

DELIBERA



SEGRETERIA DIREZIONALE
10SD

STRUTTURA PROPONENTE

COD.

N° 2025/00169

DEL 30/12/2025

Codice Unico di Progetto:

OGGETTO

Nomina Responsabile della Gestione documentale ed approvazione manuale

UFFICIO RAGIONERIA

PREIMPEGNI

Num. Preimpegno	Bilancio	Missione.Programma	Capitolo	Importo Euro

IMPEGNI

Num. Impegno	Bilancio	Missione. Programma	Capitolo	Importo Euro	Atto	Num. Prenotazione	Anno	Num. Impegno Perente

Note

Visto di regolarità contabile

IL COLLABORATORE

DATA

IL DIRIGENTE Donato Ramunno

DATA 30/12/2025

Allegati N. 4

Atto soggetto a pubblicazione ☒ Integrale ☐ Per oggetto ☐ Per oggetto + Dispositivo

IL DIRETTORE GENERALE

VISTE:

- la Legge della Regione Basilicata n. 01 del 20/01/2020, avente ad oggetto *"Riordino della disciplina dell'Agenzia per la Protezione dell'Ambiente della Basilicata (A.R.P.A.B.)"*, modificata ed integrata dalla Legge Regionale n. 12/2020;
- il Decreto del Presidente della Giunta Regionale n. 122 del 11.07.2022 concernente: *"Art. 21 Legge Regionale n.1/2020 e smi. Nomina del Direttore Generale dell'Agenzia Regionale per la Protezione dell'Ambiente della Basilicata (A.R.P.A.B.)"*;
- la proroga dell'incarico di Direttore Generale dell'ARPA Basilicata al dott. Ramunno Donato, deliberazione n. 89 del 14.07.2025;
- il Decreto del Presidente della Giunta Regionale n. 203 del 26.08.2025 concernente: *"Art. 21 Legge Regionale n.1/2020. Rinnovo rapporto di lavoro del Direttore dell'ARPAB"*;
- il contratto individuale di rinnovo dell'incarico di Direttore Generale dell'ARPAB sottoscritto in data 28.08.2025 tra il Presidente della Giunta Regionale dott. Bardi e il dott. Donato Ramunno;

CONSIDERATO che il Bilancio di Previsione Pluriennale 2025-2027 dell'A.R.P.A.B., adottato con Delibera del Direttore Generale n. 51 del 14/04/2025, è stato approvato con L.R. n.30 del 10/06/2025 e pubblicato sul B.U.R. n.31 del 10/06/2025;

RICHIAMATE

- la DDG n.107 del 19.02.2016 concernente *"Procedure transitorie per liquidazioni e pagamenti e disposizioni per la conservazione dei documenti"*;
- la DDG n.231 del 10.05.2016 di adozione del Regolamento di contabilità e gestione finanziaria dell'ARPAB, approvato con DGR n.612 del 7.06.2016;

VISTI E RICHIAMATI

- il D.LGS N.82/2005 e s.m.i. recente il Codice dell'Amministrazione digitale
- il DPCM 22 febbraio 2013 ed il successivo DPCM del 21 marzo 2013;
- le linee guida AgID "Linee guida sulla formazione, gestione e conservazione dei documenti informatici" che hanno carattere vincolante per le PP.AA.

CONSIDERATO CHE

- l'Agenzia ha istituito al suo interno una sola Area Organizzativa Omogenea (AOO) ai fini della gestione complessiva dei propri flussi documentali;
- ha posto in essere un sistema organico di protocollazione informatica denominato "Geos";
- che l'Agenzia sta attuando la migrazione in cloud del sistema GEOS e

l'aggiornamento tecnologico dello stesso alla versione evolutiva KEND.

DATO ATTO CHE

in Agenzia la gestione del protocollo generale e dei conseguenti flussi documentali è attestata alla Direzione Generale e che occorre nominare un Responsabile della gestione documentale e della conservazione;

RITENUTO DI

- individuare nella persona del funzionario dott. Lorigi Pancrazio attestato alla Direzione Generale ed al Servizio Protocollo, la figura centrale di responsabilità e coordinamento della gestione e conservazione dei flussi documentali agenziali nel loro complesso;
- di nominare quale gruppo di supporto al Responsabile della gestione documentale i dipendenti dott. Antonello Mango e dott.ssa Claudia Brindisi;
- approvare lo schema di Manuale di gestione documentale e della conservazione e correlato Titolario di classificazione, allegati alla presente deliberazione a costituirne parte integrante e sostanziale;
- di prendere atto ed approvare il manuale di conservazione sostitutiva a norma predisposto dalla funzionaria nominata dall'Agenzia dott.ssa Brigida Serpillo, allegato anch'esso a farne parte integrante e sostanziale

RITENUTO altresì,

al fine di garantire la piena rispondenza alla normativa e alle linee guida dell'Agid, nonché alla luce del nuovo sistema di protocollazione KEND, necessario completare ed aggiornare i documenti, allegati alla presente, di demandare al Responsabile della gestione documentale e al gruppo di supporto l'attività suddetta che dovrà concludersi entro la data del 31.01.2026.

DELIBERA

Giuste le premesse di cui sopra che vengono integralmente riportate nel deliberato del presente provvedimento

- di nominare Responsabile della Gestione documentale il dipendente dott. Pancrazio Lorigi;
- di nominare il gruppo di supporto nelle persone dei dipendenti dott. Mango Antonello e dott.ssa Claudia Brindisi con i compiti sopra richiamati;
- di approvare i documenti individuati nello schema del Manuale di gestione documentale, di conservazione e Titolario di classificazione allegati al presente provvedimento
- di pubblicare a cura del Responsabile il Manuale e tutti i documenti sul sito agenziale in Amministrazione Trasparente- Disposizioni generali – Atti

- amministrativi generali
- di dichiarare il presente provvedimento urgente ed immediatamente eseguibile

Donato Ramunno

DELIBERA

OGGETTO

OSSERVAZIONI

IL DIRETTORE _____

OSSERVAZIONI

Donato Ramunno 30/12/2025

IL DIRETTORE TECNICO SCIENTIFICO _____

OSSERVAZIONI

Achille Palma 30/12/2025

IL DIRETTORE GENERALE _____

Donato Ramunno

30/12/2025

Elenco Firme del provvedimento n. 2025/00169 del 30/12/2025

Numero Certificato: 16C22B1F353EF297

Rilasciato a: dnQualifier=LORD2024041855981713, CN=RAMUNNO DONATO,
SERIALNUMBER=TINIT-RMNDNT71L04F104X, G=DONATO, SN=RAMUNNO, C=IT

Valido da: 18/04/2024 17:09:00

fino a: 18/04/2027

documento firmato il : 30/12/2025

Numero Certificato: 16C22B1F353EF297

Rilasciato a: dnQualifier=LORD2024041855981713, CN=RAMUNNO DONATO,
SERIALNUMBER=TINIT-RMNDNT71L04F104X, G=DONATO, SN=RAMUNNO, C=IT

Valido da: 18/04/2024 17:09:00

fino a: 18/04/2027

documento firmato il : 30/12/2025

Numero Certificato: 0CDE0053FFD4D1E5

Rilasciato a: dnQualifier=LOPA2024041996021714, CN=PALMA ACHILLE,
SERIALNUMBER=TINIT-PLMCLL59P29H687O, G=ACHILLE, SN=PALMA, C=IT

Valido da: 19/04/2024 13:25:00

fino a: 19/04/2027

documento firmato il : 30/12/2025

Numero Certificato: 16C22B1F353EF297

Rilasciato a: dnQualifier=LORD2024041855981713, CN=RAMUNNO DONATO,
SERIALNUMBER=TINIT-RMNDNT71L04F104X, G=DONATO, SN=RAMUNNO, C=IT

Valido da: 18/04/2024 17:09:00

fino a: 18/04/2027

documento firmato il : 30/12/2025

Numero Certificato: 16C22B1F353EF297

Rilasciato a: dnQualifier=LORD2024041855981713, CN=RAMUNNO DONATO,
SERIALNUMBER=TINIT-RMNDNT71L04F104X, G=DONATO, SN=RAMUNNO, C=IT

Valido da: 18/04/2024 17:09:00

fino a: 18/04/2027

documento firmato il : 30/12/2025

A.R.P.A.B.

MANUALE PER LA GESTIONE E LA CONSERVAZIONE DOCUMENTALE

Approvato con deliberazione direttoriale n. ...

SOMMARIO

GLOSSARIO

PREMESSA

DISPOSIZIONI GENERALI

Art. 1 - Ambito di applicazione

Art. 2 - Area Organizzativa Omogenea e modello organizzativo Art. 3 -
Unicità del Protocollo Informatico

Art. 4 - Modello organizzativo adottato per la gestione dei documenti

DOCUMENTI

Art. 5 - Tipologie di documenti

Art. 6 - Documenti amministrativi informatici

Art. 7 - Immodificabilità dei documenti informatici

Art. 8 - Copie per immagine su supporto informatico di documenti analogici Art. 9 -

Documenti in arrivo, in partenza e documenti interni

DESCRIZIONE DEI FLUSSI DOCUMENTALI NELL'ARCHIVIO CORRENTE

Art. 10 - Documenti in entrata Art.

11 - Documenti in uscita

REGISTRAZIONE A PROTOCOLLO E SEGNATURA DEI DOCUMENTI

Art. 12 - La registrazione dei documenti Art. 13

- Il registro di protocollo

Art. 14 - Regole per la tenuta del registro di protocollo di emergenza Art. 15 -

Elementi obbligatori della registrazione a protocollo

Art. 16 - La segnatura dei documenti (timbro di protocollo) Art. 17

- Protocollo differito

Art. 18 - Annullamento di una registrazione Art. 19

- Documento anonimo

Art. 20 - Documenti privi di firma

Art. 21 - Uno o più esemplari di uno stesso documento inviati a più soggetti dell'ARPAB, per
competenza o per conoscenza

Art. 22 - Copie per competenza

Art. 23 - Copie per conoscenza

Art. 24 - Posta elettronica certificata

Art. 25 - Documenti smistati e assegnati erroneamente

CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

Art. 26- Il Piano di classificazione (c.d. Titolare)

Art. 27 - La formazione e l'identificazione dei fascicoli informatici

Art. 28 - Repertorio dei fascicoli

Art. 29 - Tenuta e conservazione dei fascicoli cartacei dell'archivio corrente

ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

Art. 30 - Generalità

Art. 31 – Profilazioni e permessi

CONSERVAZIONE DEI DOCUMENTI CARTACEI: ORGANIZZAZIONE, GESTIONE E STRUMENTI DELL'ARCHIVIO DI DEPOSITO

Art. 32 - Versamento dei fascicoli cartacei nell'archivio

Art. 33 - Gestione dell'archivio

Art. 34 - Strumenti per la gestione dell'archivio

Art. 35 - Selezione dei documenti per la conservazione/scarto

Art. 36 - Organizzazione, gestione e strumenti dell'archivio

CONSERVAZIONE DEI DOCUMENTI INFORMATICI: ORGANIZZAZIONE, GESTIONE E STRUMENTI PER LA CONSERVAZIONE DIGITALE

Art. 37 - Il sistema di conservazione

Art. 38 - Oggetti della conservazione

Art. 39 - Responsabile della conservazione

Art. 40 - Delegato per l'attività di conservazione

Art. 41 - Produttori e utenti

NORME FINALI

Art. 51 - Entrata in vigore

GLOSSARIO

1. Ai fini del presente manuale si intende per:

Affare: insieme delle attività svolte da ARPAB per raggiungere un obiettivo concreto e circoscritto; esso indica il caso concreto che l'Amministrazione deve portare a buon fine. **Allegato:** documento unito ad altro documento per prova, per chiarimento o per memoria: l'allegato deve rimanere sempre unito al documento cui si riferisce e riportare la stessa segnatura di protocollo.

Amministrazione: ARPAB

AOO (Area Organizzativa Omogenea): insieme di unità organizzative di una amministrazione, che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. In particolare, una AOO utilizza per il servizio di protocollazione un'unica sequenza numerica, rinnovata ogni anno solare.

ARPAB costituisce un'unica AOO.

Archivio: complesso di documenti prodotti (spediti e ricevuti) da un soggetto giuridico nel corso della sua attività.

Archivio corrente (archivio in formazione): complesso dei documenti relativi ad affari e procedimenti amministrativi in corso.

Assegnazione: individuazione, della persona fisica responsabile della trattazione dell'affare e della gestione dei documenti nella fase corrente.

Casella istituzionale di posta elettronica: casella di posta elettronica, istituita per la ricezione dall'esterno e per la spedizione all'esterno dei messaggi da registrare a protocollo. **Certificati elettronici:** attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi.

Certificati qualificati: certificati elettronici conformi ai requisiti di cui allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti fissati dall'allegato II.

Certificatori: coloro che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi alle firme elettroniche.

Certificatori accreditati: certificatori che sono accreditati in Italia ovvero in altri Stati membri dell'Unione europea, ai sensi dell'art. 3, paragrafo 2 della direttiva 1999/93/CE. **Dispositivo per la creazione di una firma sicura:** apparato strumentale, usato per la creazione di una firma elettronica, rispondente ai requisiti prescritti dalla normativa vigente.

Documento amministrativo: ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.

Documento archivistico: ogni documento che fa parte dell'archivio.

Documento informatico: rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Il documento informatico sottoscritto con firma digitale, redatto in conformità delle regole tecniche previste dalla legge, soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell'art. 2712 (*Riproduzioni meccaniche*) del codice civile.

Documento riassuntivo: documento prodotto con lo scopo dichiarato di riassumere dati e informazioni contenuti in forma analitica in altri documenti espressamente richiamati. **E-mail:** sistema di comunicazione elettronica attraverso messaggi.

Fascicolazione: operazione di riconduzione dei singoli documenti classificati in fascicoli.

Fascicolo: insieme organico di documenti relativi ad un medesimo affare amministrativo oppure alla medesima persona fisica o giuridica, classificati in maniera omogenea.

Firma digitale: particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, 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.

Firma elettronica: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica.

Firma elettronica avanzata: firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con

mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

Firma elettronica qualificata: firma elettronica basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma.

Gestione dei documenti: insieme delle attività finalizzate alla registrazione di protocollo, alla classificazione, alla fascicolazione, all'assegnazione, al reperimento, alla conservazione e all'accesso dei documenti amministrativi formati o acquisiti dal produttore di archivio. **Impronta di un documento informatico:** una sequenza di simboli binari in grado di identificarne univocamente il contenuto;

Interoperabilità: possibilità di trattamento automatico, da parte del sistema di protocollo ricevente, delle informazioni trasmesse dal sistema di protocollo mittente.

Linee Guida: le Linee Guida adottate da AgID sulla formazione, gestione e conservazione dei documenti informatici.

Massimario di selezione: componente del Piano di conservazione, che definisce le disposizioni ed i criteri di massima per attuare la selezione ed elenca le serie e i documenti la cui conservazione deve essere illimitata.

Piano di classificazione (c.d. Titolare): sistema logico precostituito (costruito cioè a priori, prima che vengano prodotti i singoli documenti) di partizioni astratte (quindi, generali, ma non generiche, e omnicomprensive dei possibili casi concreti che si possono verificare all'interno della quotidiana attività amministrativa del produttore), ordinate gerarchicamente (ha una struttura ad albero, nella quale ogni voce di un grado divisionale si suddivide a sua volta in alcuni rami di grado divisionale inferiore) individuato sulla base dell'analisi delle funzioni attribuite dalla legge al produttore dell'archivio. Si tratta quindi di un sistema logico che suddivide i documenti secondo la funzione esercitata dall'ente produttore e non secondo le competenze (ufficio che tratta l'affare) e permette di organizzare i documenti che si riferiscono ad affari e procedimenti amministrativi in maniera omogenea. Il titolare dell' ARPAB si articola, in due gradi divisionali (Titoli e classi).

Piano di conservazione: strumento, previsto dalla normativa, che definisce i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti, redatto e integrato con il sistema di classificazione adottato.

Registratura di Protocollo: operazione di registrazione quotidiana dei documenti ricevuti e spediti, assegnando contestualmente a ciascuno di essi un numero progressivo, che ricomincia da 1 all'inizio di ogni anno solare. La registrazione a protocollo attesta in modo inoppugnabile l'esistenza all'interno dell'archivio e la data archivistica del singolo documento, che viene identificato in modo univoco dal numero progressivo assegnatogli. **Registro:** supporto prestrutturato e munito di particolari garanzie di inalterabilità e conservazione, sul quale vengono trascritti e memorizzati per esteso o per sunto documenti o dati che da tale memorizzazione acquistano valenza probatoria.

Registro di protocollo: registro su cui si annotano quotidianamente i documenti ricevuti e spediti dall'ARPAB è atto pubblico di fede privilegiata.

Repertorio: registro su cui si trascrivono e nel quale si inseriscono in sequenza determinata (in genere cronologica) documenti ai quali si attribuisce un numero identificativo progressivo con valenza probatoria.

Repertorio dei fascicoli: registro sul quale si annotano con un numero identificativo progressivo i fascicoli secondo l'ordine cronologico con cui si costituiscono all'interno delle suddivisioni di livello più basso del titolare; mezzo di corredo per il reperimento dei fascicoli.

Responsabile del Procedimento Amministrativo (RPA): persona fisica individuata in base alla normativa vigente che ha la responsabilità dell'istruttoria e di ogni altro adempimento inerente un procedimento amministrativo.

Responsabile della conservazione e della gestione documentale: Il funzionario nominato, in possesso di requisiti professionali o di professionalità tecnico-archivistica, dedicato al servizio per la tenuta del protocollo informatico, dei flussi documentali e degli archivi. Svolge le attività di conservazione, in conformità a quanto disposto dal presente manuale e dalle disposizioni normative vigenti in materia.

Scarto: eliminazione fisica e irreversibile di documenti.

Segnatura: apposizione o associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile e va eseguita contestualmente alle operazioni di registrazione a protocollo.

Selezione: operazione intellettuale di vaglio dei documenti tendente a individuare quelli da destinare alla conservazione permanente e quelli da destinare allo scarto.

Serie: ciascun raggruppamento, operato dall'ARPAB stesso, di documenti o fascicoli con 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'ARPAB.

Sistema di gestione informatica dei documenti: l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dall'ARPAB per la gestione dei documenti.

Smistamento: individuazione della UOR cui trasmettere il documento, che servirà per trattare un affare o un procedimento amministrativo.

Sottofascicolo: partizione del fascicolo, al quale deve comunque rimanere unito.

Titolario: si veda "Piano di classificazione".

Unità di condizionamento: aggregazione di unità archivistiche determinata da esigenze di conservazione fisica: busta con più fascicoli, faldone.

Unità Organizzativa Responsabile (UOR): unità organizzative (Settori - Servizi - Uffici) competenti nelle diverse materie all'interno dell'Area Organizzativa Omogenea costituita da ARPAB .

Vincolo archivistico: nesso che collega in maniera logica e necessaria la documentazione che compone l'archivio prodotto da un ente, nella fattispecie dall'ARPAB.

PREMESSA

Le Pubbliche Amministrazioni sono tenute a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale. La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del D.Lgs. n. 33/2013.

Il presente "Manuale per la gestione e la conservazione documentale" è redatto in conformità alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici adottate da AgID (Agenzia dell'Italia Digitale).

Il manuale descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Nel manuale sono riportati, in particolare:

- relativamente agli aspetti organizzativi:
 - a) le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'AOO (Area Organizzativa Omogenea);
 - b) l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno dell'AOO.
Le UOR sono identificate con i Settori – Servizi – Uffici che compongono l'Organigramma dell'ARPAB;
 - c) l'indicazione delle regole di assegnazione dei documenti ricevuti;
 - d) i criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'Amministrazione, al sistema di gestione informatica dei documenti;
- relativamente ai formati dei documenti:
 - a) l'individuazione dei formati utilizzati per la formazione del documento informatico;
 - b) la descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi;
 - c) le procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento;
- relativamente al protocollo informatico e alle registrazioni particolari:
 - a) le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;
 - b) le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente;
 - c) l'elenco dei documenti esclusi dalla registrazione di protocollo, per cui è prevista registrazione particolare;
 - d) determinazione dei metadati associati ai documenti soggetti a registrazione particolare individuati, assicurando almeno quelli obbligatori previsti per il documento informatico;
 - e) i registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, riconosciuti da una norma;
- relativamente alle azioni di classificazione e selezione:
 - a) il piano di classificazione adottato dall'Amministrazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e

conservazione, con riferimento alle procedure di scarto;

- relativamente alla formazione delle aggregazioni documentali:
 - a) le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;
- relativamente ai flussi di lavorazione dei documenti in uso:
 - a) la descrizione dei flussi di lavorazione interni all'Amministrazione, anche mediante la rappresentazione formale dei processi attraverso l'uso dei linguaggi indicati da AgID, applicati per la gestione dei documenti ricevuti, inviati o ad uso interno;
- relativamente alla organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche:
 - a) la definizione della struttura dell'archivio all'interno del sistema di gestione informatica dei documenti;
- relativamente alle misure di sicurezza e protezione dei dati personali adottate:
 - a) le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali;
- relativamente alla conservazione:
 - a) il piano di conservazione è parte integrante del manuale di gestione documentale, con l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate.

Art. 1

Ambito di applicazione

1. Il presente manuale di gestione documentale disciplina il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Art. 2

Area Organizzativa Omogenea e modello organizzativo

- 1 Per la gestione documentale, l'Amministrazione individua un'unica Area Organizzativa Omogenea (AOO) denominata **arpab**.
2. All'interno della AOO il sistema di protocollazione è unico.
3. All'interno della AOO il sistema di protocollazione è centralizzato per la corrispondenza in entrata, e decentralizzato, per la corrispondenza in uscita.

Art. 3

Unicità del Protocollo Informatico

1. Nell'ambito dell'AOO la numerazione delle registrazioni di protocollo è unica e progressiva. Essa inizia da 1 all'inizio di ogni anno e si chiude al 31 dicembre.
2. Il numero di protocollo è costituito da almeno sette cifre numeriche.
3. Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo e sono eliminati tutti i sistemi di registrazione dei documenti alternativi al protocollo informatico.

Art. 4

Modello organizzativo adottato per la gestione dei documenti

- 1 Per la gestione dei documenti è adottato un modello organizzativo di tipo decentrato che prevede la partecipazione attiva di più soggetti ed uffici utente, ognuno dei quali è abilitato a svolgere le operazioni di propria competenza.
- 2 L'Ufficio Protocollo, incardinato nella Direzione Generale-Segreteria Direzionale ha la gestione informatica dei documenti, dei flussi documentali e degli archivi e svolge le funzioni di registrazione a protocollo, classificazione, segnatura e scansione dei documenti ricevuti dall'ente non in forma digitale (= corrispondenza in arrivo).
- 3 La registrazione dei documenti in uscita e le operazioni connesse (segnatura, classificazione, scansione e fascicolazione) sono effettuate direttamente dalle UOR (Settori - Servizi - Uffici), utilizzando il registro di protocollo informatico unico per tutta l'ARPAB.
- 4 Le persone abilitate nell'ambito delle UOR provvedono alla costituzione e gestione dei fascicoli. Ai Responsabili dei procedimenti amministrativi o altre persone a ciò incaricate è demandata la responsabilità della gestione della parte di loro competenza di Archivio corrente composto dai fascicoli e dai documenti relativi agli affari in corso di trattazione, curandone l'accesso interno ed esterno.
- 5 L'ufficio Protocollo svolge i seguenti compiti:
 - a) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo, gestito in maniera automatizzata e archiviato presso il servizio di conservazione a norma utilizzato da ARPAB;
 - b) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali;
 - c) su richiesta, autorizza le operazioni di annullamento delle registrazioni di protocollo.

DOCUMENTI

Art. 5 Tipologie di documenti

1. I documenti gestiti da ARPAB sono di due tipologie:
 - a) documento informatico, ossia la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
 - b) documento analogico, ossia un documento formato su supporto cartaceo mediante l'utilizzo di strumenti analogici o informatici.

Art. 6 Documenti amministrativi informatici

1. Per documento amministrativo informatico si intende l'atto formato dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse. Il documento amministrativo informatico costituisce informazione primaria ed originale da cui è possibile effettuare duplicazioni e copie per gli usi consentiti dalla legge.
2. L'Amministrazione forma gli originali dei propri documenti amministrativi con mezzi informatici nel rispetto delle disposizioni contenute nel Codice dell'Amministrazione digitale e delle Linee Guida adottate da AGID sulla formazione, gestione e conservazione dei documenti informatici.
3. Il documento amministrativo informatico è formato mediante una delle seguenti modalità:
 - a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici;
 - 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) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
 - d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.
4. Il documento informatico deve essere identificato in modo univoco e persistente:
 - l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento;
5. I documenti amministrativi informatici formati dall'Amministrazione sono convertiti in uno formato aperto previsto dalla normativa vigente
6. I documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della L. n. 4/2004.

Art. 7

Immodificabilità dei documenti informatici

1. Requisito del documento informatico è la sua immodificabilità, per cui la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.
2. L'immodificabilità ed integrità del documento informatico formato secondo la modalità prevista dal precedente art. 7 comma 2 lett. a), sono garantite da una o più delle seguenti operazioni:
 - apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
 - memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto previsto al paragrafo 3.9 delle Linee Guida;
 - il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
 - versamento ad un sistema di conservazione.
3. L'immodificabilità ed integrità del documento informatico formato secondo la modalità prevista dal precedente art. 7 comma 2 lett. b), sono garantite da una o più delle seguenti operazioni:
 - apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
 - memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto previsto al paragrafo 3.9 delle Linee Guida;
 - versamento ad un sistema di conservazione.
4. L'immodificabilità ed integrità del documento informatico formato secondo la modalità prevista dal precedente art. 7 comma 2 lett. c) e d), sono garantite da una o più delle seguenti operazioni:
 - apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
 - registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
 - produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.
5. Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i seguenti metadati previsti per la registrazione di protocollo:
 - a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
 - b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
 - c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti;
 - d) oggetto del documento, registrato in forma non modificabile;
 - e) data e protocollo del documento ricevuto, se disponibili.
6. Al documento amministrativo informatico sono associati ulteriori metadati conformemente all'Allegato 5 "Metadati" alle Linee Guida.
7. La disponibilità e la riservatezza delle informazioni contenute nel documento informatico sono garantite attraverso l'adozione delle seguenti procedure predeterminate dall'Amministrazione, in conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali: la normativa adottata è consultabile al seguente url: <https://www.arpab.it>

Art. 8

Copie per immagine su supporto informatico di documenti analogici

1. La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo aventi i requisiti tecnici descritti nell'allegato 3 "Certificazione di Processo" delle Linee Guida in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.
2. La conformità della copia per immagine ad un documento analogico è garantita:
 - mediante l'attestazione di un notaio o di un pubblico ufficiale a ciò autorizzato, che può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del pubblico ufficiale;
 - mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.
3. Le copie formate ai sensi dei commi 1 e 2 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge. L'amministrazione può procedere alla distruzione degli originali analogici a norma dell'articolo 22, commi 4 e 5 del Codice dell'Amministrazione Digitale (CAD), fatte salve le particolari tipologie di documenti individuati con decreto del Presidente del Consiglio dei Ministri, per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico.

Art. 9

Documenti in arrivo, in partenza e documenti interni

1. I documenti dell'ARPAB si distinguono in:
 - a) documenti in arrivo (= in entrata): documenti, con rilevanza giuridico - probatoria, prodotti da altri soggetti giuridici ed acquisiti da ARPAB nell'esercizio delle sue funzioni.
 - b) documenti in partenza (= in uscita): documenti, con rilevanza giuridico - probatoria, prodotti dal personale dell'ARPAB nell'esercizio delle sue funzioni e spediti a soggetti giuridici esterni.
 - c) documenti interni: documenti scambiati tra le diverse UOR dell'ARPAB.
2. Il documento informatico può essere recapitato all' ARPAB:
 - a) mediante posta elettronica certificata o convenzionale;
 - b) su supporto rimovibile (CD-Rom, USB, ecc.) consegnato direttamente ad ARPAB o inviato per posta ordinaria, posta raccomandata o corriere;
 - c) tramite servizi di e-government on line/form di caricamento precompilati.
3. Il documento su supporto cartaceo può essere recapitato:
 - a) A mano ad ARPAB;
 - b) a mezzo posta ordinaria, posta raccomandata o corriere;
 - c) a mezzo telegramma.
4. I documenti in arrivo sono registrati sul protocollo informatico unico dell'ARPAB e sono classificati a cura:
 - dell'Ufficio Protocollo, che poi provvede a smistarli sempre al Dirigente del Settore di competenza e nel caso di eventuale e specifica comunicazione da parte dello stesso, anche alla UOR di competenza (Settori - Servizi - Uffici).La fascicolazione è compito del Dirigente e/o dell'incaricato della UOR di competenza, che è responsabile delle operazioni di formazione e gestione del fascicolo relativo all'affare o al procedimento amministrativo che sta trattando.
5. I documenti in partenza sono registrati sul protocollo informatico unico dell'ARPAB e sono classificati a cura dell'incaricato della UOR, che tratta l'affare o il procedimento amministrativo ed è responsabile delle operazioni di formazione e gestione del fascicolo relativo.

DESCRIZIONE DEI FLUSSI DOCUMENTALI NELL'ARCHIVIO CORRENTE

Art. 10

Documenti in entrata

1. Tutti i documenti pervenuti all'ARPAB devono essere di regola registrati, segnati, classificati e smistati al Dirigente del settore competente e/o alla UOR di competenza contestualmente alla loro ricezione nella stessa giornata in cui sono pervenuti, compatibilmente con l'orario lavorativo degli addetti all'ufficio protocollo.
2. La ricezione dei documenti in entrata e il loro smistamento ai Dirigenti dei Settori e Servizi dell'ARPAB e/o alle competenti Unità Organizzative Responsabili (*Settori - Servizi - Uffici*), sono organizzati come di seguito, a seconda delle possibili casistiche sotto riportate.
3. Documenti su supporto cartaceo ricevuti tramite il servizio postale
I documenti su supporto cartaceo ricevuti tramite il servizio postale pervengono di regola all'Ufficio Protocollo. Prima della fase di apertura della corrispondenza, verrà appositamente separata quella riguardante "riservata", "personale", ecc. che verranno trattate come descritto nella parte V di questo manuale, tra i casi particolari.
L'Ufficio Protocollo dopo aver individuato il materiale da non protocollare indicato nell'elenco di cui all'art. 20, provvede alla registrazione, segnatura, classificazione, digitalizzazione/scansione del documento ove possibile e smistamento ai Dirigenti dei Settori e Servizi dell'ARPAB e/o alle competenti Unità Organizzative Responsabili (*Settori - Servizi - Uffici*), degli altri documenti protocollabili.
4. Le buste devono essere pinzate al documento cui si riferiscono.
5. L'Ufficio Protocollo, inserisce nella nota del protocollo lavorato, che "l'originale dell'atto è depositato presso l'ufficio protocollo".
6. Una volta concluse le operazioni di smistamento, si inserisce la corrispondenza ricevuta su supporto cartaceo e smistata, negli appositi "spazi dedicati" presso l'ufficio protocollo ai singoli UOR di competenza.
7. Il documento digitalizzato, viene inviato automaticamente dalla procedura informatizzata dell'Ente.
8. Ai documenti originali ricevuti, o al plico, viene applicata un'etichetta – segnatura, attestante il numero di protocollo e la data, al fine di favorire una corretta ricerca dell'omologo documento disponibile in formato informatico.
9. Il Dirigente del Settore e/o il responsabile di ciascuna UOR prende atto anche tramite il sistema informatico che gli sono stati smistati i documenti e procede a sua cura al ritiro.
10. documenti su supporto cartaceo ricevuti dagli operatori del protocollo
11. Per i documenti ricevuti allo sportello del protocollo, si applica la procedura di segnatura, smistamento ed assegnazione di cui al comma 3 del presente articolo.
12. Il documento digitalizzato, viene inviato automaticamente dalla procedura informatizzata dell'Ente.
- 13.

D

Documenti informatici in entrata - I documenti informatici ricevuti dalla casella istituzionale di posta elettronica certificata sono gestiti dalla procedura informatizzata del Protocollo, che provvedono alla registrazione, segnatura, classificazione e smistamento al Dirigente del settore competente e/o alle UOR di competenza.

Art. 11

Documenti in uscita

1. La redazione, registrazione, classificazione e fascicolazione dei documenti in uscita spetta alle singole UOR (*Settori - Servizi - Uffici*).
Nel caso di eventuali documenti su supporto cartaceo da spedire tramite il servizio postale, ciascun UOR deve far pervenire all'Ufficio Protocollo i documenti connessi.

REGISTRAZIONE A PROTOCOLLO E SEGNAZIONE DEI DOCUMENTI

Art. 12

La registrazione dei documenti

1. Tutti i documenti dell'ARPAB, dai quali possano nascere diritti, doveri o legittime aspettative di terzi, devono essere registrati sul protocollo informatico unico dell' ARPAB, con le modalità e le eccezioni di seguito illustrate.
2. La registrazione è l'operazione di memorizzazione delle informazioni fondamentali relative al contenuto, alla forma, all'autore e alla modalità di trasmissione di un documento. Tale operazione serve a identificare in modo univoco un documento, individuandone data, forma e provenienza certa.
3. Non è pertanto consentito l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza, neppure se l'affare si esaurisce con la risposta.
4. Al termine della registrazione, il documento è identificato da un insieme di dati in forma elettronica che può includere sin da questa fase la classificazione e si integra con il piano di organizzazione delle aggregazioni documentali, definito dal Responsabile della gestione documentale.

Art. 13

Il registro di protocollo

1. Il registro di protocollo, anche in forma digitale, è atto pubblico di fede privilegiata che certifica l'effettivo ricevimento e l'effettiva spedizione di un documento ad una certa data, indipendentemente dalla regolarità del documento stesso.
 2. Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.
 3. Al fine di garantire la non modificabilità delle registrazioni sul protocollo informatico unico, al termine di ogni giornata lavorativa, è previsto un sistema automatizzato di caricamento del registro giornaliero su sistema di conservazione a norma.
- Tale procedura automatizzata di riversamento è gestita dal Responsabile della conservazione.

Art. 14

Regole per la tenuta del registro di protocollo di emergenza

1. Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico, ogni evento deve essere registrato su un supporto alternativo, denominato *Registro di emergenza*, previa autorizzazione del Responsabile della Gestione Documentale che fornirà il relativo modello.
2. Su questo registro devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora di ripristino della piena funzionalità del sistema, nonché eventuali annotazioni ritenute rilevanti dal responsabile del protocollo informatico. Prima di autorizzare l'avvio della procedura, il Responsabile della Gestione Documentale deve impostare e verificare poi la correttezza di data e ora sui rispettivi registri di emergenza.
3. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.
4. Ogni registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Art. 15

Elementi obbligatori della registrazione a protocollo

1. Gli elementi obbligatori, in quanto giuridicamente rilevanti della registrazione a protocollo sono:
 - a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
 - b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
 - c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti;
 - d) numero e descrizione degli allegati (se presenti);
 - e) oggetto del documento, registrato in forma non modificabile;
 - f) data e protocollo del documento ricevuto, se disponibili;
 - g) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile;
 - h) la copia elettronica del documento, se l'originale viene presentato all'Ufficio in forma cartacea.
2. Alle informazioni di cui al comma 1 del presente articolo si aggiungono le informazioni inerenti all'assegnazione interna e l'eventuale classificazione.
3. La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione e per tutti i documenti informatici che non rientrano tra le tipologie specificate dai successivi articoli 19 e 20, al fine di garantirne l'identificazione univoca e certa.

Art. 16

La segnatura dei documenti (timbro di protocollo)

1. La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile.
2. La registrazione a protocollo e la segnatura costituiscono un'operazione unica e vanno effettuate contemporaneamente; hanno entrambe natura di atto pubblico.
3. La **segnatura dei documenti su supporto cartaceo** viene posta, di norma, sul davanti del primo foglio del documento in arrivo e sulla copia del documento in partenza mediante un timbro o qualsiasi altro strumento (ad esempio, l'etichetta) sul quale vanno riportate le seguenti informazioni:
 - denominazione dell'Amministrazione: ARPAB;
 - data di registrazione al protocollo;
 - numero progressivo di protocollo;
 - classificazione (titolo e classe);
 - smistamento.
4. La **segnatura dei documenti informatici** avviene tramite assegnazione automatica da parte del software con le medesime informazioni minime di cui al comma 3 del presente articolo.

Art. 17

Protocollo differito

1. Nel caso di temporaneo, eccezionale ed imprevisto carico di lavoro, che non permette di evadere la corrispondenza ricevuta nella medesima giornata lavorativa, e qualora dalla mancata registrazione di protocollo del documento nella medesima giornata lavorativa di ricezione possa venire meno un diritto di terzi, con motivato provvedimento del Responsabile della Gestione Documentale è autorizzato l'uso del protocollo differito.

Art. 18

Annullamento di una registrazione

1. Solo il Dirigente del Servizio e/o il Responsabile della Gestione Documentale è competente ad annullare la registrazione di un documento con apposito provvedimento, i cui estremi devono essere citati nella registrazione dell'annullamento. A tale Responsabile vanno trasmesse le richieste scritte, anche per email, contenenti il numero di protocollo da annullare e i motivi dell'annullamento.
2. Sul registro di protocollo devono apparire in forma ben visibile, la data e ora dell'annullamento, nonché il codice identificativo dell'operatore che ha effettuato l'annullamento e gli estremi dell'atto autorizzativo dell'annullamento.
3. Il sistema di protocollo informatico deve assicurare il tracciamento e la storicizzazione di ogni operazione, comprese le operazioni di annullamento, e la loro attribuzione all'operatore. Il sistema di protocollo informatico assicura che:
 - le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista;
 - le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
 - le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
 - per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema deve storicizzare tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili.

Art. 19

Documento anonimo

1. I documenti anonimi vanno protocollati, infatti l'ufficio protocollo, deve solo attestare che un determinato documento è pervenuto, così com'è.
Nel campo "Mittente" si indicherà la dicitura: "*Anonimo*".
L'Ufficio protocollo, provvederà ad inviare tali documenti, anche per conoscenza ai servizi informatici, ai soli fini di verifica per la sicurezza informatica.

Art. 20 Documenti privi di firma

1. I documenti in arrivo privi di firma devono essere protocollati.
2. Agli operatori del protocollo spetta solo il compito di certificare che quel documento in arrivo è pervenuto in quel modo e in quelle forme determinate, non quello di invitare il mittente a sanare la situazione.
3. Sarà poi compito del Dirigente del settore destinatario e/o della UOR, valutare caso per caso, ai fini della sua efficacia riguardo a un affare o un determinato procedimento amministrativo, le conseguenze della mancanza della firma.

Art. 21

Uno o più esemplari di uno stesso documento inviati a più soggetti dell'ARPAB, per competenza o per conoscenza

1. Ogni documento, anche se in più esemplari, deve essere individuato da un solo ed unico numero di protocollo, indipendentemente dal fatto che sia indirizzato, per competenza o per conoscenza, a una o più strutture amministrative all'interno dell'ARPAB.

Art. 22

Copie per competenza

1. Qualora un documento in entrata tratti più oggetti/argomenti afferenti a procedimenti diversi e - conseguentemente - a fascicoli diversi, l'addetto alla registrazione deve inserire "per competenza" gli altri destinatari/ responsabili dei procedimenti, ai quali smistare il documento.
2. Le "copie per competenza" verranno classificate e fascicolate distintamente.
3. L'originale sarà smistato al responsabile dell'oggetto principale e le copie per competenza agli altri responsabili. Nel caso di oggetti aventi eguale importanza l'originale è smistato al primo destinatario in indirizzo.

Art. 23

Copie per conoscenza

1. Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nell'art. 22. In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, registra sul registro di protocollo a chi sono state inviate le copie per conoscenza.

Art. 24

Posta elettronica certificata

Sono protocollati in ingresso unicamente i messaggi pervenuti sulla PEC protocollo@pec.arpab.it; non è prevista alcuna casella E-mail relativa al protocollo utilizzabile per inviare file da protocollare.

Art. 25

Documenti smistati e assegnati erroneamente

1. I documenti smistati e assegnati erroneamente, devono essere riclassificati e/o riassegnati il più velocemente possibile al Dirigente competente e/o alla UOR di competenza.

CLASSIFICAZIONE E FASCICOLAZIONE DEI DOCUMENTI

Art. 26

Il Piano di classificazione (c.d. Titolare)

1. È adottato un unico Piano di classificazione (Allegato A) secondo le Linee guida AgID.
2. Il Piano di classificazione di cui al comma 1 si applica a tutti i documenti informatici e/o cartacei prodotti e acquisiti dall'ARPAB, sottoposti o meno alla registrazione di protocollo.
Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti stessi.
3. Il Responsabile della gestione documentale verifica periodicamente, la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere e procede al suo eventuale aggiornamento.

Art. 27

La formazione e l'identificazione dei fascicoli informatici

1. ARPAB gestisce i flussi documentali mediante fascicoli informatici predisposti secondo il piano di classificazione di cui al precedente articolo
2. Il sistema per la gestione dei flussi documentali deve:
 - a) fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;
 - b) consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;
 - c) fornire informazioni statistiche sull'attività dell'ufficio;

- d) consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi.
3. La classificazione dei documenti in entrata è effettuata dall'Ufficio Protocollo, di quelli in uscita dal Dirigente di Settore o dall'UOR che li crea.
4. L'UOR assegnataria di un documento provvede ad inserire il documento in un fascicolo esistente o in un nuovo fascicolo appositamente creato, da classificarsi coerentemente con la classificazione del documento stesso. possibile istituire lo specifico fascicolo onde permettere la piena e completa tracciatura del procedimento stesso sino alla sua conclusione; nell'ambito del fascicolo possono essere creati più sotto fascicoli;
5. La fascicolazione deve avvenire contestualmente alla presa in carico di un documento da parte della UOR.

Art. 28

Repertorio dei fascicoli

1. Lo strumento di gestione e reperimento dei fascicoli è il Repertorio dei fascicoli sul quale vengono registrati con numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni minime del Piano di classificazione (nel nostro caso le classi). La sua struttura rispecchia quella del Piano di classificazione e quindi varierà in concomitanza con l'aggiornamento di quest'ultimo: Piano di classificazione (o Titolare) rappresenta, infatti, in astratto i documenti che possono essere prodotti dall'ARPAB, mentre il Repertorio dei fascicoli riguarda i documenti che nel concreto sono stati prodotti, suddivisi in fascicoli.

Art. 29

Tenuta e conservazione dei fascicoli cartacei dell'archivio corrente

1. I fascicoli cartacei dell'archivio corrente sono conservati presso le varie unità organizzative e formati a cura dei dirigenti, responsabili di procedimento e/o loro incaricati. .

ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

Art. 30

Generalità

1. Il controllo degli accessi è attuato al fine di garantire l'impiego del sistema informatico di protocollo esclusivamente secondo modalità prestabilite.

Art. 31

Profilazioni e permessi

1. I diversi livelli di autorizzazione ed i conseguenti differenti profili sono assegnati agli utenti dal Direttore Generale il quale, inoltre, provvede all'assegnazione di eventuali nuove autorizzazioni, alla revoca o alla modifica di quelle già assegnate avvalendosi dell'ufficio dedicato alla manutenzione e alla gestione del sistema informativo comunale.

CONSERVAZIONE DEI DOCUMENTI CARTACEI: ORGANIZZAZIONE, GESTIONE E STRUMENTI DELL'ARCHIVIO

Art. 32

Versamento dei fascicoli cartacei nell'archivio

1. Periodicamente, i Dirigenti, le Unità organizzative e i responsabili di procedimento individuano i fascicoli cartacei relativi ad affari o procedimenti conclusi o comunque non più necessari allo svolgimento delle attività correnti da trasferire nell'archivio. Il trasferimento deve essere effettuato

rispettando l'organizzazione che i fascicoli e le serie hanno nell'archivio corrente.

2. Prima del trasferimento presso l'archivio di deposito, i soggetti di cui al comma 1 sono tenuti a realizzare, altresì, l'operazione di sfoltimento, consistente nell'eliminazione del materiale non archivistico contenuto nei fascicoli (es. bozze e brutte copie, fotocopie, dépliant, vecchi moduli e stampati, ecc.).
3. Al termine di tale operazione il fascicolo deve essere quindi composto solo dai documenti archivistici e dai loro allegati.
4. Le serie e i repertori dei provvedimenti direttoriali e dirigenziali, nonché verbali e sedute sono conservati per cinque anni presso la Segreteria direzionale; trascorso tale termine vengono versati all'Archivio.

Art. 33

Gestione dell'archivio

1. La cura della gestione e conservazione dell'archivio è affidata al Dirigente ovvero ad un referente individuato dal singolo Dirigente rispetto al proprio settore/servizio.

Art. 34

Strumenti per la gestione dell'archivio

1. Gli strumenti per la gestione dell'archivio sono:
 - elenco di consistenza, in cui sono riportati i fascicoli conservati presso l'archivio, suddivisi per titolo, classe e per anno di apertura;
 - registro dei versamenti dei fascicoli.

Art. 35

Selezione dei documenti per la conservazione/scarto

1. Il referente incaricato, , predispone con cadenza periodica un elenco del materiale che si propone di inviare allo scarto, per il quale si segue la procedura prevista dalla normativa vigente e lo comunica al Responsabile della gestione documentale e della conservazione, deputato all'attivazione della procedura di scarto, secondo la normativa vigente.

Art. 36

Organizzazione, gestione e strumenti dell'archivio storico

1. I documenti che costituiscono l'archivio dell'ARPAB sono conservati presso le differenti sedi dei singoli settori/servizi dell'ente.

CONSERVAZIONE DEI DOCUMENTI INFORMATICI: ORGANIZZAZIONE, GESTIONE E STRUMENTI PER LA CONSERVAZIONE DIGITALE

Art. 37

Il sistema di conservazione

1. Il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell'articolo 44, comma 1-bis, del CAD:
 - a) i fascicoli informatici chiusi e le serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito;
 - b) i fascicoli informatici e le serie non ancora chiuse trasferendo i documenti in essi contenuti sulla base di specifiche esigenze del ARPAB, con particolare attenzione per i rischi di obsolescenza tecnologica.
2. Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:
 - a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
 - b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del D.P.R. n. 445/2000 e art. 44, comma 1-bis, C.A.D.
3. Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione e dalla normativa vigente.

Art. 38

Oggetti della conservazione

1. Devono essere conservati tutti i documenti informatici prodotti dall'Amministrazione secondo le indicazioni previste dalla normativa vigente.
2. I documenti informatici devono essere immutabili e possono essere anche muniti di sottoscrizione elettronica e/o di marca temporale.
3. Nell'elenco seguente sono indicati i principali formati che possono essere utilizzati per la conservazione:

Tipologia	Estensione
Documenti di testo pdf	PDF, ...
Documenti di testo office	DOCX, ODT, XLSX, PPTX, ...
Immagini	TIF, TIFF, JPG, JPEG, ...
Messaggi di posta elettronica	EML, MBOX, ...
Audio	WAV, MP3, ...
Video	MPEG4, ...
...	...

4. I documenti sottoscritti con firma digitale e i documenti con marcatura temporale sono accettati nei formati P7M, M7M e P7S.

Art. 39

Responsabile della conservazione

1. Il ruolo di Responsabile della conservazione può essere svolto anche dal responsabile della gestione documentale. Il responsabile della conservazione:
 - a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
 - b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

- c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l) predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Art. 40

Delegato per l'attività di conservazione

- 1. Il delegato per l'attività di conservazione è il soggetto pubblico o privato, accreditato presso l'Agenzia per l'Italia Digitale, nominato dal responsabile della conservazione a cui viene affidata in modo totale o parziale la conservazione dei documenti digitali.
- 2. Il delegato deve offrire idonee garanzie organizzative e tecnologiche per lo svolgimento delle funzioni affidategli.
- 3. Il delegato per l'attività di conservazione:
 - verifica che il formato dei documenti trasmessi sia fra quelli previsti nel presente manuale;
 - archivia e conserva per ciascun pacchetto di versamento le informazioni minime previste dalla normativa vigente;
 - fornisce un rapporto di versamento per ogni pacchetto di versamento;
 - adotta le misure di sicurezza necessarie relative al processo di conservazione;
 - rende disponibili all'ARPAB i documenti conservati nel caso di richiesta.

Art. 41

Produttori e utenti

- 1. Il responsabile della gestione documentale svolge il ruolo di produttore del Pacchetto di Versamento e ne assicura la trasmissione al sistema di conservazione, secondo le modalità operative definite nel presente manuale.
- 2. L'utente abilitato richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti del livello di autorizzazione attribuito dal responsabile della conservazione.

NORMA FINALE

Art. 42

Entrata in vigore

- 1. Il presente Manuale entra in vigore il giorno successivo alla data di esecutività della delibera di approvazione.

ALLEGATO A) AL MANUALE DI GESTIONE DOCUMENTALE

TITOLARIO

Titolo I. ORGANIZZAZIONE GENERALE, ATTIVITÀ E RAPPORTI ISTITUZIONALI

1. Atti di indirizzo della Direzione Strategica
2. Ordinamento degli Uffici e dei servizi
3. Partecipazione ad attività di sistema (SNPA) per governo e coordinamento delle funzioni
4. Tutela dati personali
5. Richieste di accesso agli atti
6. Sistema Gestione Qualità
7. Rapporti con il pubblico, sportello informativi e comunicazione pubblica
8. Pubblicazione dati
9. Costituzione, gestione e diffusione di informazioni di carattere ambientale
10. Servizi e sistemi informativi
11. Altro

Titolo II. SISTEMI DI CONTROLLO INTERNO ED ESTERNO

1. Valutazione e controllo strategico
2. Autorità per la Valutazione e il Merito (AVM)
3. Controllo di Gestione
4. Comitato per le pari opportunità
5. Ufficio Provvedimenti Disciplinari
6. Controllo Regionale
7. Corte dei Conti
8. Revisore Unico
9. Altro

Titolo III. ATTIVITÀ NEGOZIALE CONTRATTUALE E ASSICURATIVA

1. Contratti e Convenzioni

2. Polizze assicurative
3. Altro

Titolo IV. AFFARI LEGALI E CONTENZIOSO

1. Extragiudiziale
2. Giudiziale
3. Altro

Titolo V. RISORSE UMANE

1. Fascicoli personale dipendente
2. Programmazione di settore
3. Procedure di selezione
4. Assunzioni
5. Cessazione del rapporto di lavoro
6. Stato giuridico e vicende del rapporto di lavoro
7. Presenze e assenze del personale
8. Incarichi extraistituzionali
9. Anagrafe e prestazioni
10. Trattamento economico
11. Trattamento pensionistico
12. Adempimenti fiscali contributivi e assicurativi
13. Relazioni sindacali e contrattazione
14. Personale non dipendente
15. Altro

Titolo VI. SALUTE E SICUREZZA SUL LAVORO

1. Servizio di prevenzione e protezione
2. Prestazioni del medico competente
3. Accertamenti sanitari del personale
4. Sopralluoghi e interventi tecnici di adeguamento
5. Designazione dei responsabili e delega di funzioni
6. Designazione dei responsabili dei lavoratori per la sicurezza

7. Altro

Titolo VII. CONTABILITÀ E BILANCIO

1. Bilancio di previsione
2. Bilancio consuntivo
3. Variazioni di bilancio e assestamento
4. Entrate
5. Uscite
6. Mutui, finanziamenti
7. Cassa economale
8. Adempimenti fiscali, gestione IVA, IRAP, IRPEF, sostituto d'imposta, rapporti con uffici finanziari
9. Altro

Titolo VIII. PATRIMONIO ED APPROVVIGIONAMENTO – Attività Tecniche

1. Patrimonio e beni strumentali
2. Utenze
3. Forniture beni e servizi
4. Spese in economia
5. Gestione parco automezzi
6. Gestione magazzino
7. Attività tecniche
8. Altro

Titolo IX. MONITORAGGI AMBIENTALI

1. Monitoraggio della qualità dell'aria
2. Monitoraggio della qualità delle acque (interne e marine)
3. Monitoraggio della radioattività, delle radiazioni ionizzanti e non ionizzanti
4. Monitoraggio dei livelli di rumore ambientale
5. Monitoraggio della biodiversità
6. Altri monitoraggi di parametri fisici e qualitativi dello stato dell'ambiente

Titolo X. CONTROLLI SULLE FONTI DI PRESSIONE E DEGLI IMPATTI SU MATRICI E ASPETTI AMBIENTALI

1. Ispezioni su aziende
2. Misurazioni e valutazioni delle pressioni di origine antropica
3. Misurazioni e valutazioni delle pressioni di origine naturale
4. Interventi in emergenza per la verifica di possibili inquinamenti o danni ambientali
5. Altro

Titolo XI SVILUPPO DELLE CONOSCENZE, COMUNICAZIONE E INFORMAZIONE

1. Studi e iniziative progettuali sulle dinamiche evolutive delle componenti ambientali
2. Realizzazione e gestione del Sinanet, delle sue componenti regionali e dei catasti, degli annuari e del report di sistema
3. Comunicazione e informazione ambientale
4. Altro

Titolo XII. SUPPORTO TECNICO SCIENTIFICO PER AUTORIZZAZIONI AMBIENTALI, STRUMENTI DI PIANIFICAZIONE, VALUTAZIONE E NORMATIVA AMBIENTALE

1. Supporto tecnico per autorizzazioni ambientali e su strumenti di valutazione e sulle dinamiche evolutive delle componenti ambientali
2. Partecipazioni a commissioni previste da norme di settore e supporto tecnico per analisi di compatibilità ambientale
3. Pareri e supporto tecnico scientifico per la formulazione, l'attuazione e la valutazione delle normative ambientali
4. Istruttorie per il rilascio di autorizzazioni ambientali
5. Altro

Titolo XIII. SUPPORTO TECNICO PER ANALISI FATTORI AMBIENTALI A DANNO DELLA SALUTE PUBBLICA

1. Attività tecnica ed operativa a supporto delle iniziative a tutela della popolazione dal rischio ambientale
2. Supporto tecnico e analitico a strutture sanitarie
3. Altro

Titolo XIV. EDUCAZIONE E FORMAZIONE AMBIENTALE

1. Iniziative e supporto ad attività di educazione ambientale a livello nazionale

2. Iniziative e supporto ad attività di formazione ambientale a livello nazionale
3. Formazione e aggiornamento professionale
4. Altro

Titolo XV. FUNZIONI DI SUPPORTO TECNICO PER LO SVILUPPO E L'APPLICAZIONE DI PROCEDURE DI CERTIFICAZIONE

1. Supporto tecnico scientifico nell'ambito delle attività istruttorie previste dai regolamenti EMAS ed Ecolabel UE
2. Altro

Titolo XVI. ATTIVITÀ DI LABORATORIO

1. Analisi di campioni per monitoraggi ambientali
2. Analisi di campioni per controlli sulle fonti di pressione
3. Analisi di campioni a supporto delle strutture sanitarie
4. Altro

Nomina Responsabile CONSERVAZIONE SOSTITUTIVA

DELIBERAZIONE

MANDATO N. 239

DEL 16/05/2016

OGGETTO: INDIVIDUAZIONE E NOMINA DEL RESPONSABILE DELLA CONSERVAZIONE SOSTITUTIVA

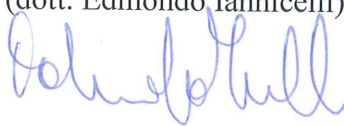
IL DIRETTORE GENERALE

- tenuto conto dei dettami legislativi in tema di mantenimento nel tempo obbligatorio della documentazione prodotta da codesta Agenzia;
- richiamata la Deliberazione CNIPA del 19 febbraio 2004, n. 11 (Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445);
- richiamato il D.lgs del 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) e sue successive modificazioni, in tema di gestione a pieno valore legale dei documenti informatici, sia in Pubblica Amministrazione sia in Strutture private, per redazione, sottoscrizione, archiviazione, trasmissione, conservazione sostitutiva, esibizione, etc.;
- visto il Decreto del Presidente Del Consiglio Dei Ministri del 3 dicembre 2013 recante 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;
- premesso che l'A.R.P.A.B. si è dotato di sistemi informativi ed amministrativi che producono documenti informatici;
- tenuto conto dell'art.43 del D.lgs n.82/05 e sue successive modificazioni, con cui si sancisce che il documento informatico deve essere mantenuto nel tempo a fini legali solo attraverso la conservazione sostitutiva;
- preso atto delle imposizioni normative e delle necessità giuridiche, organizzative e medico – legali di avviare la conservazione sostitutiva di detti documenti;
- preso atto che tale completa gestione digitale può consentire il mantenimento dell'intrinseco valore giuridico della documentazione, con aumento di quello giuridico-amministrativo, con incremento di sicurezza e riservatezza nel trattamento dei dati personali e sensibili;
- preso atto delle indicazioni delle Direzioni per realizzare una gestione documentale completamente digitale;
- preso atto che per l'utilizzo della nuova tecnologia e per ottemperare alla normativa vigente in tema di conservazione sostitutiva, risulta anche necessario individuare e nominare un Responsabile della Conservazione Sostitutiva;

DELIBERA

1. di individuare nella dr.ssa *Serpillo Brigida* la persona fisica atta per competenza a svolgere il ruolo di Responsabile della Conservazione Sostitutiva interno all'A.R.P.A.B., ai sensi del D.P.C.M. del 3 dicembre 2013 recante *"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"*, e quindi di nominarlo Responsabile aziendale di detta conservazione di documenti;
2. di dichiarare il presente mandato di nomina immediatamente esecutivo ai sensi dell'art. 17 DPR 617/80, fatte salve le determinazioni dei competenti organi di controllo.

Il Direttore Generale (dott. Edmondo Iannicelli)



Modulo Di Richiesta SERVIZIO CONSERVAZIONE SOSTITUTIVA

POTENZA lì, 21/06/16

Trasmissione a mezzo PEC all'indirizzo:

ufficio.amministrazione.digitale@cert.regione.basilicata.it

Spett.

Dirigente dell'Ufficio Amministrazione Digitale

Dipartimento Programmazione e Finanze

Via Vincenzo Verrastro, 4

85100

Potenza

OGGETTO: Azioni regionali a supporto della Conservazione Sostitutiva dei documenti informatici ai sensi D.P.C.M. del 3 dicembre 2013 recante *“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”*.

Richiesta di adesione dell'Ente A.R.P.A.B.

La sottoscritta Serpillo Brigida, in qualità di Responsabile della Conservazione Sostitutiva dell'Amministrazione A.R.P.A.B. nominato ai sensi dell'art. 7 del DPCM del 3 dicembre 2013, richiede di aderire al servizio di Conservazione Sostitutiva dei documenti informatici offerto dalla Regione Basilicata, ai termini ed alle condizioni indicate sul sito www.conservazionesostitutiva.regione.basilicata.it, che dichiara espressamente di conoscere ed accettare.

Allega alla presente la seguente documentazione:

1. Atto di delega Responsabile del Servizio di Conservazione (Allegato 1);
2. Elenco utenti finali (Allegato 2);
3. Schede di conservazione (Allegato 3);
4. Nomina Responsabile esterno del trattamento dei dati (Allegato 4);
5. Copia dell'atto di nomina del Responsabile della Conservazione Sostitutiva dell'Ente (Allegato 5);

Cordiali saluti

Il Responsabile della
Conservazione sostitutiva dell'Ente
Dr.ssa Brigida Serpillo

ATTO DI DELEGA

La sottoscritta _____ SERPILLO BRIGIDA _____ nata il 17/01/1973 a _____ ALESSANDRIA _____ Pr. (AL), c.f. _____ SRP BGD 73A57 A182D _____ nella sua qualità di (legale rappresentante) Responsabile della CONSERVAZIONE SOSTITUTIVA dell'A.R.P.A.B., con sede e domicilio fiscale in POTENZA (PZ), Via della Fisica 18 c/d ed assegnatario della P.Iva 01318260765, munito di tutti i necessari poteri per la firma del presente atto, consapevole delle responsabilità penali e civili nella quali incorre chiunque rilascia dichiarazioni mendaci, ai sensi e per gli effetti di cui all'art. 46 e 47 D.P.R. n. 445/2000, sotto la propria personale responsabilità, con la sottoscrizione del presente atto,

DICHIARA

di essere munito dei necessari poteri per impegnare l'ente quivi indicato come Utente Finale sottoscrivendo il presente atto ed i relativi allegati

e

Nella sua qualità di titolare/legale rappresentante dell'Utente finale nonché **Responsabile della conservazione**

NOMINA E DELEGA

La società **ARUBA PEC S.P.A.**, società a socio unico, in appresso denominata anche "ARUBA PEC", con sede legale in Arezzo (AR), Via Sergio Ramelli, n. 8, assegnataria del codice fiscale e numero di iscrizione al Registro delle Imprese di Arezzo: 01879020517, indirizzo e-mail - conservazione@arubapec.it, nr. Telefono: 0575-050036 nr. Fax: 39 0575 862000,

"Responsabile del servizio di conservazione" dei documenti informatici della tipologia riportata nelle Schede di conservazione allegate al Contratto, secondo quanto ivi previsto.

1. Funzioni ed attività oggetto della presente delega

1.1 In forza della presente nomina, ARUBA PEC viene formalmente delegata dall'Utente finale a svolgere le seguenti attività:

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

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

- il mantenimento dell'identificazione certa del soggetto che ha formato il documento informatico;
- l'integrità dei documenti informatici depositati in conservazione;
-

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

1.3 ARUBA PEC dovrà altresì :

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

Resta inteso che:

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

2. Deleghe di singole funzioni o fasi del processo

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

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

3. Comunicazione nuove classi documentali

3.1 Qualora l'Utente finale intenda sottoporre a conservazione documenti informatici appartenenti a tipi/classi documentali diverse e/o ulteriori rispetto a quelle indicate nell'Elenco dei documenti informatici sottoposti a conservazione allegato al contratto, dovrà formulare apposita istanza scritta ad ARUBA PEC, allegando ad essa una nuova Scheda di Conservazione dei documenti informatici sottoposti a conservazione.

Luogo POTENZA, data 21/06/16

____ Dr.ssa Brigida Serpillo ____
L'Utente Finale
(Timbro e Firma o Firma Digitale)

Si allega copia del documento di identità del firmatario in corso di validità

Scheda conservazione – Fatturazione PA

Elenco dei tipi di documenti informatici che il Cliente intende sottoporre a conservazione utilizzando il Servizio.

Dati identificativi archivio Utente		ragione sociale	Codice fiscale o partita iva	
		A.R.P.A.B.	01318260765	
Tab. A – Classi Documentali	Formati Accettati	Firma digitale	Frequenza Versamento	Foglio di Stile
FATTURA PA	☒ XML/P7M	OBBLIGATORIA	ANNO	PRESENTE http://www.fatturapa.gov.it/export/fatturazione/it/normativa/f-3.htm
NOTIFICA PA	☒ XML	FACOLTATIVA	ANNO	PRESENTE http://www.fatturapa.gov.it/export/fatturazione/it/normativa/f-3.htm

METADATI

Elenco metadati obbligatori Devono essere presenti nell'indice	TAB. B – METADATI OBBLIGATORI		
	ID pacchetto di versamento	Nome destinatario	Denominazione Soggetto Produttore
	IDDocumento (valore obbligatorio)	Codice Fiscale destinatario	Denominazione soggetto tributario
	Impronta Documento (valore obbligatorio)	Denominazione destinatario	Partita IVA soggetto tributario
	Data Chiusura	Partita Iva Destinatario	Cognome soggetto tributario
	Oggetto Documento	Cognome Soggetto Produttore	Nome soggetto tributario
	Data documento tributario (valore obbligatorio)	Nome Soggetto Produttore	Codice fiscale soggetto tributario
	Data documento	Partita Iva Soggetto produttore	
	Cognome destinatario	Codice Fiscale Soggetto Produttore	

Elenco ExtraInfo Disponibili Non sono obbligatori nell'indice Possono non essere valorizzati.	TAB. C – METADATI DISPONIBILI		
	IDENTIFICAZIONE DEL SISTEMA VERSANTE	Nr. DDT	NR. PROGRESSIVO LIBRO/REGISTRO
	ID DOCUMENTO NEL SISTEMA DI ORIGINE	NUMERO FATTURA	SOGGETTO A IMPOSTA DI BOLLO
	APPLICATIVO DI PRODUZIONE DEL DOCUMENTO	TIPOLOGIA DOCUMENTO (COME DA PROVV. PROT. N. 2010/143663)	NOTE 1
	LIVELLO DI RISERVATEZZA	CODICE TIPOLOGIA DOCUMENTO (COME DA PROVV. PROT. N. 2010/143663)	NOTE 2
	CONDIZIONI DI ACCESSO	NR. NOTA DI ACCREDITO	ALLEGATO 1
	CODICE FISCALE TITOLARE DEL CERTIFICATO DI FIRMA	SEZIONALE	ALLEGATO 2
	Id FASCICOLO	NOME DEL SEZIONALE	ESITO
	TIPO NOTIFICA		

NOTE:

L'utente finale, dopo aver comunicato ad Aruba le caratteristiche, le modalità ed i termini di versamento dei documenti informatici in conservazione, approva espressamente quanto indicato nelle tabelle descrittive sopra riportate, facendole proprie in ogni loro parte, essendo perfettamente coincidenti alle istruzioni dal medesimo impartite.

Potenza, lì 21/06/16

L'utente finaledr.ssa Brigida Serpillo.....

Scheda conservazione – PEC

Elenco dei tipi di documenti informatici che il Cliente intende sottoporre a conservazione utilizzando il Servizio.

Dati identificativi		ragione sociale	Codice fiscale o	partita iva
archivio utente		A.R.P.A.B.	01318260765	
Tab. A – Classi documentali		Formati Accettati	Caselle PEC (elenco caselle)	
PEC		☒ EML	1) protocollo@pec.arpab.it 2)@..... 3)@.....	

METADATI

Elenco metadati obbligatori Devono essere presenti nell'indice	TAB. B – METADATI OBBLIGATORI		
	ID pacchetto di versamento	Cognome destinatario	Cognome Soggetto Produttore
	IDDocumento (valore obbligatorio)	Nome destinatario	Nome Soggetto Produttore
	Impronta Documento (valore obbligatorio)	Codice Fiscale destinatario	Partita Iva Soggetto produttore
	Data Chiusura	Denominazione destinatario	Codice Fiscale Soggetto Produttore
	Oggetto Documento	Partita Iva Destinatario	Denominazione Soggetto Produttore
	Indirizzo (valore obbligatorio)	Oggetto	Da (valore obbligatorio)
	A (valore obbligatorio)	CC	Message ID (valore obbligatorio)
	Riferimento message ID	Data (valore obbligatorio)	Trasporto
	Ricevuta	Allegati	

NOTE:

L'utente finale dopo aver comunicato ad Aruba le caratteristiche, le modalità ed i termini di versamento dei documenti informatici in conservazione, approva espressamente quanto indicato nelle tabelle descrittive sopra riportate, facendole proprie in ogni loro parte, essendo perfettamente coincidenti alle istruzioni dal medesimo impartite.

Potenza, li __21/06/16__

L'utente finaledr.ssa Brigida Serpillo.....

Scheda conservazione – Registro giornaliero di protocollo

Elenco dei tipi di documenti informatici che il Cliente intende sottoporre a conservazione utilizzando il Servizio.

Dati identificativi	Ragione sociale	Codice fiscale o partita iva
archivio Utente	A.R.P.A.B.	01318260765

Registro Giornaliero di protocollo

☒ PREVISTI DALLA NORMATIVA :PDF - PDF/A, TIFF, JPG, Office Open XML (OOXML) , Open Document Format, XML, TXT, Formati Messaggi di posta elettronica

☐ NON PREVISTI DALLA NORMATIVA: 7Z, DATA, MSA, MSG, MSPP, MSWORD, PSD, RTF, XLS, ZIP

METADATI

TAB. B – METADATI OBBLIGATORI			
Elenco metadati obbligatori Devono essere presenti nell'indice	ID pacchetto di versamento	Denominazione soggetto mittente	Numero ultima registrazione effettuata sul registro
	IDDocumento (valore obbligatorio)	Partita IVA soggetto mittente	Data prima registrazione effettuata sul registro
	Impronta Documento (valore obbligatorio)	Cognome soggetto mittente	Data ultima registrazione effettuata sul registro
	Data Chiusura	Nome soggetto mittente	Amministrazione titolare del procedimento
	Oggetto Documento	Codice fiscale soggetto mittente	Amministrazioni partecipanti
	cognome destinatario	Cognome Soggetto Produttore 2	Responsabile del procedimento
	Nome destinatario	Nome Soggetto Produttore 2	Oggetto del Procedimento
	Codice Fiscale destinatario	Codice Fiscale Soggetto Produttore 2	Documenti contenuti nel procedimenti
	Denominazione destinatario	Cognome Responsabile Gestione Documentale	Numero Protocollo
	Partita Iva Destinatario	Nome Responsabile Gestione Documentale	Data Registrazione Protocollo
	Cognome Soggetto Produttore	Codice Fiscale Responsabile Gestione Documentale	AOO di riferimento
	Nome Soggetto Produttore	Codice identificativo del registro	Codice Identificativo amministrazione (IPA)
	Partita Iva Soggetto produttore	Numero Progressivo del registro	Denominazione dell'amministrazione
	Codice Fiscale Soggetto Produttore	Anno	
	Denominazione Soggetto Produttore	Numero prima registrazione effettuata sul registro	

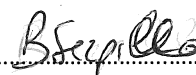
TAB. C – METADATI DISPONIBILI			
Elenco ExtraInfo Disponibili Non sono obbligatori nell'indice Possono non essere valorizzati.	IDENTIFICAZIONE DEL SISTEMA VERSANTE	DATA DI ALTRA REGISTRAZIONE	IDENTIFICATIVO DELL'UNITÀ ARCHIVISTICA
	ID DOCUMENTO NEL SISTEMA DI ORIGINE	REGISTRO	ANNOTAZIONE
	APPLICATIVO DI PRODUZIONE DEL DOCUMENTO	REPERTORIO	ANNESSO
	LIVELLO DI RISERVATEZZA	SERIE	NOTE 1
	CONDIZIONI DI ACCESSO	UFFICIO PRODUTTORE	NOTE 2
	CODICE FISCALE TITOLARE DEL CERTIFICATO DI FIRMA	ESISTENZA DI ORIGINALE ANALOGICO	ALLEGATO 1
	NUMERO DI ALTRA REGISTRAZIONE	CLASSIFICAZIONE ARCHIVISTICA	ALLEGATO 2
	ID FASCICOLO		

NOTE:

L'utente finale, dopo aver comunicato ad Aruba le caratteristiche, le modalità ed i termini di versamento dei documenti informatici in conservazione, approva espressamente quanto indicato nelle tabelle descrittive sopra riportate, facendole proprie in ogni loro parte, essendo perfettamente coincidenti alle istruzioni dal medesimo impartite.

POTENZA, lì 21/06/16

L'utente finale.....



NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

in applicazione del "Codice in materia di protezione dei dati personali" ai sensi e per gli effetti degli artt. 4, co. 1, lett. g) e 29 del D.Lgs 30 giugno 2003, n. 196

La sottoscritta _____ SERPILLO BRIGIDA _____ nata il 17/01/1973 a ALESSANDRIA Pr. (AL), c.f. SRP BGD 73A57 A182D nella sua qualità di (legale rappresentante) Responsabile della CONSERVAZIONE SOSTITUTIVA dell'A.R.P.A.B., con sede e domicilio fiscale in POTENZA (PZ), Via della Fisica 18 c/d ed assegnatario della P.Iva 01318260765, munito di tutti i necessari poteri per la firma del presente atto, consapevole delle responsabilità penali e civili nella quali incorre chiunque rilascia dichiarazioni mendaci, ai sensi e per gli effetti di cui all'art. 46 e 47 D.P.R. n. 445/2000, sotto la propria personale responsabilità, in qualità di Titolare del trattamento, come previsto dal combinato disposto degli artt. 4, co. 1, lett. f) e 28, del D.Lgs 30 giugno 2003, n. 196, di seguito, per brevità, definito "**Titolare del trattamento**";

- visto il Decreto Legislativo 30 giugno 2003, n. 196. "*Codice in materia di protezione dei dati personali*", di seguito definito "*Codice*" e s.m.i.;
- preso atto che l'art. 4, comma 1, lettera g) del suddetto Decreto definisce quale "*responsabile, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali*";
- atteso che l'art. 29, commi 2, 3, 4 e 5 del D. Lgs. n. 196/2003 dispone che:
 - 2. *Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.*
 - 3. *Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione dei compiti.*
 - 4. *I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare.*
 - 5. *Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni*;
- considerato che il compimento di tutti gli atti previsti dal Codice per il trattamento dei dati personali, spettano in via esclusiva al Titolare del trattamento;
- considerato che l'erogazione del Servizio di conservazione sostitutiva a norma comporta la necessità di trattare, in nome e per conto del suddetto Titolare, dati personali che, come tali, sono soggetti all'applicazione del Codice in materia di protezione dei dati personali;

N O M I N A

La società **ARUBA PEC S.P.A.**, in appresso denominata anche "**ARUBA PEC**", con sede legale in Arezzo (AR), Via Sergio Ramelli, n. 8, assegnataria del codice fiscale e numero di iscrizione al Registro delle Imprese di Arezzo: 01879020517, **RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI**, effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi, per quanto sia strettamente necessario alla corretta esecuzione dei servizi ed al rispetto degli obblighi assunti nel Contratto.

COMPITI PARTICOLARI DEL RESPONSABILE ESTERNO DEL TRATTAMENTO

Il Responsabile esterno del trattamento, operando nell'ambito dei principi stabiliti dal Codice, deve attenersi ai seguenti **compiti di carattere particolare**:

1. il trattamento dei dati deve essere effettuato solo per le finalità connesse allo svolgimento delle attività oggetto del Contratto, con divieto di qualsiasi altra diversa utilizzazione;
2. deve gestire il sistema informatico, nel quale risiedono i documenti informatici ed i dati del Titolare, in osservanza al disciplinare tecnico di cui all'allegato B) del Codice, attenendosi anche alle disposizioni del Titolare del trattamento in tema di sicurezza;

3. deve predisporre ed aggiornare un sistema di sicurezza informatico idoneo a rispettare le prescrizioni del Codice, adeguandolo anche alle eventuali future norme in materia di sicurezza. Più specificatamente, il Responsabile esterno del trattamento deve:

- a) adottare adeguati programmi ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal Codice ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi in conformità allo stesso disciplinare tecnico di cui all'allegato B) del Codice;
- b) adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei documenti informatici e dei dati e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure attivate in struttura. Il Responsabile esterno del trattamento dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- c) predisporre ed implementare le eventuali ulteriori misure minime di sicurezza imposte dal Disciplinare tecnico di cui all'allegato B) del Codice, per il trattamento informatico dei dati sensibili e per la conseguente tutela degli strumenti elettronici
- d) in definitiva, deve adottare adeguate e preventive misure contro i rischi di distruzione o perdita, anche accidentale, dei dati e dei documenti informatici, di accesso non autorizzato e di trattamento non consentito;

4. considerata la complessità delle operazioni tecniche di trattamento ed i compiti assegnati al punto precedente, il Titolare del trattamento autorizza il Responsabile esterno del trattamento ad affidare, sotto la propria responsabilità, l'esecuzione di operazioni di trattamento informatico a soggetti terzi che per connotazione tecnologica, esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto della legge, con particolare riguardo alla sicurezza;

5. può nominare appositi incaricati preposti alle operazioni di trattamento di cui al precedente punto 1); detti incaricati opereranno sotto la diretta autorità del Responsabile esterno del trattamento qui nominato, attenendosi alle istruzioni da questi impartite;

6. deve predisporre e tenere a disposizione, per eventuali verifiche:

- a) una breve descrizione del sistema informativo e delle procedure che utilizza per il trattamento dei dati;
- b) una descrizione delle misure messe in atto per soddisfare il dettato dell'Allegato B) del Codice, con particolare riferimento all'adozione di adeguate e preventive misure di sicurezza, contro i rischi di distruzione o perdita, anche accidentale, dei dati/documenti informatici stessi, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità connesse allo svolgimento delle attività oggetto del Contratto;
- c) la descrizione delle istruzioni impartite agli incaricati;
- d) il programma di formazione ed aggiornamento degli incaricati, in materia di privacy e sicurezza:

PRINCIPI GENERALI DA OSSERVARE A CURA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO

7. Ogni trattamento di dati personali deve avvenire, nel rispetto di quanto previsto dal Codice e nel primario rispetto dei principi di ordine generale. In particolare, per ciascun trattamento di propria competenza, il Responsabile esterno del trattamento deve fare in modo che siano sempre rispettati i seguenti presupposti:

- a) i dati devono essere trattati:
 - o secondo il principio di liceità;
 - o secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- b) i dati devono, inoltre, essere:
 - o trattati soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
 - o conservati per un periodo non superiore a quello necessario per gli scopi del trattamento

8. Ciascun trattamento deve avvenire nei limiti imposti dal principio fondamentale di riservatezza e deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

9. Il Responsabile esterno del trattamento è a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni penali (artt. 167 e ss. del Codice).

10. Il Responsabile esterno del trattamento si impegna a non divulgare, diffondere, trasmettere e comunicare i dati/documenti informatici di proprietà del Titolare del trattamento, nella piena consapevolezza che i dati/documenti rimarranno sempre e comunque di proprietà esclusiva dello stesso Titolare del trattamento, e pertanto non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti.

11. Ai sensi e per gli effetti dell'art. 30, co. 5, del Codice, il Titolare del trattamento, ha facoltà di vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza dei compiti e delle istruzioni qui impartite al Responsabile esterno del trattamento.

12. All'atto della conclusione o della revoca dei servizi oggetto del Contratto, il Responsabile esterno del trattamento dovrà consegnare al Titolare del trattamento gli archivi informatici con le modalità previste dal Contratto e dal Manuale del sistema

di conservazione e dai documenti ad essi allegati; contestualmente, ARUBA PEC, si impegna a cancellare fisicamente dai propri sistemi e dai propri archivi elettronici tutti i dati/documenti informatici di proprietà del Titolare del trattamento. E' comunque facoltà del Titolare del Trattamento, prelevare in qualsiasi momento gli archivi informatici di sua proprietà usufruendo della specifica funzione prevista dal Contratto e dal Manuale del sistema di conservazione.

13. La presente nomina è condizionata, per oggetto e durata, al Contratto in corso di esecuzione e si intenderà revocata di diritto contestualmente alla cessazione del rapporto medesimo o alla risoluzione, per qualsiasi causa, dello stesso.

Il Titolare del Trattamento nulla più pretenderà rispetto a quanto previsto nel presente atto di nomina e considererà assolto l'adempimento da parte del Responsabile esterno del trattamento con l'applicazione delle procedure sopra indicate.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

POTENZA, lì 21/06/16

L'Utente Finale.....dr.ssa Brigida Serpillo.....
(Timbro e Firma o Firma Digitale)

Si allega copia del documento di identità del firmatario in corso di validità



ENTERPRISE CUSTOMER SERVICE

Il modello organizzativo del servizio gestito Enterprise

Enterprise *Customer Service*
Aruba

Documento riservato al cliente

Indice

01. Il Service Desk suddiviso su due livelli

- 1.1 Il Service Desk 1° Livello
- 1.2 Responsabilità del 1° livello
- 1.3 Il Service Desk 2° Livello

02. Processi Gestiti

03. Processo di Incident Management

04. Processo di Service Request Management

05. Processo di Event Management

06. Processo di Problem Management

07. Processo di Change Management

08. Ruoli e Responsabilità

09. Servizio di Assistenza

10. Canali di Assistenza

11. Riferimenti Extra

01. Il Service Desk suddiviso su due livelli

Service Desk - 1° Livello

Il Service Desk di 1° livello rappresenta il **punto di contatto del cliente con il servizio di Assistenza Enterprise**.

Il contattato può avvenire tramite **chiamata telefonica** oppure attraverso l'apertura di un **ticket al portale**: <https://itsm.aruba.it/dwp/app/>

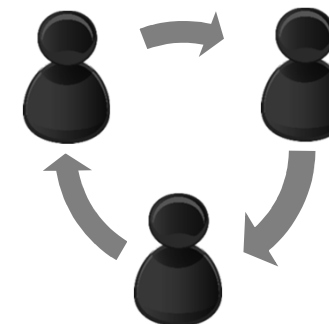
Su richiesta viene fornito anche un **indirizzo di posta** dedicato per aprire *Ticket* utilizzando la posta elettronica.



Service Desk - 2° Livello

Il Service Desk Enterprise è costituito da un **team di persone con competenze tecniche avanzate** in grado di risolvere le problematiche e le richieste più complesse.

Il 2° livello viene attivato attraverso il **processo di escalation**, che ha luogo nel momento in cui il 1° livello ne richiede il supporto.



01. Il Service Desk suddiviso su due livelli

1.1 Il Service Desk 1° Livello

Il primo livello dell'Assistenza Enterprise gestisce tutte le comunicazioni con il Cliente, per tutto il ciclo di vita del ticket sia esso di Assistenza oppure di Richiesta di Servizio.



Cliente > Service Desk

Una volta presa in carico la segnalazione, il Service Desk di 1° livello analizza la richiesta e cerca di risolverla con le competenze e gli strumenti in suo possesso.

Qualora non fosse in grado di individuare la soluzione, provvede all'inoltro al 2° livello tenendo monitorate le fasi successive, ed informando l'utente riguardo gli sviluppi del processo di risoluzione.



Service Desk > Cliente

In caso di segnalazione che proviene dal nostro sistema interno di monitoraggio, è compito del Service Desk aprire la segnalazione al cliente tramite il sistema di Trouble Ticketing e, nei casi più importanti, anche telefonicamente utilizzando i riferimenti forniti dal Cliente.

01. Il Service Desk suddiviso su due livelli

1.2 Responsabilità del 1° livello

Le principali responsabilità del Service Desk di 1° livello sono quindi le seguenti:

- ✓ Ricevere e classificare tutte le chiamate, o più in generale i contatti, da parte degli utenti;
- ✓ Dare supporto iniziale agli utenti e fare il primo tentativo per offrire una soluzione o un *workaround*;
- ✓ Inoltrare tutti gli incidenti che non possono essere risolti direttamente ai gruppi di secondo livello di supporto e monitorarne lo stato;
- ✓ Mantenere gli utenti informati dello stato delle loro richieste.
- ✓ Informare gli utenti di eventuali cambiamenti nei servizi IT;
- ✓ Fornire informazioni sulle necessità formative degli utenti dei Servizi IT rispetto ai servizi stessi;
- ✓ Produrre *reports* per il cliente e per il *management*;
- ✓ Confermare con gli utenti l'effettiva risoluzione degli incidenti.

01. Il Service Desk suddiviso su due livelli

1.3 Il Service Desk 2° Livello

Il 2° livello viene attivato attraverso il processo di *escalation* che ha luogo nel momento in cui il 1° livello ne richiede il supporto.



Compiti e responsabilità

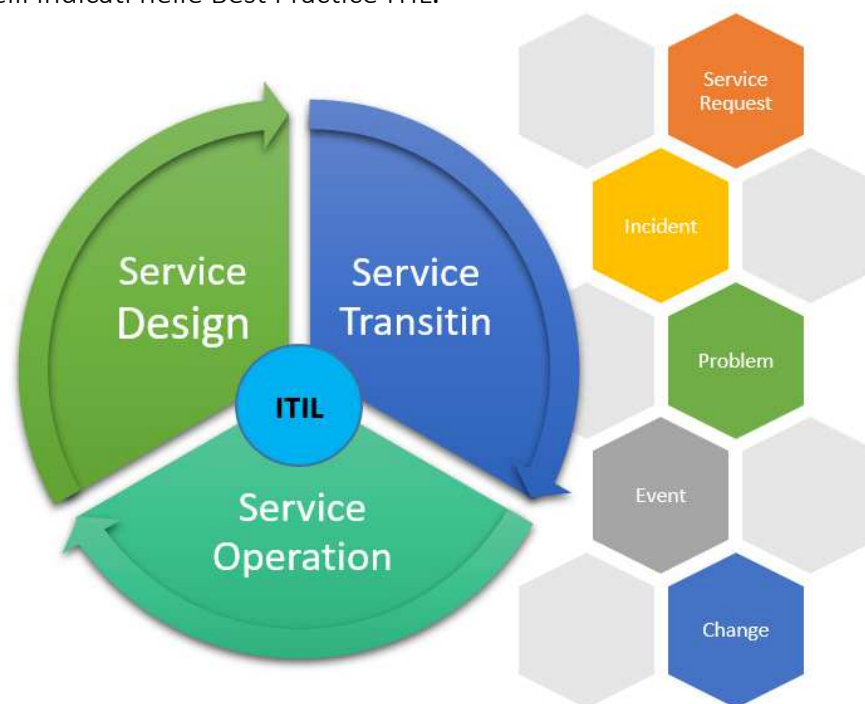
Il Service Desk di 2° livello può prendere direttamente in carico la gestione di anomalie e disservizi evidenziati dagli strumenti di monitoraggio, effettuando tutti gli interventi risolutivi o preventivi che si rendano necessari per l'ottimale funzionamento dei servizi forniti. Nei casi in cui si rilevino impatti al servizio, viene allertato il 1° livello che provvede ad informare il Cliente aprendo sul sistema il relativo Incident.

È compito di questo team gestire l'*escalation* verso i 3° livelli, rappresentati principalmente dai fornitori delle apparecchiature HW e SW oggetto del servizio.

02. Processi Gestiti

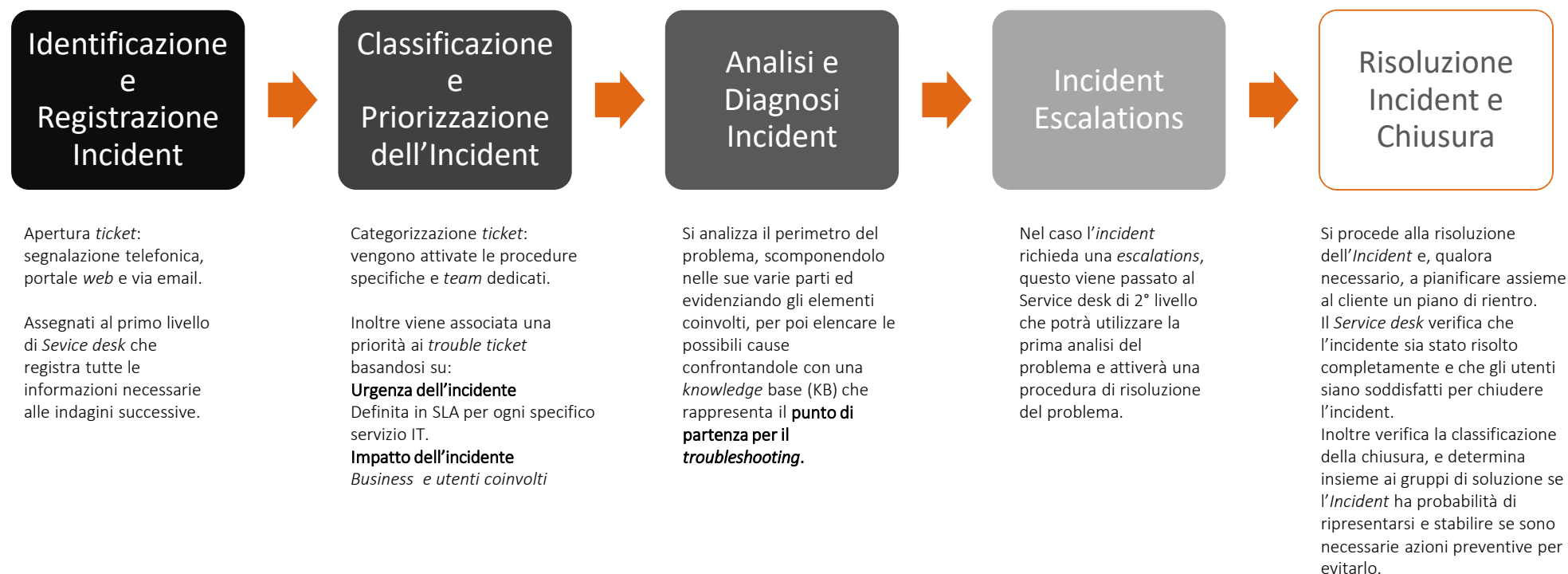
I processi che governano il funzionamento del Service Desk sono quelli indicati nelle Best Practice ITIL.

In alcuni di questi processi il Service Desk gioca un ruolo primario, in altri il contributo è legato al controllo del flusso delle informazioni, al monitoraggio degli SLA ed all'attivazione, se necessario, del processo di escalation.



03. Processo di Incident Management

Il servizio di *Incident management* ha l'obiettivo di gestire tutte le anomalie di componenti in responsabilità Aruba che si possono presentare durante la gestione del servizio.



03. Processo di Incident Management

Classificazione del Ticket

URGENZA IMPATTO	Critical	High	Medium	Low
Extensive/Widespread	Critical	Critical	High	Low
Significant/Large	Critical	High	Medium	Low
Moderate/Limited	High	High	Medium	Low
Minor/Localized	High	Medium	Medium	Low

CRITICA: il servizio è indisponibile e coinvolge uno o più dei processi critici dell'organizzazione;

ALTA: le prestazioni del servizio sono fortemente degradate e/o le funzionalità a supporto di processi critici sono parzialmente indisponibili;

MEDIA: si è verificato un degrado moderato delle prestazioni del servizio che non provoca significative ricadute sui processi aziendali;

BASSA: si sono presentate anomalie circoscritte su funzionalità di minore rilievo che tuttavia meritano una gestione proattiva.

04. Processo di Request Management

Le Requests possono essere di vario tipo

Esempi di Requests Trust

- Richiedi un Servizio
- Emissione, Attivazione, Modifica del Servizio

Esempio di Requests DC

- Richiedi intervento Smart Hands
- Richiedi un Servizio
- Richiedi supporto logistico
- Richiedi Riavvio apparato
- Richiedi Accesso al DC
- Richiedi intervento Remote Hands
- Richiedi Ispezione Visiva

Le *Requests* sono richieste di assistenza generiche, che possono essere create dal Cliente o dal Service Desk per conto del Cliente.

Nel primo caso l'utente invia una richiesta tramite un portale *web*, e il *software* applicativo instrada automaticamente la richiesta attraverso i processi opportuni per la gestione della richiesta.

Nel secondo caso, il Service Desk crea un *ticket* di servizio che serve per instradare la richiesta di assistenza.

Questo sistema consente al Cliente di tenere traccia dello stato delle sue richieste di assistenza.

05. Processo di Event Management

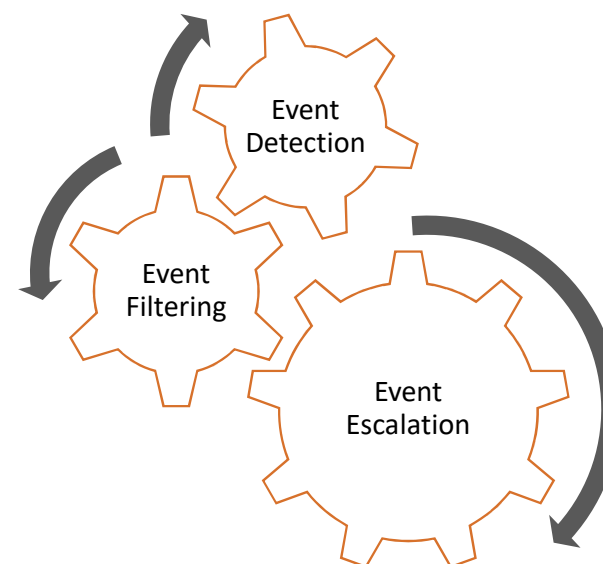
Un evento può essere definito come qualsiasi cambiamento di stato che è significativo per la gestione di un servizio.

Lo scopo del processo di *Event Management* è quello di gestire gli eventi attraverso il loro ciclo di vita, che comprende la rilevazione degli eventi (monitoraggio), il determinarne la significatività e l'assicurarsi che sia adottata la corretta risposta o azione di controllo.

Event Detection: una volta generata la notifica di un evento, viene rilevata dal tool di event management

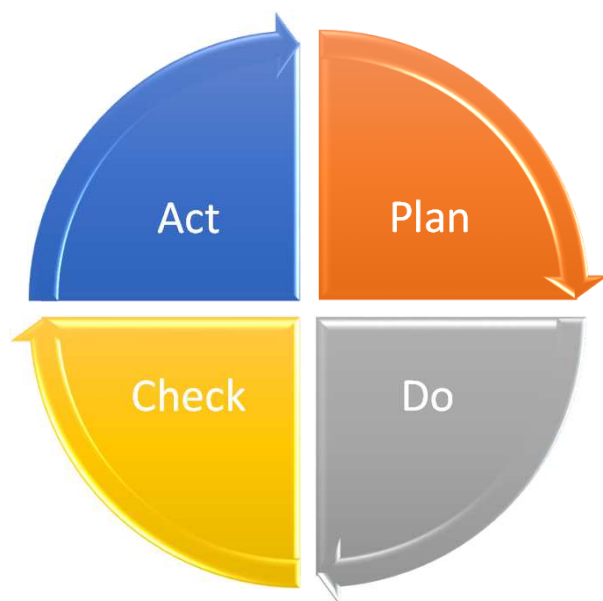
Event Filtering: il filtro serve a stabilire se l'evento va processato o ignorato (informational). Se ignorato, l'evento sarà comunque registrato in un file di log, ma non seguirà alcuna azione. In questa fase viene effettuata una prima correlazione, determinando se l'evento è informativo (*informational*), un avvertimento (*warning*) o un'eccezione (*exception*).

Event Escalation: l'evento genera quindi un'*escalation* gestita dal Service Desk che può scaturire nell'apertura di un *Incident* e nell'immediata comunicazione proattiva della situazione verso il cliente.



06. Processo di Problem Management

Obiettivo del *Problem Management* è individuare la causa alla base degli Incidenti e trovare una soluzione.



Il *Service Desk* può scoprire o sospettare la causa di uno o più incidenti e quindi aprire un *Problem Record* in modo che la causa possa essere risolta.

La segnalazione di un Incidente può arrivare dal gruppo tecnico di supporto, dal cliente o da un fornitore.

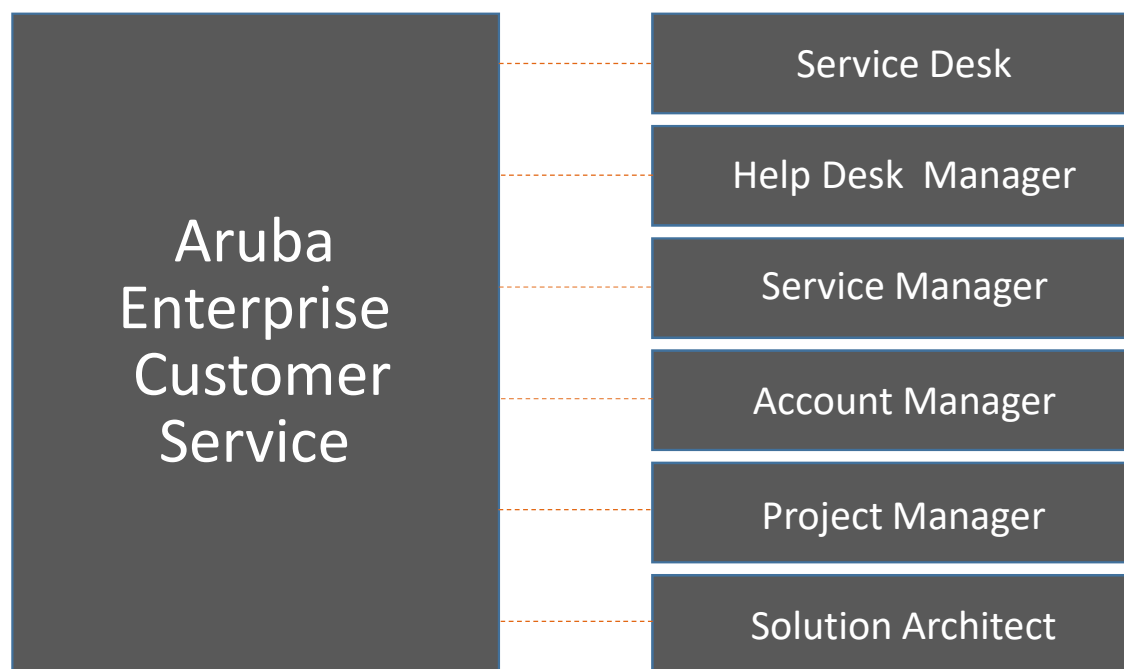
07. Processo di Change Management

Nel caso si renda necessario rispondere ai mutevoli requisiti di *business* del cliente, massimizzando il valore e riducendo al minimo gli incidenti, si genera una *Change Request* il cui **obiettivo è assicurare che i cambiamenti siano:**

- ✓ Registrati
- ✓ Valutati
- ✓ Autorizzati
- ✓ Messi in priorità
- ✓ Testati Implementati
- ✓ Documentati e revisionati in modo controllato.



08. Ruoli e Responsabilità



09. Servizio di Assistenza

Il servizio e relativi canali di Assistenza sono utilizzabili h24 x 365gg.

Il contatto telefonico è il canale più efficace per le comunicazioni di eventi critici, in particolar modo al di fuori dell'orario di lavoro. Gli orari di lavorazione, dettagliati per processo, sono riassunti nella tabella sotto riportata.

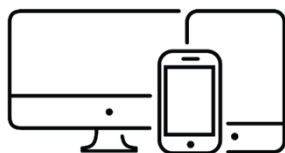
Servizio	Giorno Lavorativo 8:30 – 18:00	Giorno Lavorativo 18:00 – 08:30	Giorno Festivo e Prefestivo H24
INCIDENT MANAGEMENT	✓	✓	✓
EVENT MANGEMENT	✓	✓	✓
SERVICE REQUEST: REQUEST FULLFILMENT; INFORMATION REQUEST	✓		
BACKUP & RESTORE REQUEST	✓	✓ ¹	✓ ¹
ACCESS REQUEST	✓	✓	✓
REMOTE HANDS	✓	✓	✓
SMART HANDS	✓	✓	✓
PROBLEM MANAGEMENT	✓		
CHANGE MANAGEMENT	✓	✓ ²	✓ ²

NOTE:

¹ Solo richieste di *restore* critici necessari per superare situazioni bloccanti

² Solo per *Change* urgenti necessari per superare situazioni bloccanti

10. Canali di Assistenza



| Contattaci via web

Sito di assistenza: <https://itsm.aruba.it/dwp/app/>



| Contattaci telefonicamente

Numero dedicato: +39.0575.050032



| Contattaci per email

Email: servicedesk.enterprise@staff.aruba.it

11. Riferimenti Extra

Nel caso in cui si presentassero delle urgenze e i tempi di presa in carico non venissero rispettati, è possibile contattare i responsabili del Customer Care:

Account Manager
Salvatore Ambrosio salvatore.ambrosio@staff.aruba.it +39 3298632540

Team Customer Enrollment – ECS_Enroll@staff.aruba.it



A vostra disposizione

Enterprise Customer Service



MANUALE UTENTE

REMEDY Digital Workplace Platform (DWP)

Enterprise Customer Service

Indice

1. REMEDY - Piattaforma *Digital Workplace*

- 1.1 Digital Workplace (DWP)
- 1.2 Accesso a DWP e impostazioni profilo utente

2. Creazione e invio richieste

- 2.1 Selezione richiesta e opzioni di apertura
- 2.2 «Richiedi nuova utenza nominale»: richiesta riservata ai Referenti
- 2.3 «Segnala un disservizio», «Richiedi un servizio», «Emissione, attivazione, modifica del servizio» – Compilazione campi
- 2.4 Apertura Richieste via Email

3. Visualizzazione e Modifica Richieste inviate

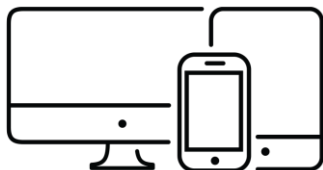
- 3.1 Visualizzazione richieste Inviato
- 3.2 Modifica richieste inviate

4. Presa incarico e invio notifiche dell'Assistenza Enterprise

5. Richiesta completata e riapertura richiesta

6. Contatti

1. REMEDY - Piattaforma Digital Workplace



Piattaforma Web a **disposizione dei soli clienti Aruba Enterprise**



Comunicazione diretta con gli operatori che si occuperanno delle vostre richieste



Remedy è il sistema a cui si accede tramite DWP

1. REMEDY - Piattaforma Digital Workplace

1.1 Digital Workplace (DWP)

Tramite **DIGITAL WORKPLACE** è possibile inviare agli operatori **Aruba Enterprise**:

Richieste Servizi Generici/Informazioni



Richiesta Nuova Utenza Nominale: dedicato ai Referenti

Consente di ottenere un'utenza nominale con la quale accedere al portale DWP e inviare richieste.



Emissione, Attivazione, Modifica di un Servizio.

Consente di inoltrare richieste per Emissione, Attivazione e Modifica di un Servizio, direttamente al Reparto competente.



Segnala un disservizio

Esempi:

- Segnalazione di malfunzionamenti o interruzioni del servizio.



Richiedi un servizio

Esempi:

- richieste informative;
- modifiche standard nei servizi (aggiungere un indirizzo mail);
- richiedere credenziali per l'accesso ad un servizio.

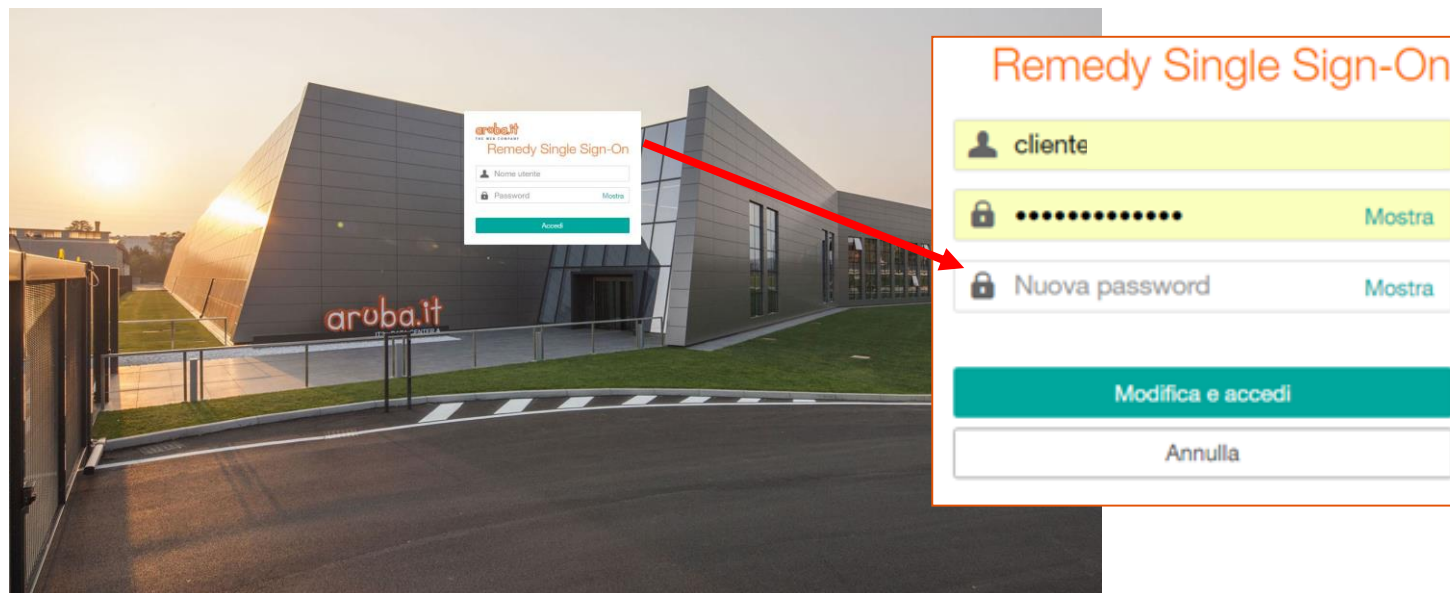
1. REMEDY - Piattaforma Digital Workplace

1.2 Accesso a DWP e impostazioni profilo utente

Ogni Utente disporrà di un'**utenza nominale** specifica per accedere alla piattaforma e richiedere assistenza.

I clienti Aruba Enterprise che hanno ottenuto via mail le Login ID devono:

1. effettuare l'accesso al link <https://itsm.aruba.it/dwp/app/>;
2. modificare obbligatoriamente la password al primo accesso.



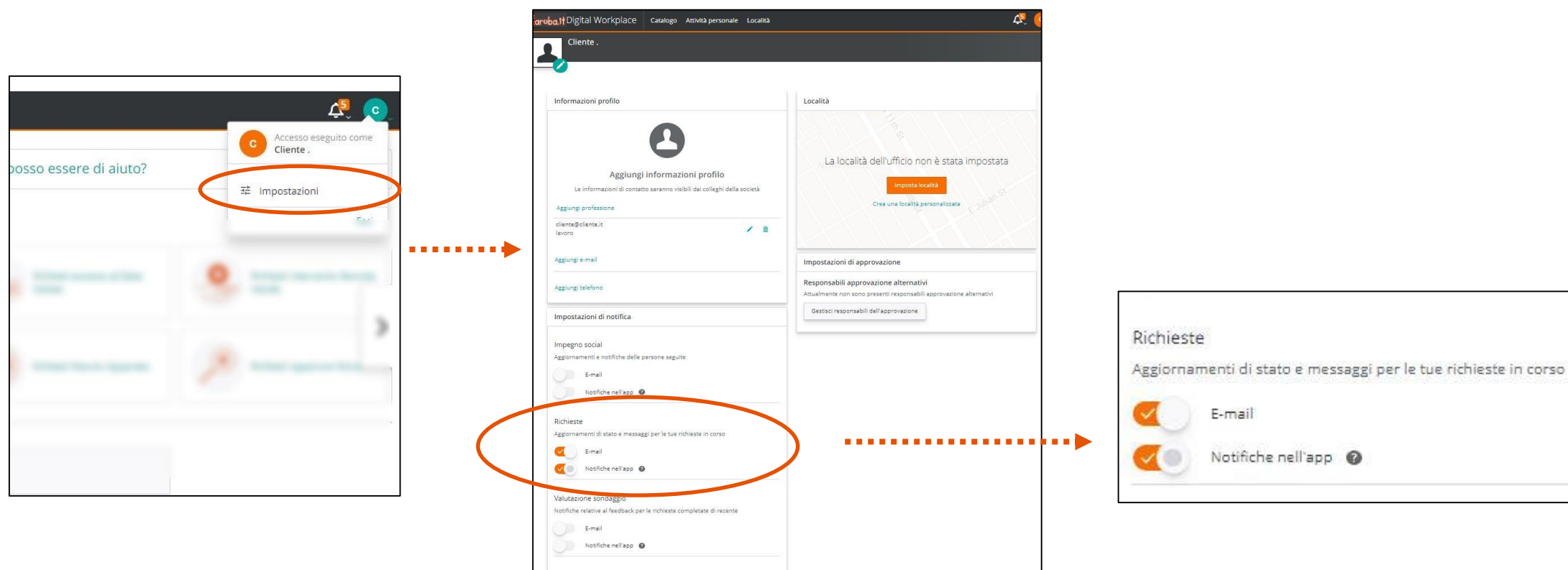
1. REMEDY - Piattaforma Digital Workplace

1.2 Accesso a DWP e impostazioni profilo utente

Una volta effettuato l'accesso, nella *Home Page* cliccare in alto a destra per **modificare le impostazioni del profilo Utente**.

Nella pagina «**Informazioni profilo**», è possibile aggiungere o modificare le informazioni relative all'utenza.

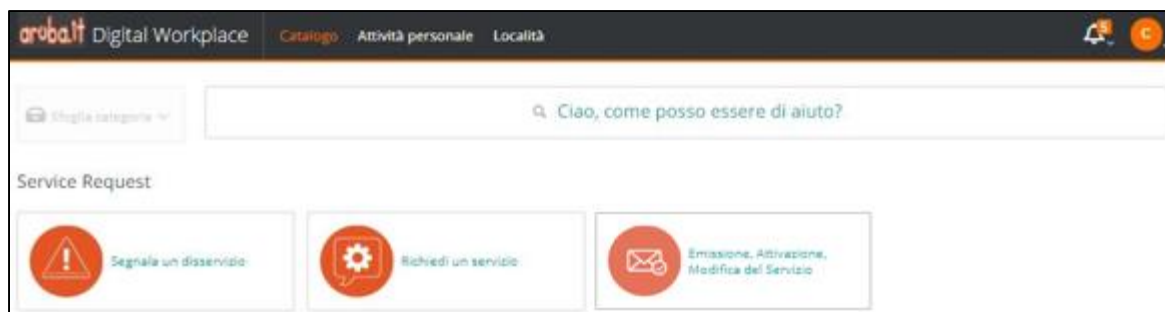
NB. E' necessario spuntare le voci nella sezione «**Impostazioni di notifica**» >> «**Richieste**» per ricevere le notifiche relative alle richieste in corso.



2. Creazione e invio richiesta

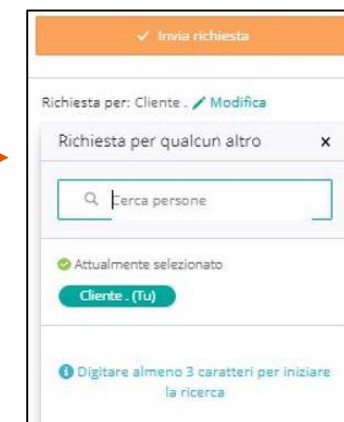
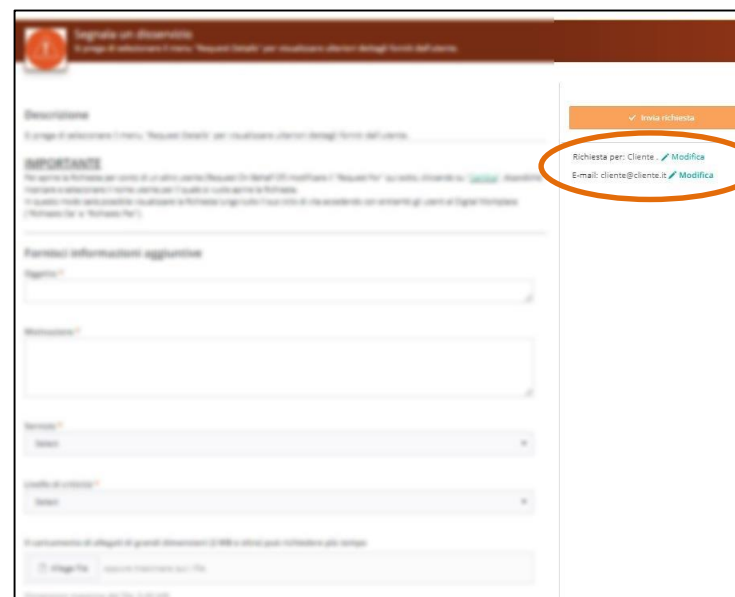
2.1 Selezione richiesta e opzioni di apertura

Per aprire una nuova richiesta, cliccare sull'icona corrispondente alla tipologia necessaria.



La richiesta può essere inviata:

- dall'utente che ha effettuato l'accesso;
- per conto di un altro utente, ricorrendo al **«Modifica»** utente. Tramite questa funzionalità, entrambi gli utenti potranno visualizzare e modificare la richiesta.



2. Creazione e invio richieste

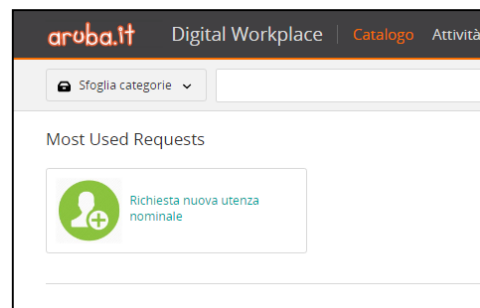
2.2 «Richiedi nuova utenza nominale»: richiesta riservata ai Referenti

I referenti potranno richiedere nuove utenze nominali per ulteriori colleghi.

La richiesta, per essere completata, deve indicare almeno:

- 1) **Nome** del nuovo utente da creare;
- 2) **Cognome** del nuovo utente da creare;
- 3) **Indirizzo mail** della nuova utenza da creare.

A seguito dell'invio della richiesta **verrà inviata un'email di conferma all'indirizzo email del Richiedente.**



Richiedi nuova utenza nominale
 Creare questa richiesta per ottenere un'utenza nominale per accedere al portale self-service Digital Workplace.

Descrizione
 Creare questa richiesta per ottenere un'utenza nominale per accedere al portale self-service Digital Workplace.

Fornisci informazioni aggiuntive
 Nome *
 Inserire il nome dell'utenza nominale da creare

Cognome *
 Inserire il cognome dell'utenza nominale da creare

Indirizzo e-mail *
 Inserire l'indirizzo e-mail dell'utenza nominale da creare

Numero di telefono
 Inserire il numero di telefono dell'utenza nominale da creare.

Ulteriori dettagli

Il caricamento di allegati di grandi dimensioni (2 MB e oltre) può richiedere più tempo
 oppure trascinare qui i file
 Dimensioni massime del file: 5.00 MB
 Numero massimo di file: 3

Richiesta per: Cliente. [Modifica](#)
 E-mail: cliente@cliente.it [Modifica](#)

2. Creazione e invio richieste

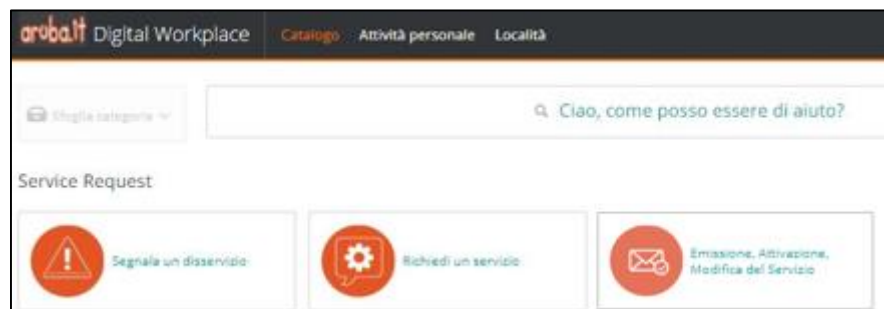
2.3 «Segnala un disservizio», «Richiedi un servizio», «Emissione, Attivazione, Modifica del Servizio» – Compilazione dei campi

I **Campi Obbligatori** sono indicati dall'asterisco arancione:

1. Oggetto;
2. Motivazione;
3. Servizio;
4. Livello di Criticità (per disservizio).

E' possibile allegare massimo 3 file o un file zip.

Una volta compilato il Form in tutte le sue parti, cliccare su **«Invia richiesta»**. L'utente riceverà una notifica email con l'identificativo della richiesta.



Descrizione

Si prega di selezionare il menu "Request Details" per visualizzare ulteriori dettagli forniti dall'utente.

IMPORTANTE
Per aprire la Richiesta per conto di un altro utente (Request On Behalf Of) modificare il "Request For" qui sotto, cliccando su "Cambia", dopodiché ricercare e selezionare il nome utente per il quale si vuole aprire la Richiesta.
In questo modo sarà possibile visualizzare la Richiesta lungo tutto il suo ciclo di vita accedendo con entrambi gli utenti al Digital Workplace ("Richiesto Da" e "Richiesto Per").

Fornisci informazioni aggiuntive

Oggetto *

Titolo sintetico del problema per cui si chiede assistenza

Motivazione *

Descrizione del problema o della richiesta per cui si chiede un intervento

Servizio *

Select Selezionare il servizio interessato

Livello di criticità *

Select Selezionare il livello di criticità della richiesta

Il caricamento di allegati di grandi dimensioni (2 MB e oltre) può richiedere più tempo

Allega file oppure trascinare qui i file

Dimensioni massime del file: 5.00 MB
Numero massimo di file: 3

Invia richiesta

Richiesta per: Cliente. Modifica

2. Creazione e invio richiesta assistenza

2.4 Apertura Richieste via Email

Se l'utente è impossibilitato ad aprire una richiesta a sistema, può procedere con l'invio di una mail all'indirizzo: servicedesk.enterprise@staff.aruba.it, che andrà a generare un ticket sulla piattaforma.

ATTENZIONE ALLA FORMA!!!

- E' necessario scrivere nell'oggetto *Trust Services*;
- Non è possibile scrivere alcun indirizzo in Copia (né Cc, né Ccn);
- Nell'oggetto NON inserire identificativi di ticket (Incident o WorkOrder, per es. INC001, WO001, ecc) e/o caratteri che contraddistinguono una mail di risposta (R: o Re: o I:);
- Per aprire una richiesta di servizio, inserire nell'oggetto «WO:» (come riportato nell'esempio), altrimenti il sistema genererà in automatico un INCIDENT.

File | Messaggio | Inserisci | Opzioni | Formato testo | Revisione | Che cosa si desidera

Taglia | Copia | Copia formato | Rubrica | Controlla nomi | Allega file

Appunti | Testo base | Nomi

A... | servicedesk.enterprise@staff.aruba.it

Cc... |

Ccn... |

Oggetto | WO:

File | Messaggio | Inserisci | Opzioni | Formato testo | Revisione | Che cosa si desidera

Taglia | Copia | Copia formato | Rubrica | Controlla nomi | Allega file

Appunti | Testo base | Nomi

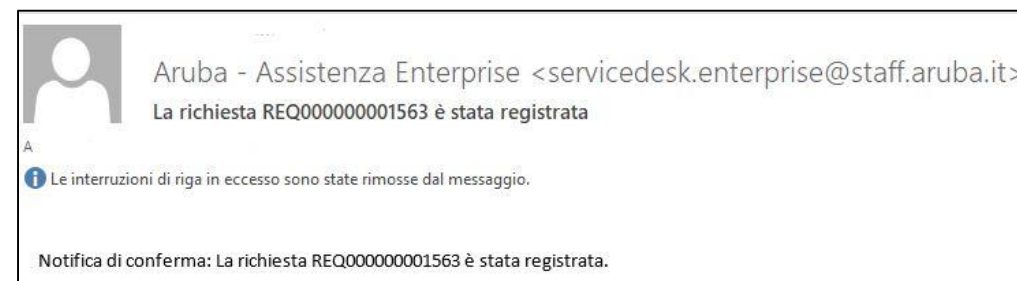
A... | servicedesk.enterprise@staff.aruba.it

Cc... | mario.rossi@staff.aruba.it

Ccn... | mario.rossi@staff.aruba.it

Oggetto | Re:

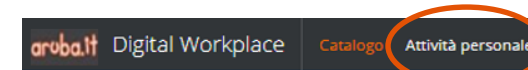
L'utente riceverà una mail di notifica dai nostri sistemi. →



3. Visualizzazione e Modifica Richieste inviate

3.1 Visualizzazione Richieste Inviare

Per visualizzare tutte le richieste inviate, cliccare su «**Attività personale**» nel menu principale dalla Home Page.



La pagina «**Attività personale**» è suddivisa in due sezioni:

- **Eventi Attivi:** richieste in stato *Iniziato*, *In Corso*, *In Attesa*.
- **Eventi Passati:** richieste in stato *Approvato*, *Rifiutato*, *Completato/Risolto*, *Chiuso*, *Annullato*, *Non Riuscito*.

Visualizza *Eventi Attivi* come RIQUADRI

Eventi attivi (3)

Richiesta di Servizio Data Center Iniziata Per: Test Cliente ID richiesta: REQ000000002215 Annula richiesta Dettagli	Segnalazione Disservizio Data Center Messaggio da Aruba Operator Per: Test Cliente ID richiesta: REQ000000002217 Annula richiesta Dettagli	Disservizio PEC Messaggio da Aruba Operator Per: Test Cliente ID richiesta: REQ000000002220 Annula richiesta Dettagli
--	--	---

Eventi passati (5)

Segnalazione Disservizio Chiusa	Per: Test Cliente	ID richiesta: REQ000000002212	Data: 4 apr 2019
Disservizio PEC Annullata	Per: Test Cliente	ID richiesta: REQ000000002213	Data: 4 apr 2019
Richiesta di servizio PEC Annullata	Per: Test Cliente	ID richiesta: REQ000000002214	Data: 4 apr 2019
Richiesta di Servizio PEC Annullata	Per: Test Cliente	ID richiesta: REQ000000002216	Data: 4 apr 2019
Segnalazione Disservizio PEC Chiusa	Per: Test Cliente	ID richiesta: REQ000000002218	Data: 4 apr 2019

Visualizza *Eventi Attivi* come ELENCO

Eventi attivi (3)

Richiesta di Servizio Data Center Iniziata	Per: Test Cliente ID richiesta: REQ000000002215	Annula richiesta Dettagli
Segnalazione Disservizio Data Center Messaggio da Aruba Operator	Per: Test Cliente ID richiesta: REQ000000002217	Annula richiesta Dettagli
Disservizio PEC Messaggio da Aruba Operator	Per: Test Cliente ID richiesta: REQ000000002220	Annula richiesta Dettagli

< Precedente Avanti >

Eventi passati (5)

Segnalazione Disservizio Chiusa	Per: Test Cliente	ID richiesta: REQ000000002212	Data: 4 apr 2019
Disservizio PEC Annullata	Per: Test Cliente	ID richiesta: REQ000000002213	Data: 4 apr 2019
Richiesta di servizio PEC Annullata	Per: Test Cliente	ID richiesta: REQ000000002214	Data: 4 apr 2019
Richiesta di Servizio PEC Annullata	Per: Test Cliente	ID richiesta: REQ000000002216	Data: 4 apr 2019
Segnalazione Disservizio PEC Chiusa	Per: Test Cliente	ID richiesta: REQ000000002218	Data: 4 apr 2019

3. Visualizzazione e Modifica Richieste inviate

3.2 Modifica Richieste Inviare

Cliccando su una richiesta, si aprirà la finestra con tutti i dettagli relativi:

- le **principali informazioni** (oggetto, priorità, identificativo richiesta);
- lo **stato della richiesta** (si aggiorna in base alle lavorazioni degli operatori);
- la **descrizione**;
- il **servizio impattato**;
- i commenti **degli operatori** del Service Desk.



ATTENZIONE AI SIMBOLI!

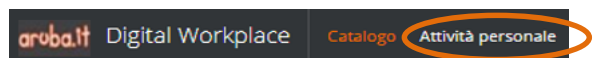
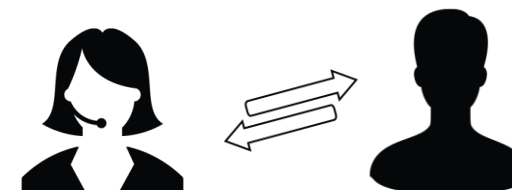
Questo simbolo indica che la richiesta è stata creata da operatori Aruba Enterprise su segnalazione telefonica-mail da parte del cliente.

Stato In corso	ID richiesta REQ000000002220	Richiesta per TC Test Cliente cliente@cliente.it	Per annullare la richiesta cliccare qui Per avanzare una nuova richiesta cliccare qui	>> Annulla richiesta >> Richiedi ancora									
Dettagli <table border="0"> <tr> <td>Priorità richiesta ALTA</td> <td>Inviato 19 mar 2019 alle 08:52</td> <td>Ultimo aggiornamento 4 apr 2019 alle 20:50</td> </tr> <tr> <td>Richiesto per telefono ###</td> <td>Richiesto per società Cliente</td> <td>Oggetto Disservizio PEC</td> </tr> <tr> <td>Descrizione Si segnala disservizio.</td> <td>Servizio PEC - Casella Pec</td> <td>Livello di criticità Alto</td> </tr> </table>					Priorità richiesta ALTA	Inviato 19 mar 2019 alle 08:52	Ultimo aggiornamento 4 apr 2019 alle 20:50	Richiesto per telefono ###	Richiesto per società Cliente	Oggetto Disservizio PEC	Descrizione Si segnala disservizio.	Servizio PEC - Casella Pec	Livello di criticità Alto
Priorità richiesta ALTA	Inviato 19 mar 2019 alle 08:52	Ultimo aggiornamento 4 apr 2019 alle 20:50											
Richiesto per telefono ###	Richiesto per società Cliente	Oggetto Disservizio PEC											
Descrizione Si segnala disservizio.	Servizio PEC - Casella Pec	Livello di criticità Alto											
Commenti (1) Aggiungi commento AO Aruba Operator 2 mesi fa Buongiorno, la segnalazione è stata presa in carico.													

4. Presa in carico e invio notifiche dell'Assistenza Enterprise

L'operatore dell'assistenza Enterprise prende in carico la richiesta inviata dall'utente ed avvia il processo di risoluzione.

Il Cliente riceve sempre una email di notifica dall'Assistenza Enterprise, con ID e titolo della richiesta a cui esse si riferiscono.



Dalla pagina **Attività Personale**, per ciascuna richiesta l'utente potrà visualizzare le note inviate dal Service Desk Enterprise.

Tramite Remedy, l'operatore Aruba invierà i commenti per specificare le operazioni svolte o per richiedere l'intervento diretto dell'utente. I commenti sono visibili nei dettagli della richiesta a cui si riferiscono.

Stato

In corso

ID richiesta

REQ000000002220

Richiesta per

TC

Test Cliente

cliente@cliente.it

Annulla richiesta

Richiedi ancora

Dettagli

Priorità richiesta ALTA	Inviato 19 mar 2019 alle 08:52	Ultimo aggiornamento 4 apr 2019 alle 20:50
Richiesto per telefono ###	Richiesto per società Cliente	Oggetto Disservizio PEC
Descrizione Si segnala disservizio.	Servizio PEC - Casella Pec	Livello di criticità Alto

Commenti (1)

Aggiungi commento

AO

Aruba Operator

Buongiorno,

la segnalazione è stata presa in carico.

2 mesi fa

<<

Campo a disposizione dell'utente per interagire con l'Assistenza

<<

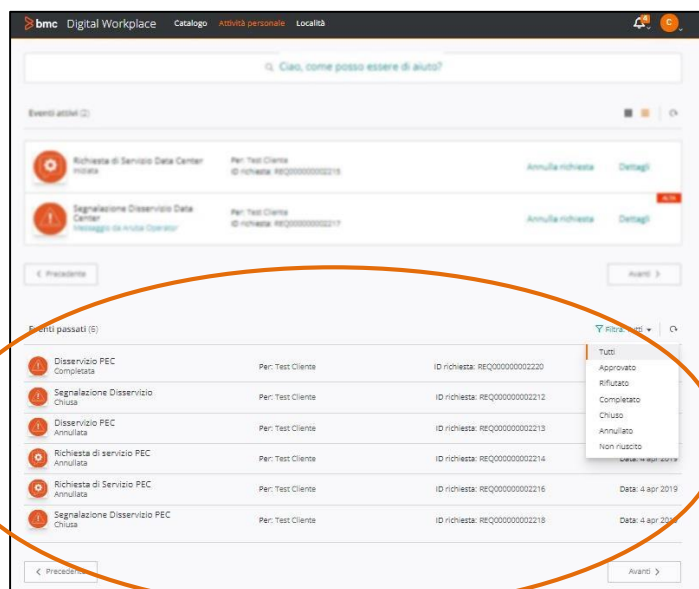
Messaggio da parte dell'Assistenza Enterprise

5. Richiesta completata e riapertura richiesta

Quando una richiesta viene considerata **COMPLETATA/RISOLTA** dal Service Desk, il **Cliente** riceve una comunicazione di avvenuta risoluzione sia su Remedy che tramite email nella sua casella di posta.

Inoltre, in automatico, la richiesta nel DWP:

- cambia lo stato passando da **In Corso** a **Completato/Risolto**;
- **viene archiviata** in automatico nella sezione «Eventi passati» della finestra «Attività personale».



			Filtra: Tutti
	Segnalazione Disservizio Chiusa	Per: Test Cliente	ID richiesta: REQ000000002212
	Disservizio PEC Annullata	Per: Test Cliente	ID richiesta: REQ000000002213
	Richiesta di servizio PEC Annullata	Per: Test Cliente	ID richiesta: REQ000000002214
	Richiesta di Servizio PEC Annullata	Per: Test Cliente	ID richiesta: REQ000000002216



FILTRO PER STATO: le richieste archiviate possono essere filtrate per stato.

5. Richiesta completata e riapertura richiesta

L'utente, se necessario, può **RIAPRIRE** la richiesta **RISOLTA/COMPLETATA** entro **10 giorni dalla risoluzione**.

N.B. Una richiesta «chiusa» NON può essere riaperta, è quindi necessario procedere con l'invio di una nuova segnalazione.

The image shows two screenshots of the Aruba.it Enterprise Customer Service interface. The left screenshot shows a request in the 'Completata' (Completed) state. A callout box points to the 'Riapri richiesta' button, stating: 'Cliccando su «Riapri richiesta» si aprirà un POP UP dove andrà indicato il motivo della riapertura.' The right screenshot shows the same request with a modal titled 'Riapri richiesta di servizio' open. The modal contains a text input field labeled 'Indica il motivo per la riapertura della richiesta.' and buttons for 'Chiudi' and 'Riapri richiesta'.

Cliccando su «Riapri richiesta» si aprirà un POP UP dove andrà indicato il motivo della riapertura.

Cliccando «Riapri» la richiesta verrà inviata all'operatore. Una volta riaperta la richiesta, lo stato si modificherà da «completato» a «in corso»

6. Contatti

- Per aprire segnalazioni via mail: servicedesk.enterprise@staff.aruba.it
- Per contattare telefonicamente il Service Desk Enterprise: [+39 0575 050032](tel:+390575050032)



A vostra disposizione

Enterprise Customer Service

Collaborating on Requests

Descrizione della funzionalità e guida al suo utilizzo

SOMMARIO

1.	COLLABORATING ON REQUESTS.....	2
2.	PERMESSI E VISIBILITA' DEI COLLABORATORI	3
3.	OPZIONI PER AGGIUNGERE COLLABORATORI ALLA REQUEST	4
3.1	IMPOSTARE AUTOMATICAMENTE UNA LISTA DI COLLABORATORI PREDEFINITA	4
3.2	AGGIUNGERE MANUALMENTE I COLLABORATORI ALLA REQUEST	5

1. COLLABORATING ON REQUESTS

E' possibile abilitare per tutti gli utenti la **funzionalità di collaborazione**, permettendo così l'aggiunta di collaboratori alle richieste aperte tramite il portale Digital Workplace (DWP).

L'utente che sottomette una Request può aggiungere altri utenti in qualità di collaboratori della richiesta, in modo tale da permettere loro la visualizzazione e gestione della stessa.

La funzionalità di collaborazione è utile nel caso in cui l'utente crea una richiesta che impatta altri utenti, oppure quando l'utente che apre la richiesta non è disponibile per rispondere al supporto tecnico o per dare un feedback alla risoluzione della Request.

2. PERMESSI E VISIBILITA' DEI COLLABORATORI

La seguente tabella descrive le azioni disponibili per il Richiedente della richiesta, l'utente *On Behalf Of* e Collaboratore durante tutte le fasi del ciclo di vita della Request.

Fasi della Request	Azioni disponibili			Note
	Richiedente ¹	Utente OBO ²	Collaboratore ³	
Apertura di una Request	- Richiedi subito - Aggiungi utente OBO	<i>Not applicable</i>	<i>Not applicable</i>	I Collaboratori non possono essere aggiunti manualmente durante la creazione di una richiesta.
Request in progress	- Cancella la richiesta - Aggiungi un commento - Gestisci i Collaboratori - Richiedi ancora	- Cancella la richiesta - Aggiungi un commento - Gestisci i Collaboratori - Richiedi ancora	- Cancella la richiesta - Aggiungi un commento - Visualizza la lista di Collaboratori (sola lettura)	L'utente OBO non può essere aggiunto (anche) come Collaboratore della Request.
La Request è Completata o Cancellata	- Richiedi ancora - Gestisci Collaboratori	- Richiedi ancora - Gestisci Collaboratori	Visualizza la lista di Collaboratori (sola lettura)	<i>Not applicable</i>

¹ Richiedente: utente che ha effettuato l'accesso sul DWP e che invia la richiesta.

² Utente OBO: utente *On Behalf of*, ovvero l'utente per conto del quale è stata aperta la richiesta.

³ Collaboratore: utente che può "collaborare" sulle richieste inviate dal Richiedente.

3. OPZIONI PER AGGIUNGERE COLLABORATORI ALLA REQUEST

Ci sono due opzioni per aggiungere Collaboratori alle Requests:

- Impostare automaticamente una lista di Collaboratori predefinita per tutte le future Requests
- Aggiungere manualmente i Collaboratori alla Request

3.1 IMPOSTARE AUTOMATICAMENTE UNA LISTA DI COLLABORATORI PREDEFINITA

Tutte le nuove Requests sono automaticamente condivise con il gruppo predefinito di Collaboratori se il richiedente ha aggiunto gli utenti nel *default group*, oltre ad aver abilitato la condivisione automatica delle Requests con il suddetto gruppo.

L'utente può configurare le impostazioni di Collaboratore accedendo alle Impostazioni del profilo personale (Figura 1):

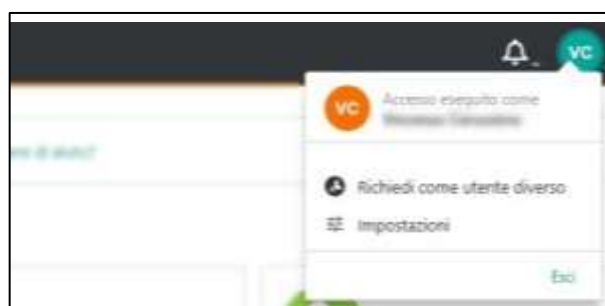


Figura 1

Cliccare su **Aggiungi persone**, poi aggiungere gli utenti al gruppo di Collaboratori (Figura 2):



Figura 2

Per rimuovere utenti dal gruppo, selezionare un utente dalla lista **Attualmente selezionato**, dopodiché cliccare su **Elimina** (Figura 3):



Figura 3

Per modificare il gruppo, cliccare sull'icona della matita e aggiungere o rimuovere utenti; per eliminare il gruppo cliccare sull'icona del cestino e confermare.

Per abilitare la condivisione di tutte le Requests con il gruppo di Collaboratori appena configurato, attivare il selettore **Auto-share** (Figura 4):

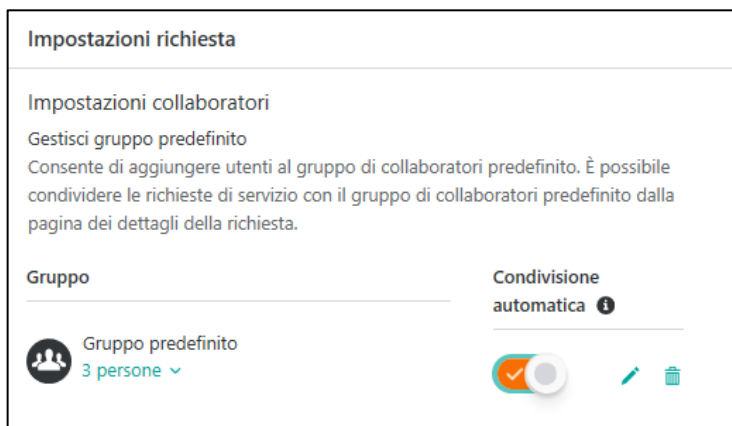


Figura 4

3.2 AGGIUNGERE MANUALMENTE I COLLABORATORI ALLA REQUEST

In qualità di richiedente della Request, è possibile aggiungere manualmente fino a 20 Collaboratori ad una Request già aperta, come mostrato in Figura 1:

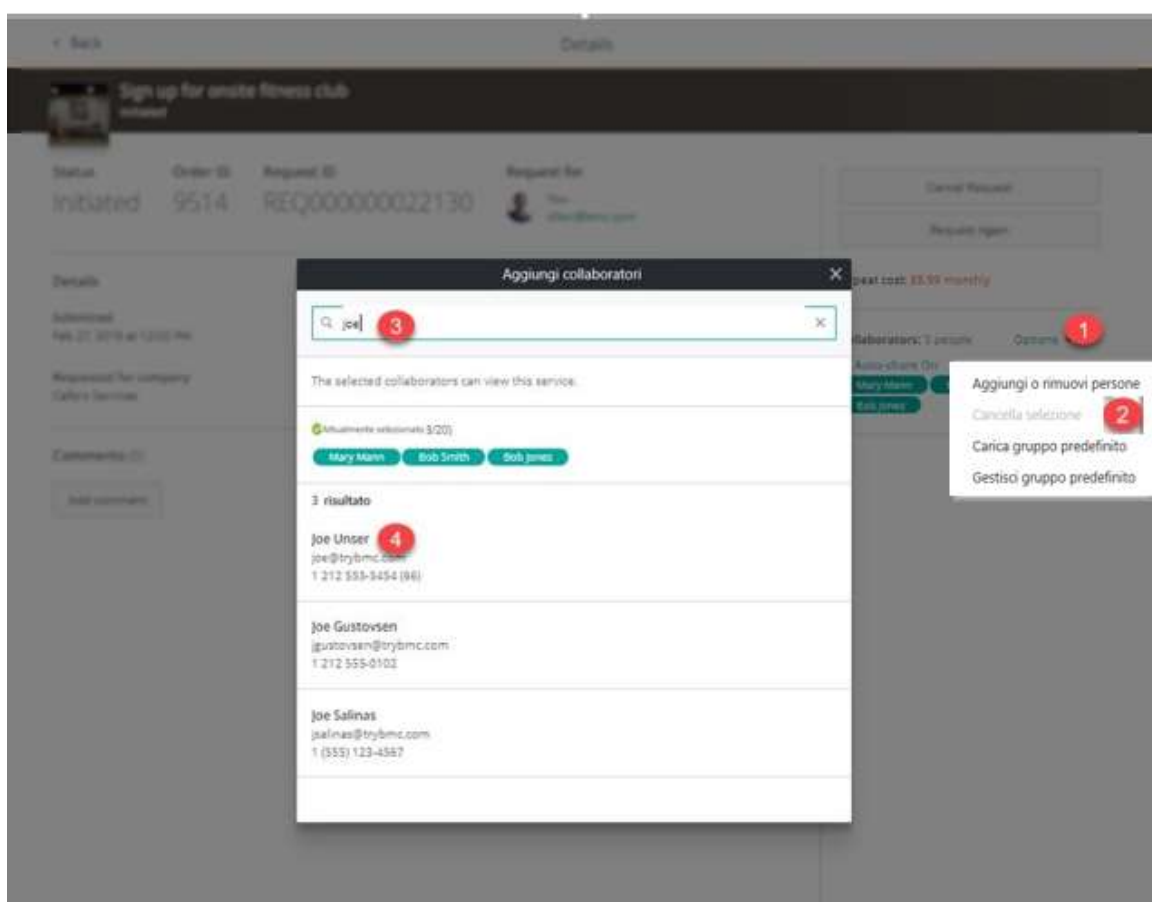


Figura 1

Sempre a partire da una Request già creata, è anche possibile caricare la lista di Collaboratori predefinita, come mostrato in Figura 2:

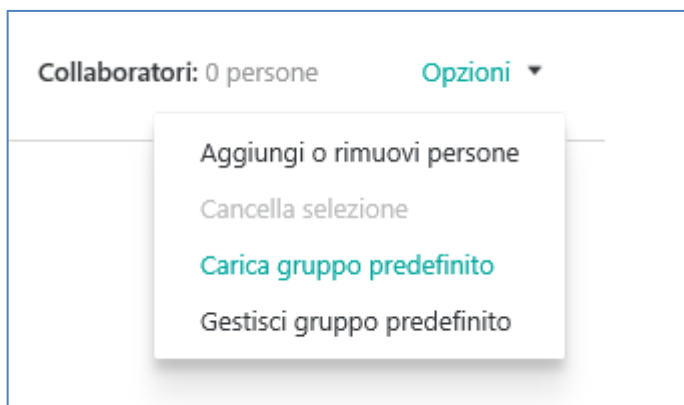


Figura 2

Una volta caricata la lista predefinita, è comunque possibile modificare i Collaboratori all'interno della lista, se necessario.

Dopo aver aggiunto i Collaboratori (e chiusa la finestra di dialogo *Aggiungi Collaboratori*) o dopo aver caricato la lista predefinita, la Request sarà subito condivisa con il gruppo di utenti.



MANUALE DI CONSERVAZIONE

VERSIONE: 1.3

Data approvazione: xx.xx.2020

Redazione: Brigida Serpillo

Verificato da: DPO

Approvato da: Direttore generale e Direttore Tecnico Scientifico

Classificazione documento: pubblico

VERSIONE N°	DATA	NATURA DELLA MODIFICA
1.0	31.10.2019	Prima versione documento
1.1	13.02.2020	Seconda versione documento
1.2	19.06.2020	Terza versione documento
1.3	xx.xx.2020	Quarta versione documento

Sommario

Sommario.....	2
1 1 Scopo e ambito del documento	4
2 2 Terminologia (glossario e acronimi)	4
2.1 Glossario dei termini e acronimi.....	5
2.2 Abbreviazioni e termini tecnici.....	7
3 3 Normativa e standard di riferimento	9
3.1 Normativa di riferimento.....	9
3.2 Standard di riferimento.....	10
4 4 Ruoli e responsabilità	11
4.1 Profili professionali all'interno della struttura organizzativa ARPAB.....	11
5 5 Struttura organizzativa per il servizio di conservazione	13
5.1 Organigramma.....	13
5.2 Strutture organizzative.....	13
6 6 Oggetti sottoposti a conservazione	15
6.1 Descrizione delle tipologie dei documenti sottoposti a conservazione.....	15
7	16

7	Il processo di conservazione.....	
7.1	Attori esterni del processo di conservazione.....	16
7.1.1	Registro di Protocollo.....	16
7.1.2	Fatturazione Elettronica.....	16
7.1.3	Servizio di Conservazione.....	16
8	8 Schema riepilogativo delle fasi del processo di conservazione.....	17
9		18
9	Il sistema di conservazione.....	
9.1	Caratteristiche generali della soluzione di conservazione.....	18
9.2	Formati gestiti.....	18
		18
9.3	Metadati.....	
9.4	Gestione e funzionalità del sistema di conservazione.....	19
9.5	Modalità di erogazione del servizio e architettura del sistema.....	19
10	10 Monitoraggio e controlli.....	20
10.1	Procedure di monitoraggio e controlli.....	20
10.2	Procedure di segnalazione anomalie.....	20
11	11 Specifiche contrattuali.....	21
12	12 Modello di funzionamento del servizio.....	21
12.1	Obblighi dell'Arpab.....	21
13	Modalità di accesso agli atti per gli aventi diritto	22
14	Protezione dati e piano nel caso di violazione dei dati personali	23
15	Elenco degli allegati	23

1 Scopo e ambito del documento

Il presente documento è il Manuale del sistema di conservazione (di seguito per brevità chiamato anche “Manuale”) dell’Agenzia Regionale della Protezione Ambientale della Basilicata (di seguito per brevità chiamata anche “A.R.P.A.B.”). Di seguito i dati identificativi della società:

Denominazione sociale: A.R.P.A.B.
--

Indirizzo della sede legale ed operativa: **Via della Fisica 18 c/d**
85100 POTENZA (PZ)
 Legale rappresentante: **Dott. Antonio Tisci**
 Partita IVA: **01318260765**
 N° di telefono (centralino): **0971 656111**
 Sito web: **<http://www.arpab.it/>**
 E-mail PEC: **protocollo@pec.arpab.it**

Il Manuale 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.

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

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

2 Terminologia (glossario e acronimi)

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:

2.1 Glossario dei termini e acronimi

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
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
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
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
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
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	E' 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.
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
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 Pacchetti di Archiviazione

	per conto di Arpab.
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.
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni.
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.
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 versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di conservazione.
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici.
Produttore	E' l'Arpab, che in proprio o attraverso i vari affidatari dei servizi da egli stesso incaricate produce il Pacchetto di versamento; nel caso di Pubblica Amministrazione è identificato 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.
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.
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 di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
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.
Scheda/e di conservazione	Elenco dei documenti informatici che il Cliente sottopone a conservazione con il Contratto.
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 per il periodo di tempo specificato nel Contratto. 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.
Titolare/i	La/e persona/e fisica/che o giuridica/che o altro tipo di società o ente che è/sono giuridicamente responsabili/e della formazione dei documenti da conservare formati in proprio ovvero formati da terzi in suo/loro nome, conto e interesse.

2.2 Abbreviazioni e termini tecnici

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, 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.
CSCD - contratto di servizio di conservazione dei documenti	Contratto di servizio di conservazione dei documenti, ove sono esplicitate chiaramente l'ambito dell'affidamento conferito, le specifiche funzioni, le attività e le responsabilità affidate dall'Arpab ad vari fornitori esterni del servizio di Conservazione.
PdV	Pacchetto di Versamento
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PSCD - Prestatore di Servizi di Conservazione dei Dati	Nella fattispecie ARUBA.
XML	Extensible Markup language

3 Normativa e standard di riferimento

3.1 Normativa di riferimento

Il sistema di conservazione di Arpab, è stato realizzato in conformità alla normativa vigente in materia di conservazione dei documenti informatici. Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990**, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000**, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo 30 giugno 2003, n. 196** e s.m.i. – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 7 marzo 2005 n. 82** e s.m.i. – Codice dell'amministrazione digitale (CAD);
- **DPCM 22 febbraio 2013**, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali;
- **DPCM 21 marzo 2013**, Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Circolare AGID 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- **D.M. 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;
- **Regolamento (UE) N. 910/2014** del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- **DPCM 13 novembre 2014**, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
- **Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- **Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale**, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- **Circolare n. 2 del 9 aprile 2018**, recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
- **Circolare n. 3 del 9 aprile 2018**, recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
- **Linee Guida sulla formazione, gestione e conservazione dei documenti informatici** emanate dall'Agid il 10/09/2020;

3.2 Standard di riferimento

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

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI) Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- **Dicom 3.0** (Digital Imaging and Communications in Medicine, immagini e comunicazione digitali in medicina);
- **Health Level 7 (HL7)** versione 2.3.1 e 2.5;
- **Integrating the Healthcare Enterprise (IHE)**;
- **UNI ISO 15489-1: 2006** Information and documentation -- Records management -- Part 1: General;
- **UNI ISO 15489-2: 2007** Information and documentation—Records management. Part 2: Guidelines;
- **ISO 9001:2015** – Quality management systems – Requirements.

4 Ruoli e responsabilità

Nel sistema di conservazione si individuano i seguenti ruoli principali:

Ruolo	Organizzazione di appartenenza
Produttore	A.R.P.A.B.
Responsabile della Conservazione	A.R.P.A.B.

Produttore Pacchetti di Versamento per Registro di Protocollo	Publisys
Produttore Pacchetti di Versamento per Fatture elettroniche	La Traccia
Responsabile del servizio di conservazione	ARUBA
Utente	A.R.P.A.B./Terzi autorizzati

A.R.P.A.B., quale **Produttore** è responsabile dei documenti che mette in conservazione e del loro contenuto.

Il **Responsabile della Conservazione** definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia, ma può delegare la sua funzione come previsto dall'art. 6 comma 6 delle regole tecniche del CAD.

Il Responsabile della Conservazione può inoltre decidere di affidare il processo/sistema di conservazione all'esterno, in outsourcing, in modo totale o parziale, a soggetti terzi pubblici o privati che offrono idonee garanzie organizzative e tecnologiche. Rimane in carico al Responsabile della Conservazione vigilare sulla corretta esecuzione del processo di conservazione.

I diversi **Produttore dei PdV** per il Registro di Protocollo (Publisys) e le Fatture elettroniche (La Traccia) sono responsabili dei rispettivi servizi di creazione dei PdV ed invio al sistema di Conservazione Aruba e della gestione dei backup e della sicurezza degli stessi servizi.

ARUBA, quale **Responsabile del servizio di conservazione** digitale dei documenti informatici di Arpab, agisce nei limiti dell'affidamento conferito 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'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.

4.1 Profili professionali all'interno della struttura organizzativa ARPAB

Qui di seguito si dà 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 processo di conservazione, prevede, le seguenti figure responsabili:

1. Responsabile della conservazione;
2. Responsabile della creazione dei PdV per il Registro di Protocollo e della sicurezza del sistema di protocollazione;
3. Responsabile della creazione dei PdV per le Fatture elettroniche e della sicurezza del sistema di fatturazione elettronica;
4. Responsabile del servizio di conservazione;
5. Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO).

Qui di seguito si riportano le attività associate a ciascuna delle figure sopra elencate:

- **Responsabile della Conservazione**
definisce e attua le politiche complessive del sistema di conservazione e vigila sulla corretta esecuzione del processo di conservazione.
- **Responsabile della creazione dei PdV per il Registro di Protocollo e della sicurezza del sistema di protocollazione**
crea i PdV e li invia al sistema di Conservazione Aruba. Inoltre gestisce i backup e garantisce la sicurezza degli stessi servizi.
- **Responsabile della creazione dei PdV per le Fatture elettroniche e della sicurezza del sistema di fatturazione**
crea i PdV e li invia al sistema di Conservazione Aruba. Inoltre gestisce i backup e garantisce la sicurezza degli stessi servizi.
- **Responsabile del servizio di conservazione**
Le attività affidate dal Responsabile della conservazione con l'Atto di Affidamento.

- **Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)**

Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali.

In particolare è tenuto a:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento UE 2016/679;
- cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Ruoli e Responsabilità					
Ruolo	Cognome	Nome	Organizzazione di appartenenza	Data Nomina	Data Cessazione
Produttore			A.R.P.A.B.		
Responsabile della Conservazione	Serpillo	Brigida	A.R.P.A.B.	24.09.2019 Del. n.261/2019	
	Dinuzzo	Giuseppe	A.R.P.A.B.	01.09.2018 Del. n.242/2018	23.09.2019
	Serpillo	Brigida	A.R.P.A.B.	16.05.2016 Del. n.239/2016	31.08.2018
Produttore PdV per Registro di Protocollo			Publisys		
Produttore PdV per Fatture elettroniche	Radogna	Nicola	La Traccia		
Responsabile del servizio di conservazione			ARUBA	25.10.2019 per aumento spazio	
				9.10.2020 per rinnovo servizio	
				22.09.2020 per aumento spazio	
				Giugno 2016 (Contratto del 21.06.16)	
DPO	Manzi	Nicola		21 Maggio 2020 DD. n.336/2020	
	Di Lecce	Francesco		Maggio 2018 DD. n.444/2018	
Utente			Arpab/Terzi autorizzati		

5 Struttura organizzativa per il servizio di conservazione

In questo capitolo sono indicate le strutture organizzative coinvolte nel servizio di conservazione comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione.

5.1 Organigramma

La figura in basso riporta le strutture organizzative coinvolte nel servizio di conservazione:

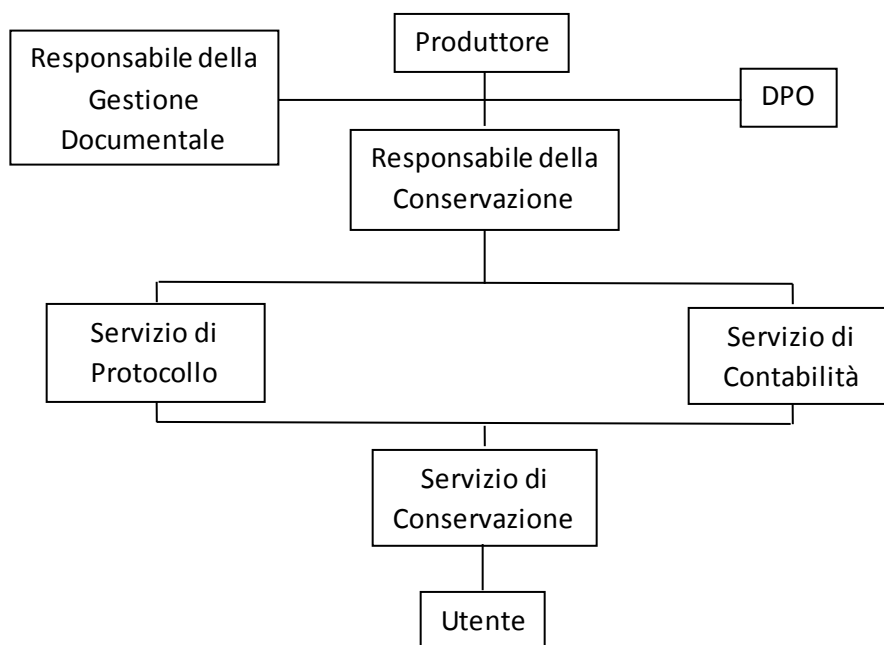


Figura 1: Rappresentazione delle strutture organizzative coinvolte nel servizio di conservazione

5.2 Strutture organizzative

Nello specifico le strutture funzionali dell'organizzazione operano in sinergia come segue:

- **Produttore**

- la Direzione Aziendale garantisce la continuità generale dell'organizzazione.

- **DPO**

- Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali.

- **Responsabile della Gestione Documentale**

- Collabora con il Responsabile della Conservazione al fine di stabilire le classi documentali, con relativi metadati, da mandare in conservazione ed i criteri.

- **Responsabile della Conservazione**

- Definisce e attua le politiche complessive del sistema di conservazione e vigila sulla corretta esecuzione del processo di conservazione.

- **Servizio di Protocollo**

- Gestisce l'applicativo che crea i PdV per la parte del Registro di Protocollo e li invia al sistema di Conservazione Aruba. Inoltre garantisce il backup dei dati e la sicurezza e prestazione del servizio, nonché cura la manutenzione software su cui il servizio gira.

- **Servizio di Contabilità**

- Gestisce l'applicativo che crea i PdV per la parte delle Fatture elettroniche e li invia al sistema di Conservazione Aruba. Inoltre garantisce il backup dei dati e la sicurezza e prestazione del servizio, nonché cura la manutenzione hardware e software su cui il servizio gira.

- **Servizio di Conservazione**

- Garantisce la gestione degli asset (hardware e software), occupandosi dell'intero processo di supply-chain del servizio di conservazione
- Provvede alla gestione delle informazioni, per l'intero ciclo di vita (dalla classificazione, al monitoraggio del sistema, fino alla protezione dei log)
- Si occupa della manutenzione ed assistenza, a garanzia della continuità operativa del servizio di conservazione
- Garantisce l'esecuzione del processo di conservazione in conformità ai requisiti tecnici normativi
- Provvede alla gestione operativa degli accessi logici e fisici, seguendo apposite procedure e mantenendo aggiornata la documentazione
- Garantisce l'attivazione e consegna dei servizi ai clienti, rispettando KPI e SLA concordati

- **Utente**

- 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 Manuale - parte Aruba.

6 Oggetti sottoposti a conservazione

6.1 Descrizione delle tipologie dei documenti sottoposti a conservazione

In conservazione vengono mandati le seguenti classi documentali:

- Registro di protocollo giornaliero;
- Fatture elettroniche attive e passive.

I formati di conservazione sono quelli previsti dalla normativa:

PDF - PDF/A, TIFF, JPG, Office Open XML (OOXML) , Open Document Format, XML, TXT, Formati Messaggi di posta elettronica.

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 *Contratto*).

I pacchetti inviati in conservazione sono correlati dei metadati come da schede allegate.

Al fine di garantire l'identificazione certa del soggetto che ha formato il documento, i documenti informatici posti in conservazione sono in genere sottoscritti con firma digitale dall'Arpab ed 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*.

7 Il processo di conservazione

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

7.1 Attori esterni del processo di conservazione

7.1.1 Registro di Protocollo

Dai primi mesi del 2019 il software per la protocollazione è Geos, fornito e gestito dalla Ditta Publisys. I dati del protocollo sono gestiti su una macchina virtuale installata su un Server presente in Arpab, in una stanza refrigerata e chiusa a chiave. La Ditta gestisce la manutenzione software del Server e della macchina virtuale e garantisce la qualità dei servizi ed il backup dei dati che vengono eseguiti giornalmente in orario notturno (sono di tipo Full per i db, invece per la parte documentale sono fatti con la sincronizzazione dei file modificati e quindi incrementale). Pertanto la creazione ed il versamento dei PdV relativi sono totalmente a cura della Ditta di cui sopra che, utilizzando dei web services, li invia in conservazione su Aruba. I formati (a norma di legge) e i metadati associati dei file da inviare in conservazione sono stati stabiliti mediante apposita convenzione e contratto con la Regione Basilicata (che si allegano al presente Manuale). Per un maggior dettaglio si rimanda al Manuale specifico redatto dalla Ditta Publisys per la parte di sua competenza.

7.1.2 Fatturazione Elettronica

Dai primi mesi del 2018 il software per la contabilità è SIC, fornito e gestito dalla Ditta La Traccia. I dati della contabilità sono in hosting presso la Server Farm della Regione Basilicata (sulla base di apposito accordo), che ne gestisce la manutenzione e garantisce la qualità dei servizi ed il backup dei dati. Pertanto la creazione ed il versamento dei PdV relativi sono totalmente a cura della Ditta di cui sopra che, utilizzando dei web services, li invia in conservazione su Aruba. I formati (a norma di legge) e i metadati associati dei file da inviare in conservazione sono stati stabiliti mediante apposita convenzione e contratto con la Regione Basilicata (che si allegano al presente Manuale). Per un maggior dettaglio si rimanda al Manuale specifico redatto dalla Ditta La Traccia per la parte di sua competenza.

7.1.3 Servizio di Conservazione

Da metà 2016, mediante apposita convenzione con la Regione Basilicata (che si allega al presente Manuale), il servizio di conservazione è stato affidato e gestito da ARUBA (per un maggior dettaglio si rimanda al Manuale specifico redatto dalla Ditta ARUBA per la parte di sua competenza). Quale riscontro finale del processo di conservazione vi è un sistema di notifiche alla PEC del Responsabile della Conservazione che gli consente di monitorare l'andamento del Servizio, oltre che dall'apposito cruscotto dedicato sul portale DocFly a cui è possibile accedere tramite username e password.

8 Schema riepilogativo delle fasi del processo di conservazione

La figura in basso riporta le fasi salienti del processo di conservazione:

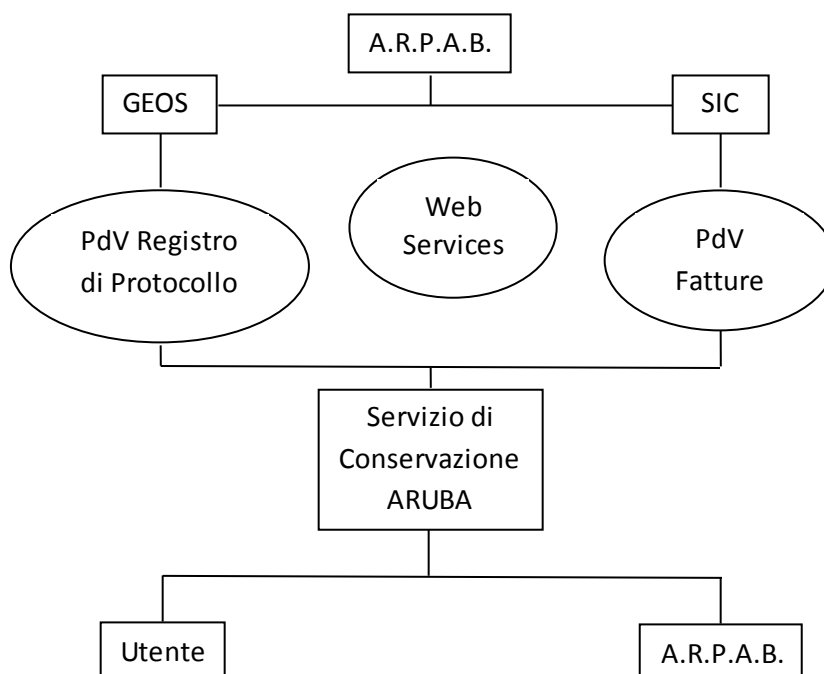


Figura 1: Rappresentazione delle fasi salienti del processo di conservazione

9 Il sistema di conservazione

9.1 Caratteristiche generali della soluzione di conservazione

L'Ente utilizza per l'Archiviazione a norma dei propri documenti il sistema di Archiviazione di ARUBA SPA, denominato DocFly. DocFly è un servizio di conservazione digitale, conforme alle disposizioni normative contenute all'interno del DPCM del 3 Dicembre 2013 ed agli standard tecnici espressamente richiamati dal decreto stesso. La soluzione permette di gestire e conservare a norma qualsiasi tipo di documento informatico, sia in ambito amministrativo che fiscale, rispondendo quindi, con un'unica soluzione, a tutte le esigenze di conservazione a norma di legge di ogni realtà produttiva.

DocFly assicura, dalla presa in carico fino all'eventuale scarto, la conservazione di documenti e fascicoli informatici, inclusi i metadati associati, garantendo al tempo stesso i requisiti di autenticità, integrità, affidabilità, leggibilità, reperibilità.

Il sistema scelto è in linea con le disposizioni vigenti e presenta le seguenti caratteristiche:

- salvaguardia dell'integrità dei documenti informatici conservati mediante apposizione della firma digitale;
- prolungamento della validità del documento con apposizione della marca temporale al pacchetto di archiviazione;
- versamento multicanale dei documenti da sottoporre in conservazione;
- accesso diretto tramite interfaccia Web sicura ai documenti informatici conservati;
- totale sicurezza nella trasmissione dei documenti informatici da sottoporre a conservazione;
- completo monitoraggio delle fasi di elaborazione dei documenti;
- gestione degli utenti con possibilità di autorizzare l'accesso solo alle classi documentali di competenza;
- reportistica relativa allo status di utilizzo del servizio DocFly. Tramite DocFly è possibile conservare correttamente documenti di vario tipo: amministrativi, a rilevanza tributaria, documenti generici e messaggi PEC.

Le classi documentali attualmente in conservazione sono il Registro di Protocollo e le Fatture elettroniche, attive e passive. I servizi di Protocollo e Contabilità, che producono tali classi documentali, sono dati in outsourcing e pertanto gestiti da due diverse Ditte esterne, rispettivamente Publisys e La Traccia, e i relativi dati sono per la prima memorizzati su un Server agenziale e per la seconda in hosting presso la Server Farm della Regione Basilicata per una questione di opportunità, livelli di sicurezza e protezione dati anche dai disaster recovery.

Le soluzioni adoperate poi si poggiano entrambe sulla messa in conservazione presso il Sistema Aruba. La scelta è ricaduta su tale fornitore poiché era inizialmente compresa nella convenzione stipulata nel 2016 con la Regione Basilicata (si allega convenzione). In fase di rinnovo nel 2019, essendo terminata la convenzione con la Regione, si è deciso di restare in conservazione su tale fornitore principalmente per questioni di comodità, affidabilità, architettura scalabile e sicurezza.

Pertanto le due Ditte Publisys e La Traccia curano la produzione dei rispettivi PdV, li firmano e li inviano in conservazione presso Aruba tramite Web Services; mentre Aruba gestisce e garantisce la parte squisitamente della conservazione delle classi documentali e l'eventuale esibizione a terzi ed accesso all'Agenzia, tramite un cruscotto ad essa dedicato accessibile da web all'indirizzo <https://conservazione.docfly.it/docfly/signin> previo accesso con username e password.

Inoltre l'esito di tali versamenti viene notificato dal sistema Aruba mediante un servizio di messaggistica all'indirizzo mail della PEC del Responsabile della Conservazione dell'Arpa.

9.2 Formati gestiti

In linea con la normativa vigente il sistema consente la conservazione dei seguenti formati: PDF/PDF-A, TIF, JPG, Office Open XML (OOXML), ODF (Open Document Format), XML, TXT, formati messaggi di posta elettronica.

9.3 Metadati

La normativa vigente esplicita i metadati minimi da associare a qualsiasi documento informatico, ovvero, gli indici che devono essere ad esso associati, a prescindere dalla specializzazione che questo assume (amministrativo, fiscale, ecc.). Oltre a quanto previsto dalla normativa è possibile specificare ulteriori metadati da associare ai documenti quali, ad esempio, il numero delle pagine, l'anno, il periodo d'imposta ed altro. Tali ulteriori metadati sono oggetto di indicizzazione da parte del sistema e costituiscono nuove chiavi di interrogazione e ricerca.

9.4 Gestione e funzionalità del sistema di conservazione

Il servizio è accessibile tramite interfaccia Web. In particolare, è previsto un pannello di gestione attraverso il quale, l'utente dispone di tutti gli strumenti utili per l'espletamento delle sue attività, in linea con i privilegi specifici che sono stati previsti per quella utenza, tra cui:

- creazione e profilazione utenti: all'attivazione del servizio è prevista la creazione di un account master che consente al cliente di creare e gestire in completa autonomia, uno o più profili, sulla base delle utenze in suo possesso;
- funzionalità di ricerca e download: tutti i documenti archiviati e conservati possono essere consultati successivamente attraverso le funzionalità di ricerca. L'utente può effettuare il semplice download dei documenti conservati o richiedere la produzione di un pacchetto di distribuzione a norma di legge;
- gestione dei processi: l'utente ha la possibilità di visualizzare lo stato reale dei processi di conservazione, incluse notifiche e log relativamente ai documenti versati sul sistema di conservazione;
- notifiche: le diverse operazioni, che si succedono lungo il processo di conservazione, sono notificate in automatico dal sistema e inviate via email (PEC) ai riferimenti indicati dal cliente;
- reportistica: il sistema permette di verificare in tempo reale l'utilizzo delle risorse allocate ad uno o più archivi collegati al cliente, ed inoltre, fornisce uno strumento di reportistica su base mensile, in grado di identificare per il periodo di riferimento scelto, l'allocato e consumato effettivo delle risorse. I report possono essere salvati e recuperati;
- alert: l'utente riceve degli alert con notifica via email relativamente alle seguenti informazioni: superamento livelli di soglia prestabiliti, rinnovo contrattuale, pagamenti ed altre informazioni relative al contratto.

9.5 Modalità di erogazione del servizio e architettura del sistema

Il servizio DocFly è erogato in modalità outsourcing tramite l'infrastruttura ospitata presso i data center del Gruppo Aruba che rispondono agli elevati standard TIER IV. I dati archiviati sono custoditi al suo interno e i massimi livelli di sicurezza adottati in queste strutture impediscono interruzioni del servizio o tentativi di intrusione e manomissione. La soluzione prevede un'architettura modulare che presenta le seguenti caratteristiche:

- affidabilità: totale ridondanza ai guasti HW e SW di ogni singolo componente;
- scalabilità: l'architettura è progettata per gestire l'elaborazione di grandi volumi di dati;
- flessibilità: la soluzione è facilmente integrabile e customizzabile;
- storage replicato: il dato posto in conservazione è sempre memorizzato in almeno due infrastrutture storage.

Il servizio DocFly in dettaglio:

Caratteristiche generali del servizio	Specifiche tecniche
SLA complessiva sul servizio	99,95% uptime nel versamento e consultazione
Assistenza	Sistema di ticketing e canale telefonico
Fasi elaborazione Pacchetti di Versamento	Riferimento - Specifiche tecniche
Presa in carico del PdV (rapporto di versamento)	Notifica al cliente entro 48 ore dal ricevimento dell'ultimo documento contenuto nel pacchetto di versamento
Invio in conservazione del PdA (costituiti da uno o più PdV)	Notifica al cliente entro 96 ore dal ricevimento dell'ultimo documento
Comunicazioni durante il processo	Specifiche tecniche
Rapporto di Versamento - PdV Validato	Notifica entro 4 ore dalla effettiva presa in carico del PdV
Rapporto di Conservazione - PdV Conservato	Notifica entro 4 ore dall'effettiva conservazione del PdV
Richiesta di Esibizione	Specifiche tecniche
Produzione del Pacchetto di Distribuzione	Notifica entro 24 ore dalla richiesta di produzione del PdD

10 Monitoraggio e controlli

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

10.1 Procedure di monitoraggio e controlli

Giornalmente, durante il periodo lavorativo, il Responsabile della Conservazione controlla le notifiche giunte dal Sistema di ARUBA sulla sua mail PEC e periodicamente verifica la situazione dello spazio, la validità del contratto e l'integrità e contenuto degli archivi posti in conservazione direttamente dal sito DocFly.

10.2 Procedure di segnalazione anomalie

In caso di notifica di anomalia da parte del sistema di conservazione, il Responsabile della Conservazione gira via mail tale segnalazione, a seconda della classe documentale interessata, alla Ditta che gestisce la creazione del relativo PdV, aprendo così un ticket che normalmente viene risolto in tempi brevi, solitamente nell'arco della stessa giornata. Diversamente in caso di notifica di altro tipo, cioè non legato squisitamente ai PdV, lo stesso contatta il riferimento Aruba o apre un ticket tramite il sistema REMEDY Digital WorkplacePlatform (DWP) fornito dalla stessa società, secondo le modalità e le tempistiche dettagliate nei relativi allegati descrittivi di tale servizio Enterprise Customer Service.

11 Specifiche contrattuali

Per il contratto con Aruba si rimette al relativo allegato al presente Manuale.

Attualmente abbiamo portato a 5 i GB di spazio per la conservazione (dai precedenti 3 GB), in quanto si è registrato un forte ed anomalo incremento dell'archivio nel periodo estivo del 2020 (causa acquisizione al protocollo di domande di concorso) che ci ha costretti ad anticipare la normale richiesta prevista tra il 2021 ed il 2022.

Le classi documentali attive sul sistema Aruba sono n.3 su 4 a nostra disposizione e sono inserite in un unico archivio.

12 Modello di funzionamento del servizio

Il compito di Arpab è quello di conservare i documenti informatici con sistemi coerenti alla normativa regolante la conservazione digitale dei documenti informatici.

In particolare, il servizio di conservazione digitale di Arpab 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.

In particolare, la conservazione è svolta affidando alle società esterne Publisys, La Traccia ed ARUBA, per quanto di loro competenza, il ruolo ed i compiti fissati nell'Atto di Affidamento.

A tal fine, l'Arpab ha 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 si allega il *Contratto* stipulato tra Arpab ed ARUBA, con 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 di Arpab;
- d) le responsabilità e gli obblighi di Arpab;
- 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.

12.1 Obblighi dell'Arpab

Il processo di conservazione impone all'Arpab l'istituzione di un'organizzazione interna idonea che garantisca la piena osservanza delle disposizioni normative in tema di gestione documentale e delle procedure 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, l'Arpab 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.

L'Arpab, quindi, all'interno della propria struttura organizzativa, ha definito:

- a) i fornitori dei diversi servizi interessati alla conservazione digitale a lungo termine dei documenti informatici (per la parte delle fatture elettroniche, del registro giornaliero di protocollo e del servizio di conservazione degli stessi);
- b) le funzioni e le attività affidate, 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;

A.R.P.A. Basilicata

Via della Fisica 18 C/D 85100 Potenza - tel.0971656111 - email PEC: protocollo@pec.arpab.it | Partita I.V.A. 01318260765

Documento Pubblico | Manuale di Conservazione ARPAB v.1.0

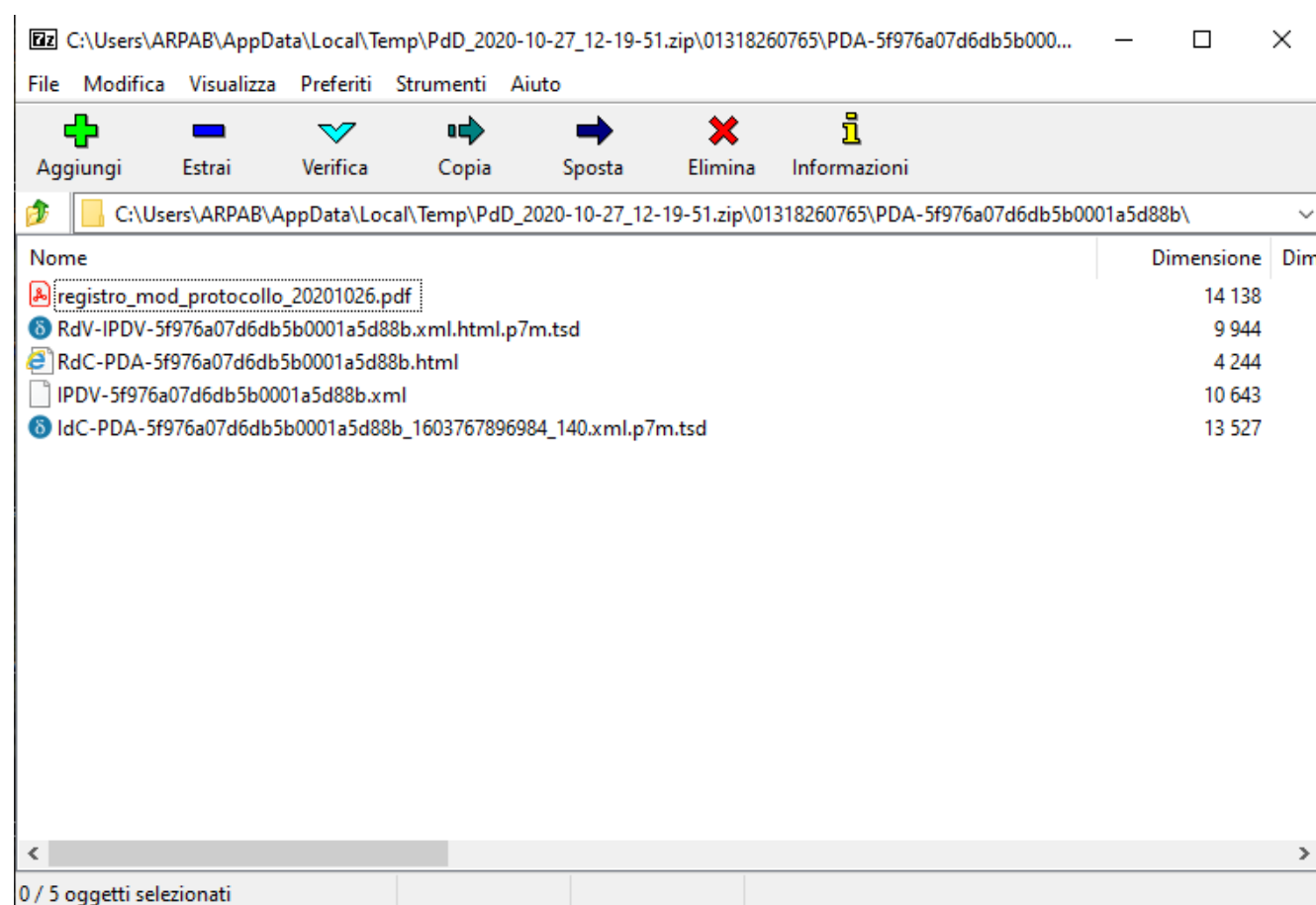
- c) la gestione delle responsabilità derivanti dalle funzioni ed attività affidate (per Sistema REGPROT: Determina n.915/2018; per Sistema FATTEL: Delibera n.96/2018; per Conservazione Sostitutiva: Delibera n.239/2016; per Protocollo e assegnazione pratiche: Delibera n.86/2016);
- d) la documentazione delle deleghe ed il relativo mantenimento;
- e) le misure organizzative e tecniche idonee ad evitare danno ad altri.

13 Modalità di accesso agli atti per gli aventi diritto

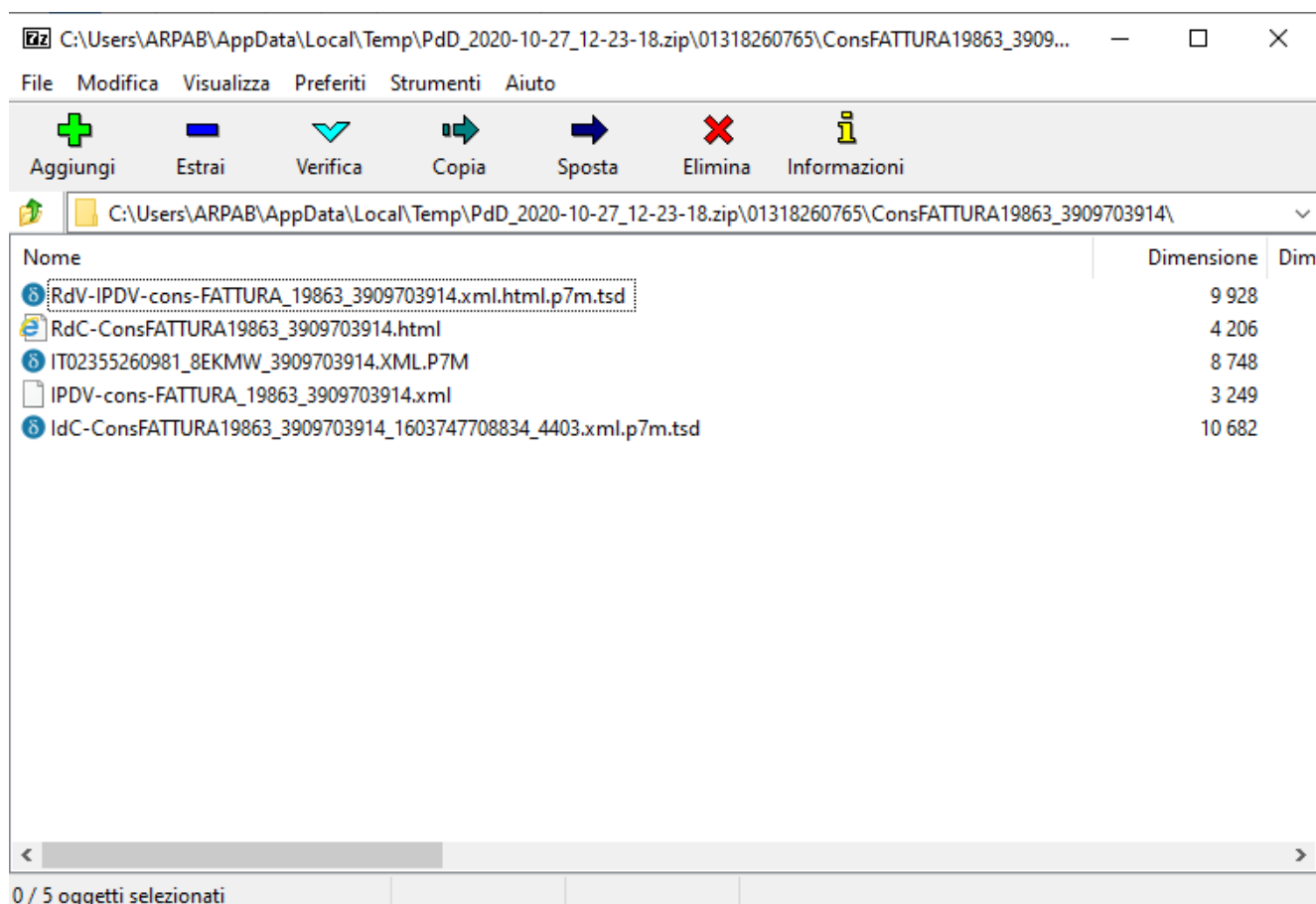
Il Sistema di Conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico.

Il Produttore, o chi per lui (Responsabile della Conservazione), può, su sua necessità o su richiesta di terzi interessati ed aventi diritto, dal sito DocFly, previa autenticazione con i giusti privilegi, scaricare il PDD (Pacchetto di Distribuzione) relativo al documento d'interesse (Registro di Protocollo o Fattura elettronica) in formato zippato.

Il file .zip scaricato contiene al suo interno una serie di file di diversa natura, come da immagini seguenti, differenti a seconda della tipologia di documento conservato:



Riferito al PDD relativo ad un Registro di Protocollo.



Riferito al PDD relativo ad una Fattura Elettronica.

Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il sistema di conservazione sono quelli indicati nel manuale del processo di conservazione adottato dal conservatore e presente sul sito dell'AGID al seguente indirizzo:

https://www.agid.gov.it/sites/default/files/repository_files/manuale_di_conservazione_aruba_pec_ver_1.5_2018_10_11.pdf.

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.

14 Protezione dati e piano nel caso di violazione dei dati personali

Il Responsabile del Servizio di Conservazione (Aruba PEC ed il Gruppo Aruba) hanno 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 (Regolamento (UE) 2016/679 e D.lgs. 196/2003 e s.m.i.).

Per maggior dettagli si fa riferimento al Capitolo 12 dell'Allegato "Manuale della Conservazione Aruba SpA" (pag.91).

15 Elenco degli allegati

Al presente Manuale risultano allegati i seguenti documenti:

- Manuale della Conservazione relativo al Registro di Protocollo (Sistema REGPROT - pag.1 dell'allegato);
- Manuale della Conservazione relativo alle Fatture (Sistema FATTEL - pag.12 dell'allegato);
- Manuale della Conservazione Aruba SpA (pag.31 dell'allegato);
- Nomina del Responsabile della Conservazione (Deliberazione Arpab n.239/2016 - pag.101 dell'allegato);
- Convenzione con Regione Basilicata (validità da giugno 2016 a settembre 2019 - pag.103 dell'allegato);
- Contratto con Aruba SpA (del 21.06.2016 - pag.103 dell'allegato);

- Classi documentali e relativi metadati (pag.106, 107 e 108 dell'allegato);
- Documenti esplicativi del servizio Enterprise Customer Service offerto da Aruba per la gestione dei ticket di assistenza (da pag.112 dell'allegato).

Aruba PEC S.p.A.

Manuale di Conservazione

Versione: 1.6

Data approvazione: 17/04/2019

Redazione: Marco Menonna

Verificato da: Mauro Manetti, Roberta Giommoni

Approvato da: Andrea Sassetti

Classificazione documento: pubblico

VERSIONE N°	DATA	NATURA DELLA MODIFICA
1.0	26/11/2014	Prima versione documento
1.1	02/02/2016	Revisione del manuale a seguito della pubblicazione del nuovo schema sul sito istituzionale dell'Agid
1.2	04/04/2016	Modifiche su terminologie utilizzate
1.3	20/09/2017	Par.3.1: aggiornata normativa di riferimento Par.4.1: aggiornati Responsabili del Servizio e date di nomina Par.6.3: rimosso Par.7.6: modificata terminologia (da "materiali" a documenti"); Inserimento Par.7.7.3: Produzione copie o duplicati su supporti rimuovibili Par. 7.11: inserito paragrafo "audit log" Par.8.6: migliorata descrizione della soluzione di conservazione Par.8.6.1: migliorata descrizione change management e inserito riferimento test di Quality Assurance Par.9.2.: modificata cadenza verifica periodica dell'integrità degli archivi. Modificata descrizione procedura leggibilità archivi. Par.9.2.1 modificata frequenza verifica integrità degli archivi Cap.11: Cambiata descrizione specifiche tecniche per "invio in conservazione del PdA" Par.12.7: ridefinite modalità di isolamento delle componenti critiche Par.12.8.3: migliorata descrizione della sicurezza organizzativa e aggiornati riferimenti normativi 12.8.4: aggiornate regole password utente Tutto il documento: aggiornati riferimenti a documenti interni e procedure di sistema

1.4	11/12/2017	Tutto il documento: inseriti testi alternativi per le immagini e verificata accessibilità Par. 1.1: Specificata denominazione societaria del Conservatore Accreditato e inseriti dati identificativi della società Par. 2.1: Uniformata terminologia relativa a IdC, IPdA e IPdV Par. 6.3.2: Aggiornata tabella formati consigliati Par 6.6.1: Aggiornati riferimenti alle specifiche specifiche del Pacchetto di Versamento Par. 6.7.1: Aggiornata terminologia relativa a IdC Par.7.5.2: Inserito paragrafo relativo a gestione PdA incompleti o non validi Par. 7.6.1: Aggiornato paragrafo e corretto refuso di terminologia sul secondo punto Par. 7.8.3: Descritta procedura per scarto immediato Par.9.2: Modificato titolo paragrafo Par. 9.2.1: Rivista descrizione delle attività di verifica dell'integrità degli archivi Par 10.1.2: Aggiornati i contenuti della Scheda di Conservazione Cap. 11: Rivisti ed aggiornati livelli di servizio (SLA)
1.5	11/10/2018	Aggiornamenti Terminologia, Normativa e Standard di Riferimento Par.4.1: Aggiornati Ruoli e Responsabilità Par.6.4: Precisazione su inserimento delle c.d. extrainfo nell' IdC. Par. 7.1: Aggiornamento modalità di acquisizione dei PdV. Inserito par. 7.5.3 Rettifica dei pacchetti di archiviazione Par.12.5: Rimosso riferimento a protocollo SSL Par. 12.6: Rivisti dettagli gestione dei backup del sistema Tutto il documento: aggiornamenti riferimenti a normativa trattamento dati personali
1.6	17/04/2019	Nuovo Template Cap.1: Aggiornato Rappresentante Legale Par.4.1: Aggiornati Ruoli e Responsabilità

Sommario

Sommario.....	3
1 Scopo e ambito del documento.....	6
2 Terminologia (glossario e acronimi)	7
2.1 Glossario dei termini e acronimi.....	7
2.2 Abbreviazioni e termini tecnici	13
3 Normativa e standard di riferimento.....	15
3.1 Normativa di riferimento.....	15
3.2 Standard di riferimento	15
4 Ruoli e responsabilità.....	16
4.1 Profili professionali all'interno della struttura organizzativa ARUBA.....	17
5 Struttura organizzativa per il servizio di conservazione	22
5.1 Organigramma	22
5.2 Strutture organizzative	22
5.3 Responsabilità e funzioni nel processo di conservazione.....	24
6 Oggetti sottoposti a conservazione	26
6.1 Descrizione delle tipologie dei documenti sottoposti a conservazione	26
6.2 Copie informatiche di documenti analogici originali unici	26
6.3 Formati gestiti.....	28
6.3.1 Caratteristiche generali dei formati.....	28
6.3.2 Formati consigliati per la conservazione.....	28
6.3.3 Identificazione.....	32
6.4 Metadati da associare alle diverse tipologie di documenti.....	33
6.5 Modalità di assolvimento dell'imposta di bollo sui documenti posti in conservazione.....	33
6.6 Pacchetto di versamento	33
6.6.1 Specifiche Pacchetto di Versamento	34
6.7 Pacchetto di Archiviazione.....	34
6.7.1 Specifiche Pacchetto di Archiviazione	34
6.8 Pacchetto di Distribuzione	34
6.9 Documenti rilevanti ai fini delle disposizioni tributarie.....	35
6.9.1 Modalità di assolvimento dell'imposta di bollo sui DIRT.....	36
6.10 Trattamento dei pacchetti di archiviazione contenenti documenti rilevanti ai fini delle disposizioni tributarie	36
7 Il processo di conservazione	37
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	37
7.1.1 Ricezione dell'indice del pacchetto di versamento.....	37
7.1.2 Ricezione documenti associati ad un pacchetto di versamento.....	38
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti	39

7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	41
7.3.1	<i>Specifiche rapporto di versamento</i>	41
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie	41
7.5	Preparazione e gestione del Pacchetto di Archiviazione	41
7.5.1	<i>Chiusura anticipata (in corso d'anno) del Pacchetto di Archiviazione</i>	42
7.5.2	<i>Gestione dei Pacchetti di Archiviazione non validi o non completi</i>	42
7.5.3	<i>Rettifica dei pacchetti di archiviazione</i>	42
7.6	Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione	43
7.6.1	<i>Attività conseguenti alla cessazione del contratto</i>	43
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	44
7.7.1	<i>Produzione di duplicati</i>	44
7.7.2	<i>Produzione di copie</i>	44
7.7.3	<i>Produzione copie o duplicati su supporti rimovibili</i>	44
7.7.4	<i>Intervento del Pubblico Ufficiale</i>	45
7.8	Scarto dei pacchetti di archiviazione	45
7.8.1	<i>Trasferimento dei documenti informatici in conservazione</i>	45
7.8.2	<i>Scarto dei documenti informatici conservati</i>	45
7.8.3	<i>Richiesta di scarto immediato</i>	46
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	46
7.10	Tabella riepilogativa delle fasi del processo di conservazione	46
7.11	Audit Log	47
8	Il sistema di conservazione	48
8.1	Infrastruttura informatica datacenter	48
8.2	Caratteristiche generali della soluzione di conservazione	48
8.3	Componenti Logiche	49
8.4	Componenti tecnologiche	49
8.5	Componenti fisiche	50
8.5.1	<i>Sito Primario (Produzione)</i>	50
8.5.2	<i>Sito Secondario (DR)</i>	51
8.6	Procedure di gestione e di evoluzione	52
8.6.1	<i>Change management</i>	52
8.6.2	<i>Verifica periodica di conformità a normativa e standard di riferimento</i>	53
9	Monitoraggio e controlli	54
9.1	Procedure di monitoraggio	54
9.2	Verifiche sugli archivi	54
9.2.1	<i>Pianificazione delle verifiche periodiche da effettuare</i>	55
9.2.2	<i>Mantenimento della firma per il periodo di conservazione</i>	55
9.3	Soluzioni adottate in caso di anomalie	55
10	Specifiche contrattuali	56
10.1.1	<i>Nomina di Aruba quale responsabile del servizio di conservazione e del trattamento dei dati</i>	56

10.1.2	Scheda di conservazione.....	56
10.1.3	Elenco Persone	56
10.2	Modello di funzionamento del servizio	56
10.2.1	Obblighi del Cliente	57
10.2.2	Obblighi di ARUBA.....	58
10.2.3	Compiti organizzativi.....	58
10.2.4	Compiti di manutenzione e controllo	58
10.2.5	Compiti operativi.....	59
10.2.6	Fasi del processo di conservazione e responsabilità.....	59
11	Livelli di servizio (SLA)	60
12	Sicurezza del sistema di conservazione	61
12.1	Privacy e requisiti di sicurezza dei dati	61
12.2	Analisi dei Rischi.....	61
12.3	Controllo Accessi.....	61
12.4	Monitoraggio Eventi e Vulnerabilità di Sicurezza	62
12.5	Cifratura	62
12.6	Backup.....	62
12.7	Isolamento delle componenti critiche	62
12.8	Sicurezza fisica datacenter del Gruppo Aruba	62
12.8.1	Sicurezza Fisica Data Center Primario	63
12.8.2	Sicurezza fisica Data Center Secondario.....	65
12.8.3	Sicurezza organizzativa comune ai due data center	65
12.8.4	Sicurezza Logica dei sistemi e degli apparati	66
12.9	Piano di Disaster Recovery e Continuità operativa	67
12.9.1	Business Impact Analysis (BIA)	68
12.9.2	Analisi dei Rischi	68
12.9.3	Classificazione dei Sistemi e delle Risorse	68
12.9.4	Modalità tecniche per la Business Continuity ed il Disaster Recovery.....	68
13	Disposizioni finali	69
13.1	Nullità o inapplicabilità di clausole	69
13.2	Interpretazione	69
13.3	Nessuna rinuncia.....	69
13.4	Comunicazioni.....	69
13.5	Intestazioni e Appendici e Allegati del presente Manuale Operativo	69
13.6	Modifiche del Manuale di conservazione.....	70
13.7	Violazioni e altri danni materiali	70
13.8	Norme Applicabili.....	70

1 Scopo e ambito del documento

Il presente documento è il Manuale del sistema di conservazione (di seguito per brevità chiamato anche “Manuale”) del Conservatore Accreditato Aruba PEC S.p.a. (da ora in avanti “ARUBA”). Di seguito i dati identificativi della società:

Denominazione sociale: **Aruba PEC S.p.A.**
Indirizzo della sede legale ed operativa: **Via S. Clemente, 53**
24036 Ponte San Pietro (BG)
Legale rappresentante: **Giorgio Cecconi** (Amministratore Unico)
N° di iscrizione al Registro Imprese di Bergamo: **01879020517 (REA n. 445886)**
Codice Fiscale e Partita IVA: **01879020517**
N° di telefono (centralino): **+39 0575 050.350**
ISO Object Identifier (OID): **1.3.6.1.4.1.29741**
Sito web principale: <https://www.pec.it>
E-mail (generale): info@arubapec.it

Il Manuale 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.

Il Manuale è costituito dalla 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 servizio di conservazione, descrivendo in modo puntuale, in caso di affidamento, i soggetti, le funzioni e gli ambiti oggetto dell'affidamento stesso;
- 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 sottoponibili 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".

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.

[Torna al sommario](#)

2 Terminologia (glossario e acronimi)

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:

[Torna al sommario](#)

2.1 Glossario dei termini e acronimi

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
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	Qualsiasi codice contenuto in un documento informatico potenzialmente idoneo a modificare la rappresentazione dell'informazione senza alterarne il contenuto binario (in via meramente esplicativa e non esaustiva: macro, codici eseguibili nascosti, formule di foglio di lavoro occulte in tutto o in parte, sequenze di caratteri occultate all'interno dei documenti informatici)
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 intestato dal Cliente al/i Titolare/i nel quale sono conservati costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico e di cui il/i medesimo/i è/sono giuridicamente responsabile/i
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
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
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	E' 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.
Elenco Persone	Elenco delle persone designate dal Cliente ad operare in suo nome, conto e interesse con ARUBA per l'esecuzione del contratto.
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.
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 sul Pacchetto di Archiviazione 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 minime	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.
Indice di Conservazione (IdC)	L'Indice del Pacchetto di Archiviazione (IPdA)
Indice del Pacchetto di Archiviazione (IPdA)	Indice che contiene le informazioni relative al Pacchetto di Archiviazione in formato xml, anche indicato nello standard SInCRO come IdC (Indice di Conservazione)
Indice del Pacchetto di Versamento (IPdV)	Indice che contiene le informazioni relative al pacchetto di versamento in formato xml.
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.
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	E' 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	E' il Cliente, di norma diverso dal Titolare, che in proprio o attraverso le persone fisiche da egli stesso incaricate produce il Pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione; nel caso di Pubblica Amministrazione è identificato 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.
Referente/i del Cliente	E'/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.
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche che trattano il procedimento, ordinati secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica.
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Responsabile della 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.
Scheda/e di conservazione	Elenco dei documenti informatici che il Cliente sottopone a conservazione con il 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 per il periodo di tempo specificato nel Contratto. 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/i	La/e persona/e fisica/che o giuridica/che o altro tipo di società o ente che è/sono giuridicamente responsabili/e della formazione dei documenti da conservare formati in proprio ovvero formati da terzi in suo/loro nome, conto e interesse.
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.

[Torna al sommario](#)

2.2 Abbreviazioni e termini tecnici

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, 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;
CSCD - contratto di servizio di conservazione dei documenti	Contratto di servizio di conservazione dei documenti, ove sono esplicitate chiaramente l'ambito dell'affidamento conferito, 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;
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;
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

[Torna al sommario](#)

3 Normativa e standard di riferimento

3.1 Normativa di riferimento

Il sistema di conservazione digitale di ARUBA, è stato realizzato in conformità alla normativa vigente in materia di conservazione dei documenti informatici. Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- **Codice Civile** [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- **Legge 7 agosto 1990**, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000**, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Regolamento (UE) 2016/679** del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
- **Regolamento (UE) N. 910/2014** del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
- **Decreto Legislativo 30 giugno 2003**, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- **Decreto Legislativo 22 gennaio 2004**, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 7 marzo 2005 n. 82** e s.m.i. – Codice dell'amministrazione digitale (CAD);
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **D.M. 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;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Circolare AGID 10 aprile 2014**, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- **Il DPR nr. 1409 del 30 settembre 1963** - (Legge archivistica) all'art. 30 prevede che le cartelle cliniche siano conservate illimitatamente. Secondo le norme vigenti, inoltre, gli originali cartacei delle cartelle cliniche in quanto originali unici, non possono essere distrutti;
- **Circolare Ministero della Sanità 19 dicembre 1986**, n. 61 - Circolare avente per oggetto il periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura
- **DM 14.2.1997** - Norma di attuazione del D.lgs n.230/95, "Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche, ai sensi dell'art. 111, comma 10, del decreto legislativo 17 marzo 1995, n. 230"
- **D.lgs 26 maggio 2000**, n. 187 - Attuazione della direttiva 97/43/Euratom in materia di protezione sanitaria delle persone contro i pericoli delle radiazioni ionizzanti connesse ad esposizioni mediche
- **Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere, 2005**
Atto di indirizzo che reca indicazioni sui tempi di conservazione dei documenti generati e/o custoditi Aziende Sanitarie pubbliche ed accreditate, redatto dal Ministero per i Beni e la Attività Culturali
- **Consiglio dei Ministri – Conferenza Stato Regioni 02 Marzo 2012** - Linee Guida per la dematerializzazione della documentazione clinica in diagnostica per immagini. Normativa e prassi.

[Torna al sommario](#)

3.2 Standard di riferimento

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

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- **Dicom 3.0** (Digital Imaging and Communications in Medicine, immagini e comunicazione digitali in medicina)
- **Health Level 7 (HL7)** versione 2.3.1 e 2.5
- Integrating the Healthcare Enterprise (IHE)
- **UNI ISO 15489-1: 2006** Information and documentation -- Records management -- Part 1: General
- **UNI ISO 15489-2: 2007** Information and documentation—Records management. Part 2: Guidelines
- **ISO 9001:2015** – Quality management systems – Requirements;

[Torna al sommario](#)

4 Ruoli e responsabilità

Nel sistema di conservazione si individuano i seguenti ruoli principali:

Ruolo	Organizzazione di appartenenza
Produttore	Cliente
Responsabile della conservazione	Cliente
Referenti del Cliente	Cliente
Responsabile del servizio di conservazione	ARUBA
Utente	Cliente/Terzi autorizzati

ARUBA, quale **Responsabile del servizio di conservazione** digitale dei documenti informatici del Cliente, agisce nei limiti dell'affidamento conferito 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 del Responsabile del servizio di conservazione, 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 opera 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 in materia.

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.

[Torna al sommario](#)

4.1 Profili professionali all'interno della struttura organizzativa ARUBA

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 processo di conservazione, prevede, le seguenti **figure responsabili** :

1. Responsabile del servizio di conservazione;
2. Responsabile della funzione archivistica di conservazione;
3. Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)
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

Qui di seguito si riportano le **attività associate a ciascuna delle figure sopra elencate**:

- **Responsabile del servizio di conservazione**

Le attività affidate dal Responsabile della conservazione con l'Atto di Affidamento.

- **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.

- **Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)**

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.

In particolare tenuto a:

- a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni relative alla protezione dei dati;
- b) sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento UE 2016/679;
- d) cooperare con l'autorità di controllo; e
- e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al

trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

- **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.

- **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 il fornitore e 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.

- **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.

Ciascuno dei responsabili sopra elencati può avvalersi, per lo svolgimento delle attività al medesimo 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.

[Torna al sommario](#)

Ruoli e responsabilità					
Ruolo	Cognome	Nome	Responsabilità	Data nomina	Data cessazione
Responsabile del servizio di conservazione	Sassetti	Andrea	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.	04/01/2019	
	Braccagni	Simone	<i>Come sopra</i>	01/09/2014	03/01/2019
Responsabile della funzione archivistica di conservazione	Boschi	Serena	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	

Responsabile del trattamento dei dati personali, ora Responsabile della protezione dei dati personali (DPO)	Giommoni	Roberta	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. In particolare tenuto a: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni relative alla protezione dei dati; b) sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento UE 2016/679; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.	24/05/2018	
Responsabile del trattamento dei dati personali	Braccagni	Simone	<i>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.</i>	01/09/2014	23/05/2018
Responsabile della sicurezza dei sistemi per la conservazione	Corsi	Matteo	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.	06/09/2017	
	Santoni	Adriano	<i>Come sopra</i>	01/09/2014	05/09/2017
Responsabile dei sistemi informativi per la conservazione	Gaverini	Angelo	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il fornitore; 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.	06/09/2017	
	Ravazza	Roberto	<i>Come sopra</i>	01/09/2014	05/09/2017

Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Mauro	Manetti	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.	06/09/2017	
	<i>Pulvirenti</i>	<i>Salvatore</i>	<i>Come sopra</i>	<i>01/09/2014</i>	<i>05/09/2017</i>

[Torna al sommario](#)

5 Struttura organizzativa per il servizio di conservazione

In questo capitolo sono indicate le strutture organizzative coinvolte nel servizio di conservazione comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione

[Torna al sommario](#)

5.1 Organigramma

La figura in basso riporta le strutture organizzative coinvolte nel servizio di conservazione:

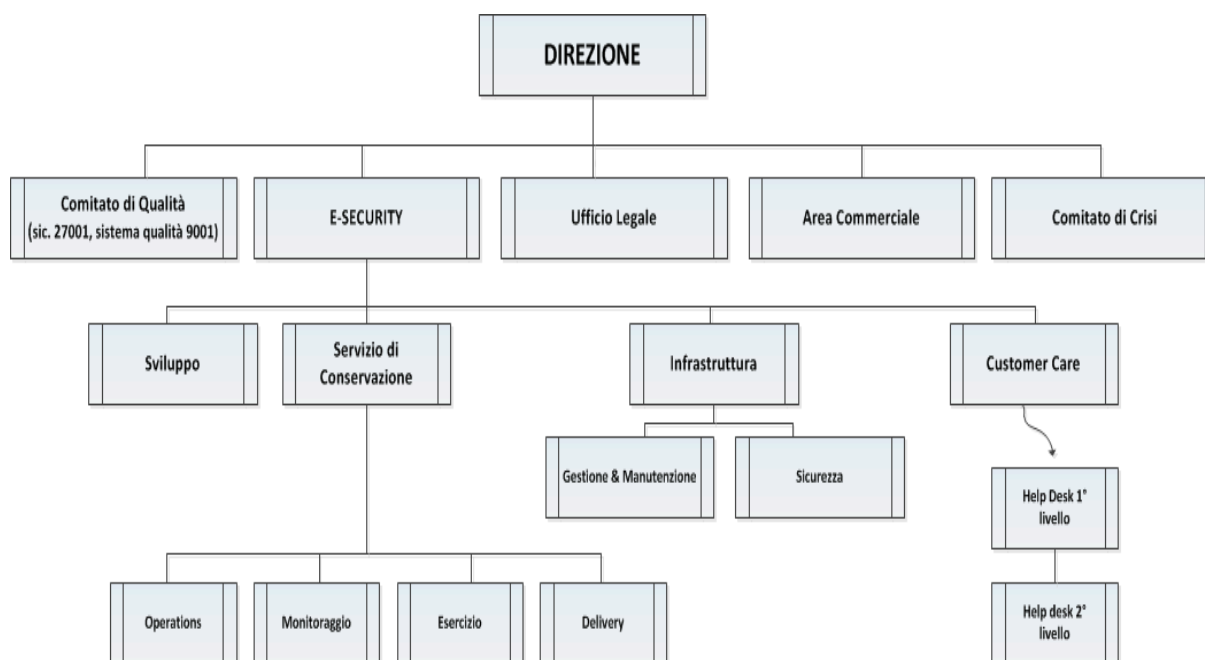


Figura 1: Rappresentazione delle strutture organizzative coinvolte nel servizio di conservazione

[Torna al sommario](#)

5.2 Strutture organizzative

Nello specifico le strutture funzionali dell'organizzazione operano in sinergia come segue:

- **Direzione**
 - ✓ la Direzione Aziendale garantisce la continuità generale dell'organizzazione
- **Comitato di Qualità**
 - ✓ garantisce la qualità operativa dei servizi ed il miglioramento di processi/procedure
- **E-Security**
 - ✓ rappresenta la Business Line che si occupa dei servizi e soluzioni di sicurezza in ambito digitale
- **Ufficio legale e Compliance**
 - ✓ garantisce la verifica periodica di conformità a normativa e standard di riferimento
- **Area Commerciale**
 - ✓ promuove il servizio di conservazione ai clienti
 - ✓ fornisce il supporto ai clienti in fase di prevendita (pre-sales)
 - ✓ partecipa attivamente al miglioramento dei servizi erogati in termini di definizione dell'offerta

- **Infrastruttura**
 - ✓ garantisce la sicurezza degli accessi logici e fisici, predisponendo appositi asset nel perimetro del data center
 - ✓ garantisce la sicurezza dell'infrastruttura tramite sistemi dedicati (video-sorveglianza, anti-intrusione, anti-incendio, etc)
 - ✓ designa, gestisce e provvede alla manutenzione delle aree sicure
- **Sviluppo**
 - ✓ fornisce know-how e supporto per lo sviluppo dei sistemi informativi
 - ✓ provvede alla progettazione di nuovi servizi e fornisce supporto per la manutenzione dei servizi attivi
 - ✓ si occupa dello studio di fattibilità per l'implementazione di nuovi servizi
 - ✓ fornisce interventi di analisi ed attività di assistenza nella fase di pre-vendita dei servizi
- **Servizio di Conservazione**
 - ✓ garantisce la gestione degli asset (hardware e software), occupandosi dell'intero processo di supply-chain del servizio di conservazione
 - ✓ provvede alla gestione delle informazioni, per l'intero ciclo di vita (dalla classificazione, al monitoraggio del sistema, fino alla protezione dei log)
 - ✓ si occupa della manutenzione ed assistenza, a garanzia della continuità operativa del servizio di conservazione
 - ✓ garantisce l'esecuzione del processo di conservazione in conformità ai requisiti tecnici normativi
 - ✓ provvede alla gestione operativa degli accessi logici e fisici, seguendo apposite procedure e mantenendo aggiornata la documentazione
 - ✓ garantisce l'attivazione e consegna dei servizi ai clienti, rispettando KPI e SLA concordati
- **Customer Care**
 - ✓ provvede all'assistenza tecnica rivolta ai clienti proprietari dei servizi
 - ✓ fornisce il supporto operativo sui servizi dei clienti
 - ✓ partecipa al miglioramento dei processi di comunicazione verso i clienti

[Torna al sommario](#)

5.3 Responsabilità e funzioni nel processo di conservazione

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

Fasi del processo	Descrizione delle fasi del processo di conservazione		COMPITI	RESPONSABILITÀ	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 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	SC	RMGO	==
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. Pacchetto di Archiviazione)				

	Descrizione sintetica	Il sistema genera il Pacchetto di Archiviazione secondo le modalità descritte al cap. 7	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 di Conservazione, 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 raccogliergli 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 DPO	==

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
- **DPO** - responsabile della protezione dei dati personali
- **RSC** - responsabile del servizio di conservazione
- **SC** - Sistema di conservazione

[Torna al sommario](#)

6 Oggetti sottoposti a conservazione

6.1 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 è impostato per accettare le seguenti tipologie di documento:

- **documenti informatici** sono la "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" come definito dal Codice dell'Amministrazione Digitale;
- **documenti amministrativi** costituenti atti amministrativi con rilevanza interna al procedimento amministrativo;
- **documenti rilevanti ai fini tributari** come stabilito nel DM del MEF del 17 giugno 2014;
- **documenti clinici** che possono contenere informazioni su osservazioni cliniche dirette, quali rivelazioni di anamnesi, segni vitali o sintomi, osservazioni indirette, derivanti, ad esempio da diagnostica strumentale, esami di laboratorio o rappresentazione iconografica di resoconti radiologici, oppure opinioni mediche quali valutazioni di osservazioni cliniche, consulti e consulenze, obiettivi da raggiungere o piani diagnostico terapeutici, azioni di natura clinico-sanitaria atte a generare osservazioni cliniche ed opinioni mediche;
- **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*.

[Torna al sommario](#)

6.2 Copie informatiche di documenti analogici originali unici

Come noto, l'art. 22 del CAD stabilisce che:

- a) (comma 2) le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e

asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.

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

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

In particolare, sarà cura e carico del Cliente:

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

successivamente:

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

oppure

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

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

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

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

oppure

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

[Torna al sommario](#)

6.3 Formati gestiti

Come noto, la leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato. Il formato di un documento informatico è la convenzione usata per rappresentare il contenuto informativo mediante una sequenza di byte.

Il sistema di conservazione ARUBA garantisce la conservazione dei documenti prodotti nei formati previsti dall'allegato 2 "Formati" del DPCM 03-12-2013.

I formati ammessi alla conservazione, devono essere specificati dal Cliente prima del versamento in conservazione e per tale ragione vengono esplicitati all'interno di uno specifico allegato, facente parte del Contratto di servizio stipulato con ARUBA (come descritto al par 10.1.2).

[Torna al sommario](#)

6.3.1 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.

[Torna al sommario](#)

6.3.2 Formati consigliati 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 immutabilità e staticità.

Pertanto, alla luce delle suddette considerazioni, i formati indicati dalla normativa per la conservazione delle diverse tipologie di documenti informatici sono i seguenti:

FORMATO	DESCRIZIONE	
PDF - 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 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
	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	
TIFF	Il TIFF è un formato utilizzato per la rappresentazione delle immagini mediante grafica raster (l'immagine digitale è formata da un insieme pixel, ordinate secondo linee e colonne).	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Immagini
	Sviluppato da	Aldus Corporation in seguito acquistata da Adobe
	Estensioni	.tif
	Tipo MIME	image/tiff
	Formato aperto	NO
	Specifiche tecniche	Pubbliche
	Ultime versioni	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
	Standard	ISO 12639 (TIFF/IT) ISO 12234 (TIFF/EP)
	Altre caratteristiche	Formato immagine raster, in versione non compressa o compressa senza perdita di informazione
		Formato utilizzato per la conversione in digitale di documenti cartacei
		Esistono parecchie versioni, alcune delle quali proprietarie (che ai fini della conservazione nel lungo periodo sarebbe bene evitare)
In genere le specifiche sono pubbliche e non soggette ad alcuna forma di limitazione		
Software necessario alla visualizzazione	ImageGlass	

FORMATO	DESCRIZIONE
JPG	Il JPG è un formato utilizzato per la rappresentazione delle immagini mediante grafica raster (l'immagine digitale è formata da un insieme pixel, ordinate secondo linee e colonne).
	Caratteristiche e dati informativi

Informazioni gestibili	Immagini
Sviluppato da	Joint Photographic Experts Group
Estensioni	.jpg, .jpeg
Tipo MIME	image/jpeg
Formato aperto	SI
Specifiche tecniche	Pubbliche
Ultima versione	2009
Standard	ISO/IEC 10918:1
Altre caratteristiche	Formato immagine raster, in versione compressa. Può comportare una perdita di qualità dell'immagine originale. JPG è il formato più utilizzato per la memorizzazione di fotografie ed è quello più comune su World Wide Web. Lo stesso gruppo che ha ideato il JPG ha prodotto il JPEG 2000 con estensione .jp2 (ISO/IEC 15444-1) che può utilizzare la compressione senza perdita di informazione. Il formato JPEG 2000 consente, inoltre, di associare metadati ad un'immagine. Nonostante queste caratteristiche la sua diffusione è tutt'oggi relativa.
Software necessario alla visualizzazione	ImageGlass

FORMATO	DESCRIZIONE
Office Open XML (OOXML)	Office Open XML, comunemente abbreviato in OOXML, è un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database.
	Caratteristiche e dati informativi
	Informazioni gestibili
	Documenti di testo, fogli di calcolo, presentazioni, grafici e database
	Sviluppato da
	Microsoft
	Estensioni principali
	.docx, .xlsx, .pptx
	Tipo MIME
	<i>application/vnd.openxmlformats-officedocument.wordprocessingml.document,application/x-tika-ooxml,application/zip</i> <i>application/vnd.ms-powerpoint,application/vnd.openxmlformats-officedocument.presentationml.template,application/vnd.ms-powerpoint.addin.macroEnabled.12,application/vnd.ms-powerpoint.presentation.macroEnabled.12,application/vnd.ms-powerpoint.template.macroEnabled.12,application/vnd.ms-powerpoint.slideshow.macroEnabled.12</i> <i>application/vnd.ms-excel,application/vnd.openxmlformats-officedocument.spreadsheetml.template,application/vnd.ms-excel.sheet.macroEnabled.12,application/vnd.ms-excel.template.macroEnabled.12,application/vnd.ms-excel.addin.macroEnabled.12,application/vnd.ms-excel.sheet.binary.macroEnabled.12,application/x-tika-msoffice</i> <i>application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,application/x-tika-ooxml</i>
	Formato aperto
	SI
	Specifiche tecniche
	Pubblicate da Microsoft dal 2007
	Ultima versione
	1.1
	Standard
	ISO/IEC DIS 29500:2008
	Altre caratteristiche
	Open XML è adottato dalla versione 2007 della suite Office di Microsoft MS Office 2007 legge e scrive file conformi a ECMA-376 Edition 1 MS Office 2010 legge e scrive file conformi a ISO/IEC 29500:2008 transitional (norme transitorie) e legge file conformi a ISO/IEC 29500:2008 strict (indicazioni fondamentali) Documenti conformi ad ISO/IEC 29500:2008 strict sono supportati da diversi prodotti informatici disponibili sul mercato

		Il formato Office Open XML dispone di alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML.
		I metadati associabili ad un documento che adotta tale formato sono previsti dallo standard ISO 29500:2008
	Software necessario alla visualizzazione	https://openxmlviewer.codeplex.com/

FORMATO	DESCRIZIONE																				
Open Document Format	ODF (Open Document Format, spesso referenziato con il termine OpenDocument) è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni. Caratteristiche e dati informativi <table> <tr> <td>Informazioni gestibili</td><td>Documenti di testo, fogli di calcolo, presentazioni e grafici.</td></tr> <tr> <td>Sviluppato da</td><td>OASIS</td></tr> <tr> <td>Estensioni principali</td><td>.ods, .odp, .odg, .odb</td></tr> <tr> <td>Tipo MIME</td><td>application/vnd.oasis.opendocument.text</td></tr> <tr> <td>Formato aperto</td><td>SI</td></tr> <tr> <td>Specifiche tecniche</td><td>Pubblicate da OASIS dal 2005</td></tr> <tr> <td>Ultima versione</td><td>1.0</td></tr> <tr> <td>Standard</td><td>ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300</td></tr> <tr> <td>Altre caratteristiche</td><td> Formato basato sul linguaggio XML Un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione Lo standard ISO/IEC IS 26300:2006 è ampiamente usato come standard documentale nativo, oltre che da OpenOffice.org, da una ampia serie di altri prodotti disponibili sulle principali piattaforme: Windows, Linux, Mac. È stato adottato come standard di riferimento da moltissime organizzazioni governative e da diversi governi ed ha una "penetrazione" di mercato che cresce giorno per giorno. </td></tr> <tr> <td>Software necessario alla visualizzazione</td><td>Open Office</td></tr> </table>	Informazioni gestibili	Documenti di testo, fogli di calcolo, presentazioni e grafici.	Sviluppato da	OASIS	Estensioni principali	.ods, .odp, .odg, .odb	Tipo MIME	application/vnd.oasis.opendocument.text	Formato aperto	SI	Specifiche tecniche	Pubblicate da OASIS dal 2005	Ultima versione	1.0	Standard	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300	Altre caratteristiche	Formato basato sul linguaggio XML Un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione Lo standard ISO/IEC IS 26300:2006 è ampiamente usato come standard documentale nativo, oltre che da OpenOffice.org, da una ampia serie di altri prodotti disponibili sulle principali piattaforme: Windows, Linux, Mac. È stato adottato come standard di riferimento da moltissime organizzazioni governative e da diversi governi ed ha una "penetrazione" di mercato che cresce giorno per giorno.	Software necessario alla visualizzazione	Open Office
Informazioni gestibili	Documenti di testo, fogli di calcolo, presentazioni e grafici.																				
Sviluppato da	OASIS																				
Estensioni principali	.ods, .odp, .odg, .odb																				
Tipo MIME	application/vnd.oasis.opendocument.text																				
Formato aperto	SI																				
Specifiche tecniche	Pubblicate da OASIS dal 2005																				
Ultima versione	1.0																				
Standard	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300																				
Altre caratteristiche	Formato basato sul linguaggio XML Un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione Lo standard ISO/IEC IS 26300:2006 è ampiamente usato come standard documentale nativo, oltre che da OpenOffice.org, da una ampia serie di altri prodotti disponibili sulle principali piattaforme: Windows, Linux, Mac. È stato adottato come standard di riferimento da moltissime organizzazioni governative e da diversi governi ed ha una "penetrazione" di mercato che cresce giorno per giorno.																				
Software necessario alla visualizzazione	Open Office																				

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 <table> <tr> <td>Informazioni gestibili</td><td>Contenuto di evidenze informatiche, dei pacchetti di versamento, archiviazione e distribuzione, ecc.</td></tr> <tr> <td>Sviluppato da</td><td>W3C - http://www.w3.org/</td></tr> <tr> <td>Estensione</td><td>.xml</td></tr> <tr> <td>Tipo MIME</td><td>Application/xml Text/xml</td></tr> <tr> <td>Formato aperto</td><td>SI</td></tr> <tr> <td>Specifiche tecniche</td><td>Pubblicate da W3C - http://www.w3.org/XML/</td></tr> <tr> <td>Altre caratteristiche</td><td>Formato di testo flessibile derivato da SGML (ISO 8879).</td></tr> <tr> <td>Software necessario alla visualizzazione</td><td>Qualsiasi editor di testo. Inoltre è possibile, concordando con il Cliente le caratteristiche di un opportuno file xslt, produrre una copia human readable con Microsoft Internet Explorer / Firefox / Google Chrome o altri browser</td></tr> </table>	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	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, produrre una copia human readable con Microsoft Internet Explorer / Firefox / Google Chrome o altri browser
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	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, produrre una copia human readable con Microsoft Internet Explorer / Firefox / Google Chrome o altri browser																

FORMATO	DESCRIZIONE
---------	-------------

TXT	File di testo semplice, non strutturato, è adatto a contenuti puramente testuali e non richiede particolari possibilità di strutturazione o informazioni aggiuntive sulla struttura o la formattazione. Non contiene quindi indicazioni di formattazione nascoste o visibili (p. es. grassetto, rientri, colori ecc.) o indicazioni strutturali (p. es. titoli, sezioni, sottosezioni, indice ecc.). Questi file molto semplici offrono, sul lungo periodo, ottime garanzie per la conservazione e leggibilità dei dati.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Testo
	Estensione	.txt
	Tipo MIME	text/plain
	Formato aperto	SI
	Specifiche tecniche	Pubbliche
	Standard	ISO 646 RFC 3629 ISO/ IEC 10646
	Altre caratteristiche	Sono ammessi i seguenti set di caratteri: • US-ASCII; • ISO 8859-1 e 8859-15 (Latin-1 e Latin-9); • Unicode (UTF-8, UTF-16) Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata.
	Software necessario alla visualizzazione	Notepad++

FORMATO	DESCRIZIONE
EML	Electronic Mail Message (EML) è un formato di testo che definisce la sintassi di messaggi di posta elettronica scambiati tra utenti
	Caratteristiche e dati informativi
	Informazioni gestibili Messaggi di posta elettronica e PEC
	Sviluppato da Internet Engineering Task Force (IETF) - 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".

[Torna al sommario](#)

6.3.3 Identificazione

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

1. l'estensione: una serie di lettere, unita al nome del file attraverso un punto, ad esempio [nome del file].doc identifica un formato sviluppato dalla Microsoft;
2. il magic number: i primi byte presenti nella sequenza binaria del file, ad esempio 0xffd8 identifica i file immagine di tipo .jpeg;
3. verifica della corrispondenza tra il tipo MIME ricavato dall'estensione del file ed il tipo MIME ricavato dal magic number;
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 restituisce 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

[Torna al sommario](#)

6.4 Metadati da associare alle diverse tipologie di documenti

Con il termine "metadati" si indicano tutte le informazioni significative associate al documento informatico, escluse quelle che costituiscono il contenuto del documento stesso. I metadati riguardano principalmente, ma non esclusivamente, i modi, i tempi ed i soggetti coinvolti nel processo della formazione del documento informatico, della sua gestione e della sua conservazione.

Metadati sono anche le informazioni riguardanti gli autori, gli eventuali sottoscrittori e le modalità di sottoscrizione e la classificazione del documento. I metadati devono essere associati al documento dal Cliente prima del versamento in conservazione e per tale ragione vengono esplicitati all'interno di uno specifico allegato, facente parte del Contratto di servizio stipulato con ARUBA (come specificato al par 10.1.2).

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.

Oltre al set minimo di metadati, il Cliente potrà decidere di associare al documento informatico eventuali ulteriori metadati c.d. "*extrainfo*". Le extra info verranno inserite, al pari degli altri metadati, nell'indice di conservazione che. 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.

[Torna al sommario](#)

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

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

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

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

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

[Torna al sommario](#)

6.6 Pacchetto di versamento

In questo paragrafo sono fornite le tipologie di pacchetto di versamento gestite e per ciascuna di esse descritta la struttura dati.

Il nostro standard prevede l'indice di un pacchetto di versamento che si caratterizza per le seguenti parti:

- area di identificazione del PDV
- area di identificazione dei documenti costituenti il pacchetto e composta dai seguenti elementi:

- metadato obbligatori
- metadati extra-info

Nella prima parte il dato importante e obbligatorio è il *pdvid* 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
- algoritmo di hashing per la generazione dell'impronta
- impronta del documento

Inoltre, poiché il sistema deve controllare la tipologia 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 dei singoli documenti del pacchetto e la data di chiusura degli stessi.

L'ultima parte dell'Indice contiene un insieme di metadati extra-info, così come definiti in fase contrattuale col Produttore
[Torna al sommario](#)

6.6.1 Specifiche Pacchetto di Versamento

Le specifiche del Pacchetto di Versamento secondo lo standard definito da ARUBA, sono disponibili all'interno di specifiche sezioni pubblicate sui siti web www.pec.it e guide.pec.it.

[Torna al sommario](#)

6.7 Pacchetto di Archiviazione

In questo paragrafo viene resa la struttura del Pacchetto di Archiviazione nonché il trattamento dei pacchetti di archiviazione.

[Torna al sommario](#)

6.7.1 Specifiche Pacchetto di Archiviazione

Il Pacchetto di Archiviazione è composto da varie parti:

- l'insieme degli elementi (documenti e/o altri PdA) che compongono il pacchetto
- l'Indice del Pacchetto di Archiviazione (IPdA) che elenca tutti gli elementi del pacchetto. Il formato dell'indice è aderente allo standard UNI SInCRO (nel quale è indicato come IdC – Indice di Conservazione) ed è marcato temporalmente e firmato elettronicamente con certificato del Responsabile del Sistema di Conservazione.

[Torna al sommario](#)

6.8 Pacchetto di Distribuzione

Il Pacchetto di Distribuzione contiene l'insieme degli elementi (documenti e/o PdA) precedentemente ricercati e selezionati dall'utente.

Viene offerto sotto forma di un archivio .zip che per ogni elemento contiene:

- una cartella contenente l'elemento stesso. Nel caso di un documento il documento stesso, nel caso di un PdA l'intero PdA, ovvero tutti gli elementi di cui è costituito
- un'altra cartella che contiene l'indice relativo all'elemento individuato, marcato temporalmente e firmato elettronicamente con certificato del Responsabile del Sistema di Conservazione

[Torna al sommario](#)

6.9 Documenti rilevanti ai fini delle disposizioni tributarie

In considerazione di quanto previsto dall'art. 21, co. 5, del CAD¹, 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 devono essere conservati in modo tale da rispettare le norme del codice civile, le disposizioni del codice dell'amministrazione digitale e delle relative regole tecniche e le altre norme tributarie riguardanti la corretta tenuta della contabilità, il Cliente deve farsi carico di versare in conservazione i propri documenti informatici assicurando, ove necessario e/o previsto dalle norme e/o dai principi contabili nazionali, l'ordine cronologico dei medesimi e senza che vi sia soluzione di continuità in relazione a ciascun periodo d'imposta o anno solare.

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

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

Funzioni di ricerca

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

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

¹ 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.”;

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.

[Torna al sommario](#)

6.9.1 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.

[Torna al sommario](#)

6.10 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.

[Torna al sommario](#)

7 Il processo di conservazione

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

[Torna al sommario](#)

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

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 metadati che li specializzano, così come già accennato precedentemente.

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
- 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 FTPS

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 prende in carico 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.

Poiché 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 servizio di Conservazione.

[Torna al sommario](#)

7.1.1 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 nel paragrafo 6.6.1.

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
- 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

[Torna al sommario](#)

7.1.2 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 due: 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 SHA256 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.

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 servizio di Conservazione.

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

[Torna al sommario](#)

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

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 è distinto per ciascun pacchetto 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 Il sistema verifica se il PdV (che contiene lo stesso ID) non sia già stato conservato. In questo caso il sistema considera il nuovo indice in sostituzione del precedente. Viene invece scartato qualora il PdV risulta essere in stato 'conservato'.
3.02	viene verificato che l'identificativo specificato nel PdV non sia già presente nel sistema di conservazione	
3.04	viene effettuato un controllo semantico sui metadati presenti nell'indice del PdV	
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)

ID	Oggetto del controllo	Azione in caso di check negativo
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: • Controllo di conformità. • Controllo Crittografico. • Controllo Catena Trusted. • Controllo Certificato. • 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 è 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
1.04	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 è quello atteso
1.05	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
1.06	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

Le eventuali anomalie e/o scarti riscontrate durante le verifiche effettuate sull'indice del pacchetto di versamento e documenti contenuti al suo interno, saranno comunicate via PEC sia al responsabile della conservazione indicato dal cliente (nel contratto di servizio) che all'utente che ha effettuato l'operazione di versamento.

Tali comunicazioni saranno conservate all'interno del sistema di posta per tutta la durata del contratto sottoscritto dal cliente.

[Torna al sommario](#)

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

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 nel paragrafo successivo (par. 7.3.1).

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:
 - o id univoco, come indicato nell'IPdV
 - o id univoco fornito dal sistema di conservazione
 - o hash
 - o data di ricezione
 - o esito della ricezione (accettato o warning)
 - o descrizione warning, ove necessario

[Torna al sommario](#)

7.3.1 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 Versamento
- 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.

[Torna al sommario](#)

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Per la gestione dei rifiuti dei pacchetti di versamento e modalità di comunicazione delle anomalie si rimanda al par. 7.2.

[Torna al sommario](#)

7.5 Preparazione e gestione del Pacchetto di Archiviazione

Il Pacchetto di Archiviazione (PdA) è quello conservato dal sistema di conservazione e possiede un insieme completo di metadati utili alla conservazione a lungo termine.

Il Pacchetto di Archiviazione viene realizzato secondo lo standard di riferimento SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che rappresenta lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Uno più pacchetti di versamento vengono trasformati in un Pacchetto di Archiviazione (PdA) in base alle regole tecniche standard del sistema conservazione previste e agli accordi contrattuali.

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 legata 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.

È 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

[Torna al sommario](#)

7.5.1 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.

[Torna al sommario](#)

7.5.2 Gestione dei Pacchetti di Archiviazione non validi o non completi

Nel caso di versamento di un PdA che non viene completato entro 4 ore dalla sua creazione, il sistema invia una email al Responsabile della Conservazione per avvertire l'utente e chiedere il completamento o la modifica del PdA.

Qualora il PdA non venga completato entro 7 giorni dalla sua creazione, il sistema provvederà a:

- a) Rimuovere i PdV incompleti presenti nel PdA e/o documenti non collegati a nessun IPdV;
- b) Conservare il PdA con i soli PdV completi e validi (con conseguente RdC);
- c) Eliminare l'intero PdA nel caso in cui non contenga alcun PdV valido;
- d) Inviare una mail di notifica all'utente dell'avvenuta cancellazione dei PdV incompleti ed eventuale conservazione del PdA con i soli PdV validi e completi;
- e) Registrare sui log il dettaglio di tutte le operazioni e dei file cancellati.

[Torna al sommario](#)

7.5.3 Rettifica dei pacchetti di archiviazione

Il sistema di conservazione prevede la possibilità di eseguire la rettifica del pacchetto di archiviazione, inviando un documento successivo rispetto a quello inviato in precedenza in conservazione. Tale operazione, riservata solamente al produttore o titolare con diritti di scrittura sulla classe documentale relativa, permette al cliente di sostituire un documento inviato in conservazione con un nuovo documento dello stesso tipo, lasciandone invariati i metadati.

Il cliente, una volta indicato il PDA sul quale applicare la rettifica, potrà procedere alla sostituzione di uno o più documenti ed inserire la motivazione relativa all'operazione. Il documento sarà sottoposto ai medesimi controlli di verifica previsti dal processo di conservazione sui documenti originariamente inviati al servizio di conservazione. Una volta sostituiti i documenti, il sistema mostrerà a video l'esito della rettifica: in caso di errori riscontrati, verrà indicato per ciascun documento la tipologia di errore, permettendo al cliente di apportare le modifiche necessarie per concludere l'operazione, altrimenti sarà confermato l'esito positivo della rettifica.

Il PDA rettificato conterrà l'IPdV ed i documenti modificati, mentre il PDA originale rimarrà a disposizione sul sistema di conservazione nel PDD e consultabile dal cliente in qualsiasi momento.

Le operazioni di rettifica verranno registrate nei log di sistema.

[Torna al sommario](#)

7.6 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione

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:

- I file/documenti richiesti così come sono stati archiviati dal sistema al momento della messa in conservazione
- Indici dei Pacchetti di Archiviazione, marcati temporalmente e firmati come all'origine, con cui sono stati conservati i documenti richiesti. Al loro interno sono contenuti tutti i metadati di tutti i documenti messi in conservazione nello stesso PdA

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.

La richiesta di produzione di un PdD implica l'invio di una comunicazione via PEC all'utente finale e altri destinatari eventualmente comunicati dal cliente nel contratto di servizio. Le comunicazioni via PEC, relative alle ricevute di invio e consegna, vengono conservate al fine di tracciare l'intera trasmissione.

La richiesta di esibizione può avvenire da due tra i canali messi a disposizione: interfaccia web e web service.

In entrambi i casi il flusso di selezione dei documenti da esibire è il medesimo:

1. ricerca dei documenti attraverso opportuni filtri
2. selezione e spostamento dei riferimenti dei documenti individuati all'interno di un area di lavoro
3. richiesta di esibizione a partire dai documenti nell'area di lavoro
4. produzione del link di download da cui scaricare il Pacchetto di Distribuzione

La ricerca dei documenti avviene tramite la selezione di filtri sui metadati. Una volta individuata la classe documentale di interesse l'utente può effettuare le ricerche inserendo i valori su cui filtrare per uno o più metadati di riferimento.

La ricerca contemporanea su più metadati implica un filtro più forte, ovvero una restrizione del numero dei documenti risultanti.

Inoltre è possibile effettuare una ricerca tra documenti di classi documentali differenti ma che sono accomunati per un particolare metadato.

Se ad esempio si volessero cercare tutti i documenti afferenti a un determinato numero pratica, dotando classi documentali di tipo differente dello stesso metadato "numero pratica" è possibile effettuare una ricerca di questo tipo.

Tutti i documenti di interesse risultanti dalle ricerche vengono quindi spostati in un'area di lavoro. Finita l'operazione di selezione l'utente può ulteriormente chiedere di esibire solo una parte dei documenti messi nell'area di lavoro.

Il Pacchetto di Distribuzione risultante dalla richiesta di esibizione contiene:

- i documenti da esibire
- gli indici dei PdA, marcati temporalmente e firmati elettronicamente così come al momento della conservazione, del flusso di conservazione relativo ai documenti scelti

Nel caso in cui tra i documenti figurino interi PdA, il Pacchetto di Distribuzione contiene tutti i documenti che lo compongono.

[Torna al sommario](#)

7.6.1 Attività conseguenti alla cessazione del contratto

In tutti i casi di cessazione del rapporto contrattuale, ARUBA consente al Cliente, nei termini previsti dalle Condizioni di

fornitura, il recupero dei propri documenti.

Non incombe su ARUBA alcun obbligo di provvedere alla materiale restituzione dei documenti informatici conservati, dal momento che l'attività di recupero dovrà essere effettuata dal Cliente con le modalità descritte di seguito:

1. Accedendo al sistema, il Cliente effettua esplicita richiesta di chiusura dell'intero Archivio
2. Il sistema in automatico genera il Pacchetto di Distribuzione contenente tutte le evidenze dei PdA (Pacchetti di Archiviazione) conservati.
3. Il Cliente riceve comunicazione via mail PEC del buon esito della procedura
4. Il Cliente, da sistema, richiede la produzione del Pacchetto di Distribuzione relativo all'intero archivio
5. Entro i termini stabiliti da contratto, il sistema rende disponibile il Pacchetto di Distribuzione che potrà essere scaricato dal cliente

[Torna al sommario](#)

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

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

[Torna al sommario](#)

7.7.1 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 inviata all'utente che ne ha fatto richiesta.

[Torna al sommario](#)

7.7.2 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.

[Torna al sommario](#)

7.7.3 Produzione copie o duplicati su supporti rimovibili

In caso di richiesta di produzione di copie o duplicati su supporto rimovibile, viene prodotto un insieme di DVD (o altro supporto), ognuno autoconsistente, e consegnati al responsabile della conservazione che ne ha fatto richiesta.

Il processo prevede l'uso di un apposito applicativo che permette la generazione di immagini complete o parziali degli archivi di conservazione che poi vengono riversate su supporto ottico da un operatore. Il software richiede in input l'identificativo dell'archivio di conservazione, le classi documentali desiderate e il periodo temporale coinvolto. L'output generato è dato dal contenuto selezionato dagli archivi di conservazione, lottizzato in pacchetti di dimensione compatibile alla capienza del supporto ottico. I supporti creati vengono etichettati con una codifica generata automaticamente che in nessun modo riporta informazioni sul contenuto.

In ogni singolo pacchetto sono presenti i documenti protetti con crittazione e il software di ricerca e accesso. Il software di ricerca e accesso permette previo inserimento di una password da parte dell'utente, di poter visionare l'indice di quanto contenuto nei pacchetti prodotti, eseguire ricerche su metadati e decriptare e visionare i singoli documenti. Qualora il cliente desiderasse anche l'evidenza della conservazione verrà consentito lo scarico, ovviamente decriptando in linea, del documento con il relativo Indice di Conservazione e tutte le evidenze necessarie.

La protezione dei documenti è quindi ottenuta tramite crittazione con un certificato pubblico, generato allo scopo. La decriptazione è eseguita tramite la chiave privata, abbinata al certificato, rilasciata col software di ricerca e accesso, e un PIN che viene recapitato a mezzo telematico al responsabile della conservazione. Insieme al PIN viene anche recapitata una descrizione del contenuto di ogni supporto: codice del supporto, evidente sull'etichetta dello stesso, archivio, classi documentali data conservazione primo Pacchetto di Archiviazione, data conservazione ultimo Pacchetto di Conservazione.

[Torna al sommario](#)

7.7.4 Intervento 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.

[Torna al sommario](#)

7.8 Scarto dei pacchetti di archiviazione

7.8.1 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.

[Torna al sommario](#)

7.8.2 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.

[Torna al sommario](#)

7.8.3 Richiesta di scarto immediato

I clienti possono richiedere ad ARUBA lo scarto di alcuni Pacchetti di Archiviazione dal sistema di conservazione. Fermo quanto definito nel precedente paragrafo, riguardante il rispetto della normativa vigente in materia, il Responsabile della Conservazione potrà, previa compilazione della modulistica messa a disposizione da ARUBA, richiedere lo scarto di uno o più PdA.

Il richiedente dovrà indicare nel modulo i riferimenti all'archivio ed ai pacchetti di archiviazione che intende scartare, unitamente alle motivazioni dello scarto ed alla conferma di disporre di tutte le autorizzazioni necessarie per l'operazione.

Il modulo dovrà essere accompagnato da firma valida ed inviato tramite email all'indirizzo pec scarto@docfly.it.

Le operazioni di scarto verranno registrate nei log di sistema.

[Torna al sommario](#)

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

In analogia allo standard SInCRO, la struttura prevista per il PdV prevede una specifica al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, la struttura dell'Indice di Conservazione 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 servizio 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.

[Torna al sommario](#)

7.10 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	Il sistema si mette in attesa dei documenti del PdV

	sintetica	
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 servizio 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. Pacchetto di Archiviazione)	
	Descrizione sintetica	Il Pacchetto di Archiviazione 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 Pacchetto di Archiviazione 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 servizio di Conservazione o di un suo delegato, per garantirne l'immodificabilità. Con la suddetta firma apposta in calce al Pacchetto di Archiviazione 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 raccogliergli il consenso	
	Descrizione sintetica	Alla scadenza dei termini di conservazione, il cliente in autonomia può decidere di cancellare i documenti in conservazione.

[Torna al sommario](#)

7.11 Audit Log

Il sistema di conservazione registra per ogni evento rilevante a quanto definito nella normativa relativa al processo di conservazione.

In particolare sono gestiti i seguenti eventi:

- Creazione PDA
- Conservazione PDA
- Invio Rapporto di Versamento
- Invio Rapporto di Conservazione
- Esibizione PDD
- Download Documento
- Scarto PDA
- Verifica Integrità PDA

Il log di audit è consultabile tramite applicativo dal produttore e attraverso il sistema di back office a chi gestisce il servizio o a pubblico ufficiale che ne faccia richiesta.

Il log viene salvato in apposito database e rimane disponibile nel tempo per consultazione. Oltre al log di audit sono presenti altri log di servizio relativi ad altri eventi generati dal sistema durante il processo di conservazione.

[Torna al sommario](#)

8 Il sistema di conservazione

8.1 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 27001:2013.

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.

[Torna al sommario](#)

8.2 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, certificato **ANSI/TIA 942-A Rating IV (ex Tier)**, sito in via Gobetti 96, Arezzo;
- architettura secondaria predisposta per consentire la doppia scrittura del dato, effettuata attraverso procedura applicativa, e la replica sincrona storage based della piattaforma virtuale, inclusi i DB documentali e gestionali, 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 necessità.

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 è implementata al 100% su infrastruttura di virtualizzazione con hypervisor VMware e garantisce 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.
- 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

[Torna al sommario](#)

8.3 Componenti Logiche

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

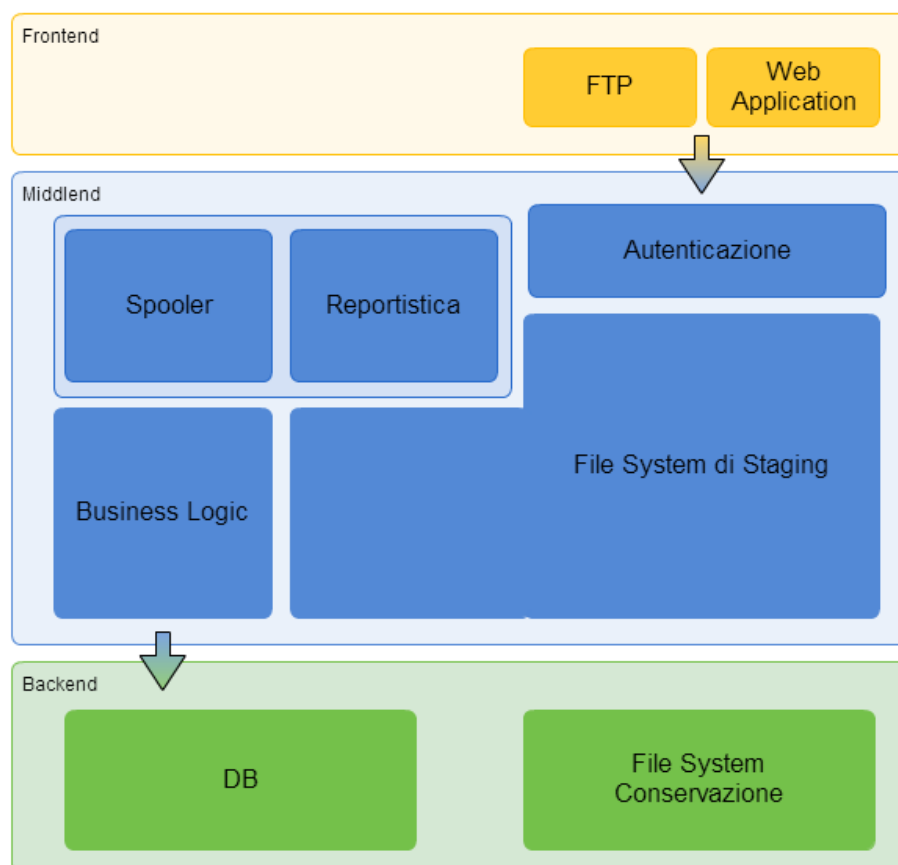


Figura 2: Rappresentazione delle componenti logiche

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 backend sia in scrittura, sia in fase di ricerca, distribuendo le query sulle varie istanze disponibili. Tutte le istanze backend sono sempre disponibili almeno in lettura
- **Store (& Database) layer:** la parte di back end è composta da diverse istanze. 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 viene replicato con strumenti di basso livello.

[Torna al sommario](#)

8.4 Componenti tecnologiche

Il sistema di conservazione Aruba PEC è composto da varie parti e tecnologie, con l'obiettivo di trarre il meglio dalla loro sinergia.

Le principali componenti software che interagiscono all'interno del sistema sono:

- Sistema documentale quale CMS di riferimento
- DB per la gestione dei dati di sistema e dei metadati legati ai materiali in conservazione
- Sistema LDAP per le operazioni di registrazione, autenticazione e controllo degli accessi degli utenti al sistema, indipendentemente dall'interfaccia scelta
- Web server e servlet container per le interfacce di frontiera (Web e Web Service)
- Un sistema di message broker per la gestione delle code in ingresso dei documenti in conservazione sulle interfacce di caricamento massivo (FTP e Web Service)
- Motore di Ricerca per la gestione dei dati di audit

[Torna al sommario](#)

8.5 Componenti fisiche

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 ampiamente riconosciute e leader del mercato di riferimento.

[Torna al sommario](#)

8.5.1 Sito Primario (Produzione)

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

- i nodi di Front-End (almeno due) per le interfacce di caricamento, esibizione e gestione,
- gli Application o Business Logic server (almeno due),
- i backend server, un singolo nodo per ogni istanza,
- un nodo virtuale dedicato al DB server di ogni istanza di backend, 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 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.

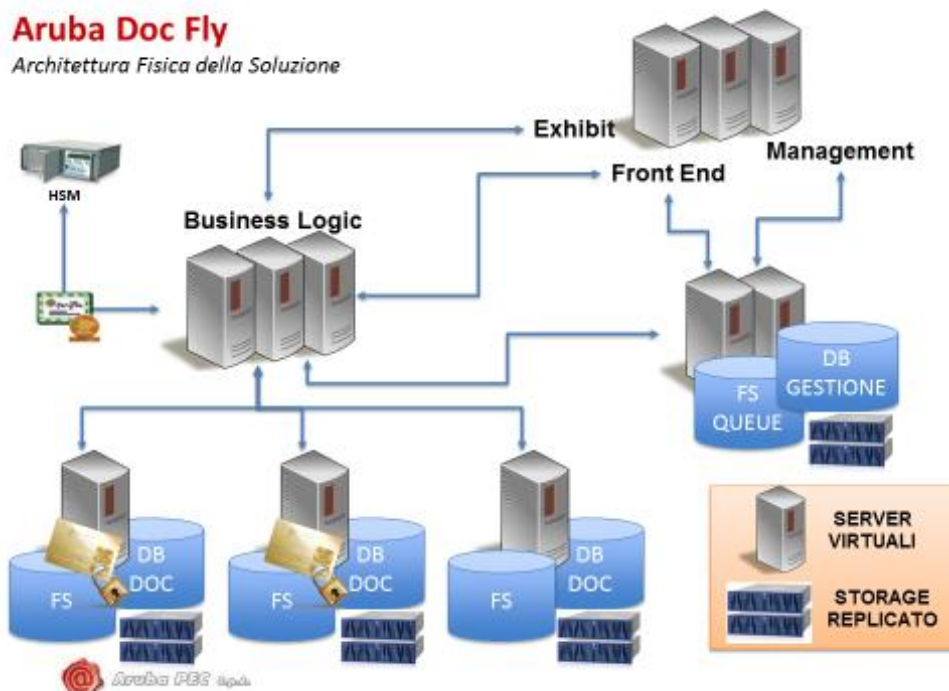


Figura 3: Rappresentazione architettura fisica della soluzione

[Torna al sommario](#)

8.5.2 Sito Secondario (DR)

Il sito secondario ospita un'infrastruttura virtuale basata su VMWare sulla quale vengono installati:

- Server di backend corrispondente ad uno dei nodi ridondati dell'ambiente di produzione
- Server DB sincronizzato in maniera sincrona (master-master) con i DB di produzione
- Storage enterprise su cui vengono sincronizzati i dati in maniera asincrona che saranno resi disponibili ai server del sito secondario per ripristinare il servizio
- Collegamenti verso i sistemi esterni di firma e Marcatura temporale (sempre situati nel sito secondario)
- Macchine virtuali replicate dal sito primario (1 per ciascuna tipologia)

Nello specifico le macchine replicate dal sito primario sono quelle che forniscono i seguenti servizi:

- Frontend Web
- Frontend WS
- Business Logic
- Indicizzazione
- Audit
- Autenticazione

La procedura di switch tra il sito primario ed il secondario è basata tramite il cambio dei puntamenti a livello di DNS.

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, configurati in Master-Master.

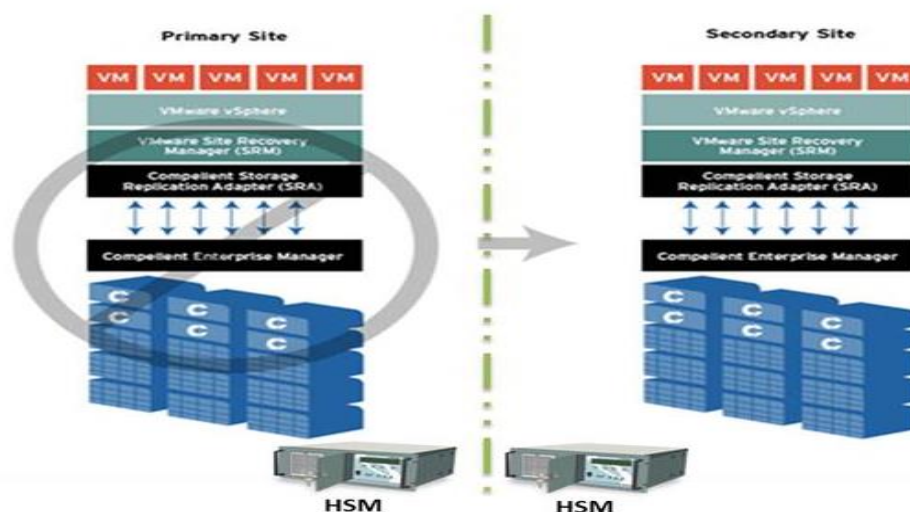


Figura 4 Schema logico della soluzione di Disaster Recovery

In caso di problemi sul sito di Produzione è possibile effettuare la riattivazione del servizio, senza perdita di dati entro 24 ore.

[Torna al sommario](#)

8.6 Procedure di gestione e di evoluzione

In linea con quanto previsto dalla circolare n° 65, nell'allegato "REQUISITI DI QUALITÀ E SICUREZZA PER L'ACCREDITAMENTO E LA VIGILANZA, sono descritte le procedure in riferimento a:

- conduzione e manutenzione del sistema di conservazione;
- gestione degli audit-log e loro conservazione;
- monitoraggio del sistema di conservazione;
- change management;
- verifica periodica di conformità a normativa e standard di riferimento

Riguardo i primi tre aspetti, si richiama il documento "MGA_A_38-01 Politica per la gestione dei beni, delle capacità e delle modifiche". I documenti in oggetto descrivono strategie di continuità, considerando tutte le componenti organizzative, operative, del business, tecnologiche, infrastrutturali che contribuiscono all'intero sistema e processo di conservazione.

[Torna al sommario](#)

8.6.1 Change management

Qualsiasi operazione di upgrade per evoluzione o bug fixing di una qualsiasi componente del sistema di conservazione Aruba PEC segue una procedura standardizzata atta a operare per garantire il minimo impatto su eventuali fermo servizio e la massima sicurezza possibile riguardo ai dati e documenti a sistema.

Tale procedura si basa sui seguenti assunti:

- ogni componente sviluppata è conservata in opportuno sistema di versionamento del codice
- i file di configurazione di ogni componente sono separati dai compilati in maniera da garantire un accesso più flessibile e veloce al personale addetto
- sono state predisposte apposite macchine di deploy per la compilazione e creazione dei pacchetti delle varie componenti da installare

Ogni aggiornamento del sistema passa da un flusso ben definito che consente contemporaneamente di mantenere stabile e sicura l'intera soluzione in uso dall'esterno e di sviluppare senza ostacoli nuove funzionalità.

Tale procedura risulta di particolare importanza anche per garantire l'accesso controllato e limitato a pochi addetti agli ambienti di produzione.

In particolare vengono messi a disposizione 4 ambienti di lavoro: sviluppo, test, collaudo e produzione.

Tutti gli sviluppi vengono condotti e testati nell'ambiente sviluppo che è di uso esclusivo agli sviluppatori per le sue caratteristiche di continua trasformazione.

Qualsiasi altro attore esterno al team di sviluppo non ha nessun accesso a tale ambiente.

Il codice sviluppato viene conservato all'interno di un sistema di versionamento organizzato in maniera da permettere qualora sia necessario l'estrazione di una qualsiasi versione del software. Una volta che un nuovo modulo software è pronto, esso viene registrato nel sistema di versionamento associandogli un tag/versione.

Per operare l'installazione sull'ambiente di test, deputato ai test pre-collaudo, i sorgenti vengono scaricati su un ambiente di deploy, esterno all'ambiente di test stesso, direttamente dal sistema di versionamento, insieme a eventuali script automatici di compilazione, installazione e configurazione.

Sull'ambiente di test il team della QA (Quality Assurance) effettua i test per verificare la corretta implementazione dei moduli rilasciati ed effettua anche i test regressione.

Solo se il processo di testing va a buon fine si procede con il rilascio dei nuovi moduli nell'ambiente di collaudo e produzione con la medesima procedura utilizzata per l'ambiente di test.

[Torna al sommario](#)

8.6.2 Verifica periodica di conformità a normativa e standard di riferimento

Aruba, in qualità di conservatore, svolge una verifica periodica della conformità alle normative ed agli standard di riferimento. A tal proposito, viene effettuata una volta l'anno, una verifica sulla rispondenza ai requisiti di qualità e sicurezza avvalendosi dello strumento di check list, sulla base dell'allegato della circolare n° 65, attraverso il quale viene registrata l'aderenza o meno alla conformità richiesta.

[Torna al sommario](#)

9 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.

[Torna al sommario](#)

9.1 Procedure di monitoraggio

ARUBA assicura la verifica periodica del funzionamento, nel tempo, del sistema di conservazione. Tali verifiche, descritte in "MGA_A_38-01 Politica per la gestione dei beni, delle capacità e delle modifiche", sono riportate in maniera dettagliata all'interno dei documenti "MGA_A_25-03 Layout Logico" e "MGA_A_35-03 Politica di Backup".

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 tracciate 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.

[Torna al sommario](#)

9.2 Verifiche sugli archivi

ARUBA assicura la verifica periodica, con cadenza non superiore a 36 mesi, 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 rendere disponibile attraverso una macchina virtuale un viewer per la visualizzazione dei documenti conservati. Il viewer specifico viene fornito sulla base dell'estensione del documento (mime type) e della versione del formato associato. Il dettaglio di tutte le tipologie supportate è definita nella procedura "Registro dei formati supportati da DocFly2". Per ogni formato presente nel registro è individuato il relativo programma che ne permette la corretta visualizzazione (viewer). Il registro viene tenuto aggiornato sulla base dei nuovi formati o di quelli che diventano obsoleti. Conseguentemente sono aggiornati i viewer presenti sulla macchina virtuale per la corretta leggibilità dei documenti conservati. Ulteriori dettagli operativi sulla verifica della leggibilità sono disponibili sulla procedura MGA_A_77-01_Procedura leggibilità documenti in conservazione a norma.
- **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).

[Torna al sommario](#)

9.2.1 Pianificazione delle verifiche periodiche da effettuare

La verifica dell'integrità degli archivi viene effettuata sui filesystems in cui i documenti sono replicati, controllando tutti i file presenti in nei PdA conservati.

Viene verificato che i file distribuiti nei filesystems siano identici mediante:

- controllo del nome e della dimensione dei file presenti sui filesystems;
- calcolo dell'hash di ogni singolo file. Il valore viene confrontato con l'hash del corrispondente file censito nell'IPdV del PdA.

Il controllo su ciascun PdA conservato viene effettuato a intervalli temporali. La prima dell'integrità del PdA verifica viene effettuata entro 36 mesi dalla conservazione del PdA. Le successive verifiche vengono effettuate entro 36 mesi dalla conclusione dell'ultima verifica effettuata.

[Torna al sommario](#)

9.2.2 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.

[Torna al sommario](#)

9.3 Soluzioni adottate in caso di anomalie

In caso di anomalie riscontrate a seguito del monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi, sono presenti apposite procedure di emergenza (contingency) e piani di Business Continuity da applicare in attesa del ripristino del servizio (così come descritto dal Disaster Recovery Plan del Gruppo Aruba)

[Torna al sommario](#)

10 Specifiche contrattuali

I documenti costituenti l'impianto contrattuale del servizio di conservazione a norma sono riportati nelle condizioni/accordo di fornitura.

ARUBA, in linea con la normativa vigente, garantisce contratti o accordi scritti che specificano e disciplinano diritti e responsabilità delle Parti, 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 ed erogazione del servizio di conservazione il Cliente sottoscrive e perfeziona il relativo Contratto. 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 specifico affidamento a tal fine sottoscritto dai suddetti terzi in favore del Cliente.

[Torna al sommario](#)

10.1.1 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 e affida ad ARUBA quale Responsabile del Servizio di Conservazione e Responsabile esterno del trattamento dei dati come previsto dalla vigente normativa in materia di protezione dei dati personali (Regolamento (UE) 2016/679 e 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 dal Cliente, mentre i ruoli di Responsabile del servizio di conservazione e di Responsabile del trattamento dei dati saranno ricoperti da ARUBA.

[Torna al sommario](#)

10.1.2 Scheda di conservazione

Il documento denominato "Scheda di conservazione" costituisce parte integrante e sostanziale del Contratto.

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

Il contenuto della Scheda di conservazione è volto a precisare:

- 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.

[Torna al sommario](#)

10.1.3 Elenco Persone

Ai fini dell'affidamento del servizio di conservazione digitale di documenti informatici, il Cliente 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 Produttore medesimo, precisandone funzione e ruolo.

[Torna al sommario](#)

10.2 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 nell'Atto di Affidamento.

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;

[Torna al sommario](#)

10.2.1 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 documentale² 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 affidate, 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 affidate;
- 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.

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;

[Torna al sommario](#)

10.2.2 Obblighi di ARUBA

ARUBA, come analiticamente descritto nel *Contratto*, limitatamente alle attività ad essa affidate, 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 affidate dal Cliente come in dettaglio riportate nel documento "*Atto di Affidamento*", nei modi e nei termini specificati nel presente *Manuale* e negli allegati ad esso relativi.

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.

[Torna al sommario](#)

10.2.3 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:

- 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;
- le procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l'esecuzione operativa di conservazione.
- le procedure informatiche ed organizzative per la corretta tenuta dei supporti su cui vengono memorizzati i documenti informatici oggetto di conservazione.
- 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*.

[Torna al sommario](#)

10.2.4 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 file system

[Torna al sommario](#)

10.2.5 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;

[Torna al sommario](#)

10.2.6 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 espletterà le attività per le quali ha ricevuto formale affidamento, 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 Elettronica	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
Sistema di conservazione digitale dei documenti informatici	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.

[Torna al sommario](#)

11 Livelli di servizio (SLA)

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.

CARATTERISTICHE GENERALI DEL SERVIZIO	SPECIFICHE TECNICHE
Disponibilità complessiva del servizio	99,95%
Assistenza	Sistema di ticketing e canale telefonico
Periodo di fatturazione	Annuale
Durata minima contratto	Un anno (eventuali upgrade richiesti in seguito alla stipula del contratto vanno 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 (Generazione del Rapporto di versamento)	Entro 48h dal ricevimento dell'ultimo documento contenuto nel pacchetto di versamento

Invio in conservazione del PdA	Entro 72h dalla presa in carico dell'ultimo PdV valido e completo contenuto nel PdA, nel caso in cui tutti i PdV contenuti nel PdA siano validi e completi ³ .
RICHIESTA DI ESIBIZIONE	SPECIFICHE TECNICHE
Produzione del Pacchetto di Distribuzione	Entro 4h dalla richiesta di produzione del PdD

[Torna al sommario](#)

12 Sicurezza del sistema di conservazione

Aruba PEC ed il Gruppo Aruba hanno 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 (Regolamento (UE) 2016/679 e D.lgs. 196/2003 e s.m.i.).

[Torna al sommario](#)

12.1 Privacy e requisiti di sicurezza dei dati

Aruba PEC tutela la riservatezza dei dati personali e garantisce ad essi la protezione necessaria da ogni evento che possa metterli a rischio di violazione, trattandoli secondo le specifiche previsioni della vigente normativa in materia.

Come previsto dal Regolamento dell'Unione Europea n. 2016/679 ("GDPR"), ed in particolare all'art. 13, sono fornite all'utente ("Interessato") tutte le informazioni richieste dalla normativa relative al trattamento dei propri dati personali mediante apposita, specifica e preventiva informativa, resa altresì sempre disponibile all'interno del proprio sito istituzionale. Con specifico riferimento ai compiti affidati con la nomina a Responsabile del trattamento dei dati personali, ARUBA comunica di ottemperare a quanto previsto dalla normativa vigente in materia ed alle prescrizioni di cui all'art. 28 del Regolamento (UE) 2016/679.

In conformità con le proprie politiche di sicurezza delle informazioni e del suo sistema di gestione ISO 27001, 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 del servizio di conservazione, tutti i principi, contenuti nelle disposizioni normative vigenti, relativi al trattamento dei dati personali e in particolare quelli contenuti nel Regolamento (UE) 2016/679 e garantisce che le informazioni personali, patrimoniali, statistiche, anagrafiche, e/o di qualunque altro genere, di cui verrà a conoscenza in conseguenza dei servizi 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.

[Torna al sommario](#)

12.2 Analisi dei Rischi

Il Gruppo Aruba 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**.

[Torna al sommario](#)

12.3 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.

[Torna al sommario](#)

³ La gestione dei PdA non validi o non completi è descritta al paragrafo 0

12.4 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.

[Torna al sommario](#)

12.5 Cifratura

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

[Torna al sommario](#)

12.6 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).

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. Sui due storage utilizzati inoltre vengono effettuate copie di sicurezza attraverso meccanismi di snapshot 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).

[Torna al sommario](#)

12.7 Isolamento delle componenti critiche

I sistemi utilizzati per il Servizio di Conservazione, da un punto dell'architettura fisica, sono posti all'interno di rack dedicati ai servizi eSecurity di Aruba PEC e isolati dagli altri sistemi del datacenter.

In particolare i server e le componenti software del Sistema di Conservazione sono separati logicamente dagli altri Servizi per mezzo di macchine virtuali ed istanze dedicate.

Per quanto concerne il livello organizzativo, questo è parzialmente separato, coerentemente coi requisiti indicati nel Piano della Sicurezza e nel Manuale della Conservazione.

[Torna al sommario](#)

12.8 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.



Figura 5: Immagine esterna del Datacenter

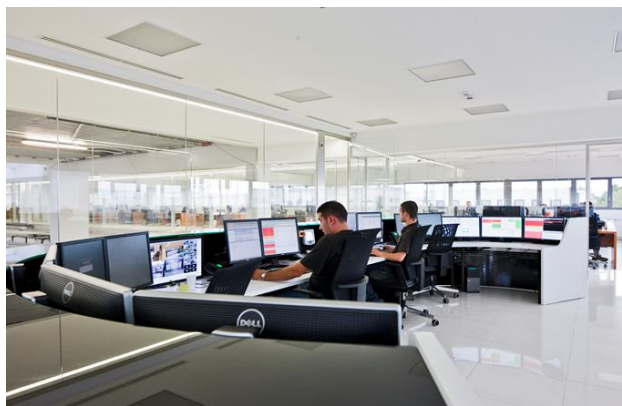


Figura 6: Immagine del Network Operations Center

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.

[Torna al sommario](#)

12.8.1 Sicurezza Fisica Data Center Primario

L'edificio primario è situato ad Arezzo in via Gobetti ed è certificato ANSI/TIA 942-A Rating IV (ex Tier). 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 video-sorveglianza (trattato di seguito). La recede 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.

[Torna al sommario](#)

12.8.2 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).

[Torna al sommario](#)

12.8.3 Sicurezza organizzativa comune ai due data center

Aruba garantisce inoltre la sicurezza organizzativa delle strutture, che viene continuamente adeguata in caso di evoluzioni delle normative. Il sistema di registrazione dei log per tutti i servizi erogati è infatti conforme alle normative vigenti ed 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 definiti ed attuati
- l'accesso alle informazioni riservate dell'Amministrazione viene permesso solo a personale autorizzato, in conformità al Regolamento (UE) 2016/679;

Aruba garantisce che tutti gli apparati necessari all'erogazione dei servizi vengano gestiti solo da personale univocamente individuato e che gli aspetti di sicurezza siano attuati in base a procedure documentate. Le procedure di sistema del Gruppo Aruba, redatte sulla base dello standard ISO27001 per la gestione della sicurezza delle informazioni, garantiscono che siano documentati:

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

[Torna al sommario](#)

12.8.4 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.
- Non devono essere facilmente identificabili. Nomi propri, nomi di prodotti, nomi di Clienti ecc. sono da evitare
- Devono contenere caratteri misti: minuscole, maiuscole, numeri, spazi, caratteri speciali (@, %, \$ ecc.)

L'utente viene invitato a cambiare con regolarità la sua password utente. Nel caso l'utente decidesse di non cambiare la propria password, riceverà quotidianamente, nelle ultime due settimane di validità della stessa, un avviso di richiesta di modifica password.

[Torna al sommario](#)

12.9 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, 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

[Torna al sommario](#)

12.9.1 Business Impact Analysis (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.

[Torna al sommario](#)

12.9.2 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...

[Torna al sommario](#)

12.9.3 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.

[Torna al sommario](#)

12.9.4 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 rottura 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 essere certificato **ANSI/TIA 942-A Rating IV (ex Tier)**, la riattivazione del servizio senza perdita di dati è prevista entro 24 ore. Nel caso di attivazione del sito secondario, questa viene eseguita manualmente seguendo apposite procedure, a seguito della dichiarazione di crisi prevista dalle procedure.

[Torna al sommario](#)

13 Disposizioni finali

13.1 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.

[Torna al sommario](#)

13.2 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.

[Torna al sommario](#)

13.3 Nessuna rinuncia

In nessun caso eventuali inadempimenti e/o comportamenti del Cliente difforni 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.

[Torna al sommario](#)

13.4 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.

[Torna al sommario](#)

13.5 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.

[Torna al sommario](#)

13.6 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.

[Torna al sommario](#)

13.7 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.

[Torna al sommario](#)

13.8 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. Simone Braccagni

[Torna al sommario](#)

A.R.P.A.B.

MANUALE DI CONSERVAZIONE PUBLISYS

CLASSI DOCUMENTALI E METADATI

1. Introduzione

L'Arpab di seguito denominato "Ente", individua nel presente documento gli atti per i quali intende avvalersi del servizio di conservazione offerto da ARUBA SPA con intermediazione tecnologica della società PUBLISYS SPA e ne determina le classi documentali.

In particolare nei paragrafi successivi vengono analizzati i seguenti aspetti:

- Elenco delle classi documentali oggetto di invio in conservazione;
- Formati di file inviabili in conservazione;
- Specifiche tecniche delle singole classi documentali.

2. Classi documentali oggetto di conservazione

L'Ente individua le seguenti classi documentali:

- Registro giornaliero di Protocollo (REGPROT);

e dispone la conservazione a norma per i relativi documenti.

I documenti conservati e i relativi metadati non possono essere oggetto di successive modifiche, in particolare, classificazioni variabili nel tempo rimarranno, per il singolo documento, quelle in vigore al momento dell'invio in conservazione.

3. Formati dei file inviabili in conservazione e strutture di imbustamento

Ai fini dell'invio in conservazione a norma, sarà privilegiato, ove possibile, l'utilizzo del formato PDF/A.

In base all' articolo 21, comma 2, del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale - CAD), confermato dalle regole tecniche di cui al DPCM 22 febbraio 2013, il documento informatico non deve contenere macroistruzioni o codici eseguibili.

Di seguito vengono elencate le tipologie di file accettati dal sistema di conservazione, ai sensi dell'allegato 2 al DPCM 3 dicembre 2013, recante "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":

- **PDF** formato PDF o PDF/A – tipo MIME application/pdf
- **GIF** – tipo MIME image/gif
- **JPG e JPEG** – tipo MIME image/jpeg
- **TIF e TIFF** – tipo MIME image/tiff
- **BMP** – tipo MIME image/bmp
- **RTF** – tipo MIME application/rtf
- **TXT** – tipo MIME text/plain
- **XML** – tipo MIME application/xml, text/xml
- **HTML** – tipo MIME text/html
- **DOCX** – tipo MIME application/vnd.openxmlformats-officedocument.wordprocessingml.document (**Office Open XML**)
- **XLSX** – tipo MIME application/vnd.openxmlformats-officedocument.spreadsheetml.sheet (**Office Open XML**)
- **ODT** – tipo MIME application/vnd.oasis.opendocument.text
- **ODP** – tipo MIME application/vnd.oasis.opendocument.presentation
- **ODG** – tipo MIME application/vnd.oasis.opendocument.graphics
- **ODB** – tipo MIME application/vnd.oasis.opendocument.base

- **ODS** – tipo MIME application/vnd.oasis.opendocument.spreadsheet
- **EML** (rfc822, rfc2822) – tipo MIME message/rfc822 e message/rfc2822

Marche temporali:

- TimeStampResponse: **.TSR**
- TimeStampToken: **.TST e .TS**

Formati di sottoscrizione:

- Busta di firma CAdES-BES: **.P7M**
- Firma PAdES: **.PDF**
- Firma XAdES: **.XML**

File che contengono altri file:

- TimeStampedData: **.TSD**
- File firmato digitalmente e marcato: **.M7M**

Eventuali altri formati, quali, ad esempio, il .XLS (Microsoft Excel), il .DOC (Microsoft Word) e il .PPT (Microsoft PowerPoint), generano un'anomalia durante la fase di presa in carico e non vengono accettati dal sistema di conservazione a norma senza specifica autorizzazione da parte del Responsabile della Conservazione. Nella tabella seguente vengono presentati i formati dei file sopra elencati ed il software di visualizzazione ad essi associato.

Tabella 1 – Formati dei file e visualizzatori associati

	Formato dei file inviabili in conservazione	Software di visualizzazione
1	Documento PKCS#7 (P7M), firme PadES e XadES (*)	DigitalSign Reader, Dike, File Protector
2	Marche temporali TSD, TSR, TST	DigitalSign Reader, Dike, File Protector
3	Documento PDF	Adobe Acrobat Reader
4	Immagine JPG (JPG e JPEG)	IrfanView
5	Immagine TIF (TIF e TIFF)	IrfanView
6	Immagine BMP	IrfanView
7	Documento RTF	MS Word Viewer
8	Documento XML	SciTE
9	Documento TXT	SciTE
10	Documento HTML	Firefox
11	Documento OOXML	MS Word Viewer
12	Documento EML	Thunderbird
13	Documento ODT, ODP, ODG, ODB, ODS	Open Office

(*) La verifica della firma e la successiva estrazione degli oggetti firmati digitalmente può essere effettuata con qualsiasi software in grado di elaborare file firmati in modo conforme alla Deliberazione CNIPA (ora AGID) 21 maggio 2009 n. 45. Possono essere firmati digitalmente esclusivamente le tipologie di documenti elencati in tabella (punti 3-13).

4. Descrizione delle classi documentali

La classe documentale definisce tutte le caratteristiche di una tipologia di documento da sottoporre a conservazione, individuando le informazioni necessarie a qualificare ed identificare univocamente ogni singolo documento. Ha parametri specifici di comportamento ed attributi o metadati propri. Alcuni metadati, o attributi di base, sono comuni a tutte classi documentali, mentre altri sono specifici e riguardano una determinata tipologia di documenti. In particolare per ciascuna classe documentale vengono individuate e definite le seguenti informazioni:

- nome classe documentale;
- anagrafica dei documenti ossia ente, area ed ufficio proprietari dei documenti;
- metadati di base e specifici della classe documentale;
- numero medio dei documenti informatici prodotti mensilmente;
- numero medio dei documenti informatici prodotti annualmente;
- dimensione media e massima dei documenti informatici;
- periodicità di invio in conservazione;
- periodicità di generazione del pacchetto di archiviazione;
- tempi di conservazione.

4.1 Registro giornaliero di protocollo: classe documentale “REGPROT”.

In questa tipologia ricadono i documenti digitali prodotti ai sensi dell’art. 7, comma 5, del DPCM 3 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”.

Anagrafica dei documenti REGPROT

L'anagrafica dei documenti del Registro giornaliero di protocollo del singolo Produttore viene impostata attraverso i seguenti descrittori univoci:

- ente (Ente di appartenenza del Produttore): **ARPAB**
- area (Area di appartenenza del Produttore): **PROTOCOLLO**
- ufficio (Ufficio di appartenenza del Produttore): **PROTOCOLLO**

Metadati REGPROT

La classe documentale REGPROT versione 1.0 , oltre ai metadati previsti dalla classe documentale base, comprende anche i seguenti metadati specifici:

Elenco metadati obbligatori Devono essere presenti nell'indice	TAB. B – METADATI OBBLIGATORI		
	ID pacchetto di versamento	Denominazione soggetto mittente	Numero ultima registrazione effettuata sul registro
	ID Documento (valore obbligatorio)	Partita IVA soggetto mittente	Data prima registrazione effettuata sul registro
	Impronta Documento (valore obbligatorio)	Cognome soggetto mittente	Data ultima registrazione effettuata sul registro
	Data Chiusura	Nome soggetto mittente	Amministrazione titolare del procedimento
	Oggetto Documento	Codice fiscale soggetto mittente	Amministrazioni partecipanti
	cognome destinatario	Cognome Soggetto Produttore 2	Responsabile del procedimento
	Nome destinatario	Nome Soggetto Produttore 2	Oggetto del Procedimento
	Codice Fiscale destinatario	Codice Fiscale Soggetto Produttore 2	Documenti contenuti nel procedimenti
	Denominazione destinatario	Cognome Responsabile Gestione Documentale	Numero Protocollo
	Partita Iva Destinatario	Nome Responsabile Gestione Documentale	Data Registrazione Protocollo
	Cognome Soggetto Produttore	Codice Fiscale Responsabile Gestione Documentale	AOO di riferimento
	Nome Soggetto Produttore	Codice identificativo del registro	Codice Identificativo amministrazione (IPA)
	Partita Iva Soggetto produttore	Numero Progressivo del registro	Denominazione dell'amministrazione
	Codice Fiscale Soggetto Produttore	Anno	
	Denominazione Soggetto Produttore	Numero prima registrazione effettuata sul registro	
Elenco ExtraInfo Disponibili Non sono obbligatori nell'indice Possono non essere valorizzati.	TAB. C – METADATI DISPONIBILI		
	IDENTIFICAZIONE DEL SISTEMA VERSANTE	DATA DI ALTRA REGISTRAZIONE	IDENTIFICATIVO DELL'UNITÀ ARCHIVISTICA
	ID DOCUMENTO NEL SISTEMA DI ORIGINE	REGISTRO	ANNOTAZIONE
	APPLICATIVO DI PRODUZIONE DEL DOCUMENTO	REPERTORIO	ANNESSO
	LIVELLO DI RISERVATEZZA	SERIE	NOTE 1
	CONDIZIONI DI ACCESSO	UFFICIO PRODUTTORE	NOTE 2
	CODICE FISCALE TITOLARE DEL CERTIFICATO DI FIRMA	ESISTENZA DI ORIGINALE ANALOGICO	ALLEGATO 1
	NUMERO DI ALTRA REGISTRAZIONE	CLASSIFICAZIONE ARCHIVISTICA	ALLEGATO 2
	ID FASCICOLO		

Produzione dei documenti REGPROT

Per l'Ente, il volume medio annuo e la dimensione media dei documenti inviati in conservazione sono:

- volume annuo: **365**
- dimensione media di un documento: **500KB**
- dimensione massima rilevata per un documento: **1 MB**

Periodicità di invio in conservazione e generazione del pacchetto di archiviazione, tempo di conservazione

Periodicità di invio in conservazione:	Giornaliera
Periodicità di generazione del pacchetto di archiviazione	Ogni giorno dopo le ore 24, più precisamente alle 01.30
Tempo di conservazione	Illimitato

Modalità di invio in conservazione.

La ricezione dei documenti avviene attraverso la costruzione di un Pacchetto di Versamento (PdV) che contiene, oltre ai documenti, i metadati ad essi associati (indice), il cui formato deve essere concordato con il conservatore Aruba PEC utilizzando l'apposita Scheda di Conservazione. Fra i diversi aspetti concordati, i principali sono: le tipologie di documenti da conservare, metadati, eventuali informazioni extra, i formati da adottare per ogni classe/tipo di documento, le modalità e canali di trasferimento dei documenti nell'archivio (ws, ftp, http) ed ulteriori. L'indice del pacchetto di versamento è un file XML che contiene le informazioni caratterizzanti il pacchetto stesso, quali, a titolo esemplificativo ma non esaustivo: id univoco del PdV, id univoco di ogni documento comprensivo della sua impronta e dei metadati che lo descrivono ed altro. Il sistema di conservazione, una volta ricevuti i pacchetti di versamento, avvia da subito dei controlli di qualità circa la regolarità di formazione del pacchetto stesso nonché dei dati relativi ai documenti che formeranno oggetto di deposito. I controlli e le notifiche riguardanti le diverse operazioni, che si succedono lungo il processo di conservazione, sono documentate all'interno del manuale del sistema di conservazione.

Processo di conservazione.

Il sistema informativo GEOS, sistema di Protocollo Informatico dell'Ente, produce tramite una procedura batch il registro di protocollo giornaliero di protocollo ed il registro delle modifiche giornaliere, secondo i metadati indicati sopra specifici della classe documentale Aruba DocFly.

Publisys adotta un proprio software per l'invio dei documenti in conservazione invocando le API ed i servizi remoti messi a disposizione da Aruba DocFly. Tale software assicura che tutto il flusso documentale, dalla presa in carico del documento fino all'eventuale scarto non possa essere manomesso. La soluzione, tramite l'adozione di regole, procedure e tecnologie garantisce le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità nel tempo dei registri di protocollo con i metadati ad essi associati.

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

- pacchetti di versamento;
- pacchetti di archiviazione.

Tutte le componenti funzionali della soluzione di conservazione, assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione. Il sistema di conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico. Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il sistema di conservazione sono quelli indicati nel manuale del processo di conservazione adottato dal conservatore e presente sul sito dell'AGID al seguente indirizzo: https://www.agid.gov.it/sites/default/files/repository_files/manuale_di_conservazione_aruba_pe_c_ver_1.5_2018_10_11.pdf.



Manuale

Indice

1	Scopo e Ambito del documento	4
2	Flussi	4
2.1	Ricezione	4
2.2	Risposte	4
2.3	Invio in Conservazione	4
2.4	Altri Flussi	5
2.5	Esigenze Rappresentate	5
3	Fattel	5
3.1	Login	5
3.2	Elenco Fatture	6
3.3	Dettaglio Fatture	7
3.4	Rifiuta Fattura	9
3.5	Accettazione Fattura	10
3.6	Intestazione Fattura – Dati Protocollo	11
3.7	Prendi in Carico	11
3.8	Stampa Fattura	11
3.9	Stampa FatturaPA	12
3.10	Download Xml Fattura	13
3.11	Utenti	14
3.12	Import Fattura	15
4	Conservazione	15
4.1	Conservazione Fatture	15
4.2	Inoltro Pacchetti di Conservazione	17
4.3	Elementi inviati in Conservazione	17
5	Servizi Web	18
5.1	Scarica PdD	18
5.2	Protocollazione Automatica	18
5.3	Invio a Registro Fatture	18
5.4	Gestione Risposte	19

Glossario termini

Server Virtuali	Tramite specifici software, un server fisico può contenere più server “virtuali” che permettono l’esecuzione di differenti sistemi operativi.
S3	Simple Storage Service (S3), sono spazi fisici di memorizzazione su cloud
Cloud	Servizi di varia natura fruibili tramite collegamento internet ai fornitori dei servizi utilizzati. Tipicamente parliamo di spazi di archiviazione, server virtuali, copie di backup
SDI	Sistema di Interscambio – La Legge Finanziaria 2008 ha stabilito che la trasmissione delle fatture elettroniche destinate all’amministrazione dello Stato debba avvenire attraverso questo Sistema.
WS	Servizi Web (Web Services) – Software sviluppati per colloquiare con altri sistemi software, consentendo lo scambio di informazioni secondo protocolli standard
CSS	Fogli di stile a cascata (Cascading Style Sheets) - è un linguaggio usato per definire la formattazione di documenti HTML, XHTML e XML applicato per rappresentare siti e relative pagine web.

1 Scopo e Ambito del documento

Il seguente documento descrive il sistema **FATTEL**, soluzione Cloud, proposta da Traccia per gestire i flussi di ricezione, risposte ed invio in Conservazione delle fatture elettroniche. Nei capitoli seguenti faremo una panoramica sui flussi presenti (in ricezione ed in risposta), sulle modalità di Invio in conservazione e sui servizi web (web services - **ws**) presenti sulla piattaforma.

Uno degli elementi distintivi di **FATTEL** è di poter interfacciare sistemi software esterni al fine di eseguire operazioni di protocollazione e/o risposta alla fattura senza interventi degli operatori.

Nel capitolo dedicato ai servizi web, vedremo una panoramica di quanto oggi presente su **FATTEL** tenendo comunque presente la possibilità di estendere questi servizi a fronte di ulteriori richieste.

2 Flussi

I flussi **Standard** presenti in **FATTEL** sono di ricezione da SDI, risposta a SDI, invio in conservazione presso un soggetto certificato.

2.1 Ricezione

Il sistema **FATTEL** può essere alimentato da più fonti.

Tipicamente riceve le fatture in automatico tramite l'uso di servizi web (web Services) che vengono attivati su richiesta del cliente.

Attraverso l'uso di Certificati Digitali, che permettono la trasmissione "sicura" e certificata dei file contenenti le fatture, queste vengono memorizzati su server virtuali in spazi dedicati S3.

In alternativa, per chi riceve le fatture attraverso il canale EMAIL PEC, **FATTEL** permette di caricare manualmente i file ricevuti tramite email (tipicamente file con estensione XML e P7M), che sono quindi memorizzati su server virtuali negli spazi S3 dedicati.

2.2 Risposte

Per ogni fattura ricevuta, gli operatori indicati dal cliente possono Accettarla o Rifiutarla. Così come per la ricezione, anche le risposte possono essere eseguite attraverso WS o manualmente.

2.3 Invio in Conservazione

Nel momento in cui le fatture sono memorizzate in Fattel, vengono inviate automaticamente al soggetto con cui il cliente ha stipulato un accordo di conservazione.

Al momento la piattaforma dispone di tutti i servizi di colloquio verso ARUBA.

Per l'utilizzo di altri provider

2.4 Altri Flussi

Altri flussi oggi sviluppati come soluzioni personalizzate per i clienti prevedono:

1. Protocollo in automatico con restituzione del numero e data protocollo.
2. Invio a sistema contabile per il trattamento della fattura stessa.
3. Gestione delle risposte alle fatture da sistemi esterni.

L'aspetto comune per tutti i clienti è l'invio in conservazione secondo le specifiche del Provider di conservazione scelto.

Al momento la piattaforma dispone di tutti i servizi di colloquio verso ARUBA.

2.5 Esigenze Rappresentate

Alcune delle esigenze rappresentate sono:

- di verificare l'adeguatezza dell'attuale infrastruttura
- ipotizzare uno scenario di adeguamento relativamente alla nuova sede in termini di hardware e software tra cui:
 - posizionamento degli elementi componenti l'IT
 - connettività interna
 - postazioni client sia in termini hardware che di software di base
 - Politiche di accesso e condivisione dati
 - Accessi da esterno
 - Gestione documentale

3 Fattel

Il portale di gestione delle

3.1 Login

Il sistema è accessibile attraverso un portale WEB a cui accedere attraverso le credenziali comunicate da Traccia al cliente.

Figura 1 - Login

Attraverso le credenziali comunicate, il referente operativo può gestire le fatture, o creare ulteriori account di accesso, nel caso sia necessario un'operatività di più utenti. Nel paragrafo Utenti è descritto come gestire gli utenti, abilitandoli o disabilitandoli all'accesso.

3.2 Elenco Fatture.

Dopo l'esecuzione della Login, viene mostrato all'utente l'elenco delle fatture in gestione con informazioni ricevute da SDI e altre integrate o da servizi web (ove previsti per il cliente) o gestiti dall'operatore (accettazione, rifiuti, data e numero protocollo).

Elenco Fatture

app.latraccia.it/fattel/?p=104:19850310483994:....

FATTEL
FATTURAZIONE ELETTRONICA

Elenco Fatture

Richiesta Di Assistenza

Utenti Importa fattura

Fattura da prendere in carico ☒ ☒ ☒
Fattura Rifiutata ☒ ☒ ☒

Anno Fattura	Tipo Documento	Numero Fattura	Data Fattura	Cedente Prestatore	Importo Totale Documento	Importo Pagamento	Iva	Pagato	Data Protocollo	Num. Protocollo	Rifer. Sdi	Motivo Scarto	Ricevuta Sdi	Codice Ufficio
2019	Fattura	19	30/09/2019		1.372,50	1.372,50	Split Payment	-	02/10/2019	18125	1697179433	-	-	UFNIHN
2019	Fattura	18	30/09/2019		2.647,40	2.647,40	Split Payment	-	02/10/2019	18124	1697058874	-	-	UFNIHN
2019	Fattura	0000146/PA	30/09/2019		366,00	300,00	Split Payment	-	02/10/2019	18123	1696740558	-	-	UFNIHN
2019	Fattura	2154-PA	30/09/2019		2.564,76	2.102,26	Split Payment	-	02/10/2019	18122	1696283620	-	-	UFNIHN
2019	Parcella	FATTPA 90_19	02/10/2019		2.942,60	2.478,76	-	-	02/10/2019	18121	1700320284	-	-	UFNIHN
2019	Fattura	2491/19FT	23/09/2019		8.848,99	7.253,27	Split Payment	-	02/10/2019	18120	1694961028	-	-	UFNIHN
2019	Fattura	17	30/09/2019		977,22	977,22	Split Payment	-	02/10/2019	18091	1696917404	-	-	UFNIHN
2019	Fattura	2019-FTEL-0002325	30/09/2019		146,40	120,00	Split Payment	-	02/10/2019	18068	1691435505	-	-	UFNIHN
2019	Fattura	2156-PA	30/09/2019		1.473,91	1.208,12	Split Payment	-	02/10/2019	18067	1696283654	-	-	UFNIHN
2019	Fattura	2155-PA	30/09/2019		1.171,81	1.171,81	-	-	02/10/2019	18066	1696283631	-	-	UFNIHN
2019	Fattura	0000146/PA	30/09/2019		366,00	300,00	Split Payment	-	02/10/2019	18043	1689505628	errato riferimento a	Fattura rifiutata con successo	UFNIHN
2019	Fattura	291/PA	24/09/2019		5.760,62	4.721,82	Split Payment	-	01/10/2019	18014	1683872467	-	-	UFNIHN
2019	Fattura	3906	01/10/2019		664,90	545,00	Split Payment	-	01/10/2019	17983	1687167488	-	-	UFNIHN
2019	Fattura	298/PA	26/09/2019		2.109,26	1.728,90	Split Payment	-	01/10/2019	17944	1683871780	-	-	UFNIHN
2019	Fattura	VB19005373	30/09/2019		1.210,86	1.164,29	Split Payment	-	30/09/2019	17938	1679326085	-	-	UFNIHN

31 - 45

Figura 2 - elenco fatture

3.3 Dettaglio Fatture.



Tramite l'icona presente in ogni rigo delle fatture, è possibile aprire una scheda di dettaglio per la singola fattura.

La scheda riporta tutte le sezioni previste da SDI e altre (come i dati del registro del protocollo) che devono essere completate o dall'operatore o dai servizi automatici.

In figura sono mostrate le sezioni:

- Accettazione/Rifiuto
- Intestazione

Fattel – Manuale 1.0

Cooperativa E.D.P. LA TRACCIA
Rec. Il Fiorentini 10 – 75100 Matera
Tel. +39 0835.336836 – Fax +39 0835.336825
www.latraccia.it info@latraccia.it

P.IVA 00317370773 N° Iscr. Albo nazionale società cooperative: A148473 Sezione: cooperative a mutualità prevalente



ISO 9001
Cert. n. 9150/TRAC

ISO 9001
Cert. n. 9194/EDP2

- Cedente Prestatore
- Rappresentante Fiscale
- Cessionario Committente
- Terzo Intermediario o Soggetto Emittente

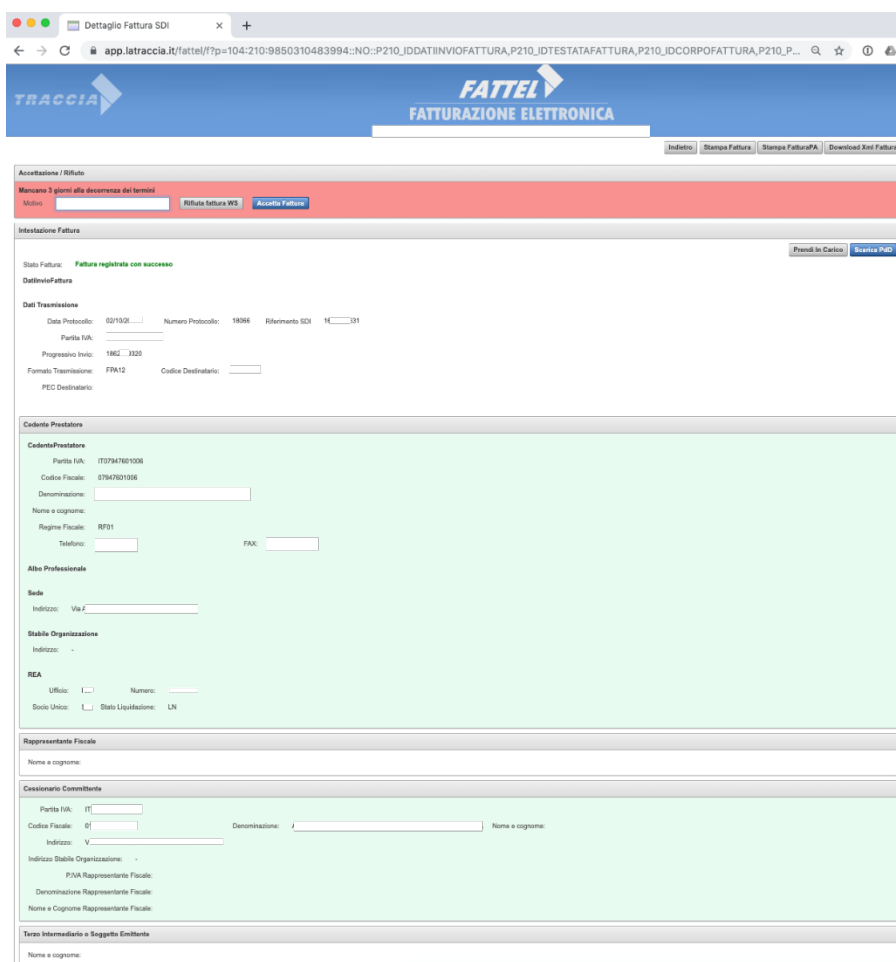


Figura 3 - Dettaglio Sezioni Fattura 1

Nella figura successiva sono mostrate le sezioni:

- Corpo Fattura
- Dettagli righe
- Riferimenti
- Dati di Riepilogo
- Dati Pagamento
- Allegati alla Fattura

Corpo Fattura

CorpoDellaFattura1

Tipo Documento: TD01 Divisa: EUR

Data: 30/09/2019

Numero: 211

Importo Totale Documento: 1171.81

Causale: ORDINE N. 28 DEL 22/03/2016 S - ADESIONE (-) - SERVIZI

DettagliCorpoFattura2

Dati Trasporto / Vettore

Partita IVA:

Indirizzo Resa:

Dati Ritenuta

Dati Bollo

Bollo Virtuale: Importo Bollo:

Dati Cassa Previdenziale

nessun dato di cassa previdenziale trovato

Sconto Maggiorazioni

nessuno sconto/maggiorazione trovato

Dettagli Righi

Numero Riga	Quantita	Unita di misura	Prezzo unitario	Prezzo totale	Aliquota Iva	Descrizione
1	1	-	1171.81	1171.81	0	ORDINE N. 28 DEL 22/03/2016 - ADESIONE (-) - SERVIZI DI F

Riferimenti

Type	Numero Linea	Codice Commessa	Data	Num.	Numero DDT	CIG	CUP
Ordine Acquisito	-	-	22/03/2016	-	-	661	-

Dati Riepilogo

Art. IVA	Natura	Spese Access.	Ammort.	Importo	Imposta	Esigibilita'	Riferimento Normativo
0	NB	-	-	1.171,81	0,00	-	Art.17 c.6 Reverse Charge D.P.R. 633/72

Dati Pagamento

Cond. Pagam.	Benef.	Modalita' Pagam.	Data Risc.	Termini Pagam.	Data Scadenza Pagam.	Importo Pagam.	COD Ufficio Postale	Cognome	Nome	CF	Qual.	Titolo	Istituto	Financ.	IBAN	ABI	CAB	BIC
TP02	-	MP05	30/09/2019	30	30/10/2019	1.171,81	-	-	-	-	-	INTE	PIAZZ	IT02C	5	02111	0511	-

Allegati

nessun dato trovato

releases 1.0

[Informativa sull'uso dei cookies](#)

Figura 4 - Dettaglio Sezioni Fattura 2

3.4 Rifiuta Fattura

La sezione di Accettazione Rifiuto è a disposizione dell'utente al fine di Rifiutare/Accettare le fatture. Il rifiuto della fattura deve avvenire indicando **obbligatoriamente** la motivazione.

Accettazione / Rifiuto

Mancano 3 giorni alla decorrenza dei termini

Motivo

Figura 5 - Rifiuto Fattura - Motivazione

Dopo l'inserimento del campo, cliccando sul bottone Rifiuta Fattura WS viene preparato un apposito file XML e, se presenti i servizi web, viene immediatamente inviato a SDI. In alternativa, se il cliente riceve la fattura tramite PEC, viene abilitato, per la fattura rifiutata,



Figura 6 - Rifiuto Fattura - Acquisizione XML Rifiuto

Il pulsante Download XML in corrispondenza della motivazione del rifiuto, o nel vertice in alto a destra della pagina.

Dopo aver cliccato, viene, a seconda della configurazione del browser utilizzato, mostrata una finestra in cui viene richiesto il salvataggio del file e di indicare la cartella.

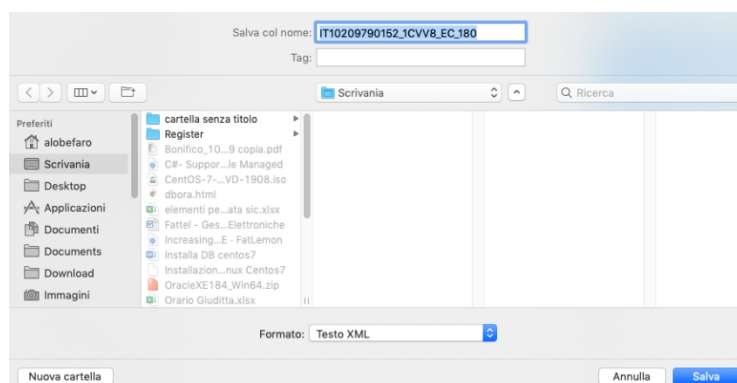


Figura 7 - Rifiuto Fattura - Salvataggio XML Rifiuto

Il file così acquisito deve essere inviato in risposta tramite il canale **e-mail pec** allo SDI.

3.5 Accettazione Fattura

L'accettazione Fattura prevede l'invio a SDI della comunicazione di accettazione della fattura ricevuta.

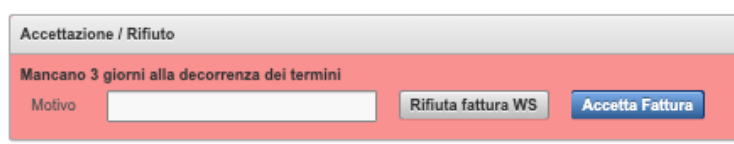


Figura 8 - Accettazione Fattura

In egual modo, viene prodotto ed inviato a SDI il file XML di avvenuta accettazione, ma al contrario della fase di rifiuto non si deve indicare nulla nel campo Motivo.

Com'è noto, se l'operatore non esegue alcuna operazione di Rifiuto/Accettazione, trascorsi 15 giorni dalla ricezione, la fattura diventa automaticamente accettata senza alcuna comunicazione a SDI.

Si può notare come, nella sezione, siano riportati i giorni mancanti alla Decorrenza Termini che rendono automaticamente la fattura accettata.

3.6 Intestazione Fattura – Dati Protocollo

Oltre che la sezione Accettazione/Rifiuto, l'unica altra sezione che prevede la possibilità di modifica da parte dell'operatore e quella dell'Intestazione, relativamente ai campi **Data Protocollo** e **Numero Protocollo**.

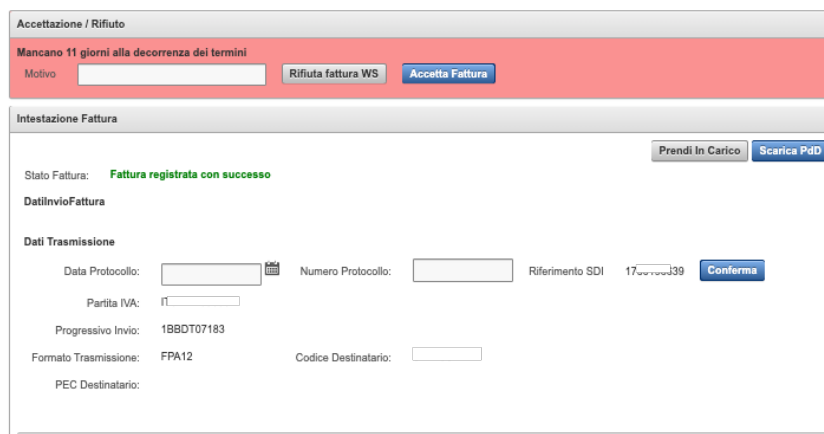


Figura 9 - Riferimenti Registro Protocollo

Anche in questo caso, se per il cliente sono presenti i servizi web di protocollazione automatica, i campi risulteranno già compilati e non modificabili in caso contrario deve indicarli e, cliccando sul tasto conferma, associarli alla fattura.

3.7 Prendi in Carico

Il bottone **Prendi in Carico**, esegue semplicemente un cambio di colore nell'elenco delle fatture al fine di evidenziare per l'operatore stesso, che la fattura è stata da lui letta.

3.8 Stampa Fattura

Attraverso questo bottone la fattura viene mostrata secondo un modello tipico delle fatture cartacee attraverso l'applicazione di un **CSS** apposito.

Download

app.latraccia.it/fattel/f?p=104:229:9850310483994::229:P229_NOME_FILE,P229_FOGGIO_DI_STILE:NL10209790152_1CVV8.XML,

Stampa Fattura

FATTURA ELETTRONICA

Versione FPA12

Dati del cedente / prestatore
Identificativo fiscale ai fini IVA: ITI 77
Codice fiscale: TRN
Denominazione: 18
Regime fiscale: RFO1 (ordinario) NO*
Indirizzo: V...
Numero civico: 1
CAP: 75100
Comune: M...
Provincia: B...
Nazione: IT

Dati del cessionario / committente
Identificativo fiscale ai fini IVA: ITI
Denominazione: A 7A
Indirizzo: V...
Numero civico: 1
CAP: 85100
Comune: I...
Provincia: P...
Nazione: IT

Dati generali del documento
Tipologia documento: TD01 (fattura)
Data documento: 2019-09-30 (30 Settembre 2019)
Numero documento: 0000146/PA

Dati dell'ordine di acquisto
Identificativo ordine di acquisto: 1C
Data ordine di acquisto: 2019-02-26 (26 Febbraio 2019)
Codice Identificativo Gara (CIG): 2

Dati relativi alle linee di dettaglio della fornitura

N°/Articolo	Valore	Descrizione	Quantita/unita di misura	Prezzo unitario	Prezzo Totale	IVA
1 Codice	SR	1	1.000	NUMERO	300.00000	300.00
2 SETTE	0.000000	0.00	22.00			
3 DETE	0.000000	0.00	22.00			

Dati di riepilogo per aliquota IVA e natura
Aliquota IVA (%): 22.00
Totale imponibile/importo: 300.00
Totale imposta: 66.00
Esigibilità IVA: S (scissione dei pagamenti)
Importo totale documento: 366.00

Dati relativi al pagamento
Condizioni di pagamento: TP02 (pagamento completo)
Dettaglio pagamento
Modalità: MP05 (bonifico)
Decorrenza termini di pagamento: 2019-09-30 (30 Settembre 2019)
Importo: 300.00
Istituto finanziario: BA...
Codice IBAN: I...
Codice ABI: 0...
Codice CAB: 1...

Dati relativi agli allegati
Nome dell'allegato: 000005996.zip
Algoritmo di compressione: ZIP
Formato: PDF
Descrizione: FATTURA IN VERSIONE PDF

Versione prodotta con foglio di stile Sdi www.latraccia.it

Figura 10 - Fattura con CSS Traccia

3.9 Stampa FatturaPA

Attraverso questo bottone la fattura viene mostrata secondo il modello previsto dalla piattaforma SDI, attraverso l'applicazione del **CSS** definito appunto da SDI.

Download

app.latraccia.it/fattel/f?p=104:229:9850310483994:::229:P229_NOME_FILE,P229_FOGLIO_DI_STIL...

Stampa Fattura

FATTURA ELETTRONICA

Versione FPA12

Dati relativi alla trasmissione

Identificativo del trasmettente: IT
 Progressivo di invio: ETE
 Formato Trasmissione: FPA12
 Codice Amministrazione destinataria: UF

Dati del cedente / prestatore

Dati anagrafici

Identificativo fiscale ai fini IVA: IT
 Codice fiscale: IT
 Denominazione: IT
 Regime fiscale: RFO1 (ordinario)

Dati della sede

Indirizzo: VI
 Numero civico: IT
 CAP: IT
 Comune: IT
 Provincia: IT
 Nazione: IT

Dati del cessionario / committente

Dati anagrafici

Identificativo fiscale ai fini IVA: IT
 Denominazione: IT

Dati della sede

Indirizzo: VI
 Numero civico: IT
 CAP: IT
 Comune: IT
 Provincia: IT
 Nazione: IT

Versione prodotta con foglio di stile Sdi www.fatturapa.gov.it

Versione FPA12

Dati generali del documento

Tipologia documento: TD01 (fattura)
 Valuta importi: EUR
 Data documento: 2019-09-30 (30 Settembre 2019)
 Numero documento: 0000146/PA
 Importo totale documento: 366.00

Dati dell'ordine di acquisto

Identificativo ordine di acquisto: 160
 Data ordine di acquisto: 2019-02-26 (26 Febbraio 2019)
 Codice Identificativo Gara (CIG): Z

Dati relativi alle linee di dettaglio della fornitura

Nr. linea: 1

Codifica articolo

Tipo: Codice
 Valore: SR

Figura 11 - Fattura con CSS SDI

3.10 Download Xml Fattura

Con questo bottone è possibile acquisire sul proprio Dispositivo la fattura nel formato standard XML definito da SDI, al fine di utilizzarlo per, ad esempio, importarlo manualmente in sistemi gestionali propri.

Dopo aver cliccato sul bottone, rispetto alle impostazioni del browser, sarà mostrata una finestra per il salvataggio del file sul dispositivo dell'operatore.

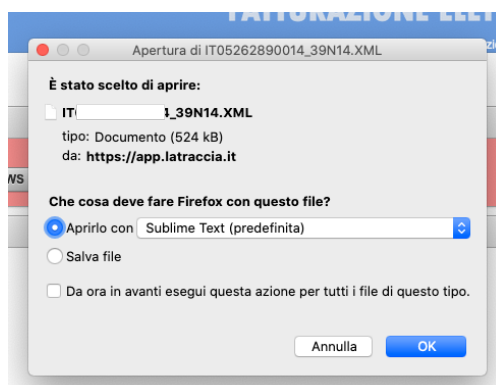


Figura 12 - Salvataggio XML Fattura

Il file così acquisito potrà essere utilizzato secondo le proprie necessità operative.
Come detto in precedenza, il formato del file è quello definito dalle regole della piattaforma SDI.

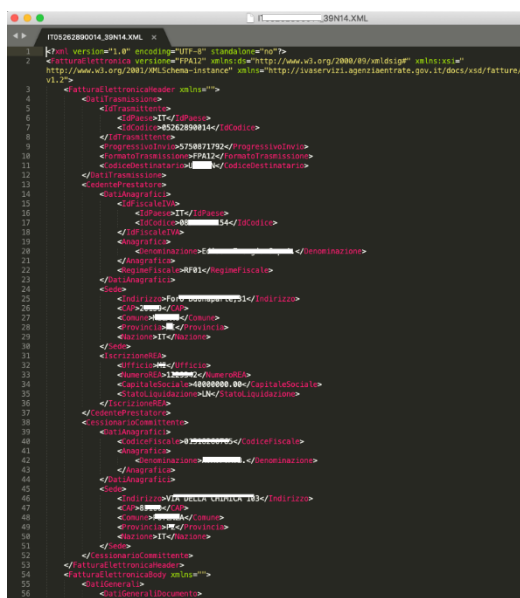


Figura 13 - Fattura in XML

3.11 Utenti

Attraverso il bottone Utenti, presente nella pagina iniziale dell'elenco fatture, è possibile gestire gli operatori abilitati al sistema Fattel.

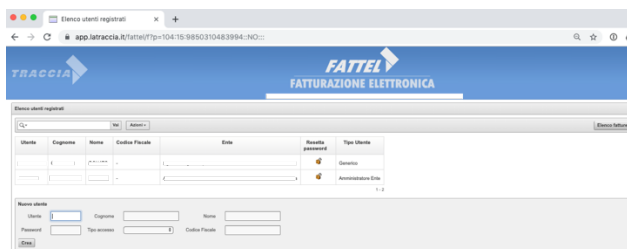


Figura 14 - Utenti

Nel momento in cui si voglia aggiungere un ulteriore utente, è necessario indicare il ruolo dello stesso tra Amministratore Ente e Operatore, dove l'unica differenza è determinata dalla possibilità appunto di gestire gli utenti.



Figura 15 - Creazione Utente

3.12 Import Fattura

Il bottone Import Fattura, presente nella pagina iniziale dell'elenco fatture, permette di caricare in **FATTEL** le fatture ricevute attraverso canali differenti (tipicamente E-mail Pec). E' necessario inserire a sistema il riferimento SDI, e attraverso i relativi pulsanti, eseguire il caricamento dei file con estensione XML e P7m.



Figura 16 - Import Fatture

4 Conservazione

La fase di conservazione prevede la creazione del pacchetto di archiviazione e il suo invio al provider indicato dal cliente, con cui ha stipulato la convenzione di conservazione. Al netto dei WS creati per il colloquio con i diversi provider, vediamo i moduli di gestione del sistema.

Qui descriviamo le modalità presenti per ARUBA.

4.1 Conservazione Fatture

Le fatture non appena ricevute da SDI sono elaborate al fine di estrarre il file XML di dettaglio. Il file (XML o P7M) è quindi immediatamente inviato in conservazione, attraverso un Pacchetto di versamento e con allegato l'Ipdv (l'indice del pacchetto di versamento, un file XML contenente le informazioni sul documento che viene inviato in conservazione).

Il pacchetto di versamento (semplicemente il file della fattura in XML o P7M) deve rispondere alla "classe documentale" definita da cliente con il provider prescelto.

L'Ipdv viene creato secondo questa guida:

Le voci obbligatorie sono:

- <pdvid>@PDVID@</pdvi>
 - Codice univoco che identifica il pacchetto di versamento stesso

- <docid>@DOCID@</docid>
 - Id del documento;
- <filename>@FILENAME@</filename>
 - Riporta il nome del File salvato su ;
- <mimetype>@MIMETYPE@</mimetype>
 - Esempio : application/pdf. Riporta la tipologia di Mimetype in relazione alla estensione del file che si vuole versare;
- <closingDate>2015-05-26T13:58:09.940Z</closingDate>
 - Data;
- <hash algorithm="@SHA-256/MD5/SHA-1@">
- <value>@HASH@</value>
 - Codice univoco che contraddistingue il documento stesso, garantendone la riconoscibilità e incorruttibilità in forma automatica e univoca.

I metadati definiti per l'invio sono i seguenti:

- Informazioni generali:
 - <name>dataDocumentoTributario</name>
<value><Data fattura></value>
 - <name>oggettodocumento</name>
<value>Conservazione fattura elettronica blocco id <num blocco> per la fattura con riferimento sdi <identificativo Sdi></value>
- Soggetto tributario:
 - <name>cognome</name>
<value><Cognome responsabile></value>
 - <name>nome</name>
<value><Nome responsabile></value>
 - <name>denominazione</name>
<value><Denominazione ente></value>
 - <name>codicefiscale</name>
<value><Codice fiscale responsabile></value>
 - <name>partitaiva</name>
<value><Codice fiscale ente></value>
- Destinatario:
 - <name>cognome</name>
<value><Cognome responsabile></value>
 - <name>nome</name>
<value><Nome responsabile></value>
 - <name>denominazione</name>
<value><Denominazione ente></value>
 - <name>codicefiscale</name>
<value><Codice fiscale responsabile> </value>

- <name>partitaiva</name>
<value><Codice fiscale ente></value>
- Soggetto produttore:
 - <name>cognome</name>
<value><Cognome cedente prestatore></value>
 - <name>nome</name>
<value><Nome cedente prestatore></value>
 - <name>denominazione</name>
<value><Denominazione cedente prestatore></value>
 - <name>codicefiscale</name>
<value><Codice fiscale cedente prestatore></value>
 - <name>partitaiva</name>
<value><Partita IVA cedente prestatore></value>

4.2 Inoltro Pacchetti di Conservazione

I file, contenuti nel pacchetto di versamento, vengono inviati al provider secondo il canale e le modalità da quest'ultimo indicato.

Per **Aruba Docfly** l'invio è in modalità FTP e i file trasmessi vengono memorizzati su di uno spazio definito ed assegnato in fase di sottoscrizione del contratto.

Nel momento in cui viene effettuato l'invio in conservazione, nella directory FTP viene creata una cartella in cui vengono salvati il file IPDV ed i file in esso elencati.

Con cadenza periodica, **Aruba Docfly** effettua una lettura del contenuto delle directory salvate nello spazio FTP. Per ciascun file elencato in ogni IPDV, Aruba Docfly calcola la codifica HASH e la confronta con la codifica specificata nei metadati. Se le codifiche coincidono il pacchetto di versamento viene conservato con successo. Viceversa, viene inoltrata una notifica di errore all'indirizzo e-mail specificato in fase di sottoscrizione del contratto.

I file P7M inviati in conservazione subiscono un'ulteriore validazione riguardante la validità della firma digitale.

4.3 Elementi inviati in Conservazione.

Gli elementi inviati in conservazione sono:

- **Fattura Passiva:**
 - File IPDV: file contenenti i metadati riferiti ai file da inviare in conservazione;
 - File XML/P7M della fattura ricevuta;
 - File XML relativo ad una notifica di accettazione/rifiuto;

- File XML relativo ad una notifica di decorrenza termini.
- **Fattura Attiva:**
 - Per la sezione di Fattura attiva, questa non è parte integrante di Fattel. Per gli utenti che adottano la ns. soluzione di Fattura Attiva, abbiamo utilizzato i servizi di Aruba che richiedono esclusivamente l'invio del file XML relativo alla fattura attiva, secondo le specifiche SDI. Il servizio di Aruba si preoccupa a sua volta dell'inoltro a SDI del file secondo le specifiche necessarie, ed all'invio in conservazione della fattura stessa. Potete far riferimento alla documentazione del portale Aruba per la gestione della conservazione delle fatture attive.

5 Servizi Web

In questo capitolo andiamo a trattare i servizi web realizzati per colloquiare con SDI, con sistemi esterni ai fini della protocollazione o contabili.

5.1 Scarica PdD

Il bottone **Scarica PdD** permette di scaricare il pacchetto inviato in conservazione direttamente dalla piattaforma Fattel, evitando di collegarsi al provider con cui si è definito l'accordo di conservazione.

Prerequisito per l'abilitazione è la disponibilità da parte del provider dei WS di interrogazione ed acquisizione del dato.

5.2 Protocollazione Automatica

I WS di Protocollazione Automatica permettono, alla ricezione delle fatture, l'invio della stessa al sistema di protocollo del cliente, attraverso i canali e le modalità messe a disposizione dallo stesso.

Al momento, i WS sviluppati permettono:

- la gestione dell'anagrafica del mittente (Creazione ed Interrogazione) relativa al mittente della fattura;
- la creazione del protocollo con l'invio dei singoli file, quali allegati al protocollo;
- La ricezione del numero e data Protocollo con l'aggiornamento in Fattel dei campi relativi;

5.3 Invio a Registro Fatture

Per alcuni clienti sono stati sviluppati appositi servizi per l'invio delle fatture, includendo i dati del protocollo, a sistemi contabili al fine di aggiornare in automatico il Registro Unico delle Fatture.

Altri sviluppi interessanti sono stati quelli di inviare le fatture anche a sistemi gestionali dei Contratti, al fine di legare, attraverso i campi CIG/CUP presenti nelle fatture, queste ultime ai contratti in modo da creare, in automatico, un fascicolo relativo ai contratti, contenente tutte le fatture e gli stati che assume durante il trattamento della stessa.

5.4 Gestione Risposte

Per alcune soluzioni, sono stati sviluppati servizi che permettono, questa volta, di ricevere le risposte di accettazione/rifiuti delle fatture, da sistemi esterni.

Nell'esempio di un sistema di gestione contratti, il Responsabile dello stesso, invece di accedere alla piattaforma Fattel, può, se la funzione è presente nel suo applicativo, inviare i file necessari all'accettazione o al rifiuto.

Le risposte sono inviate anch'esse in conservazione assieme alla fattura.