento informatico di interesse, una apposita funzione consente di effettuare il download del documento stesso, producendo quindi un duplicato.

Il documento informatico richiesto viene infatti estratto dal sistema in formato binario controllando che l'estrazione sia eseguita senza errori e quindi inviato all'utente che ne ha fatto richiesta.

19.2 Produzione di copie

La produzione di copie si rende necessaria solamente a seguito di obsolescenza tecnologica di un formato accettato in conservazione e determina, quale diretta conseguenza, l'avvio di una procedura di riversamento sostitutivo.

In tale contesto PA Digitale, previo perfezionamento di specifico accordo scritto (dove saranno concordati ruoli, modalità, tempi e corrispettivi), si renderà disponibile a collaborare col Cliente nell'effettuare le copie informatiche dei documenti informatici depositati in conservazione secondo quanto stabilito dalle regole tecniche vigenti.

20. Tempi di scarto o di trasferimento in conservazione dei documenti

In questo capitolo si riporta la descrizione dei tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel *Manuale* di gestione.

20.1 Scarto dei documenti informatici conservati

Relativamente alla possibilità di scarto, ossia di eliminare legalmente i documenti informatici conservati digitalmente a norma di legge, occorre distinguere preliminarmente la tipologia dei soggetti (Clienti) produttori, pubblici o privati.

Va preliminarmente osservato, che in ambito privato, con l'eccezione degli archivi "dichiarati di notevole interesse storico", che divengono archivi specificatamente disciplinati, l'obbligo di conservazione dei documenti è disciplinato dall'ordinamento vigente e, in particolare, dai termini prescrittivi del codice civile nonché, per le scritture contabili, le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti, segnatamente dall'art. 2220 del c.c., il quale stabilisce l'obbligo di conservazione di dieci anni dalla data dell'ultima registrazione.

In ambito pubblico, oltre alle prescrizioni civilistiche, si rendono applicabili una serie di altre disposizioni specifiche, una su tutte, il Codice dei beni culturali e ambientali, emanato con il D.Lgs. 10 gennaio 2004, n. 42.

Inoltre, con riferimento agli archivi pubblici o privati, che rivestono interesse storico-artistico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero per i beni e le attività culturali rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

Pertanto, alla luce di quanto sopra sinteticamente rappresentato, PA Digitale procederà allo scarto dei pacchetti di archiviazione del Cliente dal sistema di conservazione solo qualora ciò sia stato esplicitamente richiesto dal Cliente, dandone comunque preventiva informativa a mezzo PEC.

21. Richiesta della presenza del pubblico ufficiale

PA Digitale richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento assicurando allo stesso l'assistenza tecnica necessaria 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 dal Cliente; pertanto, qualora il Cliente non se ne sia fatto carico direttamente, PA Digitale 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.

22. Normative in vigore nei luoghi dove sono conservati i documenti

I documenti informatici sono conservati in Italia; pertanto al sistema di conservazione si rendono applicabili le norme Italiane.

23. Termini e condizioni generali

Il presente capitolo presenta i termini e le condizioni generali del presente *Manuale* di conservazione che non sono stati trattati nelle altre sezioni.

23.1 Nullità o inapplicabilità di clausole

Se una qualsivoglia disposizioni del presente *Manuale*, o relativa applicazione, risulti per qualsiasi motivo o in qualunque misura nulla o inapplicabile, il resto del presente *Manuale* (così come l'applicazione della disposizione invalida o inapplicabile ad altre persone o in altre circostanze) rimarrà valido e la disposizione nulla o inapplicabile sarà interpretata nel modo più vicino possibile agli intenti delle parti.

23.2 Interpretazione

Salvo disposizioni diverse, questo *Manuale* dovrà essere interpretato in conformità alla correttezza, buona fede ed a quanto ragionevole anche in virtù degli usi commerciali nazionali.

23.3 Nessuna rinuncia

La mancata applicazione da parte del Cliente di una delle disposizioni di cui al presente *Manuale* non sarà ritenuta rinuncia a future applicazioni di suddetta disposizione o di qualsiasi altra disposizione.

23.4 Comunicazioni

Qualora PA Digitale o il Cliente desideri o sia tenuta ad effettuare delle comunicazioni, domande o richieste in relazione al presente *Manuale*, tali comunicazioni dovranno avvenire attraverso messaggi PEC o agli indirizzi e-mail dichiarati dal Cliente in forma scritta.

Le comunicazioni scritte dovranno essere consegnate da un servizio di posta che confermi la consegna per iscritto oppure tramite assicurata convenzionale, raccomandata a/r, indirizzate presso la sede di PA Digitale. (LODI)

23.5 Intestazioni e Appendici e Allegati del presente Manuale Operativo

Le intestazioni, sottotitoli e altri titoli del presente *Manuale* sono utilizzati solo per comodità e riferimento, e non saranno utilizzati nell'interpretazione o applicazione di qualsiasi disposizione ivi contenuta.

Le appendici, gli allegati, comprese le definizioni del presente *Manuale*, sono parte integrante e vincolante del presente *Manuale* a tutti gli effetti.

23.6 Modifiche del Manuale di conservazione

PA Digitale si riserva il diritto di aggiornare periodicamente il presente *Manuale* in modo estensibile al futuro e non retroattivo. Le modifiche sostituiranno qualsiasi disposizione in conflitto con la versione di riferimento del *Manuale* di conservazione.

23.7 Violazioni e altri danni materiali

Il Cliente rappresenta e garantisce che i documenti oggetto di conservazione e le informazioni in essi contenute non interferiscano, danneggino e/o violino diritti di una qualsiasi terza parte di qualunque giurisdizione.

23.8 Norme Applicabili

Le attività di conservazione contenute nel presente *Manuale* sono assoggettate alle leggi dell'ordinamento italiano.

Il presente documento informatico è formato nel rispetto delle regole tecniche di cui all'art. 71 del D.Lgs. 7 marzo 2005 n . 82 e s.m.i. (Codice dell'amministrazione digitale) e sottoscritto con firma digitale del Sig. FABRIZIO TONINELLI

Ultima pagina

Questa pagina è lasciata intenzionalmente bianca

Manuale del sistema di Conservazione

Allegati

Allegato 1 - Documenti rilevanti ai fini delle disposizioni tributarie: Elenco tipi documento

Codice	Descrizione Tipo documento/Classe documentale	Formato	Sottoscrizione Cliente	RT[5]
1	FattureEmesse	PDF/A	Firma digitale	SI
2	FattureRicevute	PDF/A	Firma digitale	SI
3	NotaVariazioneAumento	PDF/A	Firma digitale	SI
4	NotaVariazioneDiminuzione	PDF/A	Firma digitale	SI
5	DocumTrasporto	PDF/A	Firma digitale	SI
6	Scontrino	PDF/A	Firma digitale	SI
7	Ricevuta	PDF/A	Firma digitale	SI
8	Bolla	PDF/A	Firma digitale	SI
9	LibroGiornale	PDF/A	Firma digitale	SI
10	LibroInventari	PDF/A	Firma digitale	SI
11	LibroMastro	PDF/A	Firma digitale	SI
12	RegistroCronologico	PDF/A	Firma digitale	SI
13	LibroCespiti	PDF/A	Firma digitale	SI
14	RegistroIrpef	PDF/A	Firma digitale	SI
15	RegistroFattureAcquisto	PDF/A	Firma digitale	SI
16	RegistroAcquistiAgenzieViaggio	PDF/A	Firma digitale	SI
17	RegistroFattureEmesse	PDF/A	Firma digitale	SI
18	RegistroFattureInSospeso	PDF/A	Firma digitale	SI
19	RegistroCorrispettivi	PDF/A	Firma digitale	SI
20	GiornaleFondo	PDF/A	Firma digitale	SI
21	RegistroCorrispettiviAgenzieViaggio	PDF/A	Firma digitale	SI
22	RegistroEmergenzaIva	PDF/A	Firma digitale	SI
23	Bollettario	PDF/A	Firma digitale	SI
24	RegistroPrimaNota	PDF/A	Firma digitale	SI
25	RegistroUnicoIva	PDF/A	Firma digitale	SI
26	RegistroRiepilogativoIva	PDF/A	Firma digitale	SI
27	RegistroSezionaleIvaAcquisitiIntraUe	PDF/A	Firma digitale	SI
28	RegistroAcquistiIntraUeNonComm	PDF/A	Firma digitale	SI
29	RegistroTrasferimentiIntraUe	PDF/A	Firma digitale	SI
30	RegistroDichIntentiEmesse	PDF/A	Firma digitale	SI
31	RegistroDichIntentiRicevute	PDF/A	Firma digitale	SI
32	RegistroOmaggi	PDF/A	Firma digitale	SI
33	RegistroMemoriaProdContrassegno	PDF/A	Firma digitale	SI
34	RegistroLavorazioneProdContrassegno	PDF/A	Firma digitale	SI
35	RegistroCaricoProdContrassegno	PDF/A	Firma digitale	SI
36	RegistroScaricoProdContrassegno	PDF/A	Firma digitale	SI
37	RegistroBeniInDeposito	PDF/A	Firma digitale	SI
38	RegistroBeniInContoLavorazione	PDF/A	Firma digitale	SI
39	RegistroBeniComodato	PDF/A	Firma digitale	SI
40	RegistroBeniProva	PDF/A	Firma digitale	SI
41	RegistroSezionaleIvaInterno	PDF/A	Firma digitale	SI
42	RegistroCaricoStampatiFiscali	PDF/A	Firma digitale	SI
43	RegistroSocControllantiControllate	PDF/A	Firma digitale	SI
44	RegistroCaricoScaricoRegimeMargineMetodoAnalitico	PDF/A	Firma digitale	SI
45	RegistroAcquistiRegimeMargineMetodoGlobale	PDF/A	Firma digitale	SI
46	RegistroVenditeRegimeMargineMetodoGlobale	PDF/A	Firma digitale	SI
47	RegistroCaricoCentriElabDati	PDF/A	Firma digitale	SI
48	RegistroScaricoCentriElabDati	PDF/A	Firma digitale	SI
49	RegistroSommeRicevuteDeposito	PDF/A	Firma digitale	SI
50	RegistroEditori	PDF/A	Firma digitale	SI
58	Altri registri	PDF/A	Firma digitale	SI
59	UnicoPersoneFisiche	PDF/A	Firma digitale	SI
60	UnicoSocietaPersone	PDF/A	Firma digitale	SI
61	UnicoSocietaCapitale	PDF/A	Firma digitale	SI
62	UnicoEntiNonCommerciali	PDF/A	Firma digitale	SI

[5] Riferimento Temporale

Manuale del sistema di Conservazione

63	IrapPersoneFisiche	PDF/A	Firma digitale	SI
64	IrapSocietaPersone	PDF/A	Firma digitale	SI
65	IrapSocietaCapitale	PDF/A	Firma digitale	SI
66	IrapEntiNonCommercialiEdEquiparat	PDF/A	Firma digitale	SI
67	IrapAmministrazioniEdEntiPubblici	PDF/A	Firma digitale	SI
68	Modello730	PDF/A	Firma digitale	SI
69	ModelloConsolidatoNazionaleEMondiale	PDF/A	Firma digitale	SI
70	ModelloIva	PDF/A	Firma digitale	SI
71	ModelloIvaVrRichiestaRimborsoCreditoIva	PDF/A	Firma digitale	SI
72	ModelloIva26Lp2006ProspettoLiquidazioniPeriodiche	PDF/A	Firma digitale	SI
73	ModelloIva74Bis	PDF/A	Firma digitale	SI
74	ComunicazioneAnnualeDatiIva	PDF/A	Firma digitale	SI
75	ModelloRichiestaRimborsoCreditoIvaTrimestrale	PDF/A	Firma digitale	SI
76	ModelloDatiContenutiDichiarazioneIntentoRicevute	PDF/A	Firma digitale	SI
77	Modello770Semplificato	PDF/A	Firma digitale	SI
78	Modello770Ordinario	PDF/A	Firma digitale	SI
79	ModelloCertificazioneCud	PDF/A	Firma digitale	SI
80	ModelloF23	PDF/A	Firma digitale	SI
81	ModelloF24	PDF/A	Firma digitale	SI
82	ModelliAllegatiDichiarazioneRedditiModelloUnico	PDF/A	Firma digitale	SI
83	ModelliAnnotazioneSeparata	PDF/A	Firma digitale	SI
84	RicevutaPresentazioneModelliDichiarazione	PDF/A	Firma digitale	SI
85	Altri documenti	PDF/A	Firma digitale	SI

Allegato 2
Specifiche pacchetto di versamento, descrittore evidenze e pacchetto di invio file

Il presente paragrafo descrive il significato dei campi del pacchetto di versamento, le cui specifiche sono descritte nell'XML schema (xsd).

Id: identificativo del pacchetto di versamento. Deve essere un valore intero e deve essere univoco per ciascun cliente indipendentemente dal tipo documento a cui si riferisce. Ad esempio, il cliente Trasporti Veloci S.p.A. che ha i due tipi documento Fatture e DDT, potrà avere un solo pacchetto di versamento con id 1, indipendentemente dal fatto che sia riferito alle fatture oppure ai ddt. Viceversa un altro cliente potrà anch'esso avere un pacchetto di versamento con id 1.

nomeFileEvidenza: è una stringa che deve indicare il nome del descrittore evidenze che è contenuto nel pacchetto di versamento. Deve terminare con .p7m

file: è il descrittore evidenze firmato. E' un dato binario rappresentato in base 64

hash: è il valore di hash calcolato sul descrittore evidenze firmato

algoritmoHash: è l'indicazione dell'algoritmo utilizzato per il calcolo dell'hash. E' una stringa che di default è valorizzata a "SHA-256"

Schema XSD Pacchetto di versamento:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="InvioFileEvidenza" type="InvioFileEvidenzaType"/>
 <xs:complexType name="InvioFileEvidenzaType">
   <xs:sequence>
     <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:string" name="nomeFileEvidenza" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:string" name="hash" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:string" name="algoritmoHash" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:base64Binary" name="file" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Specifiche descrittore evidenze

Il descrittore evidenze è il pacchetto informativo che descrive nel dettaglio i documenti contenuti in un singolo lotto di documenti omogenei che devono essere conservati.

Id: deve contenere il medesimo identificativo del pacchetto di versamento. Deve essere anch'esso un valore intero

DataCreazioneEvidenza: è la data in cui è stata creato il descrittore evidenze. E' una stringa e deve essere nel formato gg-mm-aaaa

OraCreazioneEvidenza: è l'ora di creazione del descrittore evidenze. E' una stringa e deve essere nel formato hh:mm:ss

nomeFileEvidenza: è il nome del descrittore evidenze. Deve essere una stringa e deve essere pari a quella riportata nel pacchetto di versamento privata delle estensioni

tipoDocumenti: è il codice identificativo della tipologia di documenti contenuti nel descrittore evidenze. E' un intero e deve essere un codice che sia stato correttamente configurato nel sistema di conservazione in quanto in caso contrario il pacchetto di versamento viene rifiutato

DataInizioPeriodo: è la data di inizio del periodo di tempo a cui si riferisce il lotto ossia il descrittore evidenze. Deve essere una stringa nel formato gg-mm-aaaa. La data di inizio è inclusa nel periodo.

DataFinePeriodo: è la data di fine del periodo di tempo a cui si riferisce il lotto ossia il descrittore evidenze. Deve essere una stringa nel formato gg-mm-aaaa. La data di fine è inclusa nel periodo.

DataInizioMacroPeriodo: è la data di inizio del periodo temporale che raggruppa tutti i lotti di un certo tipo di documento. Ad esempio il periodo potrebbe essere un mese ed il macro periodo un anno. Deve essere una stringa nel formato gg-mm-aaaa

DataFineMacroPeriodo: è la data di fine del periodo temporale che raggruppa tutti i lotti di un certo tipo di documento. Deve essere una stringa nel formato gg-mm-aaaa

DataLimite: è la data entro cui il lotto deve essere chiuso in conservazione con firma digitale del responsabile della conservazione (o di un suo delegato) e marca temporale. Deve essere una stringa nel formato gg-mm-aaaa

numeroEvidenze: è un intero che indica il numero di documenti contenuti all'interno del descrittore evidenze

evidenze: è il contenitore di tutte le descrizioni dei documenti

evidenza: è il contenitore delle informazioni relative ad un singolo documento

nomeFile: è il nome di un singolo documento. Deve essere una stringa

idFile: è l'identificativo univoco del documento. Deve essere una stringa e nel caso di sistema documentale Urbi è nel formato idtestata-idversione

formato: rappresenta l'estensione del file. Deve essere una stringa

hash: è il valore di hash calcolato sul documento. Deve essere una stringa

algoritmoHash: è l'indicazione dell'algoritmo utilizzato per il calcolo dell'hash. E' una stringa che di default è valorizzata a "SHA-256"

PeriodoDiAppartenenza: è un indicatore significativo che individua un macro periodo. Deve essere un valore intero

SottoPeriodoDiAppartenenza: è un indicatore significativo che individua un periodo all'interno di un macro periodo. Deve essere un valore intero.

DataRiferimentoDoc: è la data del documento. Deve essere una stringa nel formato gg-mm-aaaa

DataLimiteCons: è la data entro cui il documento deve essere chiuso in conservazione. Deve essere una stringa nel formato gg-mm-aaaa

DataInizioPeriodoAppartenenza: è la data di inizio del periodo temporale a cui si riferisce il documento. Nel caso di documenti che non riguardano un periodo temporale tale data deve essere uguale alla DataInizioMacroPeriodo. Deve essere una strina nel formato gg-mm-aaaa

DataFinePeriodoAppartenenza: è la data di fine del periodo temporale a cui si riferisce il documento. Nel caso di documenti che non riguardano un periodo temporale tale data deve essere uguale alla DataFineMacroPeriodo Deve essere una strina nel formato gg-mm-aaaa

DataInizioMacroPeriodo: è la data di inizio del periodo temporale che raggruppa tutti i documenti dello stesso tipo. Deve essere una stringa nel formato gg-mm-aaaa

DataFineMacroPeriodo: è la data di fine del periodo temporale che raggruppa tutti i documenti dello stesso tipo. Deve essere una stringa nel formato gg-mm-aaaa

metadati: struttura che raggruppa tutti i metadati relativi ad un singolo documento

metadatoSemplice: è il contenitore di un metadato di tipo semplice

metadatoComplesso: è il contenitore di un metadato di tipo complesso ossia costituito da una aggregazione di metadati semplici

nome: è il nome del singolo metadato. Deve essere una stringa

valore: è il valore del singolo metadato. Deve essere una stringa e deve essere contenuta all'interno di un nodo di tipo CDATA

tipo: è l'indicazione della tipologia di metadato. Deve essere una stringa e può assumere solamente i valori "Stringa", "Intero", "Data" o "Decimale"

nomeMetadato: è il nome del metadato complesso. Deve essere una stringa

elementi: è il contenitore di tutti i metadati semplici che costituiscono un singolo metadato complesso

elemento: è la descrizione di un singolo metadato semplice che appartiene ad un metadato complesso. La sua struttura è la medesima del metadato semplice

Schema XSD Descrittore evidenze

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
 <xs:element name="FileEvidenza" type="FileEvidenzaType"/>
 <xs:complexType name="FileEvidenzaType">
   <xs:sequence>
     <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="DataItaliana" name="DataCreazioneEvidenza" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="xs:string" name="OraCreazioneEvidenza" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:string" name="nomeFileEvidenza" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:int" name="tipoDocumenti" maxOccurs="1" minOccurs="1"/>
     <xs:element type="DataItaliana" name="DataInizioPeriodo" maxOccurs="1" minOccurs="1"/>
     <xs:element type="DataItaliana" name="DataFinePeriodo" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="DataItaliana" name="DataInizioMacroPeriodo" maxOccurs="1" minOccurs="1"/>
     <xs:element type="DataItaliana" name="DataFineMacroPeriodo" maxOccurs="1" minOccurs="1"/>
     <xs:element type="DataItaliana" name="DataLimite" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:int" name="numeroEvidenze" maxOccurs="1" minOccurs="1"/>
     <xs:element type="evidenzeType" name="evidenze" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
 <xs:complexType name="evidenzeType">
   <xs:sequence>
     <xs:element type="evidenzaType" name="evidenza" maxOccurs="unbounded" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
 <xs:complexType name="evidenzaType">
   <xs:sequence>
                    <xs:element type="xs:string" name="nomeFile" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="xs:string" name="idFile" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="xs:string" name="formato" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="xs:string" name="hash" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="xs:string" name="algoritmoHash" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="xs:int" name="PeriodoDiAppartenenza" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="xs:int" name="SottoPeriodoDiAppartenenza" maxOccurs="1" minOccurs="1"/>                    <xs:element type="DataItaliana" name="DataRiferimentoDoc" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="DataItaliana" name="DataLimiteCons" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="DataItaliana" name="DataInizioPeriodoAppartenenza" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="DataItaliana" name="DataFinePeriodoAppartenenza" maxOccurs="1" minOccurs="1"/>
                    <xs:element type="DataItaliana" name="DataInizioMacroPeriodo" maxOccurs="1" minOccurs="0"/>
                    <xs:element type="DataItaliana" name="DataFineMacroPeriodo" maxOccurs="1" minOccurs="0"/>
                    <xs:element type="metadatiType" name="metadati" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
 <xs:complexType name="metadatiType">
                    <xs:choice maxOccurs="unbounded" minOccurs="0">
     <xs:element type="metadatoComplessoType" name="metadatoComplesso"/>
     <xs:element type="metadatoSempliceType" name="metadatoSemplice"/>
   </xs:choice>
 </xs:complexType>
 <xs:complexType name="metadatoSempliceType">
```

```
  <xs:sequence>
    <xs:element name="tipo" maxOccurs="1" minOccurs="1">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="Stringa"/>
          <xs:enumeration value="Intero"/>
          <xs:enumeration value="Data"/>
          <xs:enumeration value="Decimale"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element type="xs:string" name="nome" maxOccurs="1" minOccurs="1"/>
    <xs:element type="xs:string" name="valore" maxOccurs="1" minOccurs="1"/>
  </xs:sequence>
 </xs:complexType>
 <xs:complexType name="metadatoComplessoType">
  <xs:sequence>
                <xs:element type="xs:string" name="nomeMetadato" maxOccurs="1" minOccurs="1"/>
                <xs:element type="elementiType" name="elementi"  maxOccurs="1" minOccurs="1"/>
  </xs:sequence>
 </xs:complexType>
 <xs:complexType name="elementiType">
  <xs:sequence>
   <xs:element type="metadatoSempliceType" name="elemento" maxOccurs="unbounded" minOccurs="1"/>
  </xs:sequence>
 </xs:complexType>
 <xs:simpleType name="DataItaliana">
                <xs:restriction base="xs:string">
                <xs:pattern value="(((0[1-9] | [12][0-9] | 3[01])([-])(0[13578] | 10 | 12)([-])(\d{4})) | (((0[1-9] | [12][0-9] | 30)([-])(0[469] | 11)([-])(\d{4})) | ((0[1-9] | 1[0-9] | 2[0-8])([-])(02)([-])(\d{4})) | ((29)([-])(02)([-])([02468][048]00)) | ((29)([-])(02)([-])([13579][26]00)) | ((29)([-])(02)([-])([0-9][0-9][0][48])) | ((29)([-])(02)([-])([0-9][0-9][2468][048])) | ((29)([-])(02)([-])([0-9][0-9][13579][26])))"/>
                </xs:restriction>
 </xs:simpleType>
</xs:schema>
```

Specifiche pacchetto di invio file

Il pacchetto di invio file è utilizzato per la spedizione dei documenti al sistema di conservazione. Ciò è possibile solo a seguito dell'invio dei pacchetti di versamento. Le specifiche complete del pacchetto di invio file sono contenute nello schema XML (xsd).

Id: identificativo univoco del documento che sta inviando. E' un intero che viene restituito dal sistema di conservazione nel rapporto di conferma.

algoritmoHash: è una stringa che indica l'algoritmo utilizzato per il calcolo dell'hash. Il valore di default è SHA-256

file: contiene il documento binario codificato in base64

hash: è una stringa che contiene l'hash calcolato sul documento con l'algoritmo specificato

Schema XSD pacchetto di invio file

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="InvioFileFisico" type="InvioFileFisicoType"/>
 <xs:complexType name="InvioFileFisicoType">
   <xs:sequence>
     <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:string" name="algoritmoHash" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:base64Binary" name="file" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:string" name="hash" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Allegato 3
Specifiche rapporto di versamento

Il presente paragrafo descrive il significato dei campi del rapporto di versamento, le cui specifiche sono descritte nell'XML schema (xsd).

Id: deve contenere il medesimo identificativo del pacchetto di versamento. Deve essere anch'esso un valore intero

DataRapporto: è la data in cui è stato creato il rapporto di versametno. Deve essere in formato dateTime e deve prevedere l'indicazione tramite attributo della timezone a cui fa riferimento

tipoDocumenti: è l'identificativo del tipo documento così come ricevuto nel pacchetto di versamento. E' un valore intero che possiede un attributo nomeTipo che rappresenta la denominazione del tipo documento così come riconosciuto sul sistema di conservazione

HashPacchettoVersamento: è il valore di hash calcolato sul pacchetto di versamento ricevuto. Deve essere una stringa

IDEVDocumentale: è l'identificativo del pacchetto di versamento ricevuto. Deve essere un valore intero

IDEVConservazione: è l'identificativo assegnato al pacchetto di versamento dal sistema di conservazione. Deve essere un valore intero

Evidenza: è un contenitore per tutte le informazioni riguardanti un singolo documento. Possiede un attributo IDFileInCons che è un intero indicante l'identificativo che è stato assegnato al singolo documento all'interno del sistema di conservazione. Possiede un ulteriore attributo NomeFile che è una stringa che riporta il nome del documento

Eccezioni: è un contenitore di tutte le eccezioni che si sono verificare nell'elaborazione del pacchetto di versamento

Eccezione: è una stringa che identifica una singola eccezione che si è verificata in fase di elaborazione

Conferma: è una stringa che fornisce conferma della corretta elaborazione del pacchetto di versamento. Deve essere una stringa

Nota: indicazione sulla validità del rapporto di versamento. E' valorizzato nel caso di rapporti di conferma in attesa della ricezione dei documenti.

PeriodoDiAppartenenza: è un indicatore significativo che individua un macro periodo. Deve essere un valore intero

SottoPeriodoDiAppartenenza: è un indicatore significativo che individua un periodo all'interno di un macro periodo. Deve essere un valore intero.

DataRiferimentoDoc: è la data del documento. Deve essere una stringa nel formato gg-mm-aaaa

DataLimiteCons: è la data entro cui il documento deve essere chiuso in conservazione. Deve essere una stringa nel formato gg-mm-aaaa

DataInizioPeriodoAppartenenza: è la data di inizio del periodo temporale a cui si riferisce il documento. Nel caso di documenti che non riguardano un periodo temporale tale data deve essere uguale alla DataInizioMacroPeriodo. Deve essere una strina nel formato gg-mm-aaaa

DataFinePeriodoAppartenenza: è la data di fine del periodo temporale a cui si riferisce il documento. Nel caso di documenti che non riguardano un periodo temporale tale data deve essere uguale alla DataFineMacroPeriodo Deve essere una strina nel formato gg-mm-aaaa

DataInizioMacroPeriodo: è la data di inizio del periodo temporale che raggruppa tutti i documenti dello stesso tipo. Deve essere una stringa nel formato gg-mm-aaaa

DataFineMacroPeriodo: è la data di fine del periodo temporale che raggruppa tutti i documenti dello stesso tipo. Deve essere una stringa nel formato gg-mm-aaaa

Metadati: struttura che raggruppa tutti i metadati relativi ad un singolo documento

MetadatoSemplice: è una stringa che rappresenta un metadato. Possiede un attributo NomeDato che è una stringa che rappresenta il nome del metadato, ed un attributo TipoDato che è una stringa che indica il tipo di metadato. Quest'ultimo attributo può assumere solamente i valori "Stringa", "Intero", "Data" o "Decimale"

MetadatoComplesso: è un contenitore di metadati semplici collegati tra loro. Prevede un attributo NomeDato che è una stringa che contiene il nome del metadato complesso

Metadato: contiene il valore di un metadato che è parte di un metadato complesso. Possiede un attributo NomeDato che è una stringa che rappresenta il nome del metadato, ed un attributo TipoDato che è una stringa che indica il tipo di metadato. Quest'ultimo attributo può assumere solamente i valori "Stringa", "Intero", "Data" o "Decimale"

idFile: è l'identificativo univoco del documento. Deve essere una stringa e nel caso di sistema documentale Urbi è nel formato "idtestata-idversione"

Errori: è il contenitore degli errori che si sono verificati in fase di elaborazione del singolo documento

Errore: è il singolo errore che si è verificato in fase di elaborazione di un documento. Deve essere una stringa

Conferma (all'interno di una evidenza): è una stringa che fornisce conferma della corretta elaborazione dei metadati di un singolo documento. Deve essere una stringa

ObbligatoriTrovati: è il contenitore di metadati che sono stati definiti come obbligatori e che sono stati individuati

ObbligatoriMancanti: è il contenitore di metadati che sono stati definiti come obbligatori ma che sono stati individuati

AggiuntiviTrovati: è il contenitore di metadati semplici che sono stati definiti come non obbligatori e che sono stati individuati. Contiene inoltre anche l'indicazione dei metadati non definiti nella configurazione del sistema di conservazione, ma che sono stati trovati nel pacchetto di versamento

AggiuntiviMancanti: è il contenitore di metadati che sono stati definiti come non obbligatori e che non sono stati individuati

Schema XSD Rapporto di versamento

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
 <xs:element name="RapportoVersamento">
  <xs:complexType>
   <xs:choice minOccurs="6" maxOccurs="unbounded">
    <xs:element ref="DataRapporto" minOccurs="1" maxOccurs="1"/>
                        <xs:element ref="tipoDocumenti" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="HashPacchettoVersamento" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="IDEVDocumentale" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="IDEVConservazione" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="Evidenza" minOccurs="1" maxOccurs="unbounded"/>
                        <xs:element ref="Eccezioni" minOccurs="0" maxOccurs="1"/>
    <xs:element ref="Conferma" minOccurs="0" maxOccurs="1"/>
    <xs:element ref="Nota" minOccurs="0" maxOccurs="1"/>
   </xs:choice>
  </xs:complexType>
 </xs:element>
 <xs:element name="DataRapporto">
  <xs:complexType>
   <xs:simpleContent>
    <xs:extension base="xs:dateTime">
     <xs:attribute name="TimeZone" use="required" type="xs:NCName"/>
    </xs:extension>
   </xs:simpleContent>
  </xs:complexType>
 </xs:element>
 <xs:element name="Eccezioni">
  <xs:complexType>
   <xs:sequence>
    <xs:element minOccurs="0" ref="Eccezione"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="Eccezione" type="xs:string"/>
 <xs:element name="Evidenza">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="PeriodoDiAppartenenza" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="SottoPeriodoDiAppartenenza" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="DataInizioPeriodoAppartenenza" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="DataFinePeriodoAppartenenza" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="DataRiferimentoDoc" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="DataLimiteCons" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="DataInizioMacroPeriodo" minOccurs="0" maxOccurs="1"/>
    <xs:element ref="DataFineMacroPeriodo" minOccurs="0" maxOccurs="1"/>
    <xs:element ref="idFile" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="Metadati" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="Errori" minOccurs="0" maxOccurs="1"/>
    <xs:element ref="Conferma" minOccurs="0" maxOccurs="1"/>
   </xs:sequence>
   <xs:attribute name="IDFileInCons" use="required" type="xs:integer"/>
   <xs:attribute name="NomeFile" use="required" type="xs:NCName"/>
  </xs:complexType>
 </xs:element>
 <xs:element name="PeriodoDiAppartenenza" type="xs:integer"/>
```

```
<xs:element name="SottoPeriodoDiAppartenenza" type="xs:integer"/>
<xs:element name="DataInizioPeriodoAppartenenza" type="DataItaliana"/>
<xs:element name="DataFinePeriodoAppartenenza" type="DataItaliana"/>
<xs:element name="DataRiferimentoDoc" type="DataItaliana"/>
<xs:element name="DataLimiteCons" type="DataItaliana"/>
<xs:element name="DataInizioMacroPeriodo" type="DataItaliana"/>
<xs:element name="DataFineMacroPeriodo" type="DataItaliana"/>
<xs:element name="idFile" type="xs:NMTOKEN"/>
<xs:element name="Metadati">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="ObbligatoriTrovati"/>
   <xs:element ref="ObbligatoriMancanti"/>
   <xs:element ref="AggiuntiviTrovati"/>
   <xs:element ref="AggiuntiviMancanti"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:element name="ObbligatoriTrovati">
 <xs:complexType>
  <xs:choice minOccurs="0" maxOccurs="unbounded">
   <xs:element ref="MetadatoComplesso"/>
   <xs:element ref="MetadatoSemplice"/>
  </xs:choice>
 </xs:complexType>
</xs:element>
<xs:element name="ObbligatoriMancanti">
 <xs:complexType>
  <xs:choice minOccurs="0" maxOccurs="unbounded">
   <xs:element ref="MetadatoComplesso"/>
   <xs:element ref="MetadatoSemplice"/>
  </xs:choice>
 </xs:complexType>
</xs:element>
<xs:element name="AggiuntiviTrovati">
 <xs:complexType>
  <xs:choice minOccurs="0" maxOccurs="unbounded">
   <xs:element ref="MetadatoComplesso"/>
   <xs:element ref="MetadatoSemplice"/>
  </xs:choice>
 </xs:complexType>
</xs:element>
<xs:element name="AggiuntiviMancanti">
 <xs:complexType>
  <xs:choice minOccurs="0" maxOccurs="unbounded">
   <xs:element ref="MetadatoComplesso"/>
   <xs:element ref="MetadatoSemplice"/>
  </xs:choice>
 </xs:complexType>
</xs:element>
<xs:element name="Errori">
 <xs:complexType>
  <xs:sequence>
   <xs:element ref="Errore"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:element name="Errore" type="xs:string"/>
<xs:element name="HashPacchettoVersamento" type="xs:string"/>
<xs:element name="IDEVDocumentale" type="xs:integer"/>
<xs:element name="IDEVConservazione" type="xs:integer"/>
<xs:element name="tipoDocumenti">
 <xs:complexType>
  <xs:simpleContent>
   <xs:extension base="xs:integer">
    <xs:attribute name="nomeTipo" use="required"/>
   </xs:extension>
  </xs:simpleContent>
 </xs:complexType>
</xs:element>
<xs:element name="MetadatoSemplice">
 <xs:complexType mixed="true">
  <xs:attribute name="NomeDato" use="required" type="xs:string"/>
  <xs:attribute name="TipoDato" use="required" type="TipiMetadato"/>
 </xs:complexType>
</xs:element>
<xs:element name="Conferma" type="xs:string"/>
<xs:element name="Nota" type="xs:string"/>
<xs:element name="MetadatoComplesso">
 <xs:complexType>
  <xs:sequence>
   <xs:element maxOccurs="unbounded" ref="Metadato"/>
  </xs:sequence>
  <xs:attribute name="NomeDato" use="required" type="xs:NCName"/>
 </xs:complexType>
</xs:element>
<xs:element name="Metadato">
```

Manuale del sistema di Conservazione

```
    <xs:complexType mixed="true">
      <xs:attribute name="NomeDato" use="required" type="xs:string"/>
      <xs:attribute name="TipoDato" use="required" type="TipiMetadato"/>
    </xs:complexType>
  </xs:element>
  <xs:simpleType name="TipiMetadato">
    <xs:restriction base="xs:string">
      <xs:enumeration value="Stringa"/>
      <xs:enumeration value="Intero"/>
      <xs:enumeration value="Data"/>
      <xs:enumeration value="Decimale"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="DataItaliana">
                <xs:restriction base="xs:string">
                <xs:pattern                value="(((0[1-9] | [12][0-9] | 3[01])([-])(0[13578] | 10 | 12)([-])(\d{4})) | (((0)[1-9] | [12][0-9] | 30)([-])(0[469] | 11)([-])(\d{4})) | ((0[1-9] | 1[0-9] | 2[0-8])([-])(02)([-])(\d{4})) | ((29)([-])(02)([-
])([02468][048]00)) | ((29)([-])(02)([-])([13579][26]00)) | ((29)([-])(02)([-])([0-9][0-9][0][48])) | ((29)([-])(02)([-])([0-9][0-9][2468][048])) | ((29)([-])(02)([-])([0-9][0-9][13579][26])))"/>
                </xs:restriction>
  </xs:simpleType>
</xs:schema
```

Allegato 4
Specifiche pacchetti per funzioni ausiliarie

Il presente allegato descrive in linea generale la struttura dei pacchetti utilizzati per le operazioni ausiliarie alla conservazione. Rientrano in questa categoria le seguenti operazioni:

- Annullamento di un lotto in conservazione: operazione possibile solo entro i termini concordati tra PA Digitale ed il cliente
- Controllo stato di chiusura di un lotto
- Richiesta hash di un documento conservato
- Richiesta di un documento conservato
- Richiesta verifica hash sul sistema di conservazione con comparazione tra hash calcolato sul documento ed hash memorizzato nel sistema
- Richiesta di generazione pacchetti di distribuzione
- Richiesta di scaricamento pacchetti di distribuzione
- Richiesta hash rapporto di versamento
- Richiesta rapporto di versamento

Le specifiche dettagliate sono descritte negli XML schema (xsd). Si riportano sotto le descrizioni degli elementi principali e ricorrenti nella maggior parte dei pacchetti.

Id: identificativo dell'oggetto richiesto. Deve essere un valore intero e deve essere univoco per la tipologia di oggetto richiesta

idDocumento: identificativo dell'documento richiesto. Deve essere un valore intero e deve essere univoco

tipoPacchetto: stringa identificativa della tipologia di pacchetto di distribuzione richiesto. Può assumere solamente i seguenti valori: GETPDA (Pacchetto di archiviazione), GETPDAF (Pacchetto di archiviazione firmato), GETPDDDOC (Pacchetto di distribuzione non firmato con documenti), GETPDDNODOC (Pacchetto di distribuzione non firmato e senza documenti), GETPDDFDOC (Pacchetto di distribuzione firmato con documenti), GETPDDFNODOC (Pacchetto di distribuzione firmato senza documenti), GETPDDS (Pacchetto di distribuzione non firmato con un singolo documento), GETPDDSF (Pacchetto di distribuzione firmato con un singolo documento), GETMT (Marca temporale)

nomePacchetto: stringa identificativa del nome del pacchetto di cui è stato richiesto lo scaricamento. Viene restituita nell'xml di risposta al pacchetto di richiesta generazione pacchetto di distribuzione

IDDownload: intero identificativo univoco del pacchetto di cui è stato richiesto lo scaricamento. Viene restituito nell'xml di risposta al pacchetto di richiesta generazione pacchetto di distribuzione

Schema XSD Pacchetto per annullamento lotto:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="AnnullaLotto" type="AnnullaLottoType"/>
 <xs:complexType name="AnnullaLottoType">
   <xs:sequence>
     <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Schema XSD Pacchetto per controllo stato di chiusura di un lotto:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="ControlloChiusura" type="ControlloChiusuraType"/>
 <xs:complexType name="ControlloChiusuraType">
```

```
  <xs:sequence>
    <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
  </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Schema XSD Pacchetto per richiesta hash di un documento conservato:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="RichiestaFileFisico" type="RichiestaFileFisicoType"/>
 <xs:complexType name="RichiestaFileFisicoType">
   <xs:sequence>
     <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Schema XSD Pacchetto per richiesta di un documento conservato:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="RichiestaFileFisicoBinario" type="RichiestaFileFisicoBinarioType"/>
 <xs:complexType name="RichiestaFileFisicoBinarioType">
   <xs:sequence>
     <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Schema XSD Pacchetto per richiesta verifica hash:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="RichiestaHash" type="RichiestaHashType"/>
 <xs:complexType name="RichiestaHashType">
   <xs:sequence>
     <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Schema XSD Pacchetto per richiesta generazione di un pacchetto di distribuzione:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="RichiestaPacchetto" type="RichiestaPacchettoType"/>
 <xs:complexType name="RichiestaPacchettoType">
   <xs:sequence>
     <xs:element type="xs:int" name="idDocumento" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:string" name="TipoPacchetto" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Schema XSD Pacchetto per scaricamento di un pacchetto di distribuzione:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="RichiestaPacchettoBinario" type="RichiestaPacchettoBinarioType"/>
 <xs:complexType name="RichiestaPacchettoBinarioType">
   <xs:sequence>
     <xs:element type="xs:int" name="idDocumento" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:string" name="TipoPacchetto" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:string" name="NomePacchetto" maxOccurs="1" minOccurs="1"/>
     <xs:element type="xs:int" name="IDDownload" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Schema XSD Pacchetto per richiesta hash rapporto di versamento:

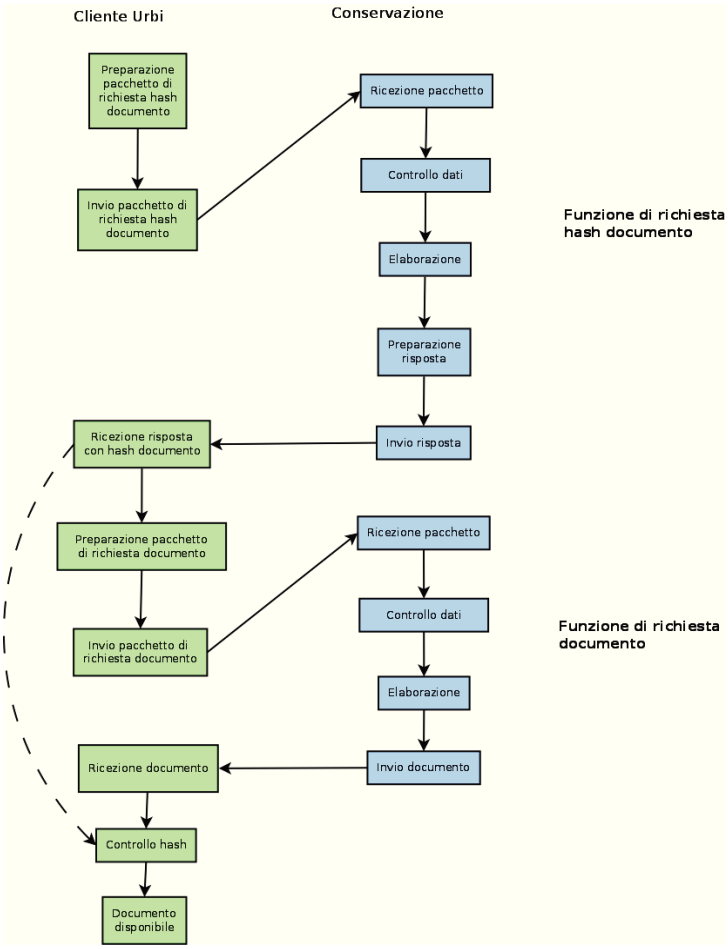
```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="RichiestaRapportoVersamento" type="RichiestaRDVType"/>
 <xs:complexType name="RichiestaRDVType">
   <xs:sequence>
     <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Schema XSD Pacchetto per richiesta rapporto di versamento:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:element name="RichiestaRapportoVersamentoBinario" type="RichiestaRDVBinType"/>
 <xs:complexType name="RichiestaRDVBinType">
   <xs:sequence>
     <xs:element type="xs:int" name="id" maxOccurs="1" minOccurs="1"/>
   </xs:sequence>
 </xs:complexType>
</xs:schema>
```

Viene riportato di seguito un esempio relative al flusso di esecuzione relativo ad una delle operazioni ausiliarie: nel caso specifico lo scaricamento di un documento dal sistema di conservazione.



Allegato 5
Specifiche descrittore XML per file EML

Il presente paragrafo descrive il significato dei campi del descrittore XML per i file EML. Tale descrittore è utilizzato solamente per la conservazione dei tipi documento indicati come PEC. Può però anche essere applicato alla conservazione di semplici email dato che le specifiche RFC per i file EML sono comuni ad entrambi gli utilizzi. Le specifiche dettagliate sono descritte nell'XML schema (xsd).

eml_source: identifica la struttura che descrive un intero file eml.

sha256: è una stringa che contiene il valore di hash calcolato con algoritmo sha256 sul file eml sorgente

datetime: contiene l'indicazione della data ed ora di ricezione di ricezione dell'eml. Deve essere in formato dateTime

from: indica il mittente della mail. Deve essere una stringa

dest: indica una struttura che contiene l'elenco di tutti i destinatari della mail

msgid: indica il message-ID univoco della mail, ossia il suo identificatore. Deve essere una stringa

destcc: indica una struttura che contiene l'elenco di tutti i destinatari in copia della mail

attachments: è una struttura che contiene tutti gli allegati alla mail. Deve possedere un attributo num di tipo intero che indica il numero di allegati presenti

emailBody: è una stringa che contiene il testo della mail

subject: è una stringa che contiene l'oggetto della mail

attachment: è una struttura che contiene la descrizione di un singolo allegato alla mail. Deve avere un attributo type di tipo stringa che indica il tipo di allegato

cc: stringa che indica un singolo indirizzo email in copia alla mail

to: stringa che indica un singolo indirizzo email destinatario della mail

filename: nome di un singolo allegato alla mail. Deve essere una stringa

size: dimensione di un singolo allegato alla mail. Deve essere un intero

Schema XSD Descrittore XML per file EML:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
 <xs:element name="eml_summary">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="eml_source" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="eml_source">
  <xs:complexType>
   <xs:all>
                <xs:element ref="sha256" minOccurs="1"/>
    <xs:element ref="datetime" minOccurs="1"/>
    <xs:element ref="from" minOccurs="1"/>
    <xs:element ref="dest" minOccurs="1"/>
    <xs:element ref="msgid" minOccurs="1"/>
                                                <xs:element ref="destcc" minOccurs="0"/>
    <xs:element ref="attachments" minOccurs="0" maxOccurs="1"/>
    <xs:element ref="emailBody" minOccurs="0" maxOccurs="1"/>
    <xs:element ref="subject" minOccurs="0" maxOccurs="1"/>
   </xs:all>
  </xs:complexType>
 </xs:element>
 <xs:element name="datetime" type="xs:dateTime"/>
 <xs:element name="from" type="xs:string"/>
 <xs:element name="to" type="xs:string"/>
 <xs:element name="cc" type="xs:string"/>
 <xs:element name="msgid" type="xs:string"/>
 <xs:element name="attachments">
  <xs:complexType>
   <xs:sequence>
    <xs:element minOccurs="0" maxOccurs="unbounded" ref="attachment"/>
   </xs:sequence>
```

Manuale del sistema di Conservazione

```
                    <xs:attribute name="num" use="required" type="xs:integer"/>
   </xs:complexType>
  </xs:element>
  <xs:element name="destcc">
   <xs:complexType>
    <xs:sequence>
     <xs:element minOccurs="0" maxOccurs="unbounded" ref="cc"/>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
   <xs:element name="dest">
   <xs:complexType>
    <xs:sequence>
     <xs:element minOccurs="1" maxOccurs="unbounded" ref="to"/>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
  <xs:element name="attachment">
   <xs:complexType>
    <xs:all>
     <xs:element ref="eml_source" minOccurs="0"/>
     <xs:element ref="filename" minOccurs="1"/>
     <xs:element ref="sha256" minOccurs="1"/>
     <xs:element ref="size" minOccurs="1"/>
    </xs:all>
    <xs:attribute name="type" type="xs:string"/>
   </xs:complexType>
  </xs:element>
  <xs:element name="filename" type="xs:string"/>
  <xs:element name="sha256" type="xs:string"/>
  <xs:element name="size" type="xs:integer"/>
  <xs:element name="emailBody" type="xs:string"/>
  <xs:element name="subject" type="xs:string"/>
</xs:schema>
```