ALLEGATO 6
PIANO DI CONSERVAZIONE DEI DOCUMENTI

Composizione del piano
Il piano di conservazione è composto anche dal quadro di classificazione (Titolario), dal massimario di scarto di selezione per la conservazione e dal censimento dei depositi documentari, dalle banche dati e dei software di gestione documentale in uso.

Formato dei documenti elettronici
Per la predisposizione dei documenti informatici si adottano formati che al minimo possiedono requisiti di leggibilità, interscambiabilità, non alterabilità durante le fasi di accesso e conservazione, immutabilità nel tempo del contenuto e della struttura, come specificato nel manuale di gestione.

Si preferiscono pertanto i seguenti formati:
- XML
- PDF-A
- TXT
- JPEG
- TIFF
- P7M
- M7M
- MIME

Per office open XML (OOXML)
- DOCX
- XLSX
- PPTX

Per open document format (open office/libre office):
- ODT
- ODS
- ODP
- ODG
- ODB

Non è consentita la produzione di documenti informatici che contengano al loro interno macroistruzioni o codici eseguibili.

I documenti elettronici spediti tramite posta elettronica certificata saranno protocollati ed inviati in conservazione.

Ai documenti interni dell'ente che non rispettano l'immodificabilità sarà associato un riferimento temporale.

Manuale del
Sistema di Conservazione

Redatto da:	**Marco Farina** Project Manager del servizio di conservazione		
Verificato da:	**Adriano Santoni** Resp. della sicurezza dei sistemi per la conservazione	_____	_____ Data
Verificato da:	**Roberto Ravazza** Resp. dei sistemi informativi per la conservazione	_____	_____ Data
Verificato da:	**Salvatore Pulvirenti** Resp. dello sviluppo e della manutenzione del sistema di conservazione	_____	_____ Data
Approvato da:	**Simone Braccagni** Resp. del servizio di Conservazione	_____	_____ Data

Il documento è :

- ***REDATTO*** *se provvisto della/e firma/e di redazione,*
- ***VERIFICATO*** *se provvisto anche della firma di verifica,*
- ***APPROVATO*** *se provvisto di tutte le firme*

Codice documento:	9035	-	05	-	01
	Codice Prog.		*N° Doc.*		*Ver-sione*

Distribuzione: Pubblica

LEGENDA DI COPERTINA

Stato del documento

Le firme sulla copertina del presente documento fanno riferimento allo standard interno di ARUBA PEC per la gestione della documentazione di servizio: hanno lo scopo di permetterne il controllo di configurazione e di indicarne lo stato di lavorazione.

Si segnala che la firma di approvazione autorizza la circolazione del documento limitatamente alla lista di distribuzione e non implica in alcun modo che il documento sia stato revisionato e/o accettato da eventuali Enti esterni.

In particolare, il documento è da intendersi **REDATTO** se provvisto della/e firma/e di chi lo ha redatto; **VERIFICATO** se ha superato con esito positivo la verifica interna e quindi provvisto della/e firma/e di verifica che ne autorizza il rilascio alla GESTIONE DELLA CONFIGURAZIONE. Nel caso in cui la revisione abbia esito negativo il documento viene modificato e verificato, con un nuovo numero di versione e una nuova data di emissione. Il documento è da intendersi **APPROVATO** se provvisto della firma di approvazione che si aggiunge alle altre.

Un documento sprovvisto di firme è in uno stato indefinito, e non può essere messo in circolazione.

Distribuzione

La distribuzione di un documento può essere:

- **PUBBLICA**, se il documento può circolare senza restrizioni;
- **INTERNA**, se il documento può circolare solo all'interno di ARUBA PEC;
- **RISTRETTA,** se il documento è distribuibile ad un numero limitato di destinatari;
- **CONTROLLATA**, se il documento è distribuibile ad un numero limitato di destinatari e ogni copia è controllata.

1 CONTESTO DI RIFERIMENTO

1.1 Riferimenti normativi e di prassi

Il sistema di conservazione digitale di ARUBA, è stato realizzato in conformità alla normativa vigente in materia di conservazione dei documenti informatici. Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato.

- **Codice civile** - R.D. del 16 marzo 1942 n. 262;
- **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.

1.2 Riferimenti tecnici

Dove non sono indicate una versione e/o una data specifica, si intende fare riferimento alla più recente versione disponibile del documento citato.

- **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.

1.3 Standard e specifiche tecniche

Di seguito si riporta l'elenco degli standard a cui ARUBA 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.

2 MODALITÀ DI COMPILAZIONE

Il documento in oggetto e' stato redatto in modo da garantire omogeneità e completezza delle informazioni necessarie per la gestione del sistema di conservazione e per la definizione dei ruoli e delle interazioni con i soggetti esterni con il quale interagisce.

2.1 Storia delle modifiche

Il presente paragrafo riporta le modifiche sono state apportate al manuale, ovvero le novità e/o versioni, introdotte rispetto alla precedente emissione

DATA	VERSIONE	PARAGRAFO	MODIFICHE	AUTORE
18/09/2014	1.0	n/a	Prima versione del documento	Marco Farina

2.2 Introduzione e 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,
d) comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
e) 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;
f) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
g) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
h) 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;
i) 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;
j) la descrizione delle procedure per la produzione di duplicati o copie;

k) i tempi entro i quali le diverse tipologie di documenti informatici devono essere oggetto di scarto/cancellazione;
l) 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;
m) 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".

Questo documento è pubblicato sul sito Web di Aruba PEC S.p.a.. (di seguito per brevità "ARUBA") nella apposita area riservata ai Clienti www.docfly.it 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 ARUBA. 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 ARUBA. 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.

2.3 Definizioni, abbreviazioni e termini tecnici

2.3.1 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 anche le definizioni contenute nel *Contratto*, da intendersi, pertanto, qui interamente riportate e trascritte, nonché le seguenti:

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 ARUBA 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; è l'entità giuridica che sottoscrive e accetta il Contratto per l'affidamento del servizio di conservazione digitale di documenti informatici;

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 ARUBA 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 ARUBA; questa persona può essere interna o esterna ad ARUBA, 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 ad ARUBA 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;

idPdV: Indice del Pacchetto di Versamento

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;

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 infor-

matiche 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 ARUBA;

Responsabile del Servizio di conservazione: è ARUBA 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 ARUBA 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 un periodo di tempo specificato nel Contratto;

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 specificato nel contratto di servizio di conservazione dei documenti in vigore. 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 Repubblica 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;

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

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;

2.3.2 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;

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;

CSCD - contratto di servizio di conservazione dei documenti: Contratto di servizio di conservazione dei documenti, ove sono esplicitate chiaramente: l'ambito della delega conferita, le specifiche funzioni, le attività e le responsabilità affidate dal Cliente ad ARUBA;

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.....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 di ARUBA, 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;

PdV: Pacchetto di Versamento

PdA: Pacchetto di Archiviazione

PdD: Pacchetto di Distribuzione

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, ARUBA;

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

3 DATI DI IDENTIFICAZIONE DEL CONSERVATORE

3.1 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* e nel **CONTRATTO PER L'AFFIDAMENTO DEL SERVIZIO DI CONSERVAZIONE DIGITALE DI DOCUMENTI INFORMATICI,** di seguito per brevità chiamato anche **"*Contratto*",** perfezionato tra ARUBA ed il Cliente medesimo.

Il suddetto Responsabile della conservazione, sotto la propria responsabilità, ha affidato ad **ARUBA**, quale **prestatore del servizio di conservazione digitale dei documenti informatici**, il servizio di conservazione digitale dei documenti informatici del Cliente, delegando le attività previste dal relativo *Contratto* di servizio, avendogli riconosciuto una specifica competenza ed esperienza in relazione alle attività ad esso delegate.

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

Contestualmente al perfezionamento del suddetto Contratto, il Cliente ha altresì nominato ARUBA 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 ARUBA.

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

ARUBA PEC S.p.a.

Sede Legale: via Sergio Ramelli, 8 CAP 52100 Arezzo

Numero Iscrizione R.I. 01879020517, Codice fiscale e Part. IVA: 01879020517
C.C.I.A.A. di Arezzo N° R.E.A.: 145843

N° Telefono (centralino): 05750500

N° FAX: 0575862020

PEC: arubapec@aruba.pec.it

Legale rappresentante: Simone Braccagni

Sito web generale (informativo): www.pec.it

Sito web del servizio di conservazione: www.docfly.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.

ARUBA espleterà, attraverso i propri incaricati e nei limiti della delega ricevuta, tutte le attività e le funzioni inerenti il processo di conservazione in relazione a quanto stabilito nel *Contratto* e nel documento riportante l'"**Elenco dei documenti informatici sottoposti a conservazione**" allegato al suddetto *Contratto*.

In particolare, ARUBA, 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 ARUBA 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 ARUBA non è in alcun modo responsabile.

ARUBA, 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. ARUBA si riserva, a proprio insindacabile giudizio, di sostituire, in qualunque momento, i suddetti incaricati.

Come precisato nel *Contratto*, ARUBA si riserva la possibilità di appaltare o subappaltare, in tutto o in parte, l'esecuzione di operazioni, singole attività, servizi relativi a funzioni o fasi del processo di conservazione, a terzi soggetti, fornitori esterni, che per conoscenza, esperienza, capacità e affidabilità forniscano idonee garanzie.

3.2 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
Actalis S.p.a.	Via dell'Aprica, 18 20158 Milano	N° REA : 1669411 N° iscrizione al Registro delle imprese: 03358520967 N° Partita IVA : 01879020517 N° Telefono (centralino) : 02 68825 1 N° FAX : 02 68825 223 e-mail PEC: amministrazione@pec.actalis.it

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

3.3 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" del *Contratto*, i cui attributi devono essere conformi agli standard riportati al capitolo 7 del presente *Manuale*.

3.4 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 ARUBA si assume piena responsabilità circa la conformità alla legge italiana dei servizi forniti.

3.5 Obblighi connessi al trattamento dei dati personali

3.5.1 Tutela e diritti degli interessati

In materia di trattamento dei dati personali ARUBA 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.).

3.5.2 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* e nel *Contratto* sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

3.5.3 Finalità del trattamento

Erogazione del servizio di conservazione digitale dei documenti informatici:

I dati raccolti sono utilizzati per il perfezionamento del *Contratto* e per l'attivazione del Servizio di conservazione digitale dei documenti informatici.

ARUBA 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:

ARUBA potrà utilizzare le coordinate di posta elettronica fornite al momento della sottoscrizione del *Contratto* 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 ad ARUBA potranno essere comunicati a soggetti pubblici, quali forze dell'ordine, Autorità pubbliche e autorità Giudiziaria per lo svolgimento delle attività di loro competenza.

3.5.4 Sicurezza dei dati

Come previsto dalle norme vigenti in materia, ARUBA 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.

4 MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE

4.1 Ruoli e responsabilità

Nel sistema di conservazione 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	ARUBA
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 il soggetto che sottoscrive il *Contratto* con ARUBA; 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,* nel *Contratto* e nei rispettivi allegati.

Il Responsabile della conservazione è il Cliente, nella persona fisica dallo stesso indicata nell'apposito allegato al *Contratto*. 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 attuazione attraverso i Servizi oggetto del *Contratto*; governa la gestione dei processi di formazione dei documenti informatici con piena responsabilità, in relazione al modello organizzativo adottato anche in conseguenza ed in funzione del *Contratto*.

Referente/i del Cliente è/sono le persone fisiche che il Cliente indica ad ARUBA 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, ARUBA.

ARUBA, 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 ARUBA 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 ARUBA, 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.

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,* dal *Contratto* e dai rispettivi allegati.

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 ARUBA 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.

4.2 Organizzazione specifica per il servizio 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. 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.

Nella pagina seguente 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)**
Braccagni	Simone	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.	01/09/2014	
Boschi	Serena	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.	01/09/2014	
Braccagni	Simone	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.	01/09/2014	

Santoni	Adriano	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.	01/09/2014	
Ravazza	Roberto	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.	01/09/2014	
Pulvirenti	Salvatore	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.	01/09/2014	

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	**Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico**				
	Descrizione sintetica	Il sistema di conservazione riceve l'indice del pacchetto di versamento contenente le informazioni sugli oggetti digitali che saranno inviati in conservazione.	**SC**	**RMGO**	**==**
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	Viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard DocFly. Viene verificato che il PdV è versato nei termini contrattuali e di servizio stabiliti col produttore	**SC**	**RMGO**	**==**
FASE 3	**Preparazione del rapporto di conferma**				
	Descrizione sintetica	Il sistema, una volta effettuate le verifiche dell'idPdV rimane in attesa dell'invio dei documenti	**SC**	**RMGO**	**==**
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	Il sistema scarta l'intero pacchetto e invia notifica in automatico	**SC**	**RMGO**	**==**
FASE 5	**Ricezione e verifica dei documenti**				
	Descrizione sintetica	Per ognuno di documenti inviati viene verificato che l'hash del documento informatico sia corrispondente all'hash dichiarato all'interno del	**SC**	**RMGO**	**==**

		medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata. Vengono inoltre effettuati controlli di leggibilità, integrità e che i documenti non siano già presenti a sistema			
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	Il sistema genera in automatico il rapporto di versamento per ognuno dei PdV che ha superato i controlli qualitativi	**SC**	**RMGO**	**==**
FASE 8	**Sottoscrizione del rapporto di versamento con firma digitale apposta da ARUBA**				
	Descrizione sintetica	Il sistema provvede in automatico alla sottoscrizione digitale del rapporto di versamento con certificato del RSC e alla marcatura temporale del rapporto.	**SC**	**RMGO**	**RSC**
FASE 9	**Preparazione e gestione del pacchetto di archiviazione (c.d. File di chiusura)**				
	Descrizione sintetica	Il sistema genera il pacchetto di archiviazione secondo le modalità descritte al cap. 9	**SC**	**RMGO**	**==**
FASE 10	**Sottoscrizione del pacchetto di archiviazione con firma digitale apposta da ARUBA 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	Come previsto da normativa l'indice del pacchetto di archiviazione, viene sottoscritto digitalmente dal RSC, una volta passato nello stato "conservato".	**SC**	**RMGO**	**RSC**

FASE 11	**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	Come previsto da normativa il PdD viene sottoscritto digitalmente dal RSC	**SC**	**RER**	**RSC**
FASE 12	**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	Richieste di duplicati o copie informatiche vengono sottoscritte digitalmente dal RSC in modo da attestarne l'autenticità rispetto al documento sorgente	**SC**	**RER**	**RSC**
FASE 13	**Eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal contratto di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso**				
	Descrizione sintetica	Una volta scaduti i termini di conservazione previsti dal contratto, il sistema provvede a inviare una mail di notifica al client, il quale potrà decidere in autonomia se cancellarli dal sistema.	**SC**	**RCD** **RP**	**==**

Legenda:
- **RMGO** - responsabile del monitoraggio della gestione ordinaria del sistema e dei processi di base di conservazione
- **RER** - responsabile dell'esibizione/restituzione dei documenti informatici conservati
- **RIS** - responsabile dell'infrastruttura sistemistica, del piano di Disaster Recovery / Piano di continuità operativa (Business Continuity Plan) e della sicurezza
- **RCD** - responsabile della cancellazione dei documenti e dei dati digitali
- **RP** - responsabile privacy
- **RAC** - responsabile dell'assistenza cliente
- **RSC** - Responsabile del servizio di conservazione
- **SC** - **Sistema di conservazione**

5 RIFERIMENTI CONTRATTUALI

In questo capitolo sono riportati i documenti costituenti l'impianto contrattuale del servizio di conservazione a norma tra Produttore e Conservatore.

5.1 Impianto contrattuale

ARUBA, in linea con la normativa vigente, garantisce contratti o accordi scritti che specificano tutti gli aspetti di: diritti e responsabilità, versamento e acquisizione, mantenimento, accesso, ritiro, deposito, diritti e responsabilità di conservazione sui i documenti che tratta, natura economica e di servizio

Ai fini dell'attivazione e l'erogazione del servizio di conservazione, il soggetto Produttore sottoscrive il contratto di servizio e suoi allegati:

- Contratto per l'affidamento del servizio di conservazione digitale di documenti informatici
- Nomina di ARUBA quale Responsabile del Servizio di Conservazione;
- Nomina di ARUBA quale Responsabile esterno del Trattamento dei dati;
- Elenco dei documenti informatici sottoposti a conservazione;
- Persone designate dal soggetto Produttore per i rapporti con ARUBA

5.1.1 Contratto per l'affidamento del servizio di conservazione

SI tratta del contratto con il quale il Cliente affida ad ARUBA la conservazione digitale dei documenti informatici di cui è titolare nonché dei documenti informatici di titolarità di terzi soggetti dallo stesso prodotti, sottoscritti digitalmente e versati in conservazione in virtù di specifica delega a tal fine rilasciata dai suddetti terzi in favore del Cliente.

5.1.2 Nomina di Aruba quale responsabile del servizio di conservazione e del trattamento dei dati

Ai fini dell'erogazione del servizio di conservazione digitale a norma, il Cliente nomina ARUBA quale Responsabile del Servizio di Conservazione e 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.) e indicato all'art 6 co. 8 delle nuove regole tecniche (DPCM del 3 Dic 2013).

Pertanto, i ruoli di Responsabile della conservazione e di Titolare del trattamento sono ricoperti dall'ente comunale, mentre i ruoli di Responsabile del servizio di conservazione e di Responsabile esterno del trattamento dei dati saranno ricoperti da ARUBA.

In questo modo, la responsabilità della conservazione digitale dei documenti informatici è interamente delegata ad ARUBA. Il Cliente è, di conseguenza, sollevato da tutti i complessi adempimenti e oneri conseguenti agli obblighi imposti dalla Normativa regolante la conservazione digitale di documenti informatici, come il rispetto dei termini temporali di conservazione, la salvaguardia dell'integrità e leggibilità dei documenti, la gestione della sicurezza fisica ed informatica del sistema di conservazione, l'aggiornamento tecnologico e normativo

5.1.3 Elenco dei documenti informatici sottoposti a conservazione

Tale documento costituisce parte integrante e sostanziale del contratto per l'affidamento del servizio di conservazione digitale di documenti informatici.

Il soggetto Produttore condivide con il conservatore ARUBA le caratteristiche, le modalità ed i termini di versamento dei documenti informatici da sottoporre a conservazione digitale, approvando espressamente quanto indicato nelle scheda conservazione.

Fra i diversi aspetti da concordare attraverso la scheda di conservazione, i principali sono:

- le tipologie di documenti da conservare;
- i metadati minimi riferiti ad ogni classe/tipo documento
- eventuali (metadati) extrainfo riferiti ad ogni classe/tipo documento sui quali effettuare specifici controlli;
- i formati da adottare per ogni classe/tipo documento;
- i software in grado di interpretare e rendere leggibili per l'uomo i formati prescelti in caso di formati fuori standard;
- i fogli di stile da utilizzare per la corretta rappresentazione dei documenti in formato XML;
- le modalità e canali di trasferimento dei documenti nell'archivio
- modalità e termini di comunicazione tra conservatore e produttore;
- condizioni per la corretta conservazione dei pacchetti;

5.1.4 Persone designate dal soggetto Produttore per i rapporti con ARUBA

Ai fini dell'affidamento del servizio di conservazione digitale di documenti informatici, il soggetto Produttore comunica l'identità delle persone fisiche dallo stesso ufficialmente incaricate di mantenere i rapporti con ARUBA e titolate ad operare in nome e per conto del soggetto Produttore medesimo, precisandone funzione e ruolo.

Il documento contenente le informazioni relativamente alle persone designate ai rapporti con ARUBA, diviene parte integrante e sostanziale del contratto per l'affidamento del servizio di conservazione digitale di documenti informatici.

5.2 Modello di funzionamento del servizio

L'obiettivo ed il compito di ARUBA 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 ARUBA 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 ad ARUBA il ruolo ed i compiti fissati nel documento di nomina a Responsabile del servizio di conservazione.

A tal fine, ARUBA 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.

Pertanto, al fine di attivare il servizio di conservazione digitale dei documenti informatici è necessario che il Cliente abbia sottoscritto il *Contratto* e gli allegati ad esso relativi, all'interno dei quali vengono, fra l'altro, specificati:

a) i contenuti e le caratteristiche generali del Servizio di conservazione digitale;

b) i termini di decorrenza e la durata del Servizio di conservazione digitale;

c) gli eventuali Servizi Estesi erogati su richiesta del Cliente;

d) le responsabilità e gli obblighi del Cliente;

e) le responsabilità e gli obblighi di ARUBA;

f) le modalità di produzione/formazione/emissione/sottoscrizione dei documenti informatici;

g) la descrizione delle tipologie e delle classi dei documenti informatici da sottoporre a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;

h) la definizione dell'intervallo di conservazione ossia dell'intervallo di tempo intercorrente tra la presa in carico del pacchetto di versamento e la chiusura del pacchetto di archiviazione.

i) Le modalità di distribuzione/esibizione dei documenti informatici conservati;

5.2.1 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* e dal *Contratto*.

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*, alle prescrizioni previste nel *Contratto* e negli allegati ad esso relativi.

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

5.2.2 Obblighi di ARUBA

ARUBA, come analiticamente descritto nel *Contratto*, 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.

In particolare, ARUBA, ai fini dell'erogazione del Servizio oggetto del *Contratto*, 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.

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

Pertanto è obbligo di ARUBA 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 ARUBA è in grado di esibire tutti i documenti informatici in esso conservati in qualsiasi momento del periodo di conservazione; a tal fine, ARUBA 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 ARUBA, 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 ARUBA la conservazione di documenti analogici.

5.2.3 Compiti organizzativi

ARUBA 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* e nel *Contratto* attuati adottando procedure di tracciabilità tali da garantire la corretta conservazione, l'accessibilità a ogni singolo documento e la sua esibizione.

ARUBA 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.

ARUBA 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*.

5.2.4 Compiti di manutenzione e controllo

ARUBA 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 comprensivo delle risoluzioni adottate per rimuovere eventuali anomalie;
- 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;
- verificare il buon funzionamento del filesystem

5.2.5 Compiti operativi

ARUBA 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;

5.2.6 Fasi del processo di conservazione e responsabilità

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 e formalizzati nel *Contratto* e negli allegati ad esso relativi che garantiscono la sua distinzione logica dal sistema di gestione documentale del Cliente, qualora esistente.

Pertanto, la conservazione non viene svolta all'interno della struttura organizzativa del Cliente (soggetto titolare dei documenti informatici da conservare), ma è affidata ad ARUBA, 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	ARUBA
Sistema di gestione documentale del Cliente	1	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati	X	
	2	Produzione del pacchetto di versamento	X	
	3	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati	X	
Servizio di Fatturazione PA e PEC	1a	Produzione/formazione/emissione a norma dei documenti informatici e contestuale generazione dei relativi metadati		X
	2a	Produzione del pacchetto di versamento		X
	3a	Deposito in conservazione del pacchetto di versamento e dei relativi documenti informatici completi di metadati		X
Sistema di Firma Digitale	4	Servizio di Firma Automatica e di eventuale apposizione marca temporale, da effettuare sui documenti tributari prima dell'invio al sistema di conservazione.	X	X
ne digitale e dei	5	Acquisizione da parte del sistema di conservazione del pacchetto di versamento prodotto dal Cliente per la sua presa in carico		X

	6	Verifica che il pacchetto di versamento ed i documenti informatici in esso descritti siano coerenti e conformi alle prescrizioni stabilite dal Contratto di servizio		X
	7	Eventuale rifiuto del pacchetto di versamento o dei documenti informatici, nel caso in cui le verifiche di cui alla fase 6 abbiano evidenziato delle anomalie		X
	8	Generazione, in modo automatico, del rapporto di versamento relativo a ciascun pacchetto di versamento		X
	9	Invio al Cliente del rapporto di versamento		X
	10	Preparazione e gestione del pacchetto di archiviazione		X
	11	"Chiusura" del pacchetto di archiviazione mediante sottoscrizione con firma digitale di ARUBA e apposizione di marca temporale		X
	12	Richieste di esibizione dei documenti informatici conservati	X	
	13	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
	14	Richiesta del Cliente di duplicati informatici	X	
	15	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 ARUBA dovranno definire, attraverso il perfezionamento del *Contratto* e degli allegati ad esso relativi, 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.

6 IL SISTEMA DI CONSERVAZIONE A NORMA

6.1 Infrastruttura informatica datacenter

I Data Center dal quale sono erogati i servizi si trovano sul territorio nazionale e sono conformi ai requisiti della normativa ISO/IEC 27001:2005.

Nelle due strutture che verranno messe a disposizione per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti tutta una serie di sistemi che permettono di garantire integrità degli ambienti e dei servizi.

Per maggiori dettagli si rimanda al paragrafo 12

6.2 Caratteristiche generali della soluzione di conservazione

La soluzione, come meglio descritto in seguito, presenta le seguenti caratteristiche peculiari:

- architettura di produzione implementata su infrastruttura virtuale e storage dedicati predisposta totalmente ridondata (HA) presso il Data Center di proprietà del gruppo Aruba, che rispetta le caratteristiche proprie della certificazione Tier IV dell'Uptime Institute, sito in via Gobetti 96, Arezzo;

- architettura secondaria predisposta per consentire la doppia scrittura del dato, effettuata applicativamente, e la replica sincrona storage based della piattaforma virtuale, inclusi i DB documentali e di gestione, situata presso il Data Center di proprietà del gruppo Aruba, sito in via Ramelli, Arezzo;

Il Sistema di Conservazione è sviluppato in modo modulare consentendo una facile scalabilità semplicemente aggiungendo unità e potenza elaborativa ai moduli sottoposti al maggior carico. Vista l'esperienza del Gruppo Aruba nell'ambito della gestione di grandi volumi di dati è sempre stato un obiettivo per il Gruppo creare architetture che possiamo definire elastiche: "espandibili" in caso di aumento del carico di lavoro oppure "limitabili" nel caso di una riduzione delle necessita.

L'intera soluzione è stata progettata per essere quindi in grado di gestire l'elaborazione di grandi volumi di dati, scalando sia verticalmente che orizzontalmente in ognuna delle sue singole componenti, con un elevato livello di affidabilità, distribuendo su più server fisici nodi con il medesimo ruolo ed evitando single point of failure.

L'architettura modulare del sistema e' implementata al 100% su infrastruttura di virtualizzazione con hypervisor vMWare e garantisce i sintesi i seguenti vantaggi:

Affidabilità - Totale ridondanza ai guasti HW

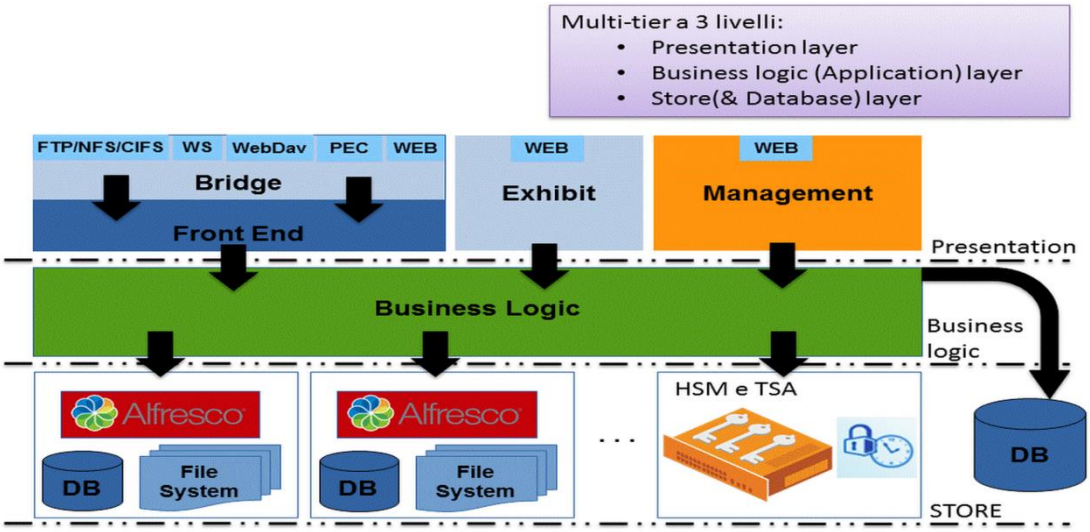
- Funzionalità di HA implementata dall'architettura virtuale.
- Almeno due moduli con il medesimo ruolo posizionati su server fisici separati.
- DBMS in configurazione Master-Master.
- Sistemi documentali duplicati "gemelli"
- Doppia scrittura dei documenti
- Utilizzo di sistemi di firma e marca ad alte prestazioni in HA

Architettura scalabile

- Nodi di Front-End ed Application multipli e contemporaneamente attivi.
- Storage di livello Enterprise ad alte prestazioni per la piattaforma VMware e le componenti DB
- Funzionalità di replica

6.3 Architettura logica

Di seguito riportiamo l'immagine rappresentativa delle componenti logiche del sistema di conservazione:



Come si evince dalla figura l'architettura è basata su una soluzione multi-tier a 3 livelli:

- **Presentation layer**: L'applicazione è pensata per essere scalabile, aumentando il numero dei Web container attraverso una logica di server clustering, gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client

- **Business logic (o application) layer**: La Business Logic implementa l'intelligenza necessaria per gestire le varie istanze di Alfresco sia in scrittura, duplicando l'informazione su almeno due di esse, sia in fase di ricerca, distribuendo le query sulle varie istanze disponibili. Tutte le istanze Alfresco sono sempre disponibili almeno in lettura

- **Store (& Database) layer**: la parte di back end è composta da diverse coppie di istanze di Alfresco. Ogni istanza è costituita dal DB e dal relativo file system. Il DB è duplicato in modalità Master-Master su due nodi predisposti sull'ambiente virtuale e contiene i metadati conservati; il FS contiene l'archivio (dati conservati) e non necessita di replica in quanto il dato viene scritto sempre su almeno due istanze (replica applicativa). Ognuna delle istanze è quindi replicata a livello applicativo e tale replica garantisce sia la salvaguardia delle informazioni trattate sia la continuità operativa in consultazione, qualora uno dei due nodi "gemelli" non dovesse essere disponibile.

6.4 Architettura fisica

La soluzione è composta da due infrastrutture fra loro interconnesse:

- un sito di Produzione completamente autosufficiente e con tutte le componenti ridondate in HA e collegato tramite fibre ottiche dedicate e di proprietà, con doppia via, al sito secondario,
- un sito Secondario di DR predisposto alla replica dei dati e con le componenti necessarie ad una ripartenza del servizio.

Tutte le componenti utilizzate sono di tipologia enterprise e, come tutte le soluzioni implementate da ARUBA, utilizzano prodotti di marche ampliamente riconosciute e leader del meracto di riferimento.

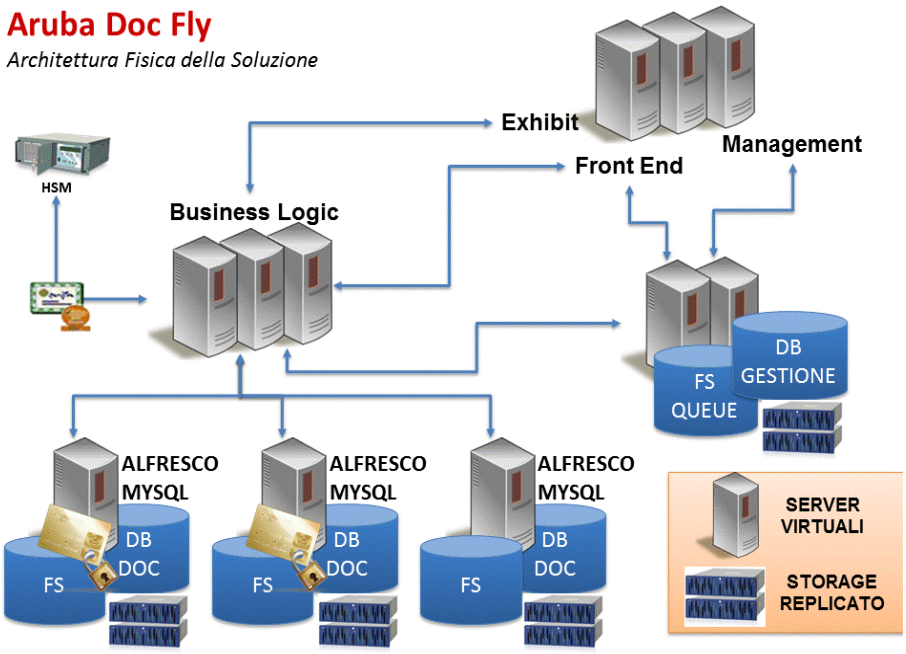
6.4.1 Sito Primario (Produzione)

Il sito di produzione ospita una infrastruttura virtuale basata su soluzione VMware sul quale vengono istallati:

- i nodi di Front-End (almeno due) per le interfacce di caricamento, esibizione e gestione,
- gli Application o Business Logic server (almeno due),
- le istanze della soluzione documentale Alfresco, un singolo nodo per ogni istanza,
- un nodo virtuale dedicato al DB server MSQL di ogni istanza Alfresco, la seconda copia in Master-Master è installata sul sito secondario,
- un nodo virtuale per la gestione delle code del sistema di caricamento,
- un nodo virtuale che implementa il DB MySQl che contiene tutte le informazioni per la gestione dell'infrastruttura (configurazione, accounting, etc.), la seconda copia in Master-Master è installata sul sito secondario,
- Storage di livello enterprise per l'archiviazione dei documenti;
- Link ed interfacce verso i sistemi di Firma e Marcatura presenti nel medesimo data Center

La figura sottostante schematizza quanto implementato sul sito principale senza entrare nelle specifiche modalità di replica.

Al fine di garantire i ridondanza e bilanciamento del traffico vengono utilizzati dispositivi di load balancing in grado di distribuire il carico di lavoro su un numero di macchine virtualmente illimitato. Questo meccanismo permette di risolvere oltre a problemi prestazionali con la semplice aggiunta a caldo di nuove macchine, anche problemi relativi ad eventuali guasti delle componenti bilanciate, nonché la manutenzione programmata dei singoli nodi.

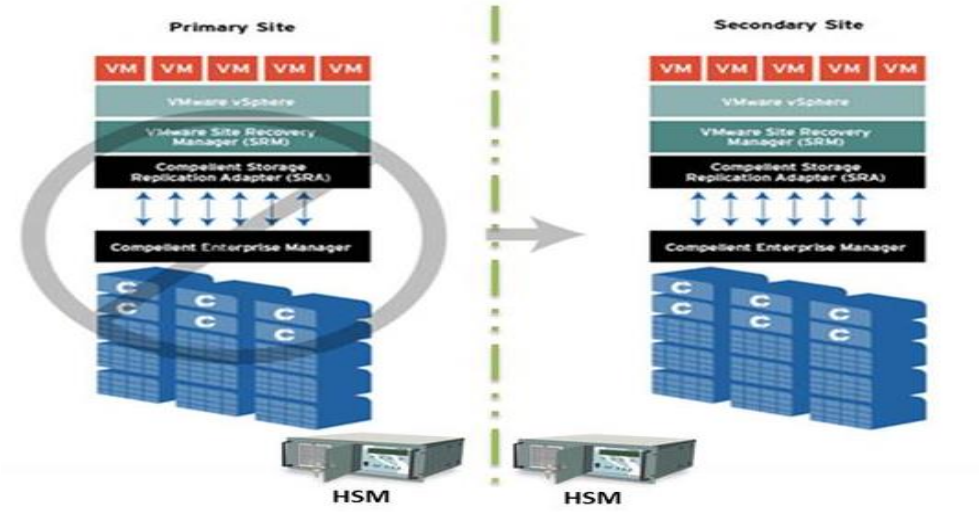


6.4.2 Sito Secondario (DR)

Il sito secondario ospita una infrastruttura virtuale basata su soluzione VMware sul quale vengono istallati:

- le istanze della soluzione documentale Alfresco, un singolo nodo per ogni istanza, gemelle di quelle presenti in produzioni,
- un nodo virtuale dedicato al DB server MSQL di ogni istanza Alfresco, la seconda copia in Master-Master è installata sul sito primario,
- un nodo virtuale che implementa la copia del DB MySQl che contiene tutte le informazioni per la gestione dell'infrastruttura (configurazione, accounting, etc.), in configurazione Master-Master,
- Storage di livello enterprise per l'archiviazione dei documenti;
- Link ed interfacce verso i sistemi di Firma e Marcatura presenti nel medesimo data Center;
- Predisposizione di tutte le altre componenti necessarie per l'erogazione del servizio dal sito secondario attraverso la replica delle macchine virtuali predisposte sul sito prioomario. I nodi virtuali replicati e da attivare in caso di necessità sono:
- i nodi di Front-End,
- gli Application o Business Logic server,
- il nodo virtuale per la gestione delle code del sistema di caricamento.

La figura sottostante schematizza la modalità di replica delle componenti non replicate applicativamente, ad esclusione quindi dei dati archiviati, replicati con doppia scrittura e DB MySQL, configurati in Master-Master.



In caso di problemi sul sito di Produzione è possibile effettuare:

- l'immediata riattivazione delle VM alla dichiarazione di Disastro,
- riconfigurazione dei collegamenti di rete,
- riattivazione del servizio con nessuna perdita di dati (RPO=0)
- raggiungibilità del servizio (che di fatto rappresenta l'RTO) pari alla diffusione del nuovo indirizzamento nei sistemi DNS
-

7 I LIVELLI DI SERVIZIO

I livelli di servizio relativi all'offerta standard, sono riportati nella tabella in basso e rappresentano le metriche di servizio che devono essere rispettate dal conservatore ARUBA nei confronti dei propri clienti/utenti. Di fatto, una volta stipulato il contratto, assumono il significato di obblighi contrattuali.

Caratteristiche Generali del Servizio	Specifiche Tecniche
SLA complessiva sul servizio	99,95%
Assistenza	Inclusa attraverso il canale ticketing e telefonico
Periodo di fatturazione	Annuale
Durata minima contratto	Un anno (eventuali upgrade richiesti in seguito alla stipula del contratto andranno ad allinearsi alla scadenza riportata sul contratto stesso)
Datacenter su cui è attivabile il servizio	DC1-IT (http://datacenter.aruba.it)
Fasi elaborazione Pacchetti di Versamento	**Specifiche Tecniche**
Presa in carico del PdV (rapporto di versamento)	Entro 48h dal ricevimento dell'ultimo documento contenuto nel pacchetto di versamento
Invio in conservazione del PdV	Entro 96h dal ricevimento dell'ultimo documento contenuto nel pacchetto di versamento

Comunicazioni durante il processo	Specifiche Tecniche
Rapporto di Protocollo – PdV Caricato	Entro 4h dalla ricezione dell'indice del PdV
Rapporto di Verifica – PdV Verificato	Entro 6h dalla ricezione dell'indice del PdV
Rapporto di Versamento – PdV Validato	Entro 4h dalla effettiva presa in carico del PdV
Rapporto di Consegna – PdV Conservato	Entro 4h dall'effettiva conservazione del PdV
Richiesta di Esibizione	**Specifiche Tecniche**
Produzione del Pacchetto di Distribuzione	Entro 24h dalla richiesta di produzione del PdD

8 I PROCESSI

In questo capitolo sono riportate tutte le fasi inerenti il processo di conservazione dei documenti informatici

8.1 Descrizione dei pacchetti di versamento e predisposizione del 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,* nel *Contratto* e nei rispettivi allegati.

L'operazione di versamento consiste nella trasmissione dei documenti da conservare e dei meteadati che li specializzano, così come già accennato precedentemente

8.1.1 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: ricezione dell'Indice del Pacchetto di Versamento (IPdV) e ricezione dei documenti che fanno parte del Pacchetto di Versamento (PdV).

L'uno e gli altri possono essere trasmessi al sistema di conservazione attraverso canali diversi. Alternativamente essi possono essere:

- interfaccia web
- invocazione di metodi tramite web service REST
- invio in allegato a una mail PEC
- trasferimento via protocollo FTP

Ogni canale messo a disposizione è provvisto di opportuni accorgimenti per la trasmissione dei dati in modalità sicura:

- l'interfaccia web viaggia su protocollo HTTPS
- il web service REST è contattabile tramite protocollo HTTPS
- la PEC nativamente garantisce autenticità della provenienza e notifica di consegna in modalità sicura

- il server FTP è raggiungibile via SFTP

Per il completamento delle operazioni di conservazione di un PdV non è necessario scegliere esclusivamente uno dei canali sopra citati. La ricezione, anche in maniera asincrona, dei singoli componenti di un PdV possono arrivare anche da canali diversi.

Il sistema di conservazione si assume la responsabilità della presa in carico di un PdV solo dopo che tutte le sue parti (IPdV e relativi documenti) vengono correttamente ricevuti e superano con esito positivo i relativi controlli.

Tale operazione viene ufficialmente sancita dalla produzione del cosiddetto Rapporto di Versamento (RdV) che viene consegnato al cliente all'indirizzo PEC fornito nella fase contrattuale.

Poichè la produzione del RdV rappresenta formalmente la presa in carico del PdV da parte del sistema di conservazione, il RdV viene marcato temporalmente e firmato digitalmente direttamente o via delega dal Responsabile del Sistema di Conservazione.

8.1.2 Ricezione dell'indice del pacchetto di versamento

L'IPdV è un'evidenza informatica, ovvero un file, che descrive il versamento stesso e i documenti che ne fanno parte attraverso l'uso di metadati. Questi sono di carattere diverso a seconda che descrivano proprietà e qualità del pacchetto in genere o dei singoli documenti.

E' bene sottolineare che ogni PdV può contenere esclusivamente documenti della stessa tipologia, ovvero della stessa Classe Documentale. In questo senso l'elenco dei metadati dei singoli documenti è in qualche modo omogeneo.

Per consentire l'elaborazione automatica dei metadati il sistema di conservazione Aruba richiede l'incapsulamento degli stessi in un determinato formato XML, che di fatto costituisce l'IPdV.

In tale file sono contenute sezioni diverse che identificano la qualità dei metadati. Essi infatti possono essere caratteristici del PdV e del soggetto versante, rappresentare direttive speciali di elaborazione per la conservazione, descrittivi dei singoli documenti che si vogliono conservare, a loro volta distinti in standard, come indicato nel paragrafo 12.4, o definiti insieme al Cliente in fase di stipula del contratto e infine caratteristici del formato del documento.

La struttura dell'indice del pacchetto di versamento è definita nell'appendice 2.

La funzione di ricezione degli indici dei pacchetti di versamento nel sistema di conservazione effettua, per ogni indice, i seguenti controlli:

- abilitazione alla conservazione da parte del sistema di gestione documentale versante e in particolare dell'utente che effettua il versamento. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- controllo formale dell'indice versato. In particolare viene verificato che sia un formato XML valido per una delle Classi Documentali registrate a sistema. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- verifica, tramite l'id univoco contenuto nell'indice, dell'eventuale presenza del PdV già nel sistema. In caso di esito positivo il nuovo indice sostituisce in toto il vecchio. Di conseguenza vengono aggiornati tutti i metadati, tutti i documenti eventualmente versati e non più presenti nel nuovo indice vengono cancellati dal sistema e viene restituito un warning al Cliente
- controllo sulla completezza e correttezza formale dei metadati, in relazione alla Classe Documentale rilevata. In caso di esito negativo il sistema rifiuta il tentativo di versamento
- controllo sulla tipologia di documenti che si vuole versare. Ogni documento deve appartenere ad almeno uno dei formati ammessi dalla tipologia di Classe Documentale. In caso di esito negativo il sistema rifiuta il tentativo di versamento

- eventuali controlli supplementari definiti insieme al Cliente. La gestione degli esiti negativi va formalizzato in sede contrattuale

8.1.3 Ricezione documenti associati ad un pacchetto di versamento

La ricezione dell'IPdV permette al sistema di conservazione di registrare i metadati del PdV e di mettersi in attesa dei documenti per la conservazione del pacchetto.

Relativamente al singolo documento tra i metadati indicati nell'IPdV sono di particolare importanza quelli utili all'identificazione dello stesso. Essi sono principalmente 2: un identificativo univoco utile all'identificazione human readable del documento e un hash del file stesso, ovvero una stringa di caratteri che normalizza con un particolare algoritmo in maniera univoca il documento stesso.

In particolare l'hash, che per il sistema di conservazione Aruba deve essere in formato SHA256 base64, garantisce la riconoscibilità e incorruttibilità del documento in forma automatica e univoca.

Nel momento in cui un documento viene ricevuto da uno qualsiasi dei canali esposti precedentemente, ne viene calcolato l'hash in SHA265 e base64. Se il risultato è tra quelli precedentemente comunicati in uno dei IPdV ricevuti e non ancora in conservazione, allora il file viene accettato.

Successivamente la funzione di ricezione dei documenti informatici nel sistema di conservazione effettua una serie di controlli atti a verificare formalmente leggibilità, integrità e la corrispondenza del documento alle regolamentazioni stabilite per la Classe Documentale di appartenenza. Per operare ciò il sistema determina il formato dello stesso sulla base di quanto esposto in precedenza (estensione e mimetype).

La mancata identificazione del formato del file causa il rifiuto dello stesso con conseguente restituzione di un errore.

Una volta individuato il formato del documento viene controllato che questo sia tra i formati ammessi per la Classe Documentale di appartenenza. Nel caso di esito negativo il file viene rifiutato e viene restituito un errore. Superati i primi controlli, ne vengono operati degli altri relativamente alla qualità dello stesso.

Di seguito sono elencati i controlli eseguiti per ciascun formato trattato dal sistema di conservazione di ARUBA:

- **file PDF/A** viene preventivamente controllata la incorruttibilità del file simulandone l'apertura con un opportunno viewer
- **file P7M** viene controllata la validità e della marca temporale e della firma apposta sul documento. Nel caso di esito negativo il file viene rifiutato e viene restituito un errore. I controlli sulla firma prevedono le seguenti verifiche:
  - controllo di conformità.
  - controllo Crittografico.
  - controllo Catena Trusted.
  - controllo Certificato.
  - controllo CRL
- **file XML** viene controllata la correttezza formale del file mediante l'uso di un parser software. Nel caso venga fornito in fase contrattuale un file xsd che ne descriva le caratteristiche, esso viene applicato in maniera da verificarne l'aderenza.
- **File EML** vengono controllati gli header del file per verificare che si tratti realmente di una mail. Nel caso di mail PEC viene controllata anche la validità del certificato

Per i file in formati diversi da quelli sopra indicati i controlli vanno concordati col Cliente in fase contrattuale e a seconda delle caratteristiche tipiche del formato. Nel caso in cui nel sistema vengano inseriti dei formati imbustati (rar, zip, tar ad esempio), essi non vengono conservati. Vengono invece sbustati estraendone i documenti contenuti e procedendo con l'analisi di questi ultimi secondo quanto indicato nel presente capitolo.

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.

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

Tale rapporto viene anche inviato via email da un indirizzo PEC all'indirizzo PEC fornito dal cliente in fase contrattuale.

8.1.4 Predisposizione dei rapporti di versamento

Il sistema di conservazione predispone, per ciascun pacchetto di versamento, un **rapporto di versamento** che viene firmato dal Responsabile del Sistema di Conservazione. Lo schema del rapporto di versamento è illustrato nell'Appendice 3.

In particolare il rapporto di versamento contiene, tra l'altro, le seguenti informazioni:

- identificativo unico del PdV, come indicato nel relativo IPdV
- identificativo unico del PdV fornito dal sistema di conservazione
- data di ricezione dell'IPdV
- per ogni documento accettato viene indicato:
  - id univoco, come indicato nell'IPdV
  - id univoco fornito dal sistema di conservazione
  - hash
  - data di ricezione
  - esito della ricezione (accettato o warning)
  - descrizione warning, ove necessario

8.2 Controlli di Sistema e Gestione degli scarti

Le funzionalità attivate nel processo di versamento/acquisizione del pacchetto di versamento prevedono dei controlli sia nella fase di ricezione dell'indice del PdV che sui singoli documenti inviati e corrispondenti a quanto previsto nell'indice stesso. La tabella riportata in basso elenca le diverse tipologie di controlli effettuati e per ognuna di esse indica l'azione prevista da sistema. Quest'ultima può tradursi in una operazione di scarto o notifica di un warning.

Controlli dell'indice del Pacchetto di versamento

Il deposito di un pacchetto di versamento e' distinto per ciascun lotto di documenti informatici omogenei (documenti omogenei, ossia aventi la stessa classe documentale). Pertanto, a classi documentali diverse corrispondono diversi PdV e versamenti, uno per ogni classe.

Controlli nella fase di ricezione dell'indice del PdV

ID	Oggetto del controllo	Azione in caso di check negativo
Verifica Autorizzazioni		
1.01	viene verificato che l'utente che effettua il versamento sia abilitato all'invio dei Pdv	Il sistema scarta l'intero pacchetto
Verifica formale indice del PdV		

2.01	viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard DocFly	Il sistema scarta l'intero pacchetto
2.02	viene verificato che il PdV è versato nei termini contrattuali e di servizio stabiliti col produttore	WARNING: Il sistema accetta il PdV ma non garantisce la conservazione nei termini concordati
Verifica presenza dati-documenti nell'indice del PdV		
3.01	viene verificato che l'indicazione del sistema di conservazione sia corretta	Il sistema scarta il PdV poiché il metadato contenuto nell'indice indica un sistema di conservazione diverso da DocFly
3.02	viene verificato che l'identificativo specificato nel Pdv non sia già presente nel sistema di conservazione	Il sistema verifica se il PdV (che contiene lo stesso ID) non sia già stato conservato. In questo caso il sistema considera il nuove indice in sostituzione del precedente. Viene invece scartato qualora il PdV risulta essere in stato 'conservato'.
3.04	viene effettuato un controllo semantico sui metadati presenti nell'indice del PdV	Il sistema scarta il PdV poiché uno o piu' metadati non rispettano il formato condiviso nel contratti di servizio
3.05	viene controllato che per ciascun documento dichiarato e descritto all'interno dell'indice del Pdv: a. tutti i metadati minimi obbligatori siano presenti e nel formato corretto; b. il formato del documento è un formato ammesso c. l'estensione del documento sia tra quelle ammesse per il tipo documento; d. il formato dichiarato sia corrispondente all'estensione del nome file	Il sistema scarta il PdV perché le verifiche formali sui documenti dichiarati nell'indice del PdV hanno avuto esito negativo
Verifiche Paternità		
4.01	viene verificato che il Pdv, nel caso abbia estensione P7M, sia firmato con certificato valido	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo
4.02	viene verificato che tutte le firme apposte al Pdv siano valide	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo

Controlli nella fase di ricezione dei documenti

A seguito della corretta ricezione dell'indice del PdV, il sistema di conservazione è pronto per la ricezione dei relativi documenti informatici (files) descritti nel pacchetto stesso

Controlli nella fase di ricezione dei documenti (files)

Controllo ricezione documenti		
1.01	viene verificato che l'hash del documento informatico inviato sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta correttamente e che l'integrità del documento informatico ricevuto sia assicurata	Il sistema scarta il documento poiché non atteso
1.02	in caso di file P7M viene verificata la validità della firma apposta su ogni singolo documento: o Controllo di conformità. o Controllo Crittografico. o Controllo Catena Trusted. o Controllo Certificato. o Controllo CRL	Il sistema scarta il documento qualora il certificato di firma non sia valido WARNING: in caso di documenti firmati e il certificato di firma utilizzato e' prossimo alla scadenza, il sistema evidenzia un warning.
1.03	viene verificato che il documento sia leggibile	Il sistema scarta il documento nel caso questo non sia leggibile
1.02	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.	Il sistema scarta il documento poiché il formato non e' quello atteso
1.03	viene verificato che i documenti ricevuti non siano già presenti nel sistema di conservazione;	WARNING: il documento viene accettato e il sistema invia una notifica
1.04	viene verificato che la ricezione dei documenti si sia correttamente conclusa entro la data limite di ricezione stabilita col produttore nel contratto di servizio	WARNING: il documento viene accettato ma il sistema non garantisce la conservazione nei termini concordati

8.3 Descrizione delle tipologie dei documenti sottoposti a conservazione

Come chiaramente esplicitato nel *Contratto*, 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 ARUBA, evidenziandone le caratteristiche nell'apposito allegato del *Contratto*.

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

ARUBA 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 (vedi apposito allegato al *Contratto*).

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 ARUBA e configurato sul servizio.

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.

E' prevista la possibilità di depositare in conservazione documenti informatici non sottoscritti. In tal caso deve necessariamente essere preventivamente dichiarata, per ogni classe/tipo di documento, nell'apposito allegato del *Contratto*.

8.4 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 imma-

gine 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.

8.5 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.

8.5.1 Caratteristiche generali dei formati

I formati scelti devono essere, puntualmente richiamati nell'apposito allegato al *Contratto.* ARUBA, comunque 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, ARUBA 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.

8.5.2 Formati per la conservazione

Oltre al soddisfacimento delle caratteristiche suddette, nella scelta dei formati idonei alla conservazione, ARUBA 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 ARUBA** 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 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 - http://www.w3.org/
	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 Qualsiasi editor di testo. Inoltre è possibile, concordando con il Cliente le caratteristiche di un opportuno file xslt, produrne una copia human readable con Microsoft Internet Explorer / Firefox / Google Chrome o altri browser	

Formato	**Descrizione**
EML	Electronic Mail Message (EML) è un formato di testo che definisce la sintassi di messaggi di posta elet-

	tronica scambiati tra utenti	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Messaggi di posta elettronica e PEC
	Sviluppato da	Internet Engineering Task Force (IETF) - http://www.ietf.org/
	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 nell'apposito allegato del *Contratto*, **sono esclusivamente quelli richiamati nel presente capitolo**.

8.5.3 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;
4. l'utilizzo di tool automatici specifici come Apache TIKA

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

1	**Fase di IDENTIFICAZIONE**	Ogni documento che viene inviato al sistema di conservazione deve essere stato precedentemente ed espressamente indicato dal sistema versante. In questo modo tutti i documenti non noti vengono automaticamente non riconosciuti e quindi rifiutati
2	**Fase di RICEZIONE**	Il sistema Aruba, una volta noti i documenti che il Cliente vuole mettere in conservazione si mette in attesa, secondo i canali concordati, della loro ricezione
3	**Fase di VALIDAZIONE**	Una volta che i documenti vengono recepiti dal sistema di conservazione la prima elaborazione effettuata sugli stessi è quella del rilevamento della

		tipologia corretta del documento. Solo se questo esame restiutisce esito positivo vengono realizzate ulteriori validazioni atte a garantire la correttezza formale del documento, secondo gli standard qui esposti e gli accordi convenuto col Cliente

8.5.4 Verifica della leggibilità dei documenti informatici

Per assicurare la leggibilità dei documenti informatici ARUBA 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, ARUBA 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.

ARUBA, 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:

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

Il controllo di leggibilità eseguito da ARUBA 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).

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.

8.5.5 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.

8.6 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 decidere di 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 nello spazio ad essi riservato nell'apposito allegato del *Contratto* e verranno opportunamente gestiti da Aruba come in esso concordato.

8.6.1 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
   - Codice Fiscale
5. l'eventuale destinatario
   - nome
   - cognome

- Codice Fiscale (unico dato obbligatorio del destinatario)

come meglio di seguito definiti:

01		
Informazione	**Valori Ammessi**	**Tipo dato**
Identificativo univoco e persistente	Come da sistema di identificazione formalmente definito.	Alfanumerico 20 caratteri

02		
Informazione	**Valori Ammessi**	**Tipo dato**
Data di chiusura	Data	Data formato gg/mm/aaaa

03		
Informazione	**Valori Ammessi**	**Tipo dato**
Oggetto	Testo libero	Alfanumerico 100 caratteri

04		
Informazione	**Valori Ammessi**	**Tipo dato**
Soggetto che ha formato il documento (Produttore)	nome: Testo libero	Alfanumerico 40 caratteri
	cognome: testo libero	Alfanumerico 40 caratteri
	Codice fiscale: Codice Fiscale	Alfanumerico 16 caratteri

05		
Informazione	**Valori Ammessi**	**Tipo dato**
Destinatario	nome: Testo libero	Alfanumerico 40 caratteri
	cognome: testo libero	Alfanumerico 40 caratteri
	Codice fiscale: Codice Fiscale	Alfanumerico 16 caratteri

8.6.2 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
numero di protocollo del documento	Come da sistema di protocollo del Cliente	Numerico

02

Informazione	Valori Ammessi	Tipo dato
data di registrazione di protocollo	Data	Data formato gg/mm/aaaa

03

Informazione	**Valori Ammessi**	**Tipo dato**
mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti	Testo Libero	Alfanumerico 255 caratteri

04

Informazione	**Valori Ammessi**	**Tipo dato**
Oggetto del documento	Testo libero	Alfanumerico 2000 caratteri

05

Informazione	**Valori Ammessi**	**Tipo dato**
data e protocollo del documento ricevuto, (se disponibile)	Come da sistema di protocollo del Cliente	Numerico
	Data	Data formato gg/mm/aaaa

06

Informazione	**Valori Ammessi**	**Tipo dato**
l'impronta del documento informatico	Hash documento	SHA-256

Oltre al set minimo di metadati, il Cliente potrà decidere di 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 nell’o spazio ad essi riservato nell’apposito allegato del *Contratto* e verranno opportunamente gestiti da Aruba come in esso concordato.

8.6.3 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 Appendice 1 "*Documenti rilevanti ai fini delle disposizioni tributarie: Elenco tipi documento*";

come meglio di seguito definiti:

01		
Informazione	**Valori Ammessi**	**Tipo dato**
cognome	Testo libero	Alfanumerico da 1 a 60 caratteri

02		
Informazione	**Valori Ammessi**	**Tipo dato**
Nome	Testo libero	Alfanumerico da 1 a 30 caratteri

03		
Informazione	**Valori Ammessi**	**Tipo dato**
denominazione	Testo libero	Alfanumerico da 1 a 60 caratteri

04		
Informazione	**Valori Ammessi**	**Tipo dato**
Codice fiscale	Testo formattato secondo le regole previste per il codice fiscale	Alfanumerico di 16 caratteri

05		
Informazione	**Valori Ammessi**	**Tipo dato**
Partita IVA	Numeri interi secondo le regole previste per la partita IVA	Sequenza di 11 numeri

06		
Informazione	**Valori Ammessi**	**Tipo dato**
Data documento	Data	Data formato gg/mm/aaaa

07		
Informazione	**Valori Ammessi**	**Tipo dato**
Periodo d'imposta di riferi-	Da Data a Data	Data formato da gg/mm/aaaa a

mento		gg/mm/aaaa

08		
Informazione	**Valori Ammessi**	**Tipo dato**
Tipo documento	Identificativo univoco del tipo di documento di appartenenza	Valore numerico compreso da 1 e 999999999999

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, nell'apposito allegato del *Contratto*, 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 decidere di 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 nello spazio ad essi riservato nell'apposito allegato del *Contratto* e verranno opportunamente gestiti da Aruba come in esso concordato.

8.7 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.

8.8 Trattamento dei pacchetti di archiviazione

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

8.8.1 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 ARUBA per la "chiusura" del pacchetto di archiviazione.

Con la sottoscrizione dei pacchetti di archiviazione ARUBA 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.

8.8.2 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 ARUBA 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.

8.8.3 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.

8.8.4 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.

8.9 Processo di esibizione 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.

8.10 Modalità di svolgimento del processo di esibizione

L'utente può richiedere la creazione di un pacchetto di distribuzione contenente il documento digitale o l'insieme dei documenti digitali, corredati da tutti o parte dei metadati previsti nel pacchetto di archiviazione. Nel modello OAIS e in linea con la normativa vigente, il pacchetto di distribuzione è strutturato nel modello dati come il pacchetto di archiviazione . La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).

In questo caso, un PdD può anche non coincidere con il pacchetto di archiviazione originale conservato: anzi, molto spesso, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un PdA. Può anche verificarsi il caso di pacchetto di distribuzione che sono il frutto di più PdA che vengono "spacchettati" e reimpacchettati per un più fruibile utilizzo da parte dell'utente.

Un utente autorizzato da un soggetto produttore, quindi, è in grado di interrogare il sistema per ricevere in uscita uno specifico pacchetto di distribuzione. L'utente utilizzerà le funzionalità di richiesta di esibizione di un documento o di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.

In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema di conservazione risponderà restituendo un PdD che nel caso più completo conterrà:

- Nome (ID) dei files/ documenti richiesti nel formato previsto per la loro visualizzazione e conetnuti nel pacchetto.
- Un'estrazione dei metadati associati ai documenti.
- L'indice di conservazione firmato e marcato dal Responsabile del Servizio di Conservazione o delegato.
- Indice del Pacchetto di Archiviazione di appartenenza (qualora richiesto)
- I viewer necessaria alla visualizzazione dei documenti del pacchetto

A fronte di una richiesta di produzione del pacchetto di distribuzione, il sistema effettua delle verifiche di coerenza e correttezza del pacchetto e dei documenti in esso contenuti. A tal proposito, il sistema di conservazione verifica che le impronte dei documenti restituiti nel PdD corrispondano a quelle presenti nel relativo indice del pacchetto di archiviazione; in modo da garantire che i documenti stessi non abbiano subito alterazioni o modifiche nei contenuti.

8.11 Tabella riepilogativa delle fasi del 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	Consiste nella ricezione dell'IPdV

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 In questa fase vengono condotti i controlli sull'IPdV

FASE 3	Preparazione del rapporto di conferma
	Descrizione sintetica A seconda dell'esito del controllo sull'IPdV viene prodotto un rapporto di conferma che viene restituito al sistema versante. **NOTA BENE:** il rapporto di conferma non implica la presa in carico del versamento da parte del sistema

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 Alternativamente alla fase 3 viene restituito al sistema versante l'indicazione di eventuali anomalie. In tale caso il versamento viene rifiutato

FASE 5	Ricezione dei documenti
	Descrizione sintetica Il sistema si mette in attesa dei documenti del PdV

FASE 6	Verifica dei documenti
	Descrizione sintetica In questa fase vengono condotti i controlli specifici del documento ricevuto

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 Una volta ricevuti correttamente, o con warning, tutti i documenti del PdV viene prodotto il PdV

FASE 8	Sottoscrizione del rapporto di versamento con firma digitale apposta da ARUBA
	Descrizione sintetica Il RdV viene firmato digitalmente dal Responsabile del Sistema di Conservazione o da un suo delegato. Infine il RdV viene inviato al Cliente via email PEC. In questa fase Aruba prende in carico il versamento ufficialmente

FASE 9	Preparazione e gestione del pacchetto di archiviazione (c.d. File di chiusura)	
	Descrizione sintetica	Il File di Chiusura è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualificata, corroborata da una marca temporale. La struttura del file di chiusura è costruita sulla base delle specifiche della struttura dati (UNI 11386:2010) contenute nell'allegato 4 alle regole tecniche e secondo le modalità riportate nel manuale della conservazione

FASE 10	Sottoscrizione del pacchetto di archiviazione con firma digitale apposta da ARUBA 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	Il Pacchetto di Archiviazione (PdA), che viene costruito dal versamento di uno o più PdV, viene "chiuso" nel momento in cui tutti i PdV sono stati presi in carico dal sistema. La chiusura viene sancita dall'apposizione di opportuna marca temporale, per stabilirne l'istante di creazione, e firma digitale del Responsabile del Sistema di Conservazione o di un suo delegato, per garantirne l'immodificabilità. Con la suddetta firma apposta in calce al file di chiusura e la suddetta dichiarazione il conservatore NON SOTTOSCRIVE il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel rispetto delle norme giuridiche e delle indicazioni contrattuali di servizio.

FASE 11	Preparazione e sottoscrizione con firma digitale di ARUBA del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente	
	Descrizione sintetica	Il pacchetto di distribuzione (PdD) è definito in base alle esigenze del richiedente e può contenere anche un set parziale di metadati. È generato a partire dai pacchetti di archiviazione. Nel caso più semplice il PdD contiene dei duplicati del PdA. In alternativa esso può essere costituito da una scelta di documenti conservati selezionati attraverso una o più interrogazioni. I risultati di tali ricerche possono essere raccolti in un'area di lavoro e da qui può essere prodotto il PdD voluto.

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	Per duplicato informatico si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche in materia di formazione del documento informatico, ovvero se contiene la stessa sequenza di bit del documento informatico di origine.

FASE 13	Eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dal *Contratto* di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso	
	Descrizione sintetica	Alla scadenza dei termini di conservazione, il cliente in autonomia puo' decidere di cancellar ei documenti in conservazione.

8.12 Procedure per la produzione di duplicati o copie

Nei successivi paragrafi vengono descritte le procedure adottate per la produzione di duplicati o copie.

8.12.1 Produzione di duplicati

La produzione di duplicati informatici dei documenti conservati può avvenire a seguito di una richiesta proveniente dal dipartimento tecnico 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 dal sistema di conservazione. 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.

8.12.2 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 ARUBA, 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.

8.13 Tempi di scarto o di trasferimento in conservazione dei documenti

8.13.1 Trasferimento dei documenti informatici in conservazione

Nella scheda di conservazione, parte integrante del contratto di servizio e sottoscritta dal cliente, sono indicati i tempi entro i quali le diverse tipologie di documenti devono essere trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel Manuale di gestione.

8.13.2 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, una volta scaduti i termini previsti dalla legge il Cliente riceve una notifica via PEC dal sistema di conservazione e in autonomia può decidere di eliminare i documenti conservati attraverso le funzionalità previste dal sistema di conservazione.

9 DOCUMENTI RILEVANTI AI FINI DELLE DISPOSIZIONI TRIBUTARIE

9.1 Caratteristiche dei documenti rilevanti ai fini delle disposizioni tributarie

In considerazione di quanto previsto dall'art. 21, co. 5, del CAD[3], 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 ARUBA.

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

[3] 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.";

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

ARUBA 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.

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* (ed, eventualmente, degli ulteriori previsti nell'apposito allegato del *Contratto*) 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.

9.1.1 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.

9.2 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 ad ARUBA il pacchetto di versamento, contenente i DIRT da sottoporre a conservazione, rigorosamente entro i termini stabiliti nell'apposito allegato del *Contratto*; tale termine è necessario ad ARUBA per "chiudere" in conservazione il pacchetto di archiviazione entro i termini perentori previsti dalla legge.

10 SICUREZZA DEL SISTEMA DI CONSERVAZIONE

ArubaPEC ha implementato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO 27001. Nell'ambito del Sistema di Conservazione proposto sono adottate misure di sicurezza fisica, logica e organizzativa coerenti con tale SGSI e con la normativa vigente in tema di protezione dei dati personali (D.lgs. 196/2003).

10.1 Privacy e requisiti di sicurezza dei dati

ARUBA esegue il trattamento dei dati personali in conformità a quanto previsto dal D.lgs. 196/2003 e dalla normativa vigente in materia; ciascun trattamento di dati personali è improntato ai principi di correttezza, liceità e trasparenza nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Tutte le misure minime di sicurezza obbligatorie previste dal Disciplinare Tecnico allegato al D.lgs. 196/2003, sono adottate dalla scrivente società, nonché quelle ulteriori previste dalla normativa vigente e dai Provvedimenti del Garante per la Protezione dei Dati Personali, e si è dotata di adeguate misure informatiche ed organizzative atte a garantire la sicurezza, l'integrità e la riservatezza dei dati personali trattati.

Con specifico riferimento ai compiti affidati con la nomina a Responsabile esterno al trattamento dei dati personali ai sensi dell'art. 29 D.Lgs. n. 196/2003, ARUBA comunica di ottemperare alle seguenti attività in merito a: (i) la designazione per iscritto delle persone fisiche incaricate del trattamento e l'individuazione dei diversi livelli di accesso di ciascun incaricato del trattamento in corrispondenza delle specifiche mansioni ad esso attribuite; (ii) il rispetto delle prescrizioni del Garante per la protezione dei dati personali del 27 novembre 2008, "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle funzioni di amministratore di sistema*" e successive modifiche e integrazioni; (iii) il rispetto delle prescrizioni di cui al *Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazione di dati personali (c.d. data breach) – 4 aprile 2013* emesso dal Garante per la Protezione dei Dati Personali e l'impegno di comunicare senza indebito ritardo al Cliente e comunque entro i termini previsti nel predetto provvedimento gli eventi e le informazioni necessarie a consentire al Cliente di adempiere agli obblighi di notifica al Garante e al contraente della violazione dei dati personali, come previsto dall'art. 32-bis co. 1 e 2 D. Lgs n. 196/03.

ARUBA adotta tutte le misure ivi richieste per il trattamento dei dati personali effettuato nell'erogazione dei servizi di Conservazione Sostitutiva ed in genere nell'esecuzione delle prestazioni ad essa affidate, nonché di quelle ulteriori prescritte dalla normativa vigente e dai Provvedimenti del Garante per la Protezione dei Dati Personali in merito.

ARUBA s'impegna a non divulgare, comunicare o diffondere le informazioni e i dati dei quali verrà a conoscenza durante l'espletamento delle attività. Inoltre si impegna a rispettare, nello svolgimento delle attività oggetto dell'appalto, tutti i principi, contenuti nelle disposizioni normative vigenti, relativi al trattamento dei dati personali e in particolare quelli contenuti nel D.Lgs n° 196/03 e garantisce che le informazioni personali, patrimoniali, statistiche, anagrafiche, e/o di qualunque altro genere, di cui verrà a conoscenza in conseguenza dei servi-

zi resi, in qualsiasi modo acquisite, vengano considerati riservati e come tali trattati. Si impegnerà infine a dare istruzioni al proprio personale affinché tutti i dati e le informazioni vengano trattati nel rispetto della normativa di riferimento.

10.2 Analisi dei Rischi

ArubaPEC ha svolto un'analisi dei rischi sul Sistema di Conservazione estesa agli aspetti di sicurezza fisica, logica ed organizzativa, incluso il coinvolgimento di enti esterni (fornitori); l'analisi è riportata nel relativo **Piano della Sicurezza** .

10.3 Controllo Accessi

Gli utenti possono accedere – previa identificazione ed autenticazione – solamente alle risorse (es. sistemi, funzionalità, informazioni) per cui sono stati esplicitamente autorizzati in base al ruolo ricoperto. I permessi sono attribuiti alle utenze secondo il principio del "least privilege" e rivisti periodicamente per mitigare il rischio di abuso di privilegi. Ad ogni persona (interna od esterna) viene assegnata un'utenza personale e univoca. Le utenze di gruppo sono usate solo per esigenze particolari ed espressamente autorizzate.

10.4 Monitoraggio Eventi e Vulnerabilità di Sicurezza

Nell'ambito del Servizio di Conservazione, viene conservata e periodicamente esaminata una traccia (**audit log**) delle operazioni svolte dagli utenti e dai processi, in modo che tali azioni possano essere documentate ed attribuite a chi le ha eseguite o causate (accountability), anche allo scopo di rilevare eventi di sicurezza, incidenti e vulnerabilità associati ai sistemi coinvolti nel processo di conservazione. Tali log vengono archiviati su supporto permanente e non è permesso agli utenti non autorizzati di accedervi.

10.5 Cifratura

Come previsto dal Piano della Sicurezza del Servizio di Conservazione di ArubaPEC, tutte le comunicazioni tra il Sistema e gli utenti (interattivi o applicativi) sono protette col protocollo sicuro SSL/TLS e pertanto sono cifrate. Per la cifratura del canale, si utilizzano algoritmi di cifratura con chiavi di lunghezza ≥ 128 bit.

10.6 Backup

Nell'ambito della gestione operativa del Servizio di Conservazione, sono definite ed applicate procedure di backup finalizzate alla creazione e conservazione di copie di sicurezza dei dati, dei software applicativi, delle loro configurazioni e di ogni altra informazione necessaria per ripristinare il servizio in caso di necessità (per es. a fronte di guasti hardware o incidenti più severi).

Nello specifico ARUBA realizzerà il servizio di Backup geografico nel sito di Disaster Recovery: un server dedicato ad alte prestazioni gestirà in automatico i backup in uno spazio riservato, offrendo servizio di retention 8-4-3, ovvero 8 backup giornalieri, 4 settimanali e 3 mensili su tutti i dati di produzione.

Il backup geografico su macchina dedicata è una soluzione che permette di garantire un recovery dei dati ottimale per il fatto che esso è connesso con link dedicato a 1Gbps su una diversa sede. Anche in caso di disastro quindi è possibile accedere ai dati di backup di settimane e mesi precedenti.

I dati vengono scritti e salvati sempre in duplice copia sincrona sui sistemi di storage distribuiti geograficamente con la garanzia dell'effettiva scrittura su entrambi i siti. Su i due storage utilizzati inoltre vengono effettuate copie di sicurezza attraverso meccanismi di snapshot e backup per garantire la massima salvaguardia del dato.

I metadati e i dati utenti sono salvati su istanze dedicate distribuite su due siti geografici distinti e configurate in mirror transazionale in modo da avere una duplicazione non solo del dato ma anche di tutti i metadati necessari alla propria reperibilità e ricerca.

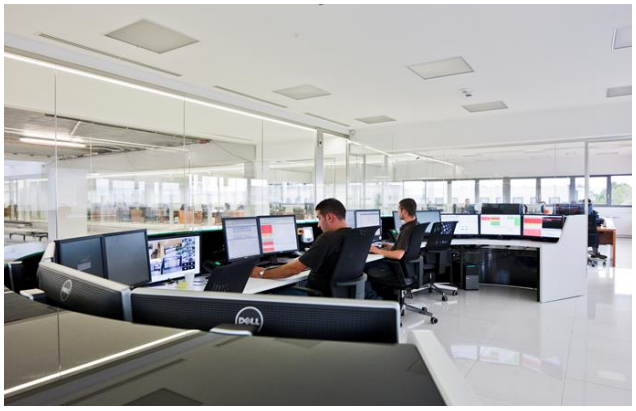
Per quanto riguarda i **documenti**, si fa presente che essi sono sempre conservati in **doppia copia**, ciascuna presso un data center separato (per i documenti, dunque, non vi è una reale distinzione tra copia di produzione e copia di backup).

10.7 Isolamento delle componenti critiche

I sistemi e le risorse tecnologiche alla base del Servizio di Conservazione sono isolate dagli altri ambienti di elaborazione a livello fisico e logico (in quanto risiedono su hardware dedicato a tale Servizio), nonché parzialmente a livello organizzativo, in coerenza coi requisiti indicati nel Piano della Sicurezza e nel Manuale della Conservazione.

10.8 Sicurezza fisica datacenter del Gruppo Aruba

Nelle due strutture che verranno messe a disposizione per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti tutta una serie di sistemi che permettono di garantire integrità degli ambienti e dei servizi.



I datacenter sono situati in un'area classificata come di "basso rischio idrogeologico", inoltre l'edificio è completamente antisismico ed è posto ad un piano rialzato dal livello stradale, in modo da risultare maggiormente protetto alle calamità naturali.

Sia il datacenter primario che quello secondario, sono continuamente monitorati e dotati delle soluzioni di sicurezza più avanzate descritte in seguito.

10.8.1 Sicurezza Fisica Data Center Primario

L'edificio primario e' situato ad Arezzo in via Gobetti e risponde ai requisiti stringenti TIER IV. Il datacenter è stato progettato ponendo la massima attenzione alla **sicurezza fisica degli accessi**:

- le **porte esterne** sono di tipo blindato;
- le **finestre** e le **superfici vetrate esterne** a piano terra sono dotate di vetro antiproiettile dello spessore di 21 mm;
- le **griglie per il passaggio dell'aria** necessaria al raffreddamento della sala dati sono protette da sbarre trasversali in acciaio del diametro di 20 mm.

L'**accesso dei visitatori** avviene attraverso una "**bussola**" a due ante rotanti e interbloccate, analoga a quelle normalmente utilizzate negli istituti bancari - anch'essa dotata di vetri anti-proiettile da 21 mm di spessore. Una volta avuto accesso all'interno, è presente una seconda barriera, costituita da varchi motorizzati. Per attraversare tali varchi è necessario essere accreditati alla antistante Reception, con lo scopo di ottenere un badge abilitato. Per la registrazione dei visitatori, è istituito un apposito registro conservato in conformità con quanto previsto dalla **normativa ISO 27001**.

Superata la barriera dei varchi motorizzati, si trova davanti la sala dati principale, delimitata da una parete in vetro antiproiettile da 21 mm. L'accesso, consentito solo al personale abilitato, avviene tramite porte scorrevoli di sicurezza assoggettate al controllo accessi. L'intero stabile è circondato da una resede che lo separa su tutti i lati dalle altre proprietà, e protetto da una recinzione rigida in metallo dell'altezza di 260 cm. La struttura è presidiata e sorvegliata 24x7x365.

Il **data center** è dotato di un **sistema di controllo accessi** esteso a tutti i varchi, sia esterni (ingresso principale, uscite di sicurezza, magazzini, locali tecnici) che interni (sale dati, locali tecnici, uffici). Il riconoscimento è basato su un doppio criterio di autenticazione, mediante l'utilizzo di una tessera di prossimità e la digitazione di un pin. Il sistema di gestione degli accessi prevede la possibilità di abilitare e disabilitare le singole tessere in base alle aree, agli orari ed ad altri parametri, in modo da garantire sia la massima sicurezza degli ambienti che la necessaria fluidità degli accessi. E' possibile generare dettagliati report (per utente, per varco, per data) in modo da ricostruire con la massima precisione - se necessario - i percorsi effettuati da ogni singolo visitatore.

L'edificio è dotato di un **sistema anti-intrusione** che utilizza sensori volumetrici a doppia tecnologia, assieme a sensori a contatti su infissi e sensori di vibrazione sui vetri delle sale dati.

L'impianto è integrato da sistemi evoluti di analisi delle immagini rese disponibili dall'impianto di videosorveglianza (trattato di seguito). La resede esterna è protetta tramite barriere a raggi infrarossi applicate lungo tutto il perimetro della recinzione esterna. L'impianto anti-intrusione è integrato con il sistema di controllo accessi.

L'**impianto di video-sorveglianza** è costituito da un cospicuo numero di telecamere (oltre 120) posizionate sia all'interno dell'edificio (lungo tutti i punti di passaggio e all'interno dei locali sensibili) che all'esterno (lungo la recinzione, sulla copertura dell'edificio e nella zona dove sono ubicati i gruppi elettrogeni). Le telecamere utilizzate sono di tipologie diverse in base alle diverse esigenze derivanti dai singoli posizionamenti (angolo e distanza di visuale, tipologia di illuminazione, ecc). Le immagini vengono rese disponibili in real-time al personale di presidio mediante appositi monitor presenti all'interno del **NOC**.
Tutte le immagini acquisite vengono immagazzinate tramite videoregistratori digitali, situati in ambienti protetti e conservate per 24H, come previsto dalle vigenti **normative in ambito Privacy**.

Tutto l'edificio è dotato di un **sistema di rilevamento dei fumi** costituito da sensori ottici posizionati in ambiente, sotto al pavimento flottante e sopra il controsoffitto. I sensori sono collegati tra loro in loop e mediante cavo antifiamma, in modo da garantire il loro funzionamento anche in caso di interruzione di un collegamento. Sono stati previsti opportuni sensori in grado di verificare la presenza di fumo all'interno delle condotte per il ricambio dell'aria degli ambienti.

La gestione dell'impianto è demandata ad una centrale a 6 loop, con il compito di rilevare i segnali provenienti dai sensori, attivando gli allarmi ottici e acustici, nonché provvedendo all'attivazione dell'impianto di spegnimento mediante apposite unità di spegnimento. Le aree sensibili e/o a maggiore rischio (2 sale dati, 2 sale tlc, 6 power center, 6 sale trasformatori MT e 2 sale quadri MT) sono dotate di sistema di spegnimento a gas inerte (Azoto).

Il **metodo di spegnimento** è quello della diluizione d'ossigeno, ottenuto mediante una scarica di un'adeguata quantità di azoto in grado di ridurre la percentuale di ossigeno dal 23% presente normalmente in atmosfera al 12% circa, valore che non consente la combustione. Tale scarica non rappresenta un pericolo per la salute delle persone eventualmente ancora presenti nell'ambiente al momento della scarica (comunque annunciata con un anticipo di 60 secondi da allarmi acustici e ottici) e preserva gli apparati consentendo la continuità nell'erogazione dei servizi.

I gruppi elettrogeni di emergenza presenti, posizionati all'esterno, sono dotati di impianti di rilevazione e di spegnimento incendi (ad anidride carbonica) dedicati e autonomi. Tali gruppi sono dotati inoltre di sistema di intercettazione del carburante, in grado di interrompere l'afflusso in caso di incendio. E' inoltre presente la normale dotazione di estintori portatili e carrellati.

I vari locali dell'edificio sono dotati di sensori per il **rilevamento della presenza di liquidi**, posizionati sotto il pavimento flottante. Per quanto riguarda la possibilità di allagamento derivante da rottura delle tubazioni per l'acqua dei servizi igienici (o dalla dimenticanza di rubinetti aperti), è stato previsto un sistema costituito da sensori (flussostati e rilevatori di presenza) e da una logica che, nel caso in cui venga rilevato il flusso di acqua in assenza di persone all'interno dei singoli servizi igienici, provvede all'interruzione dell'erogazione dell'acqua nel medesimo ambiente tramite l'attivazione di una elettrovalvola, eliminando la possibilità di riversamento di acqua a terra.

Le eventuali problematiche derivanti da alluvioni sono scongiurate, in quanto la struttura è ubicata in zona pianeggiante ed in posizione rilevata di circa un metro rispetto al piano di campagna. In fase progettuale si è provveduto inoltre a evitare il posizionamento di impianti strategici o di parte di essi a quota inferiore a tale valore: ciò esclude la necessità di sistemi anti-allagamento dotati di pompe idrauliche.

I server dislocati presso il Centro Servizi saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati. Gli armadi rack sono tutti dotati di sportelli metallici con serratura a chiave e i supporti di memorizzazione contenenti dati sono conservati in luogo sicuro. Gli apparati attivi di rete saranno posizionati in armadi di cablaggio con chiusura a chiave che inibisce l'accesso fisico ai dischi locali e ne impedisce la rimozione.

Tutti gli impianti sopradescritti, assieme agli impianti e sistemi strategici (gruppi elettrogeni, ups, quadri elettrici, condizionamento di potenza) e agli impianti standard (illuminazione, condizionamento uffici) sono supervisionati da un sistema **BMS** (**Building Management System**) a mappe, in grado di gestire tutti gli eventi e gli allarmi, di interpretarli e di assegnare loro le opportune priorità, generando le conseguenti notifiche in modo da ridurre al massimo i tempi di interpretazione e individuazione degli eventi. Il **BMS** - controllato dal personale di presidio del **NOC** (**Network Operation Center**) - è accessibile anche da remoto ed in grado di provvedere alla notifica degli allarmi tramite i consueti canali (e-mail, SMS, ecc).

La pavimentazione flottante è realizzata mediante pannelli in conglomerato ad alta resistenza appoggiate su struttura composta da tubolari in acciaio ed offre adeguate capacità di carico e di resistenza. Al fine di verificare la corrispondenza con i dati del fornitore sono state eseguite prove di carico in laboratorio.

10.8.2 Sicurezza fisica Data Center Secondario

La **sicurezza fisica** del **data center** secondario viene garantita attraverso:

- un sistema di video-sorveglianza che utilizza telecamere motorizzate per tenere sotto controllo i punti nevralgici della struttura;
- un sistema di allarme che rileva automaticamente eventuali vibrazioni o aperture non autorizzate di ingressi e di infissi;

- un impianto anti-intrusione – monitorato dal NOC - che utilizza rilevatori di presenza a doppia tecnologia (micro-onde e raggi infrarossi), contatti magnetici e barriere a raggi infrarossi per proteggere le zone in cui gli ambienti sono suddivisi e prevenire l'apertura non autorizzata di ingressi ed infissi;
- sistema di controllo accessi che permette l'accesso al solo personale autorizzato, dotato di badge con tecnologia RFID e codice PIN personale;
- un sistema anti-incendio a gas inerti (non tossici) - connesso a rilevatori di fumo posti sopra e sotto al pavimento flottante – che si attiva automaticamente inondando di gas solo la zona colpita;
- un sistema di rilevazione liquidi che permette di intercettare - dal NOC e tramite appositi allarmi acustici in loco - eventuali fuoriuscite di liquido dagli impianti tecnologici;
- un sistema centrale server per archiviare e consultare (da personale autorizzato tramite accesso protetto) qualsiasi accesso ai locali, che solo avviene attraverso RFID associato a codice numerico.

Anche nel sito secondario, i server saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati: gli armadi rack sono provvisti di sportelli metallici con serratura a chiave; i supporti di memoria dati sono conservati in un luogo sicuro ed i server sono protetti da un apposito sportello con chiusura a chiave (come inibizione dell'accesso fisico e della rimozione).

10.8.3 Sicurezza organizzativa comune ai due data center

Aruba garantisce inoltre la sicurezza organizzativa delle strutture, che verrà adeguata in caso di evoluzioni delle normative. Il sistema di registrazione dei log per tutti i servizi erogati è infatti conforme alle normative vigenti e verrà adeguato in caso di evoluzioni.

A tale proposito viene garantito che:

- i processi attuati per il monitoraggio e la rilevazione di eventuali intrusioni o anomalie sono regolati e descritti all'interno del **Piano di Sicurezza dei Data Center**;
- l'accesso alle informazioni riservate dell'Amministrazione sarà permesso solo a personale autorizzato, in conformità al D.Lsg. 196/2003 e successive modifiche;
- l'erogazione di servizi e dei sistemi coinvolti sia conforme alla Legge 82/2005 (Codice Amministrazione Digitale).

Aruba garantisce che tutti gli apparati necessari all'erogazione dei servizi saranno gestiti solo da personale univocamente individuato e che gli aspetti di sicurezza vengano attuati in base a procedure documentate. All'interno del piano della sicurezza delle strutture, redatto sulla base delle linee guida della certificazione ISO27001, sono documentati:

- accesso fisico delle persone agli edifici in cui sono situati apparati;
- accesso fisico delle persone ai locali contenenti apparati;
- regole per l'accesso da parte di personale esterno (fornitori, addetti alla manutenzione, visitatori, etc.);
- gestione degli strumenti per l'accesso ad eventuali casseforti ed armadi blindati (combinazioni delle casseforti, chiavi degli armadi, etc.);
- gestione degli archivi cartacei (regole per la conservazione, modalità di consultazione, eventuale registrazione degli accessi, etc.);
- gestione di situazioni anomale;
- ripristino dell'interruzione dell'erogazione di energia elettrica;
- procedure di backup e di restore;
- procedure di escalation.

Le **postazioni di lavoro** si trovano in uffici interdetti all'accesso del pubblico. Le postazioni condivise, messe a disposizione della clientela, risiedono su reti e uffici separati (sale riunioni attrezzate), e sono dotate di opportune limitazioni di accesso.

Per l'**accesso alle postazioni di lavoro**, i dipendenti dispongono di token hardware personali protetti da apposito **PIN** associato a credenziali nella forma nome.cognome e password, di tipo strong, conosciute solo dagli stessi. Attraverso l'**Active Directory aziendale** è possibile offrire cambio password con obbligo di password in base a policy standard condivise.

L'accesso ai server viene garantito attraverso le stesse credenziali personali sia per ambienti windows che per ambienti linux. Le password vengono mantenute nella massima riservatezza e non possono essere trascritte.

Tutti i log di accesso ai server sono centralizzati su un apposito server. Ogni notte viene generato un report e mandato all'addetto di controllo dei report. Esso con cadenza giornaliera controlla tale report e verifica la regolarità degli accessi, verificando che non ci siano accessi da reti esterne, che non ci siano accessi con esito negativo e che non ci siano accessi di personale che non aveva motivo di accedere. Se la verifica ha avuto esito positivo vengono eseguite verifiche sui controlli e informato immediatamente il responsabile della sicurezza.

10.8.4 Sicurezza Logica dei sistemi e degli apparati

I protocolli ed i servizi utilizzati per la gestione degli apparati (SNMP, RADIUS, NTP, Log, LDAP) vengono erogati solo verso le reti di management mediante l'utilizzo di ACL (Access Control List). All'interno delle reti dedicate, se il protocollo/servizio lo supporta, è in ogni caso necessario autenticarsi.

Tutti i protocolli previsti per l'accesso ed il controllo dei sistemi sono di tipo sicuro cifrato, prevedendo ssh, https o rdp.

All'interno dei singoli apparati i servizi non necessari vengono disattivati e quelli necessari vengono erogati solo verso le interfacce che richiedono che tali servizi vengano resi disponibili.

Le politiche e le conseguenti architetture e configurazioni di rete adottate garantiscono fra l'altro:

- L'impossibilità di effettuare IP spoofing da un qualsiasi utente connesso direttamente alla rete
- L'impossibilità di effettuare attacchi smurf, fraggle, land tramite limitazione nell'accesso agli indirizzi di broadcast e filtraggio dei pacchetti che riportano un indirizzo sorgente palesemente scorretto
- La capacità di reagire tempestivamente a qualsiasi tipo di attacco alle proprie infrastrutture anche tramite la possibilità di configurare in qualsiasi punto della rete qualsiasi regola di filtraggio atta a mitigare il fenomeno evidenziato

Gli enti/gruppi che operano sulla configurazione dei sistemi hanno diverse esigenze in termini di necessità d'accesso alle classi d'apparati. L'autorizzazione all'accesso alla configurazione di un apparato è nominale, non di gruppo. L'accesso ad una specifica classe d'apparati dipende dall'appartenenza dell'utente ad uno specifico gruppo. L'associazione dell'utenza al Gruppo permette di confinare l'accesso degli utenti ai soli apparati la cui gestione è in carico al Gruppo. Sulla base di tale appartenenza, l'utente potrà autenticarsi sull'apparato utilizzando una login ed una password personali nel caso di apparati con tecnologia IP mentre per quanto riguarda apparati di trasporto (SDH e DWDM) l'autenticazione si esegue a livello dei sistemi di gestione. Sono stati inoltre introdotti dei meccanismi di gestione delle password (lunghezza minima, presenza di caratteri numerici, ecc.) di enable e delle password locali in modo da ottenere un bilanciamento tra l'esigenza di avere un adeguato livello di sicurezza e le esigenze di implementazione/gestione delle linee guida.

L'inserimento di un nuovo utente in un gruppo deve essere richiesto dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di Trasporto.

Successivamente alla configurazione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al responsabile del gruppo. La rimozione di un utente da un gruppo deve essere richiesta dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di trasporto.

Successivamente alla rimozione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al responsabile del gruppo. Le password utilizzate dagli utenti dovranno seguire le seguenti regole:

- Non inferiori agli 8 caratteri (in accordo con la legge delega 127/2001 Allegato B comma 7)
- Non devono essere facilmente indovinabili. Nomi propri, nomi di prodotti, nomi di Clienti ecc.. sono da evitare
- Devono contenere caratteri misti: minuscole, maiuscole, numeri, spazi, caratteri speciali (@, %, $ ecc.)
- Non devono coincidere con le password utilizzate per altri servizi di rete.

L'utente viene invitato a cambiare con regolarità la sua password utente. Nel caso l'utente decidesse di non cambiare la propria password vengono adottate le seguenti misure:

Trascorsi due mesi, dall'ultimo cambio di password effettuato, l'utente riceverà dei solleciti settimanali per cambiare

10.9 Piano di Disaster Recovery e Continuità operativa

Aruba ha sviluppato e adotta appositi piani di Disaster Recovery e Business Continuity allo scopo di gestire e mediare i rischi cui può essere soggetta.

Tali documenti definiscono ed elencano le azioni da intraprendere prima, durante e dopo una condizione di emergenza per assicurare il ripristino (Disaster Recovery) e la continuità (Business Continuity) dei servizi erogati. Essi forniscono indicazioni e dove possibile istruzioni passo-passo atte ad assicurare la continuità dei servizi critici di Aruba anche in presenza di eventi indesiderati che possano causare il fermo prolungato dei sistemi informatici.

I Piani di Disaster Recovery sono stati redatti tenendo presente le "Linee Guida per il disaster recovery delle PA" dell'Agenzia per l'Italia Digitale, ex DigitPA ed è dunque ispirato al ciclo di Deming (Plan, Do, Check, Act) prevedendo, dopo la fase iniziale di studio/analisi del contesto, il disegno della soluzione tecnologico-organizzativa che meglio risponde alle esigenze di continuità richieste, la realizzazione e il mantenimento della soluzione. Tale piano viene dettagliato maggiormente in fase di setup dell'infrastruttura.

La continuità operativa sarà garantita anche in caso di blocchi prolungati, quali, a titolo esemplificativo:

- distruzione o inaccessibilità di una struttura nella quale sono allocate unità operative o apparecchiature critiche;
- indisponibilità di personale essenziale per il funzionamento dell'azienda;
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, ecc.);
- alterazione dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche;
- danneggiamenti gravi provocati da dipendenti

10.9.1 Business Impact Analisys (BIA)

Come prima cosa si valutano gli elementi che più risentirebbero dell'interruzione del servizio, ovvero si valuterà con il cliente quali sono gli aspetti maggiormente critici del servizio offerto.

La BIA valuta normalmente l'impatto di un evento sull'operatività economica, nel caso della conservazione documentale però l'interruzione dei servizi erogati comporta danni non immediatamente "monetizzabili". Le perdite (e dunque l'impatto) saranno valutate assieme al cliente tenendo conto dell'insieme dei seguenti aspetti:

- Aspetti economici
- Aspetti sociali
- Aspetti reputazionali;
- Aspetti normativi.

10.9.2 Analisi dei Rischi

In questa fase si identificheranno quali siano gli scenari di rischio che insistono sul patrimonio informativo attraverso i quali si qualificano gli eventi / minacce che presentano maggior probabilità di concretizzarsi (e.g. in funzione dei livelli di vulnerabilità, delle contromisure in essere, dell'appetibilità dei servizi offerti), generando un danno per il cliente. Si individueranno pertanto le possibili cause di indisponibilità quali ad esempio diffusione di virus, interruzione dell'alimentazione elettrica, incendio alla sala CED, etc...

10.9.3 Classificazione dei Sistemi e delle Risorse

Allo scopo di indirizzare le priorità di ripristino in caso di disastro, nonché realizzare un efficiente utilizzo delle risorse, si ritiene indispensabile classificare i sistemi presenti all'interno delle infrastrutture di ARUBA a seconda della loro criticità in caso di disastro.

Sono stati individuati quattro livelli di criticità, così definiti:

- Sistemi critici:

  Sono quei sistemi indispensabili per fornire un minimo ed accettabile livello di servizio in caso di evento disastroso e/o necessari per il funzionamento degli altri sistemi a minore criticità.
- Sistemi importanti:

  Sono quei sistemi necessari per garantire un livello standard di servizi, che quindi hanno una significativa importanza operativa.
- Sistemi semi-importanti:

  Si tratta di sistemi necessari per le normali operazioni, tuttavia risultano avere una minore importanza operativa rispetto a quelli del punto precedente.
- Sistemi non-critici:

  Sono i sistemi che rivestono la minore importanza (quali servizi accessori ecc.) operativa per cui il ripristino non riveste carattere di priorità.

Verrà inoltre fornito l'elenco del personale, il responsabile della Continuità Operativa e le procedure di escalation da utilizzare per dichiarare lo stato di disastro.

10.9.4 Modalità tecniche per la Business Continuity ed il Disaster Recovery

Come descritto nell'architettura fisica della soluzione il sistema implementa i seguenti livelli di sicurezza:

1) Il sistema di produzione è completamente ridondato senza alcun Single Point of Failure. Alcune componenti sono per convenienza distribuite sui due Data Center connessi in ambito metropolitano in modo tale da essere totalmente resilienti a qualsiasi guasto HW o SW che possa colpire un singolo nodo fisico o virtuale. Per come è costruito il sistema inoltre l'impatto sulle performance dovuto alla rot-

tura di un singolo componente può essere considerato irrilevante e comunque la configurazione normale ripristinata nel giro di pochi minuti.

2) La presenza di un sito collegato in ambito metropolitano e già parzialmente attivo garantisce la piena operatività della soluzione anche nel caso di fermo del data center principale. Le uniche operazioni necessarie sono la riconfigurazione della rete, per il corretto raggiungimento del sistema, e la riattivazione dei nodi di Front-end ed Application sull'apposita infrastruttura virtuale. Per tutti gli eventi che abbiano impatto sul data center di produzione, che ricordiamo avere caratteristiche di livello TIER IV, la ripartenza è possibile con un RTO pari a circa 1 ora ed un RPO pari a 0.

Nel caso di attivazione del sito secondario, questa viene eseguita manualmente seguendo apposite procedure, a seguito della dichiarazione di crisi prevista dalle procedure.

11 MONITORAGGIO E CONTROLLI

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:

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

11.1 Procedure di monitoraggio della funzionalità del sistema di conservazione

ARUBA 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.

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.

11.2 Verifiche sull'integrità degli archivi

ARUBA 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.

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).

11.2.1 Pianificazione delle verifiche periodiche da effettuare

Il controllo periodico dell'integrità degli archivi avviene con una frequenza di una volta al mese.

11.2.2 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.

12 RICHIESTA DELLA PRESENZA DEL PUBBLICO UFFICIALE

ARUBA 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, ARUBA 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.

13 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.

14 DISPOSIZIONI FINALI

14.1 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.

14.2 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.

14.3 Nessuna rinuncia

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

14.4 Comunicazioni

Qualora ARUBA o il Cliente desiderino o siano tenuti ad effettuare delle comunicazioni, domande o richieste in relazione al presente Manuale, tali comunicazioni dovranno avvenire nelle modalità ed ai riferimenti indicati nel Contratto.

.

14.5 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.

14.6 Modifiche del Manuale di conservazione

ARUBA 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.

14.7 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.

14.8 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……..

15 APPENDICI

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

Codice	Descrizione Tipo documento/Classe documentale	Formato	Sottoscrizione Cliente	RT[4]
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

[4] Riferimento Temporale

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
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	ModelloI-va26Lp2006ProspettoLiquidazioniPeriodiche	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

15.2 Appendice 2 – Specifiche Pacchetto di Versamento

L'Indice di un PDV si caratterizza per le seguenti parti:

- area di identificazione del PDV
- area di identificazione dei documenti costituenti il pacchetto e dei loro metadati obbligatori

- area di identificazione dei metadati extra-info

Nella prima parte il dato importante e obbligatorio è *pid* ovvero l'identificativo del PDV. Esso deve essere unico all'interno dello spazio gestito dal produttore, quindi indipendentemente dall'archivio.

La seconda parte prevede una lista di elementi, uno per ogni documento da versare. Ogni singolo file deve essere per prima cosa identificato. A questo scopo sono necessari i seguenti dati:

- nome file
- formato di hashing per la generazione dell'impronta
- impronta del documento

Inoltre, poiché il sistema deve controllare la tipoligia di documento per valutarne l'aderenza alle condizioni espresse in fase di contratto, deve essere indicato il MIME type del documento.

Per rimanere poi aderenti alla norma vigente devono essere passati anche un id unico del documento e la data di chiusura dello stesso.

La terza parte dell'Indice contiene un insieme di metadati extra-info, così come definiti in fase contrattuale col Produttore

Di seguito è riportato l'indice di un Pacchetto di Versamento standard

```
<?xml version="1.0"?>
<PDV>
	<pid>460</pid>
	<docode namespace="conservazione.doc">propostaAcquisto</docode>
	<file>
		<nomefile>Doc 1.pdf</nomefile>
		<formato>application/pdf</formato>
		<hash>
			<algoritmo>SHA256</algoritmo>
		<valore>G84IOmhWmA5SEKg6LJI0bcaoaBVwHMgh8z0Abw5nwbk=</valore>
		</hash>
		<data>2014-07-23T11:44:59Z</data>
		<metadati>
			<richiesti>
				<id>
					<namespace>conservazione.doc</namespace>
					<tipo>String</tipo>
					<nome>id</nome>
					<valore>MRC25072014OK</valore>
				</id>
				<metadato>
```

```
                    <namespace>conservazione.doc</namespace>
                    <tipo>String</tipo>
                    <nome>pid</nome>
                    <valore>460</valore>
                </metadato>
                <metadato>
                    <namespace>conservazione.doc</namespace>
                    <tipo>String</tipo>
                    <nome>hash</nome>

<valore>G84IOmhWmA5SEKg6LJI0bcaoaBVwHMgh8z0Abw5nwbk=</valore>
                </metadato>
                <metadato>
                    <namespace>conservazione.doc</namespace>
                    <tipo>String</tipo>
                    <nome>datachiusuraMax</nome>
                    <valore>2014-09-14T23:59:59Z</valore>
                </metadato>
                <metadato>
                    <namespace>conservazione.doc</namespace>
                    <tipo>String</tipo>
                    <nome>oggettodocumento</nome>
                    <valore>Modulo Richiesta Certificato</valore>
                </metadato>
                <metadato>
                    <namespace>conservazione.doc</namespace>
                    <tipo>String</tipo>
                    <nome>formatoFile</nome>
                    <valore>application/pdf</valore>
                </metadato>
                <metadato>
                    <namespace>conservazione.doc</namespace>
                    <tipo>String</tipo>
                    <nome>sistemaVersanteID</nome>
                    <valore>Documentale Pippo v. 0.11</valore>
```

```
                    </metadato>
                    <metadato>
                        <namespace>conservazione.doc</namespace>
                        <tipo>String</tipo>
                        <nome>sistemaVersanteType</nome>
                        <valore>sugar crm aruba</valore>
                    </metadato>
                    <metadato>
                        <namespace>conservazione.doc</namespace>
                        <tipo>String</tipo>
                        <nome>ruoloSoggettoCreatore</nome>
                        <valore>Direttore IT</valore>
                    </metadato>
                    <metadato>
                        <namespace>conservazione.doc</namespace>
                        <tipo>Int</tipo>
                        <nome>retentionPeriod</nome>
                        <valore>12816</valore>
                    </metadato>
                    <metadato>
                        <namespace>conservazione.doc</namespace>
                        <tipo>Int</tipo>
                        <nome>IDOrdine</nome>
                        <valore>2</valore>
                    </metadato>
                    <associazione namespace="conservazione.doc"
nome="soggettoproduttoreEsteso" namespaceNodo="conservazione.soggetti"
                        nomeNodo="soggettoEsteso">
                        <dato>
                            <namespace>conservazione.soggetti</namespace>
                            <tipo>String</tipo>
                            <nome>nome</nome>
                            <valore>Mario</valore>
                        </dato>
                        <dato>
```

```
                                        <namespace>conservazione.soggetti</namespace>
                                        <tipo>String</tipo>
                                        <nome>cognome</nome>
                                        <valore>Rossi</valore>
                                    </dato>
                                    <dato>
                                        <namespace>conservazione.soggetti</namespace>
                                        <tipo>String</tipo>
                                        <nome>codicefiscale</nome>
                                        <valore>RSSMRA56A87T890X</valore>
                                    </dato>
                                    <dato>
                                        <namespace>conservazione.soggetti</namespace>
                                        <tipo>String</tipo>
                                        <nome>residenza</nome>
                                        <valore>Arezzo</valore>
                                    </dato>
                                    <dato>
                                        <namespace>conservazione.soggetti</namespace>
                                        <tipo>String</tipo>
                                        <nome>provincia</nome>
                                        <valore>Arezzo</valore>
                                    </dato>
                                </associazione>
                                <associazione namespace="conservazione.doc" nome="destinatarioEsteso"
namespaceNodo="conservazione.soggetti"
                                    nomeNodo="soggettoEsteso">
                                    <dato>
                                        <namespace>conservazione.soggetti</namespace>
                                        <tipo>String</tipo>
                                        <nome>nome</nome>
                                        <valore>Luigi</valore>
                                    </dato>
                                    <dato>
                                        <namespace>conservazione.soggetti</namespace>
```

```
                    <tipo>String</tipo>
                    <nome>cognome</nome>
                    <valore>Bianchi</valore>
                </dato>
                <dato>
                    <namespace>conservazione.soggetti</namespace>
                    <tipo>String</tipo>
                    <nome>codicefiscale</nome>
                    <valore>BNGLGI67R43E123Z</valore>
                </dato>
                <dato>
                    <namespace>conservazione.soggetti</namespace>
                    <tipo>String</tipo>
                    <nome>residenza</nome>
                    <valore>Arezzo</valore>
                </dato>
                <dato>
                    <namespace>conservazione.soggetti</namespace>
                    <tipo>String</tipo>
                    <nome>provincia</nome>
                    <valore>Arezzo</valore>
                </dato>
            </associazione>
            <associazione namespace="conservazione.doc"
nome="soggettoResponsabileVersamento" namespaceNodo="conservazione.soggetti"
                nomeNodo="soggettoEsteso">
                <dato>
                    <namespace>conservazione.soggetti</namespace>
                    <tipo>String</tipo>
                    <nome>nome</nome>
                    <valore>Andrea</valore>
                </dato>
                <dato>
                    <namespace>conservazione.soggetti</namespace>
                    <tipo>String</tipo>
```

```
                                        <nome>cognome</nome>
                                        <valore>Malatesti</valore>
                                    </dato>
                                    <dato>
                                        <namespace>conservazione.soggetti</namespace>
                                        <tipo>String</tipo>
                                        <nome>codicefiscale</nome>
                                        <valore>mltndr87h11a390l</valore>
                                    </dato>
                                    <dato>
                                        <namespace>conservazione.soggetti</namespace>
                                        <tipo>String</tipo>
                                        <nome>residenza</nome>
                                        <valore>Arezzo</valore>
                                    </dato>
                                    <dato>
                                        <namespace>conservazione.soggetti</namespace>
                                        <tipo>String</tipo>
                                        <nome>provincia</nome>
                                        <valore>Arezzo</valore>
                                    </dato>
                                </associazione>
                            </richiesti>
                        </metadati>
                    </file>
</PDV>
```

15.3 Appendice 3 – Specifiche Rapporto di Versamento

Il Rapporto di Versamento è basilare nel processo di conservazione, in quanto è documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

Esso viene prodotto nel momento in cui tutti gli elementi utili per la conservazione del pacchetto di versamento sono stati consegnati al sistema.

In esso sono presenti sempre i seguenti dati:

- id del Pacchetto di V ersamento
- id del Rapporto di Versamento
- riferimento temporale (UTC) di generazione del Rapporto di Versamento
- lista dei documenti afferenti al pacchetto. Per ognuno di essi sono distinguibili:
  - id come indicato nell'Indice del PdV
  - id assegnato dal sistema
  - impronta del documento
  - nome del documento
  - data di ricezione del file
  - esito controllo firma digitale (ove previsto)
  - esito controllo marca temporale (ove previsto)

Il Rapporto di Versamento viene sempre firmato digitalmente con certificato del Responsabile di Conservazione. In questo modo viene reso non modificabile.