

Manuale di gestione documentale

Comune di Sale

Provincia di Alessandria

INDICE

Sezione 1 Disposizioni generali

- 1.1** *Ambito di applicazione*
- 1.2** *Definizioni dei termini*
- 1.3** *Storia delle versioni del documento*
- 1.4** *Area organizzativa omogenea*
- 1.5** *Servizio per la gestione documentale e i suoi responsabili*
- 1.6** *Unicità del protocollo informatico*
- 1.7** *Modello operativo adottato per la gestione dei documenti*

Sezione 2 Formazione dei documenti

- 2.1** *Requisiti minimi del documento*
- 2.2** *Formazione dei documenti informatici*
- 2.3** *Formato dei documenti informatici*
- 2.4** *Metadati dei documenti informatici*
- 2.5** *Sottoscrizione dei documenti informatici*

Sezione 3 Ricezione dei documenti

- 3.1** *Ricezione dei documenti su supporto cartaceo*
- 3.2** *Ricezione dei documenti informatici*
- 3.3** *Formato e firma dei documenti informatici ricevuti*
- 3.4** *Acquisizione dei documenti analogici tramite copia immagine e copia informatica*
- 3.5** *Ricevute attestanti la ricezione dei documenti*
- 3.6** *Apertura della posta*
- 3.7** *Conservazione delle buste o altri contenitori di documentazione analogica*
- 3.8** *Conservazione delle ricevute attestanti la consegna dei documenti spediti tramite posta elettronica certificata*
- 3.9** *Orari di apertura per il ricevimento della documentazione cartacea*

Sezione 4 Registrazione dei documenti

- 4.1** *Documenti soggetti a registrazione di protocollo*
- 4.2** *Documenti non soggetti a registrazione di protocollo*
- 4.3** *Registrazione di protocollo dei documenti ricevuti e spediti*
- 4.4** *Registrazione dei documenti interni*
- 4.5** *Formazione di registri e repertori informatici particolari*
- 4.6** *Registrazione degli allegati*
- 4.7** *Segnatura di protocollo*
- 4.8** *Annullamento delle registrazioni di protocollo*
- 4.9** *Differimento dei termini di protocollazione*
- 4.10** *Registro giornaliero e registro delle modifiche*
- 4.11** *Registro di emergenza*

Sezione 5 Documentazione particolare

- 5.1** *Deliberazioni di Giunta e Consiglio, determinazioni dirigenziali, decreti, ordinanze, contratti, verbali sanzioni amministrative polizia locale e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti, pubblicazioni all'albo on line e notifiche*
- 5.2** *Documentazione di gare d'appalto*
- 5.3** *Documenti con mittente non identificabile, posta personale*
- 5.4** *Protocollo riservato*
- 5.5** *Documenti informatici con certificato di firma scaduto o revocato*
- 5.6** *Documenti inviati via fax*
- 5.7** *Corrispondenza con più destinatari*
- 5.8** *Allegati*

- 5.9 Documenti di competenza di altre amministrazioni
- 5.10 Oggetti plurimi
- 5.11 Documentazione prodotta e registrata in appositi gestionali
- 5.12 Modelli pubblicati di documenti
- 5.13 Trasmissioni telematiche e procedimenti amministrativi on line
- 5.14 Produzione di copie cartacee di documenti informatici e di copie informatiche di documenti cartacei
- 5.15 Amministrazione trasparente
- 5.16 Albo on line

Sezione 6 Posta elettronica

- 6.1 Posta elettronica certificata
- 6.2 Gestione della posta elettronica
- 6.3 Posta elettronica per le comunicazioni interne
- 6.4 Posta elettronica ricevuta da cittadini o altri soggetti privati
- 6.5 Posta elettronica ricevuta da altre pubbliche amministrazioni

Sezione 7 Assegnazione dei documenti

- 7.1 Assegnazione
- 7.2 Modifica delle assegnazioni
- 7.3 Consegna dei documenti

Sezione 8 Classificazione e fascicolazione dei documenti

- 8.1 Classificazione dei documenti
- 8.2 Formazione e identificazione dei fascicoli
- 8.3 Processo di fascicolazione
- 8.4 Modifica delle assegnazioni dei fascicoli
- 8.5 Fascicolo ibrido
- 8.6 Fascicolo informatico
- 8.7 Metadati dei fascicoli informatici
- 8.8 Tenuta dei fascicoli dell'archivio corrente

Sezione 9 Invio dei documenti destinati all'esterno

- 9.1 Invio dei documenti informatici
- 9.2 Spedizione dei documenti analogici

Sezione 10 Scansione dei documenti su supporto cartaceo

- 10.1 Documenti soggetti a scansione
- 10.2 Processo di scansione

Sezione 11 Conservazione e tenuta dei documenti

- 11.1 Sistema informatico
- 11.2 Gestione delle password
- 11.3 Conservazione e memorizzazione dei documenti analogici, informatici e delle rappresentazioni digitali dei documenti cartacei
- 11.4 Sistema di conservazione dei documenti informatici
- 11.5 Pacchetti di versamento
- 11.6 Conservazione dei documenti analogici
- 11.7 Trasferimento delle unità archivistiche analogiche negli archivi di deposito e storico e conservazione dei fascicoli informatici
- 11.8 Selezione e conservazione dei documenti
- 11.9 Gestione dell'archivio storico

Sezione 12 Accesso a dati, informazioni e documenti - Pubblicità legale e trasparenza amministrativa

12.1 *Accessibilità da parte degli utenti appartenenti all'Amministrazione*

12.2 *Accesso esterno*

12.3 *Accesso da parte di altre amministrazioni*

Sezione 13 Approvazione, Revisione e Pubblicazione

13.1 *Approvazione*

13.2 *Revisione*

13.3 *Pubblicazione e divulgazione*

1 Disposizioni generali

1.1 Ambito di applicazione

Il presente manuale è adottato ai sensi del Codice dell'Amministrazione digitale Dlgs 82/2005 e delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (di seguito indicate come Linee Guida di Agid), Determinazioni Agid 407/2020 e 371/2021, in vigore dal 10 settembre 2020 e con adozione obbligatoria dal 1 gennaio 2022.

Il manuale di gestione documentale costituisce lo strumento operativo che descrive e disciplina il sistema di produzione e di gestione documenti.

Il sistema documentale dell'Ente è composto da:

- archivio corrente, documentazione relativa ad affari in corso di trattazione;
- archivio di deposito, documentazione relativa ad affari esauriti, non più occorrente alla trattazione degli affari in corso, che riveste comunque una valenza giuridico-amministrativa, non ancora destinata, prelieve le opportune operazioni di selezione e scarto, alla conservazione permanente;
- archivio storico, il complesso di documenti relativi ad affari esauriti da almeno quaranta anni, che rivestono una valenza storico-culturale, destinati alla conservazione permanente e consultabili da parte del pubblico.

Il manuale sovrintende alla gestione dell'archivio corrente.

Il manuale è costituito dall'insieme delle regole tecniche ed organizzative per l'attuazione del protocollo informatico e la gestione del flusso documentale e, in particolare, disciplina le attività di formazione, protocollazione, registrazione, classificazione, fascicolazione, gestione, archiviazione e conservazione dei documenti su qualsiasi supporto formati, considerate come flusso di lavorazione degli stessi.

Regolamenta inoltre le fasi operative per la gestione informatica dei documenti, nel rispetto della normativa vigente in materia di trasparenza degli atti amministrativi, di tutela della privacy e delle politiche di sicurezza.

Il manuale è adottato dalla Giunta comunale con suo provvedimento proprio, su proposta del responsabile della gestione documentale.

Il Manuale di gestione è reso pubblico tramite la sua diffusione sul sito internet dell'Amministrazione e la pubblicazione all'albo on-line degli atti di adozione e revisione.

L'Amministrazione ha adottato un sistema di gestione documentale avanzato di protocollazione informatica sicuro, certificato e con piena validità giuridica, che consente di avviare progressivamente processi di dematerializzazione della documentazione.

Sono state intraprese le iniziative necessarie all'attuazione delle disposizioni normative in materia di gestione informatica dei documenti e dematerializzazione, perseguendo gli obiettivi di ammodernamento della pubblica amministrazione, miglioramento dei servizi, trasparenza, contenimento dei costi secondo i criteri di economicità, efficacia e pubblicità dell'azione amministrativa, coordinamento dei flussi documentali con il protocollo informatico e i procedimenti amministrativi.

Il manuale di gestione documentale fornisce le indicazioni per realizzare i processi di innovazione, che porteranno ad attuare, tramite le nuove tecnologie, la gestione documentale in modalità esclusivamente informatiche.

Al fine di garantire lo sviluppo del processo di digitalizzazione previsto dalla normativa vigente l'Ente provvede a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese.

Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid, entrate in vigore il 10 settembre 2020, sono applicabili dal 1° gennaio 2022 e comportano l'abrogazione delle Regole tecniche per il protocollo informatico DPCM 3/12/2013, Regole tecniche in materia di sistema di conservazione DPCM 3/12/2013 e Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici DPCM 13/11/2014.

1.2 Definizioni dei termini

Per quanto riguarda la definizione dei termini, che costituisce la corretta interpretazione del dettato del presente manuale, si rimanda al Glossario dei termini e degli acronimi allegato alle Linee guida di Agid (Documento n. 1), all'articolo 1 Definizioni del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017 e all'articolo 3 Definizioni del Regolamento (UE) N. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

1.3 Storia delle versioni del documento

Prima versione del Manuale di gestione documentale.

1.4 Area organizzativa omogenea

Ai fini della gestione dei documenti è individuata una sola area organizzativa omogenea denominata Comune di Sale, composta dall'insieme di tutte le sue unità organizzative come da elenco allegato (Documento n. 2). L'Ente è accreditato all'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi (IPA), contenente informazioni dettagliate sugli enti e le relative strutture organizzative; i codici che identificano il Comune sono:

codice IPA	c h694
codice univoco AOO	A46D13E

Il Comune fa parte dell'Unione Terre di Fiume.

Per qualsiasi informazione relativa all'Amministrazione si rimanda alle pagine del sito istituzionale.

1.5 Servizio per la gestione documentale e i suoi responsabili

Nell'ambito dell'area organizzativa omogenea, ai sensi della normativa vigente, è istituito il Servizio per la gestione documentale, con competenza sulla gestione dell'intera documentazione archivistica dell'Ente, ovunque trattata, distribuita o conservata, ai fini della sua corretta registrazione, classificazione, conservazione, selezione e ordinamento.

Il servizio per la gestione documentale è attribuito alla struttura Servizi Amministrativi - Demografici ed ausiliari - Segreteria – URP, che include l'Ufficio Protocollo.

Il servizio, in accordo e nel rispetto della normativa vigente, nonché della struttura organizzativa dell'Ente e delle disposizioni che lo regolano:

- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, compreso il sistema dei livelli di autorizzazione e delle abilitazioni adottato (Documento n. 2);
- garantisce che le operazioni di registrazione, di segnatura, la produzione e conservazione del registro di protocollo si svolgano nel rispetto della normativa vigente e autorizza le operazioni di annullamento delle registrazioni di protocollo;
- verifica e cura l'osservanza delle disposizioni del presente manuale;
- cura, per quanto di competenza, i processi di dematerializzazione dei flussi documentali e della digitalizzazione dei documenti;
- autorizza, con appositi provvedimenti, le operazioni di annullamento delle registrazioni di protocollo;
- cura il costante aggiornamento del presente manuale di gestione e di tutti i suoi allegati.

Il responsabile della gestione documentale coincide con il responsabile della struttura di cui sopra, e quest'ultimo per casi di vacanza, assenza o impedimento può nominare un vicario che lo sostituisca, definendone le funzioni meramente operative.

È nominato il responsabile della conservazione (Documento n. 12), che d'intesa con il responsabile della gestione documentale svolge le funzioni definite dal paragrafo 4.7 delle Linee guida di Agid, tra cui la predisposizione e l'aggiornamento del Manuale di conservazione (Documento n. 13), garantendo la conservazione integrata dei documenti e delle informazioni di contesto generale, prodotte sia nelle fasi di gestione sia in quelle di conservazione degli stessi, come strumenti di descrizione, ricerca, gestione e conservazione dei documenti.

Come previsto dall'articolo 17 del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017, è individuato l'ufficio che sovrintende la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, e nominato il responsabile (Documento n. 14).

1.6 Unicità del protocollo informatico

La numerazione delle registrazioni di protocollo è unica, progressiva, corrisponde all'anno solare ed è composta da almeno sette numeri, tuttavia a norma dell'articolo 53, comma 5 del DPR 445/2000 sono possibili registrazioni particolari. L'Ente non riconosce validità a registrazioni particolari che non siano quelle individuate nell'elenco allegato (Documento n. 3). Il sistema informatico di gestione del protocollo è

sincronizzato per il calcolo dell'ora con un orologio atomico, tramite server NTP Network time protocol, che garantisce data e ora certe.

A ogni documento è dato un solo numero, che non può essere utilizzato per la registrazione di altri documenti anche se correlati allo stesso.

1.7 Modello operativo adottato per la gestione dei documenti

Per la gestione dei documenti è adottato un modello operativo decentrato che prevede la partecipazione attiva di più soggetti e uffici utenti abilitati a svolgere soltanto le operazioni di loro competenza di cui all'elenco allegato (Documento n. 2), le abilitazioni sono definite dal responsabile della gestione documentale.

I dirigenti sono responsabili, secondo i principi stabiliti dalla normativa vigente, della corretta applicazione delle disposizioni contenute nel presente manuale in relazione all'attività della struttura cui sono preposti, con particolare riguardo alle operazioni di protocollazione, classificazione, fascicolazione, conservazione e gestione dei documenti.

Il sistema di gestione documentale e il protocollo informatico sono condotti in modalità cloud computing e consentono all'Ente di usufruire dei servizi di protocollazione e gestione documentale messi a disposizione dall'applicativo Protel di Golem software, come descritto nel Piano di sicurezza dei documenti informatici (Documento n. 15).

L'archivio storico e di deposito analogico è conservato presso la sede dell'Ente in locali di proprietà.

L'Archivio corrente analogico è conservato presso le unità organizzative. La documentazione informatica è gestita secondo le modalità descritte nel Piano di sicurezza dei documenti informatici (Documento n. 15), per la conservazione l'Ente si avvale del servizio di conservazione digitale a norma erogato da Aruba SpA e adotta il Manuale di conservazione (Documento n. 13).

2 Formazione dei documenti

2.1 Requisiti minimi del documento

Le modalità di formazione dei documenti, del loro contenuto e della loro struttura sono determinate dal responsabile della gestione documentale e da quanto previsto dal presente manuale; per quanto riguarda i documenti informatici, la loro produzione è regolata come descritto nel Piano di sicurezza dei documenti informatici (Documento n. 15), sulla base di modelli standard presenti nel sistema informatico di gestione documentale. I documenti prodotti e con rilevanza giuridico-amministrativa, indipendentemente dal supporto sul quale sono formati, contengono i seguenti dati ed elementi formali o l'associazione permanente ad essi:

- denominazione dell'Amministrazione, comprensiva del codice fiscale e del codice identificativo di cui all'articolo 1.4; per quanto riguarda i documenti su supporto cartaceo si utilizza il formato predisposto dall'Amministrazione (carta intestata);
- indicazione del settore, servizio o ufficio che ha prodotto il documento;
- indirizzo completo (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, numero di fax, indirizzo di posta elettronica certificata e posta elettronica ordinaria);
- data: luogo, giorno, mese, anno;
- destinatario/i, per i documenti in partenza;
- oggetto del documento, sufficientemente esaustivo (ogni documento deve trattare un solo oggetto);
- classificazione;
- fascicolo;
- numero degli allegati, se presenti;
- numero di protocollo;
- testo;
- indicazione dello scrittore del documento (nome e cognome anche abbreviato);
- estremi identificativi del responsabile del procedimento (L. 241/1990);
- sottoscrizione autografa o elettronico/digitale.

Per i documenti informatici il numero di protocollo è associato al documento nel sistema tramite l'apposizione di metadati che lo identificano all'interno del documentale.

2.2 Formazione dei documenti informatici

L'Ente forma gli originali dei propri documenti con mezzi informatici secondo le regole tecniche di cui all'articolo 71 del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017, mediante l'utilizzo di appositi strumenti software. Le tipologie particolari di documenti per i quali si stabiliscono modalità di trattamento specifiche e/o prodotti mediante modelli standard sono indicati nella Sezione 5.

2.3 Formato dei documenti informatici

I documenti informatici prodotti dall'Ente, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma elettronica/digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di documenti informatici (Linee Guida di Agid, Allegato 2 Formati di file e riversamento), al fine di garantire la loro inalterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura. Il formato prescelto e utilizzato è pdf/A, che garantisce staticità e immodificabilità, ma al contempo assicura la leggibilità dei documenti.

2.4 Metadati dei documenti informatici

Al documento informatico è associato l'insieme dei metadati, come definito dalla normativa vigente in materia di documenti informatici (articolo 53 del DPR 445/2000; articolo 9 del DPCM 3/12/2013 Regole tecniche per il protocollo informatico e Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati).

Per metadati si intendono i dati associati a un documento informatico per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.

I metadati aggiuntivi e i metadati dei documenti informatici soggetti a registrazione particolare (Documento n.

3) sono individuati nel Manuale di conservazione (Documento n. 13).

2.5 Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma elettronico/digitale conforme alle disposizioni di legge.

L'Ente utilizza:

- firme elettroniche semplici (come la posta elettronica);
- firme elettroniche avanzata (come l'accreditamento per le procedure telematiche e sistema di validazione delle fasi procedurali, di comunicazione interna e abilitazione allo svolgimento di attività specifiche);
- firme digitali o di altro tipo di firma elettronica qualificata.

L'Ente ha stipulato un contratto di fornitura di servizio di firme digitali con un certificatore accreditato. Gli strumenti tecnologici utilizzati sono: token USB e firma remota.

I responsabili di Servizio e alcuni dipendenti con specifiche mansioni e ruoli con rilevanza esterna, in base all'organigramma dell'Ente, sono dotati di firma digitale.

Il dispositivo per la generazione della firma digitale è usato esclusivamente dal titolare designato dall'Ente; ai sensi della normativa vigente tale utilizzo si presume comunque riconducibile al titolare, salvo che questi dia prova contraria.

La scadenza dei certificati di firma è controllata dai titolari ed in autonomia è effettuato l'eventuale rinnovo in prossimità della scadenza.

3 Ricezione dei documenti

3.1 Ricezione dei documenti su supporto cartaceo

I documenti su supporto cartaceo possono arrivare all'Ente attraverso:

- il servizio postale e corrieri;
- la consegna diretta agli uffici, ai funzionari, agli sportelli abilitati presso l'Amministrazione al ricevimento della documentazione;
- gli apparecchi telefax.

I documenti, esclusi quelli non soggetti a registrazione di protocollo, devono pervenire al protocollo per la loro registrazione. Quelli arrivati via telefax sono soggetti alle stesse regole di registrazione degli altri documenti cartacei.

La corrispondenza indirizzata alla cortese attenzione del personale dell'Ente è regolarmente aperta e registrata a protocollo. Non è ammessa la ricezione di corrispondenza di carattere personale; l'ufficio che provvede alla protocollazione è in ogni caso tenuto a verificare il contenuto della corrispondenza pervenuta.

I documenti analogici ricevuti sono messi a disposizione dei singoli uffici in apposite cassette una volta protocollati. I responsabili di procedimento sono poi autonomi nel ritirare la documentazione e conservarla presso le singole unità operative. Qualora i documenti non vengano ritirati, saranno recapitati nei singoli uffici dagli addetti dell'ufficio Protocollo una volta l'anno.

3.2 Ricezione dei documenti informatici

La ricezione di comunicazioni, documenti e dati informatici è assicurata tramite:

- casella di posta elettronica certificata eletta a domicilio digitale e integrata con il sistema informatico di protocollazione, accessibile all'Ufficio Protocollo, che effettua la protocollazione. Il responsabile della gestione documentale provvede a rendere pubblico e a trasmettere all'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi IPA (ai sensi delle Linee guida Agid, versione 1.0 del 27 febbraio 2019) gli indirizzi delle caselle di posta elettronica certificata.

La casella di posta elettronica certificata riceve messaggi sia da caselle di posta certificata che da caselle di posta ordinaria.

Per la gestione della posta elettronica si veda quanto previsto alla Sezione 6.

L'Amministrazione riceve e trasmette documenti informatici mediante flussi telematici di dati (si veda l'articolo 5.13 Trasmissioni telematiche e procedimenti amministrativi on line).

3.3 Formato e firma dei documenti informatici ricevuti

L'Ente assicura l'accettazione dei documenti elettronici ricevuti tramite la casella di posta elettronica certificata, i servizi telematici o consegnati su supporto informatico quando prodotti in uno dei formati indicati dalle Linee Guida di Agid, Allegato 2 Formati di file e riversamento.

In tutti gli altri casi, laddove il documento inviato o consegnato all'Ente sia prodotto in formati tali da non consentirne una corretta gestione, l'Ente ne darà comunicazione al mittente richiedendo contestualmente la ripetizione dell'invio o della consegna in uno dei formati adeguati.

Le verifiche dei documenti sono effettuate dall'Ufficio Protocollo e dai servizi che hanno competenza sul documento. Il certificato di firma è verificato da parte delle postazioni abilitate alla registrazione dei documenti in ingresso e/o dal responsabile del procedimento. In caso di certificati scaduti o revocati si rimanda alla Sezione 5.

3.4 Acquisizione dei documenti analogici tramite copia informatica

L'Ente può acquisire i documenti analogici originali attraverso la copia per immagine su supporto informatico o la copia informatica.

Dei documenti analogici ricevuti viene effettuata copia immagine da associare alla registrazione di protocollo e il documento originale viene poi reso disponibile all'ufficio competente. Le immagini digitali dei documenti cartacei acquisite con lo scanner sono rese disponibili agli uffici, o ai responsabili di procedimento, tramite il sistema informatico di gestione documentale. Il processo di scansione della documentazione cartacea è descritto nella Sezione 10.

Le copie informatiche di documenti analogici sono acquisite nel sistema mediante processi e strumenti che assicurino che il documento informatico abbia contenuto identico a quello del documento analogico da cui è

tratto.

L'unitarietà è garantita dal sistema mediante il numero di protocollo, l'indice di classificazione e il numero di fascicolo.

3.5 Ricevute attestanti la ricezione dei documenti

La ricevuta della consegna di un documento analogico può essere costituita dalla fotocopia del primo foglio del documento stesso con un timbro che attesti il giorno della consegna. Compatibilmente con le esigenze del servizio, si procederà alla protocollazione del documento: in tal caso verrà consegnata la ricevuta prodotta automaticamente del sistema di protocollo informatico.

Nel caso di ricezione dei documenti informatici, la notifica al mittente dell'avvenuto ricevimento è assicurata dal sistema elettronico.

Per istanze, segnalazioni o comunicazioni è rilasciata immediata ricevuta ai sensi dell'articolo 18 bis della L. 241/1990. La data di protocollazione non può comunque essere diversa da quella di effettiva presentazione, in seguito alla protocollazione del documento il sistema genera in automatico una ricevuta che riporta anche il numero di protocollo assegnato.

3.6 Apertura della posta

Il responsabile del Servizio per la gestione documentale apre tutta la corrispondenza pervenuta all'Ente, salvo i casi particolari specificati nella Sezione 5, compresa la posta elettronica certificata e la posta elettronica istituzionale.

3.7 Conservazione delle buste o altri contenitori di documentazione analogica

Le buste dei documenti analogici pervenuti non si inoltrano agli uffici destinatari e non si conservano a meno che non contengano dati essenziali.

3.8 Conservazione delle ricevute attestanti la consegna dei documenti spediti tramite posta elettronica certificata

Le ricevute relative alla trasmissione di documenti informatici tramite casella di posta elettronica certificata, in quanto documenti informatici, sono soggette alle operazioni di conservazione.

Il sistema di protocollo informatico associa in automatico le ricevute pec alla registrazione di protocollo.

3.9 Orari di apertura per il ricevimento della documentazione cartacea

L'Ufficio protocollo riceve la documentazione negli orari di apertura al pubblico, pubblicati sul sito internet istituzionale.

4 Registrazione dei documenti

4.1 Documenti soggetti a registrazione di protocollo

Tutti i documenti prodotti e ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, a eccezione di quelli indicati nel successivo articolo, sono registrati al protocollo.

I documenti ai fini della gestione documentale si distinguono in:

- documenti in arrivo, cioè documenti ricevuti dall'esterno dall'Ente;
- documenti in partenza, cioè i documenti prodotti e spediti all'esterno dall'Ente;
- documenti interni, cioè documenti prodotti all'interno dell'Ente, che siano o meno scambiati tra strutture.

4.2 Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo: gazzette ufficiali, bollettini ufficiali, notiziari della pubblica amministrazione, note di ricezione delle circolari e di altre disposizioni, materiale statistico ricevuto, atti preparatori interni, giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti quei documenti già soggetti a registrazione particolare da parte dell'Ente il cui elenco è allegato al presente manuale (Documento n. 3).

Inoltre, sono escluse dalla protocollazione le seguenti categorie di documenti:

- comunicazioni d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti, ecc.);
- richieste di ferie ed altri permessi;
- richieste di rimborso spese e missioni;
- pubblicità conoscitiva di convegni;
- pubblicità in generale;
- estratti conto bancari e relativi a Poste Italiane;
- offerte, i listini prezzi e i preventivi di terzi non richiesti;
- ricevute di ritorno delle raccomandate A.R.;
- tutti i documenti che, per loro natura, non rivestono alcuna rilevanza giuridico amministrativa presente o futura.

4.3 Registrazione di protocollo dei documenti ricevuti e spediti

La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione. I requisiti necessari di ciascuna registrazione di protocollo sono:

- numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e numero di protocollo dei documenti ricevuti, se disponibili;
- impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
- classificazione (si veda titolario allegato Documento n. 5);
- assegnazione.

Inoltre possono essere aggiunti:

- data di arrivo;
- allegati (numero e descrizione);
- estremi del provvedimento differimento dei termini di registrazione;
- mezzo di ricezione/spedizione;
- tipo di documento;
- livello di riservatezza;
- elementi identificativi del procedimento amministrativo;
- classificazione e fascicolazione del documento ricevuto.

La fascicolazione dei documenti ricevuti è effettuata successivamente alla registrazione di protocollo, da parte dell'ufficio assegnatario del documento. I documenti in partenza sono fascicolati contestualmente

all'operazione di registrazione, dall'ufficio produttore del documento.

Per il corretto inserimento dei dati relativi a mittenti e destinatari nella banca dati dei soggetti si applicano le Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico (Documento n. 4).

4.4 Registrazione dei documenti interni

I documenti prodotti dall'Ente a solo uso interno, che non rientrano in quelli esclusi da protocollazione, indipendentemente dal supporto sul quale sono formati, sono protocollati. Questi verranno fascicolati dal mittente in fase di registrazione.

4.5 Formazione di registri e repertori informatici particolari

L'Ente forma i propri registri e repertori informatici particolari (Documento n. 3) mediante la generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, secondo una struttura logica predeterminata e memorizzata in forma statica.

Ogni registrazione deve riportare necessariamente:

- dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile);
- numero di repertorio progressivo e annuale (generato in modo non modificabile).

4.6 Registrazione degli allegati

Il numero e la descrizione degli allegati sono elementi essenziali per l'efficacia di una registrazione. Nella registrazione di protocollo/particolare si riporta la descrizione della tipologia degli allegati e, se significativi, anche dei loro estremi (data, numero, ecc).

Tutti gli allegati devono pervenire con il documento principale alle postazioni abilitate alla protocollazione al fine di essere inseriti nel sistema di gestione documentale.

Per tutti i documenti delle singole unità operative, l'etichetta di protocollo viene apposta sul solo documento principale.

Per i documenti di competenza dell'area Tecnica (Lavori Pubblici ed Edilizia Privata), l'etichetta viene apposta anche su tutti gli allegati.

4.7 Segnatura di protocollo

La segnatura di protocollo è l'associazione ai documenti in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, utile alla sua identificazione univoca e certa.

In merito l'articolo 55, comma 1, del DPR 445/2000 individua le informazioni che caratterizzano la segnatura di protocollo.

Le operazioni di segnatura e registrazione di protocollo sono effettuate contemporaneamente.

Gli standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime e accessorie comunemente scambiate tra le Pubbliche Amministrazioni e associate ai documenti protocollati sono definiti dalle Linee Guida di Agid, Allegato 6 Comunicazione tra AOO di Documenti Amministrativi Protocollati.

Per i documenti informatici trasmessi i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML); per i documenti cartacei la segnatura di protocollo è apposta al documento mediante timbro o tramite l'apposizione di etichette.

4.8 Annullamento delle registrazioni di protocollo

Le registrazioni di protocollo possono essere annullate e/o modificate con una specifica funzione del sistema di gestione informatica dei documenti, a seguito di motivata richiesta scritta al responsabile della gestione documentale o per iniziativa dello stesso. Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema. Il sistema durante la fase di annullamento registra le motivazioni che hanno comportato l'annullamento.

Le richieste di annullamento dei numeri di protocollo devono pervenire all'Ufficio Protocollo.

Sui documenti cartacei è apposto il timbro di annullamento; il documento è conservato, anche fotoriprodotta,

a cura dell'Ufficio Protocollo.

Non è possibile annullare il solo numero di protocollo e mantenere valide le altre informazioni della registrazione.

4.9 Differimento dei termini di protocollazione

La registrazione della documentazione pervenuta avviene nell'arco della giornata o nella successiva giornata lavorativa. Il responsabile della gestione documentale, con apposito provvedimento motivato, può autorizzare la registrazione in tempi successivi, fissando un limite di tempo entro il quale i documenti devono essere protocollati. Ai fini giuridici i termini decorrono dalla data di ricezione riportata sul documento analogico tramite un apposito timbro e dalla data di consegna telematica (tramite pec o servizi on line) per i documenti informatici.

4.10 Registro giornaliero e registro delle modifiche

Il registro giornaliero di protocollo comprende tutte le registrazioni effettuate nell'arco dello stesso giorno; ciascuna registrazione include le informazioni minime previste dal DPR 445/2000, articolo 53.

Il registro delle modifiche comprende le registrazioni annullate e modificate; viene creato solo se nella giornata sono stati effettuati annullamenti o modifiche a protocolli precedentemente acquisiti.

Il registro giornaliero e il registro delle modifiche sono trasmessi entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto. Si tratta di documenti informatici creati in PDF/A, formato adeguato (Linee Guida di Agid, Allegato 2 Formati di file e riversamento) che assicura staticità e immodificabilità, ma al contempo ne consente la leggibilità. Il registro giornaliero e il registro delle modifiche sono integrati con i relativi metadati di identificazione, di profilo generali e specifici, che ne definiscono contesto, contenuto e struttura. La produzione del registro giornaliero e del registro delle modifiche è effettuata automaticamente dal sistema dopo lo scattare della mezzanotte della giornata di riferimento.

Il trasferimento nel sistema di conservazione avviene generando un pacchetto di versamento secondo le modalità concordate con il responsabile della conservazione. Il sistema di conservazione produce un rapporto dell'esito del versamento.

La conservazione del Registro giornaliero di protocollo è affidata ad Aruba SpA. Il sistema di conservazione è descritto nel Manuale di conservazione (Documento n. 13); le iniziative di prevenzione e gestione degli incidenti di sicurezza informatica sono illustrate nel Piano di sicurezza dei documenti informatici (Documento n. 15).

Per quanto riguarda le procedure di conservazione della memoria informatica si veda anche la Sezione 11.

4.11 Registro di emergenza

Il responsabile della gestione documentale autorizza lo svolgimento delle operazioni di protocollo su un registro di emergenza a norma dell'articolo 63 del DPR 445/2000 e provvede successivamente a impartire le disposizioni per il riversamento dei dati nel protocollo informatico (Documento n. 8). All'inizio di ogni anno il responsabile della gestione documentale provvede a istituire il registro di emergenza su supporto cartaceo.

5 Documentazione particolare

5.1 Deliberazioni di Giunta e Consiglio del Comune, determinazioni, decreti, ordinanze, contratti, verbali sanzioni amministrative polizia locale e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti, pubblicazioni all'albo on line e notifiche

Le deliberazioni di Giunta e Consiglio, le determinazioni dei responsabili, i decreti, le ordinanze, i contratti, i verbali della polizia locale e altri tipi di verbalizzazioni previsti dalla legge o da regolamenti, se sono documenti già soggetti a registrazione particolare da parte dell'Ente possono non essere registrati al protocollo.

L'elenco dettagliato delle registrazioni particolari è fornito in allegato (Documento n. 3).

Il sistema di produzione e conservazione di queste tipologie particolari di documenti deve consentire di eseguire su di essa tutte le operazioni previste nell'ambito della gestione dei documenti e del sistema adottato per il protocollo informatico. Ogni registrazione deve riportare necessariamente:

- dati identificativi di ciascun atto (autore, destinatario, oggetto, data, generati in modo non modificabile);
- numero di repertorio progressivo e annuale (generato in modo non modificabile).

Per le pubblicazioni all'albo on line si rimanda alle apposite linee guida di pubblicazione (Documento n. 9).

5.2 Documentazione di gare d'appalto

L'Ente si avvale del Mercato della Pubblica Amministrazione (Me.Pa) e del Sistema Telematico Acquisti Regionale SINTEL, per attivare e gestire gare telematiche. Per procedure nel mercato elettronico o acquisti effettuati mediante piattaforme informatiche, tutta la documentazione è ricevuta telematicamente direttamente nel sistema, che ne garantisce la sicurezza e riservatezza, acquisita nel sistema di gestione documentale e registrata nel protocollo informatico dell'Ente.

5.3 Documenti con mittente non identificabile, posta personale

I documenti, sia analogici che digitali, indirizzati nominalmente al personale dell'Ente sono regolarmente aperti e registrati al protocollo.

Non è ammessa la ricezione di corrispondenza di carattere personale; nel caso in cui risulti esplicita l'attribuzione "personale" o "riservata personale", il documento sarà trasmesso al destinatario, che potrà chiederne la protocollazione. L'ufficio che provvede alla protocollazione è in ogni caso tenuto a verificare il contenuto della corrispondenza pervenuta.

I documenti di cui non sia identificabile il mittente vengono protocollati con indicazione di mittente "anonimo".

5.4 Protocollo riservato

Sono previste particolari forme di riservatezza per la registrazione e l'accesso a:

- documenti legati a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi noti, possono ostacolare il raggiungimento degli obiettivi prefissati;
- documenti dalla cui conoscenza, anche da parte del personale dell'Ente, possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- documenti riguardanti dati sensibili e relativi a ordine pubblico, prevenzione e repressione dei reati, in particolare la corrispondenza tenuta dai tribunali con l'Ufficio Servizi sociali e quella riguardante atti di polizia giudiziaria.

Il responsabile della gestione documentale dispone la registrazione riservata informatica dei documenti. La registrazione è effettuata nel registro del protocollo generale da personale al tal fine autorizzato. Tali documenti se cartacei, dopo le operazioni di protocollo, vengono reinseriti nella busta opportunamente chiusa ed inviati agli uffici di competenza.

5.5 Documenti informatici con certificato di firma scaduto o revocato

Nel caso in cui l'Ente riceva documenti informatici firmati digitalmente il cui certificato di firma risulta scaduto o revocato, questi verranno protocollati, il responsabile di procedimento effettuerà le necessarie verifiche e

darà opportuna comunicazione al mittente.

5.6 Documenti inviati via fax

Sulla base della normativa vigente, la corrispondenza con pubbliche amministrazioni, imprese e professionisti deve avvenire di norma tramite l'uso della posta elettronica. Pertanto non si scambiano documenti via fax tra enti pubblici, aziende e professionisti. In caso di necessità è consentito l'utilizzo del fax verso destinatari coi quali risulti impossibile comunicare in altro modo.

I documenti ricevuti e inviati via fax sono registrati al protocollo. Di norma al fax non segue mai l'originale; qualora l'originale sia spedito a seguito del fax deve essere apposta/associata al documento la dicitura "già inviato via fax". Al documento inviato/ricevuto successivamente al fax deve essere apposto/associato lo stesso numero di protocollo. Il timbro di segnature/etichetta di protocollo va posto sul documento e non sulla copertina di trasmissione del fax.

5.7 Corrispondenza con più destinatari

Tutte le comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo.

5.8 Allegati

Tutti gli allegati devono essere trasmessi con i documenti a cui afferiscono all'ufficio/postazioni decentrate di protocollo per la registrazione. Il sistema informatico provvede automaticamente a registrare gli allegati come parte integrante di un documento informatico. Nel caso in cui allegati illeggibili pervengano tramite posta elettronica certificata, si dovrà chiedere chiarimenti al mittente in merito al documento. Su ogni allegato analogico è riportato il timbro/etichetta della segnature di protocollo.

5.9 Documenti di competenza di altre amministrazioni

Qualora pervengano all'Ente documenti di competenza di amministrazioni, ma facenti parte dell'Unione, questi vengono normalmente protocollati.

Qualora invece lo stesso documento venga recapitato a più enti contemporaneamente (Unione e singoli comuni), il personale si coordina al fine di registrare il documento una sola volta col protocollo dell'ente competente in merito.

Se l'ente destinatario invece è un soggetto terzo, il documento viene comunque registrato in ingresso e poi in uscita inoltrandolo al soggetto di competenza qualora questo sia individuabile. In caso contrario, si avvisa il mittente dell'errato invio.

5.10 Oggetti plurimi

Qualora un documento in entrata presenti più oggetti, relativi a procedimenti diversi, il documento dovrà essere assegnato agli uffici competenti e verrà classificato e fascicolato in base all'argomento o affare trattato, pertanto potrà essere inserito in più fascicoli diversi. Nel caso in cui l'individuazione di più oggetti venga effettuata successivamente da parte dell'ufficio assegnatario, questi deve inviare all'Ufficio Protocollo apposita comunicazione affinché si provveda alle ulteriori assegnazioni necessarie.

Ciascun documento in uscita avrà un unico oggetto.

5.11 Documentazione prodotta e registrata in appositi gestionali

Il Servizio Ragioneria è responsabile della gestione delle fatture attraverso un sistema informatico di gestione della contabilità. Le fatture pervenute vengono registrate automaticamente dal sistema di protocollo informatico.

I mandati di pagamento e le reversali d'incasso sono gestiti tramite ordinativi informatici; i movimenti sono gestiti e inviati alla Tesoreria attraverso flusso informatico dei relativi tracciati. L'Ente, con credenziali di accesso fornite dalla banca della Tesoreria stessa, accede direttamente alla piattaforma di scambio dei flussi.

5.12 Modelli pubblicati di documenti

Tutti i modelli sono pubblicati sul sito internet o sulla rete intranet dell'Ente nei formati indicati nelle Linee Guida di Agid, Allegato 2 Formati di file e riversamento e sono classificati secondo il piano di classificazione in uso (Documento n. 5).

5.13 Trasmissioni telematiche e procedimenti amministrativi on line

I documenti di cui all'allegato Documento n. 7 sono trasmessi dall'Ente con immissione diretta dei dati nel sistema dell'ente destinatario. I documenti possono essere privi di firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate e a identificazione univoca, attivate con i singoli enti destinatari. Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione.

L'Ente tramite i servizi on line, disponibili dal sito istituzionale, riceve e protocolla documenti relativi a specifici procedimenti amministrativi. Il sistema effettua la verifica formale di accettabilità e identifica i mittenti in modo certo tramite autenticazione e identità digitale. I servizi on line sono integrati con il sistema di protocollo informatico, che effettua la registrazione automatica dei documenti conferiti.

5.14 Produzione di copie cartacee di documenti informatici e di copie informatiche di documenti cartacei

Nel caso di produzione di copie cartacee di documenti informatici dovranno essere obbligatoriamente redatte attestazioni che riportino dati e indicazioni previsti dai modelli predisposti (Documento n. 10).

Dei documenti analogici prodotti/pervenuti, per i quali è necessaria la distribuzione interna all'Ente, si faranno copie informatiche degli stessi.

5.15 Amministrazione trasparente

Sul sito internet istituzionale dell'Ente è stata attivata la "Sezione Amministrazione trasparente", recante i dati e le informazioni di pubblica evidenza che l'Amministrazione deve rendere disponibili on-line in applicazione del Dlgs 33/2013. Ciascuna unità operativa cura la pubblicazione dei dati di propria competenza così come indicato nel Piano triennale di prevenzione della corruzione e della trasparenza.

5.16 Albo online

Sul sito istituzionale dell'Ente è stata attivata la sezione "Albo on line", tramite la quale si accede agli atti e ai provvedimenti sottoposti a periodi di pubblicazione on-line a termine. La pubblicazione sull'Albo soddisfa il requisito di pubblicità legale garantendo il principio generale di trasparenza amministrativa, imparzialità e buona amministrazione.

L'organizzazione e le modalità di svolgimento del servizio sono dettagliate nelle apposite Linee guida per le pubblicazioni all'Albo on-line (Documento n. 9).

6 Posta elettronica

6.1 Posta elettronica certificata

La casella istituzionale di posta elettronica certificata dell'Amministrazione, integrata con il sistema di protocollo informatico, è adeguata allo scambio di messaggi con altre pubbliche amministrazioni e rappresenta l'indirizzo ufficiale anche per cittadini, imprese, professionisti e altri soggetti dotati di analoghi strumenti di trasmissione. L'Amministrazione accetta le istanze e le dichiarazioni trasmesse attraverso la casella di posta elettronica certificata. Vengono protocollati i documenti-file allegati e anche il solo corpo del messaggio, se privo di allegati. Qualora i file non siano corredati di firma digitale, verranno protocollati e assegnati all'ufficio competente, successivamente il responsabile del procedimento provvederà alla valutazione del contenuto del documento e della sua ammissibilità ai fini del procedimento amministrativo a cui si riferisce.

L'Ente ha adempiuto agli obblighi normativi dotandosi di un indirizzo di posta elettronica certificata, pubblicando tale indirizzo sulla home page del sito internet istituzionale e comunicandolo all'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi (IPA).

6.2 Gestione della posta elettronica

La posta elettronica viene utilizzata per l'invio di comunicazioni, informazioni e documenti sia all'interno dell'Ente, che nei rapporti con i cittadini e altri soggetti privati e con altre pubbliche amministrazioni.

La trasmissione di documenti tramite la posta elettronica deve attenersi alle norme e alle regole vigenti al fine di garantirne la validità legale e amministrativa, nonché la corretta gestione nel protocollo informatico, nel sistema di gestione documentale e nel sistema di conservazione dell'Ente.

Le comunicazioni formali e la trasmissione di documenti informatici, il cui contenuto impegni l'Ente verso terzi, avvengono tramite la casella di posta elettronica certificata istituzionale, eletta come domicilio digitale e le caselle di posta elettronica certificata attribuite ai servizi.

Le semplici comunicazioni informali ricevute o trasmesse per posta elettronica, che consistano in scambio di informazioni, possono non essere protocollate.

Qualora risulti necessario attribuire efficacia probatoria a documenti informatici e messaggi pervenuti alle caselle di posta degli uffici, questi dovranno essere acquisiti tramite il sistema di protocollo informatico.

Non è possibile inviare messaggi dalla casella di posta elettronica personale quando il contenuto di questi impegni l'Amministrazione verso terzi. Per quanto riguarda la gestione della posta elettronica nelle pubbliche amministrazioni, si rimanda agli articoli 45-49 del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017.

La posta elettronica nominativa non può essere utilizzata per la ricezione o la spedizione di documenti a firma digitale, per i quali è prevista apposita casella istituzionale.

6.3 Posta elettronica per le comunicazioni interne

Le comunicazioni tra l'Ente e i propri dipendenti, nonché tra le varie strutture, avvengono di norma mediante l'utilizzo della casella di posta elettronica ordinaria dei rispettivi uffici o nominative, nel rispetto delle norme in materia di protezione dei dati personali, nonché previa informativa agli interessati circa il grado di riservatezza degli strumenti utilizzati.

Nell'ambito dell'attività amministrativa interna è sufficiente un semplice messaggio di posta elettronica per:

- convocare riunioni interne all'Ente;
- inviare comunicazioni di servizio o notizie, dirette ai dipendenti in merito a informazioni generali di organizzazione;
- diffondere circolari, ordini di servizio, copie di documenti (gli originali si conservano nel fascicolo specifico debitamente registrati).

6.4 Posta elettronica ricevuta da cittadini o altri soggetti privati

Le istanze e le dichiarazioni trasmesse per via telematica all'indirizzo istituzionale devono ritenersi valide a tutti gli effetti di legge qualora:

- sono trasmesse via posta elettronica o via posta elettronica certificata, regolarmente sottoscritte con firma elettronica/digitale dotata di certificato valido rilasciato da un certificatore accreditato;
- l'autore del documento è identificato attraverso il sistema pubblico di identità digitale (SPID), la carta di identità elettronica o la carta nazionale dei servizi;

- sono formate tramite il punto di accesso telematico per i dispositivi mobili, IO APP, definito dall'articolo 64-bis del Codice dell'Amministrazione digitale Dlgs 82/2005;
- siano sottoscritte e presentate unitamente alla copia del documento d'identità;
- sono trasmesse da domicilio digitale oppure da un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato

Al di fuori delle predette ipotesi, le comunicazioni di posta elettronica che pervengono all'indirizzo istituzionale, dei singoli servizi o a quelli nominativi, sono valutate in ragione della loro rispondenza a ragionevoli criteri di attendibilità e riconducibilità al mittente dichiarato, e successivamente soggette, se del caso, a protocollazione. Spetterà al responsabile del procedimento, ove ne rilevi la necessità, richiedere al mittente la regolarizzazione dell'istanza o della dichiarazione, acquisendo ogni utile documentazione integrativa.

6.5 Posta elettronica ricevuta da altre pubbliche amministrazioni

Le comunicazioni e i documenti ricevuti da altre pubbliche amministrazioni sono valide ai fini del procedimento una volta che ne sia verificata la provenienza, ovvero quando:

- sono trasmessi attraverso sistemi di posta elettronica certificata o altro servizio elettronico di recapito certificato;
- sono sottoscritti con firma elettronica/digitale;
- sono dotati di segnatura di protocollo.

7 Assegnazione dei documenti

7.1 Assegnazione

L'assegnazione dei documenti agli uffici è effettuata dagli operatori dell'Ufficio Protocollo, delegati dal responsabile della gestione documentale sulla base dell'elenco degli uffici (Documento n. 2) e dei responsabili di procedimento, tramite il sistema di gestione documentale. Le abilitazioni all'assegnazione dei documenti, effettuate da altri uffici, sono rilasciate dal responsabile della gestione documentale.

Anche le assegnazioni per conoscenza devono essere effettuate tramite il sistema di gestione documentale. Il responsabile dell'Area, o suo delegato, provvede a smistare ciascun documento in arrivo al responsabile del procedimento. Spettano al responsabile del procedimento amministrativo le incombenze relative alla gestione del documento, l'inserimento nel fascicolo di competenza.

Per quanto riguarda l'Area Affari generali, la corrispondenza viene assegnata direttamente al responsabile di procedimento senza passare dal responsabile di Area, che mantiene comunque presidio e visibilità di quanto protocollato attraverso il gestionale di protocollo.

I documenti ricevuti dall'Ente, al termine delle operazioni di registrazione, classificazione, segnatura e assegnazione, sono fatti pervenire in originale agli uffici competenti tramite l'uso di cassette.

7.2 Modifica delle assegnazioni

Nel caso di assegnazione errata dei documenti, l'ufficio che ha ricevuto il documento identificato come "principale" è tenuto a restituirlo all'Ufficio protocollo, che provvederà alla riassegnazione al corretto assegnatario.

Il sistema di gestione informatica dei documenti tiene traccia delle rassegnazioni e dei movimenti dei documenti.

7.3 Consegna dei documenti

I documenti informatici e le immagini digitali dei documenti cartacei acquisite con lo scanner sono resi disponibili agli uffici tramite il sistema informatico di gestione documentale. Si veda anche la Sezione 10.

I documenti analogici protocollati e assegnati sono resi disponibili ai destinatari mediante l'uso di cassette.

8 Classificazione e fascicolazione dei documenti

8.1 Classificazione dei documenti

Tutti i documenti ricevuti o prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al titolario (Documento n. 5).

I documenti in arrivo sono classificati dall'Ufficio Protocollo, i documenti prodotti dall'Ente sono classificati dalle postazioni di protocollo in uscita.

Il sistema in fase di protocollazione classifica in automatico le fatture elettroniche e le istanze presentate tramite i servizi on line.

8.2 Formazione e identificazione dei fascicoli

Tutti i documenti, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli o serie documentarie. L'apertura dei fascicoli è effettuata dai responsabili di servizio o di procedimento, o dai collaboratori abilitati a questa funzione (Documento n. 2). La formazione di un nuovo fascicolo avviene attraverso l'operazione di apertura, che prevede la registrazione nel sistema informatico delle seguenti informazioni:

- classificazione;
- numero del fascicolo (la numerazione dei fascicoli è annuale e indipendente per classificazione);
- oggetto del fascicolo;
- data di apertura;
- ufficio assegnatario;
- responsabile del procedimento, se informazione disponibile.

Il sistema di protocollo informatico aggiorna automaticamente il repertorio/elenco dei fascicoli.

Il responsabile della gestione documentale, coadiuvato dai propri collaboratori, fornisce supporto alle singole unità organizzative dell'Ente, per redigere il piano della fascicolazione per l'anno successivo, fermo restando la responsabilità di ogni utente, di organizzare i fascicoli che movimentata secondo il criterio a lui più funzionale, ma sempre all'interno di un perimetro di prassi predefinite e condivise coi colleghi.

8.3 Processo di fascicolazione

In presenza di un documento da inserire in un fascicolo, i responsabili di servizio e procedimento o i collaboratori stabiliscono, consultando le funzioni del protocollo informatico, se esso si colloca nell'ambito di un affare o procedimento in corso oppure se da avvio a un nuovo procedimento, in quest'ultimo caso aprono un nuovo fascicolo (seguendo le procedure descritte nell'articolo precedente).

I responsabili di servizio e procedimento o i collaboratori, hanno cura di inserire nei fascicoli i documenti in arrivo, già protocollati e classificati dall'Ufficio Protocollo/uffici protocollo decentrati presso i servizi. I documenti prodotti dall'Ente sono fascicolati da chi li scrive, pertanto perverranno alle postazioni di protocollo già con l'indicazione dell'identificativo di fascicolo.

Nel caso di documenti informatici il sistema provvede automaticamente, dopo l'assegnazione del numero di fascicolo, a inserire il documento nel fascicolo informatico stesso. I documenti analogici sono fisicamente inseriti nei fascicoli cartacei dal responsabile di servizio/procedimento.

Ai documenti informatici prodotti tramite gli applicativi gestionali e l'utilizzo di modelli standard o creati dall'utente attraverso moduli e formulari, resi disponibili mediante servizi on line, sono associati automaticamente dal sistema di gestione documentale i metadati del fascicolo informatico o aggregazione documentale informatica cui appartengono o a cui danno avvio.

Il responsabile della gestione documentale e i suoi collaboratori mantengono comunque un'attività di controllo a cadenza almeno annuale sulla formazione e sulla gestione dei fascicoli.

8.4 Modifica delle assegnazioni dei fascicoli

La riassegnazione di un fascicolo è effettuata, su istanza scritta dell'ufficio che ha in carico il fascicolo, dal Servizio per la gestione documentale che provvede a modificare le informazioni del sistema informatico e del repertorio dei fascicoli e inviare il fascicolo all'ufficio del responsabile del procedimento di nuova assegnazione. Delle operazioni di riassegnazione è conservata traccia nel sistema informatico di gestione dei documenti.

8.5 Fascicolo ibrido

Il fascicolo ibrido è composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti a un affare o procedimento amministrativo che dà origine a due unità archivistiche di conservazione differenti. L'unitarietà del fascicolo è garantita dal sistema di gestione documentale mediante il codice del fascicolo (formato da indice di classificazione, anno di apertura e numero del fascicolo).

8.6 Fascicolo informatico

Il fascicolo informatico costituisce un'aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e trattato secondo le disposizioni stabilite dall'articolo 41 del Codice dell'Amministrazione digitale Dlgs 82/2005 come modificato dal Dlgs 217/2017.

Il fascicolo informatico è gestito tramite il sistema di gestione documentale e protocollo informatico.

Il fascicolo informatico può contenere sia documenti digitali che copie immagine e copie informatiche di documenti analogici.

8.7 Metadati dei fascicoli informatici

Al fascicolo informatico è associato l'insieme dei metadati, come definito dalla normativa vigente in materia di documenti informatici (sino al 1° gennaio 2022 DPCM 13/11/2014, Allegato 5 Metadati e successivamente Linee Guida di Agid, Allegato 5 I metadati).

8.8 Tenuta dei fascicoli dell'archivio corrente

I fascicoli dell'archivio corrente, relativi agli affari in corso di trattazione o comunque necessari allo svolgimento delle attività correnti, sono formati e gestiti a cura dei responsabili di procedimento e conservati, fino al trasferimento nell'archivio di deposito, presso gli uffici di competenza.

I documenti e i fascicoli informatici sono gestiti e conservati nei sistemi Protel di Golem software erogati in modalità cloud computing.

La sicurezza e la conservazione dei documenti e dei fascicoli informatici sono descritte e garantite dal Manuale di conservazione (Documento n. 13) e dal Piano di sicurezza dei documenti informatici (Documento n. 15). Si veda anche la Sezione 11.

9 Invio dei documenti destinati all'esterno

9.1 Invio dei documenti informatici

La spedizione dei documenti informatici avviene tramite il sistema informatico di gestione dei documenti, dopo che sono stati classificati, fascicolati e protocollati, secondo i seguenti criteri generali:

- i documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari abilitato alla ricezione della posta per via telematica;
- per la spedizione, l'Amministrazione si avvale di casella di posta elettronica certificata istituzionale;
- l'Ufficio Protocollo/le postazioni decentrate di protocollo provvedono a
 - effettuare l'invio telematico utilizzando i servizi di autenticazione
 - verificare l'avvenuto recapito dei documenti spediti per via telematica
- le ricevute elettroniche si collegano automaticamente alle registrazioni di protocollo.

I soggetti corrispondenti dell'Ente sono inseriti e descritti nell'anagrafica unica del sistema, secondo le prescrizioni contenute nelle Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico e per la compilazione della banca dati dei soggetti (Documento n. 4).

Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dall'articolo 49 del Codice dell'Amministrazione digitale Dlgs 82/2005.

Per l'uso della posta elettronica si rimanda alla Sezione 6.

La spedizione di documenti informatici al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni senza che a questa l'Amministrazione riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

9.2 Spedizione dei documenti analogici

Qualora sia necessario spedire documenti analogici originali questi devono essere completi della firma autografa del responsabile del procedimento, della classificazione e del riferimento al fascicolo nonché delle eventuali indicazioni necessarie a individuare il procedimento amministrativo di cui fanno parte.

Nel caso in cui vengano inviate copie cartacee di documenti informatici si utilizzano i modelli preposti (Documento n. 10), che ne attestano la conformità all'originale informatico.

I documenti da spedire sono trasmessi all'Ufficio Protocollo che provvederà all'imbustamento, ad eccezione degli atti giudiziari che vengono imbustati in autonomia dall'ufficio Polizia Locale. Nel caso di spedizione che utilizzi pezze di accompagnamento (raccomandate, posta celere, corriere o altro mezzo di spedizione), queste devono essere compilate a cura dell'ufficio produttore.

Eventuali situazioni di urgenza che modifichino la procedura descritta devono essere valutate e autorizzate dal responsabile del Servizio per la gestione documentale.

10 Scansione dei documenti su supporto cartaceo

10.1 Documenti soggetti a scansione

I documenti in arrivo e in partenza su supporto cartaceo sono acquisiti all'interno del sistema di protocollo informatico in formato immagine con l'ausilio di scanner, prima/successivamente/in fase delle operazioni di registrazione.

L'Ente adotta il seguente modello operativo:

- sono prodotti documenti informatici a firma elettronico/digitale;
- tutti i documenti sono classificati e fascicolati;
- i documenti ricevuti dall'esterno su formato cartaceo vengono registrati al protocollo e classificati, timbrati/etichettati e scansionati; la copia immagine del documento è allegata alla relativa registrazione di protocollo e resa disponibile all'ufficio assegnatario/sulla postazione di lavoro del responsabile del procedimento;
- i documenti informatici sono spediti all'esterno tramite la casella di posta elettronica certificata agli indirizzi di posta elettronica dei destinatari oppure in copie cartacee tramite i servizi di posta ordinaria; per effettuare copia cartacea di documenti informatici si utilizzano i modelli preposti (Documento n. 10), che ne attestano la conformità all'originale informatico.

10.2 Processo di scansione

Il processo di scansione si articola di massima nelle seguenti fasi:

- acquisizione delle immagini in modo che a ogni documento, anche composto da più fogli, corrisponda un unico file in un formato standard;
- tutti i tipi di documenti in formato A4, comunque separabili o leggibili dagli scanner vengono digitalizzati. In caso di planimetrie o volumi non sperabili si potrà fare scansione del frontespizio;
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- collegamento delle rispettive immagini alla registrazione di protocollo, in modo non modificabile;
- memorizzazione delle immagini, in modo non modificabile.

I documenti analogici soggetti a scansione si conservano nell'archivio dell'Ente fino a procedimento legale di scarto.

In merito alla produzione di copie immagini su supporto informatico di documenti analogici si veda anche l'articolo 3.4 Acquisizione dei documenti analogici tramite copia immagine e copia informatica.

11 Conservazione e tenuta dei documenti

11.1 Sistema informatico

Il sistema informatico, le misure di sicurezza fisica e logica, le procedure comportamentali adottate per la gestione del sistema documentale e del sistema informatico sono descritti nel Piano di sicurezza dei documenti informatici (Documento n. 15). Il piano per la sicurezza informatica è predisposto e regolarmente aggiornato.

11.2 Gestione delle password

Il sistema garantisce la gestione e la conservazione delle password di accesso al sistema stesso e ai servizi online degli utenti interni ed esterni secondo le modalità descritte nel Piano per la sicurezza dei documenti informatici (Documento n. 15).

11.3 Conservazione e memorizzazione dei documenti analogici, informatici e delle rappresentazioni digitali dei documenti cartacei

I documenti dell'Ente, prodotti su supporti e nei formati previsti, sono conservati a cura del Servizio di gestione documentale.

La documentazione analogica corrente è custodita a cura del responsabile del procedimento fino al trasferimento in archivio di deposito.

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

Le rappresentazioni digitali dei documenti originali su supporto cartaceo, acquisite con l'ausilio dello scanner, sono memorizzate nel sistema, in modo non modificabile, al termine del processo di scansione, associazione alle corrispondenti registrazioni di protocollo e fascicolazione.

11.4 Sistema di conservazione dei documenti informatici

La conservazione dei documenti informatici è assicurata dai requisiti funzionali del sistema di conservazione, in modo da garantire autenticità, integrità, identificazione univoca, mantenimento stabile di tutte le relazioni istituite nel contesto di produzione, gestione e tenuta del documento e leggibilità nel tempo. I requisiti adottati sono conformi agli standard internazionali e alle norme nazionali.

Al fine di dare solidità al sistema e di consentire la presunzione di autenticità, viene conservata tutta la documentazione relativa alle fasi di trattamento dei documenti. Le soluzioni di sicurezza adottate avvengono secondo le modalità specificate negli standard, nelle Linee Guida di Agid.

Il responsabile per la gestione documentale provvede altresì alla conservazione degli strumenti di descrizione, ricerca, gestione e conservazione dei documenti (inventari, indici, quadri di classificazione e relativi massimari di selezione e scarto, repertori).

Ai sensi del paragrafo 4.5 delle Linee Guida di Agid, l'Ente ha individuato il responsabile della conservazione (Documento n. 12).

Il responsabile della conservazione definisce e attua le politiche di conservazione dei documenti.

L'Ente si avvale del servizio di conservazione digitale a norma erogato da Aruba SpA. Il Manuale di conservazione illustra l'organizzazione del sistema di conservazione, individua i soggetti coinvolti e i ruoli da essi svolti, descrive il processo di conservazione, le architetture e le infrastrutture utilizzate, le modalità di accesso ai documenti e le misure di sicurezza. Il responsabile della conservazione delega formalmente la trattazione del processo di conservazione digitale al conservatore accreditato e vigila periodicamente sullo svolgimento dell'attività.

I documenti informatici, i fascicoli informatici e le aggregazioni documentali informatiche sono versati nel sistema di conservazione, corredati dai metadati previsti sino al 1° gennaio 2022 dal DPCM 3/12/2013 Regole tecniche in materia di sistema di conservazione, Allegato 5 Metadati e successivamente dalle Linee Guida di Agid, Allegato 5 I metadati, e descritti nel Manuale di conservazione (Documento n. 13), in modo non modificabile. I formati dei documenti destinati alla conservazione sono i formati previsti per la conservazione dalla normativa vigente in materia (Linee guida di Agid, Allegato 2 Formati di file e riversamenti).

In caso di migrazione dei documenti informatici, la corrispondenza fra il formato originale e quello migrato è garantita dal responsabile della conservazione.

11.5 Pacchetti di versamento

Il responsabile della gestione documentale assicura la trasmissione del contenuto del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel Manuale di conservazione (Documento n. 13)

Il responsabile del servizio di conservazione fornisce il rapporto di versamento relativo ai pacchetti di versamento generato dal sistema di conservazione, secondo le modalità descritte nel Manuale di conservazione (Documento n. 13).

11.6 Conservazione dei documenti analogici

L'archivio corrente analogico è conservato presso le unità organizzative.

L'archivio di deposito e l'archivio storico analogici sono conservati presso la sede dell'Ente in locali di proprietà.

11.7 Trasferimento delle unità archivistiche analogiche negli archivi di deposito e storico e conservazione dei fascicoli informatici

Gli uffici individuano i fascicoli relativi ad affari e procedimenti conclusi, o comunque non più necessari allo svolgimento delle attività correnti, di norma all'inizio di ogni anno e comunque con cadenza periodica, dandone comunicazione al responsabile della gestione documentale, il quale provvede al loro trasferimento all'archivio di deposito e compila il relativo elenco. Il trasferimento è effettuato rispettando l'organizzazione dei fascicoli e delle serie nell'archivio corrente.

Prima di effettuare il conferimento dei fascicoli chiusi, il responsabile di procedimento verifica:

- l'effettiva conclusione della pratica;
- la trascrizione dell'esaurimento della pratica nel repertorio dei fascicoli, gestito tramite il sistema di protocollo informatico;
- il corretto aggiornamento della data di chiusura sulla camicia del fascicolo cartaceo;
- lo sfoltimento di eventuali copie e fotocopie di documentazione passibile di macero, al fine di garantire;
- la presenza di tutti e soli documenti pertinenti alla pratica.

Di norma sono versati all'archivio storico tutti i documenti anteriori all'ultimo quarantennio. E' tuttavia possibile depositare anche documentazione successiva al quarantennio purché non rivesta più un preminente carattere giuridico-amministrativo per l'Ente.

La gestione dell'archivio di deposito, la consultazione e il prelevamento dei documenti dallo stesso, l'archiviazione e la custodia dei documenti contenenti dati personali avvengono in conformità alla normativa vigente.

Il responsabile della gestione documentale cura la formazione e la conservazione dell'elenco dei fascicoli e delle serie trasferite e conservate nell'archivio di deposito.

I fascicoli informatici, mediante specifiche funzionalità di sistema, vengono trasferiti nel sistema di conservazione adottato. Delle operazioni di trasferimento è lasciata traccia documentale.

11.8 Selezione e conservazione dei documenti

In base al Piano di conservazione – Massimario di selezione per la conservazione dei documenti (Documento n. 6), viene effettuata la procedura di selezione della documentazione da proporre allo scarto e attivato il procedimento amministrativo di scarto documentale con l'invio della proposta alla competente Soprintendenza archivistica. I documenti e i fascicoli non soggetti a operazioni di scarto sono trasferiti nell'archivio storico per la conservazione permanente.

Lo scarto dei documenti informatici avviene mediante le specifiche funzionalità del sistema di conservazione.

11.9 Gestione dell'archivio storico

L'archivio storico è costituito dal complesso dei documenti relativi ad affari esauriti e destinati, previa operazioni di selezione, alla conservazione permanente per garantirne la consultazione al pubblico. In base alla normativa vigente l'archivio storico è formato dai documenti relativi ad affari esauriti da oltre 40 anni: l'archivio storico deve essere conservato nella sua organicità e in luogo idoneo alla conservazione permanente. Ogni spostamento dell'archivio storico in altra sede deve essere comunicato e autorizzato dalla

Soprintendenza archivistica. L'Ente ha inoltre l'obbligo di ordinare e inventariare l'archivio storico. Come previsto dal Codice dei beni culturali Dlgs 42/2004, l'Ente cura la conservazione, promozione, valorizzazione e assicura la fruizione del patrimonio documentario, garantendo a tutti l'accesso gratuito.

12 Accesso a dati, informazioni e documenti - Pubblicità legale e trasparenza amministrativa

12.1 Accessibilità da parte degli utenti appartenenti all'Amministrazione

La sicurezza e la riservatezza delle registrazioni di protocollo e dei documenti informatici e il controllo degli accessi al sistema sono garantiti attraverso l'uso di profili e password, o altre tecniche e dispositivi di autenticazione sicura.

Sulla base della struttura organizzativa e funzionale dell'Ente, il responsabile della gestione documentale attribuisce i livelli di autorizzazione (consultazione, inserimento, cancellazione e modifica delle informazioni), come descritto nel Piano per la sicurezza dei documenti informatici (Documento n. 15).

12.2 Accesso esterno

L'accesso al sistema informatico da parte di utenti esterni può avvenire nei casi di procedimenti amministrativi attraverso il Sistema pubblico per la gestione dell'identità digitale, oppure con l'uso della carta d'identità elettronica e della carta nazionale dei servizi; sino alla data da stabilire con decreto del Presidente del Consiglio dei ministri o del Ministro per la semplificazione e la pubblica amministrazione, come previsto dall'articolo 64 del Dlgs 82/2005 come modificato dal DL 76/2020, possono essere utilizzati anche altri strumenti informatici messi a disposizione dall'Ente che consentano l'individuazione certa del soggetto richiedente.

Come previsto dal Dlgs. 33/2013, è garantito a tutti i cittadini, mediante l'istituzione dell'Accesso civico, la libera consultazione degli atti dell'Ente per i quali è prevista la pubblicazione. Sul sito istituzionale è consultabile l'apposita "Sezione Amministrazione Trasparente", a cui il cittadino ha libero accesso e nella quale sono disponibili informazioni integre e conformi all'originale, secondo quanto previsto dalla normativa e come specificato nel Piano triennale di prevenzione della corruzione e della trasparenza.

I documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria sono pubblicati in formato di tipo aperto.

12.3 Accesso da parte di altre amministrazioni

L'accesso al sistema informatico documentale da parte di pubbliche amministrazioni è realizzato applicando le norme e i criteri tecnici emanati per la realizzazione della rete unitaria delle pubbliche amministrazioni o nell'ambito di altre convenzioni, attraverso modalità di interoperabilità.

13 *Approvazione, Revisione e Pubblicazione*

13.1 *Approvazione*

Il presente manuale è adottato dall'organo esecutivo dell'ente con deliberazione di Giunta del Comune, su proposta del responsabile della gestione documentale.

13.2 *Revisione*

Il presente manuale è rivisto, ordinariamente, ogni due anni su iniziativa del responsabile della gestione documentale. La modifica o l'aggiornamento di uno o tutti i documenti allegati al presente manuale non comporta la revisione del manuale stesso. Qualora se ne presenti la necessità, si potrà procedere a revisione o integrazione del manuale anche prima della scadenza prevista.

13.3 *Pubblicazione e divulgazione*

Il Manuale di gestione è reso pubblico tramite la sua diffusione sul sito internet istituzionale dell'Ente nella "Sezione Amministrazione trasparente", la pubblicazione all'albo on line degli atti di adozione e revisione.

Glossario dei termini e degli acronimi

Allegato 1 al documento “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici”.

Indice

Sommario

Indice.....	2
CAPITOLO 1.....	4
Premessa	4
1.1 Scopo e campo di applicazione del documento	4
1.2 Glossario dei termini.....	4
1.3 Glossario degli Acronimi	14

Questo allegato è parte integrante al testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

CAPITOLO 1

Premessa

1.3 Scopo e campo di applicazione del documento

Lo scopo del presente allegato è il seguente:

- esplicitare il significato dei termini maggiormente utilizzati nel documento *linea guida sulla formazione, gestione e conservazione dei documenti informatici*, che necessitano una spiegazione.

1.4 Glossario dei termini

TERMINE	DEFINIZIONE
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme 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 dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
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 in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
Codec	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un <i>wrapper</i> (codifica), così come di estrarli da esso (decodifica).
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
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

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
	adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
Coordinatore della Gestione Documentale	Soggetto 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 nei casi di amministrazioni che abbiano istituito più AOO.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato.
<i>Digest</i>	Vedi Impronta crittografica.
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
<i>eSeal</i>	Vedi sigillo elettronico.
Esibizione	operazione che consente di visualizzare un documento conservato
<i>eSignature</i>	Vedi firma elettronica.
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di <i>bit</i> che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
<i>File container</i>	Vedi Formato contenitore.
<i>File wrapper</i>	Vedi Formato contenitore.
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
<i>Filesystem</i>	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS.
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS.
Flusso (binario)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o <i>wrapping</i>), in uno stesso file, di una o più

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
	evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
Funzione di <i>hash</i> crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o <i>digest</i> (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
<i>hash</i>	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o " <i>digest</i> " (vedi).
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di <i>hash</i> crittografica a un'evidenza informatica.

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
<i>Naming convention</i>	Vedi Convenzioni di denominazione
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con 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 di accesso a oggetti di conservazione.
Pacchetto di file (<i>file package</i>)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
<i>Path</i>	Percorso (<i>vedi</i>).
<i>Pathname</i>	Concatenazione ordinata del percorso di un file e del suo nome.
<i>Percorso</i>	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
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.
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.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i 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.
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
<i>qSeal</i>	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
<i>qSignature</i>	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
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.

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 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.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Responsabile del servizio di conservazione	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della funzione archivistica di conservazione	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.

Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
Sidecar (file)	File-manifesto (vedi).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito

TERMINE	DEFINIZIONE
	della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di <i>timeline</i> un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente abilitato	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.
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce 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.

1.5 Glossario degli Acronimi

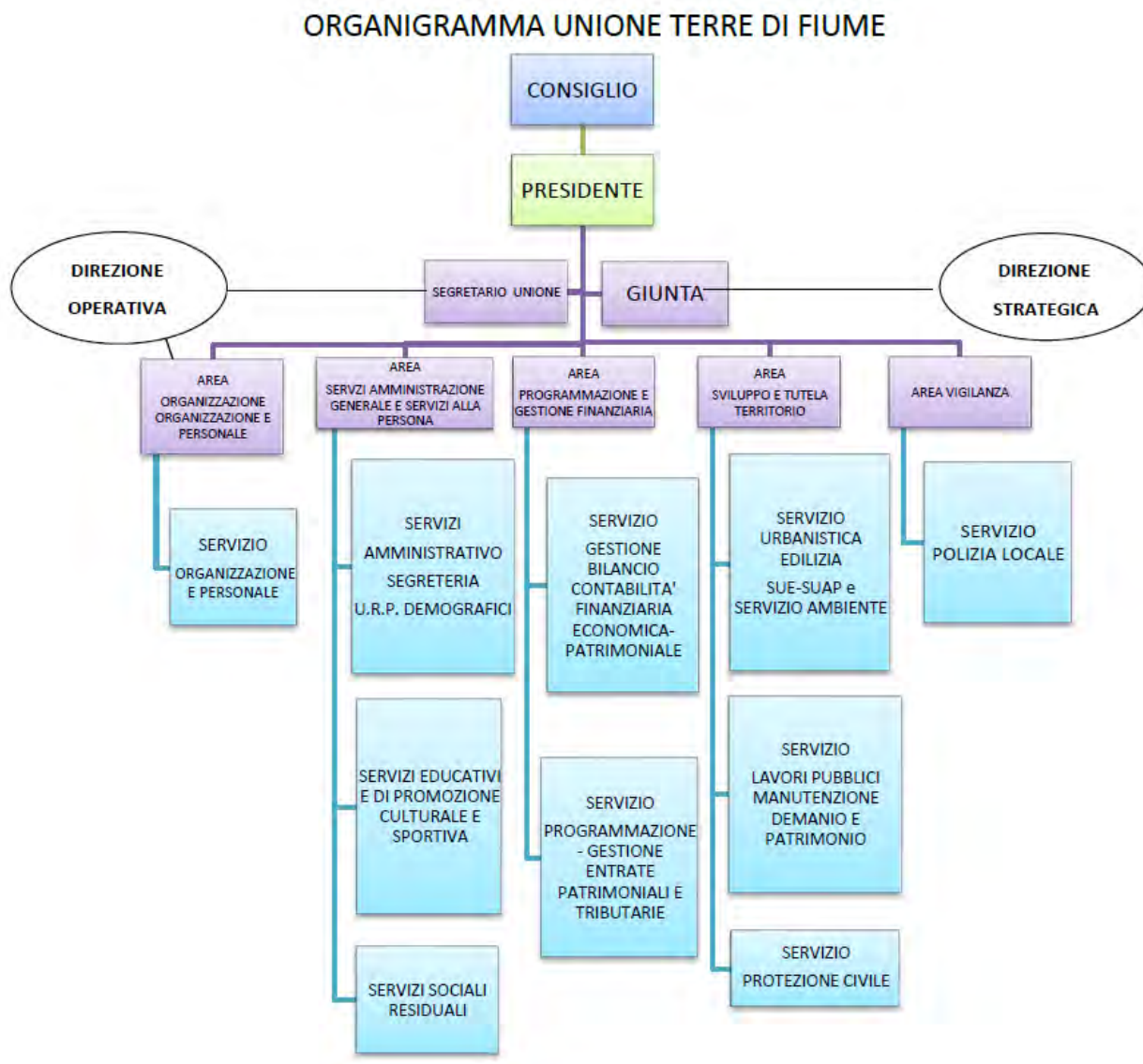
ACRONIMO	DEFINIZIONE
AGID	Agenzia per l'Italia digitale

Allegato 1 - Glossario dei termini e degli acronimi

ACRONIMO	DEFINIZIONE
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
eIDAS	Regolamento (UE) № 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.
FEA	Vedi firma elettronica avanzata.
FEQ	Vedi firma elettronica qualifica.
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 (<i>"General Data Protection Regulation"</i>), 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.
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
UOR	Unità Organizzativa Responsabile

**Elenco dei servizi e degli uffici del Comune di Sale
abilitati all'utilizzo del sistema di gestione documentale
del protocollo informatico e all'inserimento dei dati**

Documento n. 2



Abilitazioni all'utilizzo delle funzionalità del sistema di gestione documentale e protocollo informatico:

- registrazione dei documenti in arrivo: Ufficio Protocollo
- registrazione dei documenti in partenza e interni: tutte le postazioni dei vari uffici
- classificazione e fascicolazione dei documenti: tutte le postazioni dei vari uffici
- consultazione: tutte le postazioni dei vari uffici, in base all'assegnazione-competenza dei documenti
- definizione delle liste di controllo degli accessi (ACL) e del ruolo degli utenti: responsabili delle strutture
- assegnazione documenti: Ufficio Protocollo
- aggiornamento anagrafica mittente/destinatario sul Sistema: tutte le postazioni dei vari uffici
- protocollazione dei documenti nel registro di emergenza: Ufficio Protocollo

Postazioni abilitate: *una postazione per ogni dipendente che si occupa della trattazione di documenti*

Elenco delle registrazioni particolari

Documento n. 3

Albo on-line
Atti di Polizia Giudiziaria
Autorizzazioni in materia paesaggistica
Autorizzazioni apertura medie e grandi strutture di vendita
Autorizzazioni commercio su aree pubbliche con posteggio e itinerante
Autorizzazioni manifestazioni
Autorizzazioni trasporti pubblici non di linea
Autorizzazioni di occupazione suolo pubblico
Contratti pubblici in forma amministrativa
Contratti di lavoro individuali
Convenzioni
Decreti del sindaco
Deliberazioni di Consiglio del Comune
Deliberazioni di Giunta del Comune
Accertamenti ICI, IMU
Accertamenti TIA, TARES
Determinazioni
Fatture emesse
Mandati di pagamento
Notifiche
Numeri di matricola degli ascensori
Ordinanze
Permessi pass disabili
Permessi pass veicoli
Permessi di costruire
Riversali
Segnalazioni certificate inizio attività produttive SCIA
Verbalì accertamenti violazione Codice della strada
Verbalì della delegazione trattante per la contrattazione integrativa
Verbalì delle violazioni comunicazioni ospitalità stranieri
Verbalì delle violazioni in materia di commercio su aree pubbliche e private
Verbalì delle violazioni per ritardata/omessa denuncia di infortunio
Verbalì delle violazioni pubblici esercizi
Verbalì di fermo amministrativo e sequestro di veicoli

Linee guida per l'inserimento e l'aggiornamento dei dati nel protocollo informatico e per la compilazione della banca dati dei soggetti[□]

Documento n. 4

Maiuscole e minuscole

Di norma per l'inserimento dei dati si devono usare le maiuscole e le minuscole secondo l'uso attuale. Per quanto riguarda il protocollo informatico dell'ente e la banca dati dell'anagrafica unica si è scelto di usare sempre la maiuscola.

Abbreviazioni

Tutte le abbreviazioni devono essere sciolte; non devono essere abbreviati i nomi degli enti, e qualora una abbreviazione facesse parte del nome ufficiale dell'istituto -e non sia possibile scioglierla- deve essere riportata così come compare nell'intestazione originale:

no AVV. ROSSI MARIO - STUDIO LEGALE ASSOCIATO;
si AVVOCATO ROSSI MARIO – STUDIO LEGALE ASSOCIATO

no CENSIS
si CENTRO STUDI INVESTIMENTI SOCIALI - CENSIS

no C.C.I.A.
si CAMERA DI COMMERCIO INDUSTRIA E ARTIGIANATO - CCIA

Segni di interpunzione

Al fine di consentire una facile interrogazione delle informazioni inserite nelle banche dati si deve limitare l'uso dei segni di interpunzione nelle intitolazioni di nomi collettivi, di enti, ditte ecc.; questi sono consentiti nel caso facciano parte integrante dell'intitolazione.

Nell'indicazione della ragione sociale (spa, srl ecc.) delle ditte (individuali o società) non si useranno i punti fermi:

no S.P.A., S.R.L., S.p.a., S.p.A., S.r.l., S.r.L.
si SPA, SRL

L'eventuale nome di una ditta o di un ente scritto fra virgolette non andrà inserito con le virgolette:

no ASSOCIAZIONE "AMICI DELLA MUSICA"
si ASSOCIAZIONE AMICI DELLA MUSICA

Nell'utilizzo dei segni di interpunzione si rimanda alle regole di scrittura: non deve mai precedere al segno uno spazio; dopo il segno e prima della parola successiva uno spazio; prima e dopo la lineetta uno spazio; la lineetta quando è tra due parole che esprimono un termine composto non deve avere spazi; il segno di parentesi segue la parola preceduto da uno spazio, all'interno della parentesi la prima parola è scritta subito dopo il segno di parentesi senza essere preceduta da uno spazio:

no LUNEDÌ , MARTEDÌ; LUNEDÌ,MARTEDÌ; LUNEDÌ ,MARTEDÌ
si LUNEDÌ, MARTEDÌ

no I COLORI SONO : GIALLO, ROSSO, ECC.; I COLORI SONO:GIALLO, ROSSO, ECC.; I COLORI SONO :GIALLO, ROSSO, ecc.
si I COLORI SONO: GIALLO, ROSSO, ecc.

no REGIONE SARDEGNA-DIREZIONE GENERALE

[□] Per la redazione delle seguenti linee guida si veda: ARRABBITO LOREDANA - BUCCARELLI TERESA - MAZZETTO DONATELLA, *Linee guida per l'inserimento dei dati nel protocollo informatico*, in Archivi & Computer, X, 1, Pisa 2000.

si REGIONE SARDEGNA - DIREZIONE GENERALE

no GIURIDICO - AMMINISTRATIVO

si GIURIDICO-AMMINISTRATIVO

no (GIALLO, ROSSO)

si (GIALLO, ROSSO)

Nomi di persona

Sono esclusi tutti i titoli di cortesia (eccellenza, reverendo, ecc.), di onorificenza, predicati nobiliari (N.H., N.D. ecc.), i titoli accademici (dott., ing. ecc.), quelli professionali (rag., geom. ecc.) e tutto ciò che non corrisponda al nome:

no DOTT. AVV. ROSSI MARIO;

no ROSSI AVV. MARIO;

si ROSSI MARIO.

Nomi di persona giuridica, ditte individuali, enti pubblici, società

Le denominazione delle persone giuridiche ecc. devono essere inserite come appaiono nella carta intestata facendo attenzione fra il logo e l'intestazione che spesso non corrispondono, scegliendo fra le due l'intestazione:

no AVV. ROSSI MARIO - STUDIO LEGALE ASSOCIATO;

si AVVOCATO ROSSI MARIO – STUDIO LEGALE ASSOCIATO

si STUDIO LEGALE ROSSI MARIO.

In mancanza dell'intestazione completa si preferisca il logo, oppure ricorrendo al responsabile del procedimento si rintracci la definizione originale da immettere nella banca dati. La tipologia della società (srl ecc.) va scritta non puntata (vedi sopra).

I nomi di enti o persone giuridiche nonché quelli di enti collettivi vanno scritti completi e per esteso, senza abbreviazioni; qualora l'ente o la persona giuridica sono meglio conosciuti con l'acronimo, questo va inserito dopo il nome completo in maiuscolo non puntato dopo un trattino preceduto e seguito da uno spazio:

no CENSIS

si CENTRO STUDI INVESTIMENTI SOCIALI - CENSIS

no C.C.I.A.

si CAMERA DI COMMERCIO INDUSTRIA E ARTIGIANATO - CCIA

no MIN. LAV. E PREV. SOCIALE;

si MINISTERO DEL LAVORO E DELLA PREVIDENZA SOCIALE

si MINISTERO DEL LAVORO E DELLA PREVIDENZA SOCIALE - MLPS

no INPS - IST. NAZ. PREVIDENZA SOCIALE

si ISTITUTO NAZIONALE PREVIDENZA SOCIALE - INPS

Molti enti hanno più sedi e sezioni o strutture, per l'inserimento dei dati valgono le stesse regole con l'aggiunta della denominazione della sede distaccata o sezione dopo la lineetta preceduta e seguita da uno spazio

no DIREZIONE GENERALE CULTURA REGIONE LOMBARDIA;

si REGIONE LOMBARDIA - DIREZIONE GENERALE CULTURA.

Intestazione, ufficio, firmatario

Nell'inserimento dell'intestazione di una lettera deve essere distinto il firmatario dall'ente o persona giuridica, dalla ditta individuale o società. Il firmatario o la provenienza/destinazione particolare vanno inseriti nell'apposita stringa dell'anagrafica:

no SINDACO DEL COMUNE DI SASSARI
si COMUNE DI SASSARI (nell'apposita stringa dell'anagrafica verrà inserito: IL SINDACO).

no IL MINISTRO DEL LAVORO E PREVIDENZA SOCIALE;
si MINISTERO DEL LAVORO E DELLA PREVIDENZA SOCIALE (nell'apposita stringa dell'anagrafica verrà inserito: IL MINISTRO).

no IL PRESIDENTE DELLA PROVINCIA DI MILANO;
si PROVINCIA DI CREMONA (nell'apposita stringa dell'anagrafica verrà inserito: IL PRESIDENTE).

Nomi stranieri

I nomi di persona, di città, o di qualsiasi ente straniero vanno inseriti nella versione originale, solo lo stato va scritto in lingua italiana

Indirizzo

Per quanto riguarda gli indirizzi di residenza quando devono essere inseriti quelli dichiarati nella carta intestata; per quelli degli enti pubblici andrà sempre inserito l'indirizzo giuridico dichiarato; per gli uffici decentrati quello della sede dell'ufficio; non devono essere inserite posizioni in anagrafica incomplete di parte dell'indirizzo: luogo, provincia, via, numero civico, codice avviamento postale.

Casi particolari

Tutti i casi particolari vengano discussi con il Responsabile del servizio archivio-protocollo prima dell'inserimento nella banca dati.

La banca dati dell'anagrafica non deve essere compilata con dati parziali.

Piano di classificazione

Documento n. 5

dic. 2005	Schema riassuntivo del piano di classificazione per l'archivio dell'ente
I	Amministrazione generale 1. Legislazione e circolari esplicative 2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica 3. Statuto 4. Regolamenti 5. Stemma, gonfalone, sigillo 6. Archivio generale 7. Sistema informativo 8. Informazioni e relazioni con il pubblico 9. Politica del personale; ordinamento degli uffici e dei servizi 10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale 11. Controlli interni ed esterni 12. Editoria e attività informativo-promozionale interna ed esterna 13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti 14. Interventi di carattere politico e umanitario; rapporti istituzionali 15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni 16. Area e città metropolitana 17. Associazionismo e partecipazione
II	Organi di governo, gestione, controllo, consulenza e garanzia 1. Sindaco 2. Vice-Sindaco 3. Consiglio 4. Presidente del Consiglio 5. Conferenza dei capigruppo e Commissioni del Consiglio 6. Gruppi consiliari 7. Giunta 8. Commissario prefettizio e straordinario 9. Segretario e Vice-segretario 10. Direttore generale e dirigenza 11. Revisori dei conti 12. Difensore civico 13. Commissario ad acta 14. Organi di controllo interni 15. Organi consultivi 16. Consigli circoscrizionali 17. Presidente dei Consigli circoscrizionali 18. Organi esecutivi circoscrizionali 19. Commissioni dei Consigli circoscrizionali 20. Segretari delle circoscrizioni 21. Commissario ad acta delle circoscrizioni 22. Conferenza dei Presidenti di quartiere
III	Risorse umane 1. Concorsi, selezioni, colloqui 2. Assunzioni e cessazioni 3. Comandi e distacchi; mobilità 4. Attribuzione di funzioni, ordini di servizio e missioni 5. Inquadramenti e applicazione contratti collettivi di lavoro 6. Retribuzioni e compensi 7. Trattamento fiscale, contributivo e assicurativo 8. Tutela della salute e sicurezza sul luogo di lavoro 9. Dichiarazioni di infermità ed equo indennizzo 10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza 11. Servizi al personale su richiesta 12. Orario di lavoro, presenze e assenze 13. Giudizi, responsabilità e provvedimenti disciplinari

	14. Formazione e aggiornamento professionale 15. Collaboratori esterni
IV	Risorse finanziarie e patrimonio 1. Bilancio preventivo e Piano esecutivo di gestione (PEG) 2. Gestione del bilancio e del PEG (con eventuali variazioni) 3. Gestione delle entrate: accertamento, riscossione, versamento 4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento 5. Partecipazioni finanziarie 6. Rendiconto della gestione; adempimenti e verifiche contabili 7. Adempimenti fiscali, contributivi e assicurativi 8. Beni immobili 9. Beni mobili 10. Economato 11. Oggetti smarriti e recuperati 12. Tesoreria 13. Concessionari ed altri incaricati della riscossione delle entrate 14. Pubblicità e pubbliche affissioni
V	Affari legali 1. Contenzioso 2. Responsabilità civile e patrimoniale verso terzi; assicurazioni 3. Pareri e consulenze
VI	Pianificazione e gestione del territorio 1. Urbanistica: piano regolatore generale e varianti 2. Urbanistica: strumenti di attuazione del piano regolatore generale 3. Edilizia privata 4. Edilizia pubblica 5. Opere pubbliche 6. Catasto 7. Viabilità 8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi 9. Ambiente: autorizzazioni, monitoraggio e controllo 10. Protezione civile ed emergenze
VII	Servizi alla persona 1. Diritto allo studio e servizi 2. Asili nido e scuola materna 3. Promozione e sostegno delle istituzioni di istruzione e della loro attività 4. Orientamento professionale; educazione degli adulti; mediazione culturale 5. Istituti culturali (Musei, Biblioteche, Teatri, Scuola comunale di musica, etc.) 6. Attività ed eventi culturali 7. Attività ed eventi sportivi 8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale 9. Prevenzione, recupero e reintegrazione dei soggetti a rischio 10. Informazione, consulenza ed educazione civica 11. Tutela e curatela di incapaci 12. Assistenza diretta e indiretta, benefici economici 13. Attività ricreativa e di socializzazione 14. Politiche per la casa 15. Politiche per il sociale
VIII	Attività economiche 1. Agricoltura e pesca 2. Artigianato 3. Industria 4. Commercio 5. Fiere e mercati 6. Esercizi turistici e strutture ricettive 7. Promozione e servizi
IX	Polizia locale e sicurezza pubblica 1. Prevenzione ed educazione stradale 2. Polizia stradale 3. Informative 4. Sicurezza e ordine pubblico
X	Tutela della salute 1. Salute e igiene pubblica 2. Trattamento Sanitario Obbligatorio

	3. Farmacie 4. Zooprofilassi veterinaria 5. Randagismo animale e ricoveri
XI	Servizi demografici 1. Stato civile 2. Anagrafe e certificazioni 3. Censimenti 4. Polizia mortuaria e cimiteri
XII	Elezioni ed iniziative popolari 1. Albi elettorali 2. Liste elettorali 3. Elezioni 4. Referendum 5. Istanze, petizioni e iniziative popolari
XIII	Affari militari 1. Leva e servizio civile sostitutivo 2. Ruoli matricolari 3. Caserme, alloggi e servitù militari 4. Requisizioni per utilità militari
XIV	Oggetti diversi

**Gruppo di lavoro per la formulazione di proposte e modelli
per la riorganizzazione dell'archivio dei Comuni**

**Piano di conservazione
Massimario di selezione per la conservazione dei documenti**

Dicembre 2005

Documento n. 6

Premessa

L'art. 68 del DPR 445/2000 prevede che ogni amministrazione debba dotarsi di un «piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti». La normativa quindi, accogliendo le posizioni e le riflessioni dei teorici dell'archivistica, concepisce la selezione come operazione critica di vaglio della documentazione prodotta, funzionale a una migliore conservazione dell'archivio. La selezione, cioè il momento valutativo, difatti non intacca la complessità e l'unitarietà dell'archivio; ma, procedendo all'individuazione dei documenti strumentali e transitori, da destinare allo scarto, vale a dire alla distruzione fisica, evidenzia i nessi fra i documenti essenziali da conservare permanentemente. Perciò l'eliminazione di taluni documenti deve essere preceduta dalla valutazione delle procedure di produzione documentaria, in modo che vengano assicurati la comprensione dell'attività dell'ente produttore e il mantenimento delle attestazioni di diritti.

Pertanto il mandato conferito, tramite decreto, al Gruppo dal Direttore generale per gli archivi del Ministero per i beni e le attività culturali comprende, oltre alla predisposizione del piano di classificazione (titolario), anche la redazione del piano di conservazione che al titolare è strettamente connesso.

L'adozione del titolare proposto dal Gruppo a tutti i Comuni italiani e studiato alla luce della interoperabilità tra sistemi informativi diversi comporta come conseguenza l'adozione del piano di conservazione che da esso discende.

In merito allo scarto archivistico, è opportuno ricordare che gli enti pubblici – e tra questi i Comuni – devono ottenere per tale intervento l'autorizzazione del Ministero per i beni e le attività culturali, ai sensi dell'art. 21, comma 1, lettera d) del Codice dei beni culturali e del paesaggio (D. lgs. 22 gennaio 2004, n. 42). L'adozione del Piano di conservazione proposto dal Gruppo non esime quindi le amministrazioni dagli adempimenti relativi alla procedura di scarto, che si sostanzia in un provvedimento formale dell'amministrazione (deliberazione della Giunta o determinazione dirigenziale) e nella acquisizione dell'autorizzazione da parte degli organi periferici del citato Ministero, vale a dire le Soprintendenze archivistiche competenti per territorio.

Il Gruppo di lavoro ha proceduto alla stesura del Piano di conservazione avendo presenti i precedenti Massimari di scarto per gli archivi dei Comuni, in particolare quello elaborato dalla Soprintendenza archivistica per la Toscana e aggiornato dalla Soprintendenza archivistica per la Lombardia, che mantiene la sua validità in riferimento alla documentazione prodotta e classificata sulla base del Titolare Astengo, ma ha ritenuto necessario rielaborare l'intero Piano di conservazione in considerazione del mutamento sostanziale dell'impianto del nuovo titolare e della necessità di ridurre ulteriormente i tempi di conservazione, andando incontro alle esigenze avvertite dagli enti.

Nell'attuale scenario normativo e tecnologico molto si è ragionato rispetto al supporto e alle problematiche connesse alla conservazione o allo scarto del documento informatico, alla sua riproduzione in formato cartaceo e all'uso del supporto ottico sostitutivo. Pur nella consapevolezza che le prospettive di utilizzo del documento elettronico saranno sempre più ampie e considerando che il tema della conservazione permanente dei documenti digitali è, a tutt'oggi, oggetto di studi e di riflessioni da parte di gruppi di lavoro tecnici interministeriali al fine di stabilirne gli standard, si è giunti alla conclusione che il supporto cartaceo sia comunque, nella fase attuale, quello ancora più utilizzato e più sicuro per la conservazione della documentazione di carattere permanente. Il Gruppo inoltre segnala ai Comuni che un sistema di gestione documentale deve avere precisi requisiti per assicurare la conservazione permanente dei documenti digitali (e tra questi, prima di tutto, l'esistenza di un responsabile di livello dirigenziale) e li invita a effettuare un'analisi accurata e una valutazione dei costi e dei benefici sul lungo periodo prima di optare per la soluzione digitale.

Il presente documento si compone di due parti:

- la prima nella quale vengono definiti i principi generali e le indicazioni di massima
- la seconda che contiene nello specifico per ogni titolo e classe del Titolare l'indicazione delle tipologie documentarie prodotte e dei relativi tempi di conservazione. Per quanto riguarda le tipologie documentarie, si fa riferimento alle «Linee guida per l'organizzazione dei fascicoli e delle serie dei documenti prodotti dai Comuni italiani in riferimento al piano di classificazione» proposte da Giorgetta Bonfiglio-Dosio al Gruppo e disponibili per la sperimentazione.

Principi generali

Ambito e criteri generali di applicazione

- Il presupposto per il corretto utilizzo di questo strumento è l'organizzazione dell'archivio basata sul Piano di classificazione prodotto dal Gruppo di lavoro.
- Lo scarto della documentazione prodotta e classificata sino all'adozione del nuovo titolario deve essere valutato sulla base del massimario precedente.
- I termini cronologici indicati devono essere conteggiati dalla chiusura dell'affare per i fascicoli oppure dall'ultima registrazione effettuata, nel caso dei registri.
- In generale, si sono ridotti, rispetto a quelli indicati dal massimario di scarto precedentemente in vigore, i termini di conservazione dei documenti, in linea con la normativa generale civilistica e con la normativa specifica ove contempli termini per la conservazione degli atti.
- Il materiale non archivistico non viene preso in considerazione dal presente Piano, in quanto non devono essere considerati documenti gli stampati in bianco, la modulistica, le raccolte normative o altro materiale analogo (ad esempio, copie della normativa da consegnare all'utenza).
- L'applicazione del piano di conservazione non può comunque essere automatica, ma deve valutare caso per caso le eventuali particolarità adottate dal Comune nell'organizzazione dei documenti prodotti.
- Lo scarto, se non viene effettuato regolarmente ogni anno e su un archivio organizzato, potrà essere deciso e valutato solo dopo che l'intero complesso archivistico sia stato analizzato e almeno sommariamente riordinato.

I fondamenti della conservazione permanente

- In genere, salvo poche eccezioni, tutti i repertori devono essere conservati permanentemente.
- Il Comune non deve scartare i documenti considerati "vitali" (quelli che – mutuando una definizione formulata da Luciana Duranti¹ – in caso di disastro, sono necessari a ricreare lo stato giuridico dell'ente e la sua situazione legale e finanziaria, a garantire i diritti dei dipendenti e dei cittadini, a soddisfare i suoi obblighi e a proteggere i suoi interessi esterni).

Alcune considerazioni sulla dimensione culturale degli archivi

- Lo scarto si effettua di norma sui documenti dell'archivio di deposito.
- Non vanno scartati i documenti prodotti durante la prima e la seconda guerra mondiale e vanno vagliati con estrema attenzione quelli degli anni del dopoguerra e della ricostruzione, perché tali archivi costituiscono una miniera di informazioni e di dati ancora sconosciuti e finora inesplorati dagli storici, oltre che un serbatoio di informazioni rilevanti dal punto di vista giuridico..

¹ L. DURANTI, *I documenti archivistici. La gestione dell'archivio da parte dell'ente produttore*, Roma 1997 (Pubblicazioni degli Archivi di Stato. Quaderni della «Rassegna degli Archivi di Stato», 82), p. 93

Documenti originali e documenti prodotti in copia

- Lo scarto dei documenti in copia può essere facilmente effettuato qualora sia prevista la conservazione permanente dei documenti in originale e qualora le copie non contengano annotazioni amministrative o visti essenziali per ricostruire il procedimento nella sua correttezza.
- È opportuno prevedere repertori di documenti di interesse generale per tutte le UOR del Comune, resi disponibili sul sito interno del Comune, che quindi diventano depositi di documenti ad alto carattere informativo, in modo da evitare copie multiple, superflue, che contribuiscono ad appesantire inutilmente la conservazione documentale nelle diverse UOR, a scapito dei documenti essenziali e specifici.
- È altresì opportuno che ciascun RPA, durante la formazione dell'archivio corrente, abbia cura di non inserire nel fascicolo copie superflue di normative o atti repertoriati di carattere generale, facilmente reperibili in un sistema informatico-archivistico ben organizzato.
- Sarebbe anche auspicabile che il fascicolo venisse organizzato in sottofascicoli nei quali inserire i documenti soggetti a scarto periodico, in modo da facilitare, a tempo debito, le operazioni di scarto.

Avvertenze per la lettura del piano di conservazione

- Quando si usa la formula “previo sfoltimento del carteggio di carattere transitorio e strumentale” si allude all’operazione che estrae dal fascicolo le copie e i documenti, che hanno appunto carattere strumentale e transitorio, utilizzati dal RPA per espletare il procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad esempio, appunti, promemoria, copie di normativa e documenti di carattere generale).
- Se i documenti sono inseriti integralmente o per estratto in una banca dati, l’archivio dispone solo degli esemplari più aggiornati e perde memoria delle fasi storiche. In certi casi, nei quali la memoria è ritenuta essenziale, si suggerisce nel corso del Piano di eseguire periodicamente, a cadenza prestabilita, un salvataggio (copia di back-up) o una stampa della banca dati.

Indice dei titoli

Titolo I. Amministrazione generale	6
Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia	11
Titolo III. Risorse umane	14
Titolo IV. Risorse finanziarie e patrimoniali	19
Titolo V. Affari legali	23
Titolo VI. Pianificazione e gestione del territorio	24

Titolo VII. Servizi alla persona	28
Titolo VIII. Attività economiche	32
Titolo IX. Polizia locale e sicurezza pubblica	34
Titolo X. Tutela della salute	35
Titolo XI. Servizi demografici	36
Titolo XII. Elezioni e iniziative popolari	38
Titolo XIII. Affari militari	40

Titolo I. Amministrazione generale

Classi	Tipologie documentarie	Conservazione	Note
1. Legislazione e circolari esplicative			
	Pareri chiesti dal Comune su leggi specifiche	Permanente	
	Circolari pervenute: repertorio annuale	Permanente	
	Circolari emanate dal Comune: repertorio annuale	Permanente	
2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica			
	Denominazione del Comune	Permanente	
	Attribuzione del titolo di città	Permanente	
	Confini del Comune	Permanente	
	Costituzione delle circoscrizioni	Permanente	
	Verbalì e deliberazioni della Commissione comunale per la toponomastica: repertorio annuale	Permanente	
3. Statuto			
	Redazione, modifiche e interpretazioni dello statuto	Permanente, dopo sfolto-mento del materiale informativo relativo ad altri Comuni	
4. Regolamenti			
	Regolamenti emessi dal Comune: repertorio annuale	Permanente	
	Redazione dei regolamenti: un fasc. per ciascun affare	Permanente, previo sfolto-mento dei documenti di carattere transitorio	Tenere un solo esemplare, scartare gli altri
5. Stemma, gonfalone, sigillo			
	Definizione, modifica, riconoscimento dello stemma	Permanente	
	Definizione, modifica, riconoscimento del gonfalone	Permanente	
	Definizione, modifica, riconoscimento del sigillo	Permanente	
	Concessione del patrocinio gratuito e del connesso uso dello stemma del Comune: fasc. annuale per attività	Permanente	Perché documenta attività che si svolgono nel territorio
6. Archivio generale			

	Registro di protocollo	Permanente	
	Repertorio dei fascicoli	Permanente	
	Organizzazione del servizio e dell'attività ordinaria (aggiornamento del manuale di gestione con titolare e piano di conservazione, selezione periodica, riordino, inventariazione, spostamenti e versamenti di materiale, depositi e comodati):	Permanente	
	Interventi straordinari (ad esempio, traslochi, restauri, gestione servizi esterni, scelta del software di gestione)	Permanente	
	Richieste di accesso per fini amministrativi	1 anno dalla ricollocazione del materiale	
	Richieste di informazioni archivistiche e richieste per motivi di studio	Permanente	
	Richieste di pubblicazione all'albo pretorio	1 anno	
	Registro dell'Albo pretorio	20 anni	
	Richieste di notifica presso la casa comunale (con allegati)	2 anni	
	Registro delle notifiche	20 anni	
	Registri delle spedizioni e delle spese postali	1 anno	
	Ordinanze del Sindaco: repertorio	Permanente	
	Decreti del Sindaco: repertorio	Permanente	
	Ordinanze dei dirigenti: repertorio	Permanente	
	Determinazioni dei dirigenti: repertorio	Permanente	
	Deliberazioni del Consiglio comunale: repertorio	Permanente	
	Deliberazioni della Giunta comunale: repertorio	Permanente	
	Verbali delle adunanze del Consiglio comunale: repertorio	Permanente	
	Verbali delle adunanze della Giunta comunale: repertorio	Permanente	
	Verbali degli altri organi collegiali del Comune: repertorio	Permanente	
	Verbali delle adunanze dei Consigli circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Deliberazioni dei Consigli circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Verbali delle adunanze degli Esecutivi circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Deliberazioni degli Esecutivi circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	

	Verbal dei organi collegiali delle circoscrizioni: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Registro dell'Albo della circoscrizione: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Contratti e convenzioni: repertorio	Permanente	20 anni per un'eventuale serie separata di contratti di scarsa rilevanza
	Contratti e convenzioni delle circoscrizioni: un repertorio per ciascuna circoscrizione	Permanente	20 anni per un'eventuale serie separata di contratti di scarsa rilevanza
	Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa)	Permanente	
7. Sistema informativo			
	Organizzazione del sistema	Permanente	
	Statistiche	Permanente, dopo l'eliminazione dei materiali preparatori	
8. Informazioni e relazioni con il pubblico			
	Iniziative specifiche dell'URP: un fasc. per ciascun affare	Permanente, dopo sfoltoimento del carteggio di carattere transitorio e strumentale	
	Reclami dei cittadini (comunque pervenuti)	Permanente	
	Atti del Difensore civico	Permanente	
	Bandi e avvisi a stampa	Permanente	
	Materiali preparatori per il sito Web	Permanente	
9. Politica del personale; ordinamento degli uffici e dei servizi			
	Attribuzione di competenze agli uffici	Permanente	
	Organigramma: un fasc. per ciascuna definizione dell'organigramma	Permanente	
	Organizzazione degli uffici: un fasc. per ciascun affare	Permanente	
	Orari di apertura degli uffici comunali e degli altri uffici e attività insistenti sul territorio comunale	Permanente	
	Materiale preparatorio per le deliberazioni in materia di politica del personale	10 anni	

10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale			
	Rapporti di carattere generale	Permanente	
	Costituzione delle rappresentanze del personale	Permanente	
	Verballi della Delegazione trattante per la contrattazione integrativa decentrata	Permanente	
11. Controlli esterni			
	Controlli	Permanente	
12. Editoria e attività informativo-promozionale interna ed esterna			
	Pubblicazioni istituzionali del Comune (libri, riviste, inserzioni o altro)	Permanente	
	Pubblicazioni istituzionali del Comune (materiali preparatori)	2 anni	
	Comunicati stampa	Permanente	
13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti			
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente	
	Onorificenze (concesse e ricevute): un fasc. per ciascun evento	Permanente	
	Concessione dell'uso del sigillo: un fasc. annuale	Permanente	
14. Interventi di carattere politico e umanitario; rapporti istituzionali			
	Iniziative specifiche (ad esempio, adesione a movimenti di opinione): un fasc. per ciascun affare	Permanente	
	Gemellaggi	Permanente	
	Promozione di comitati: un fasc. per ciascun affare	Permanente	

15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni			
	Costituzione di enti controllati dal Comune (comprensivo della nomina dei rappresentanti e dei verbali inviati per approvazione)	Permanente, previo sfoltimento del carteggio di carattere transitorio	
	Partecipazione del Comune a enti e associazioni (comprensivo della nomina dei rappresentanti)	Permanente, previo sfoltimento del carteggio di carattere transitorio	
16. Area e città metropolitana			
	Costituzione e rapporti istituzionali	Permanente	
17. Associazionismo e partecipazione			
	Politica di incoraggiamento e appoggio alle associazioni	Permanente	
	Albo dell'associazionismo: elenco delle associazioni accreditate	Permanente	
	Fascicoli delle associazioni che chiedono l'iscrizione all'albo	Permanente	

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

Classi	Tipologie documentarie	Conservazione	Note
1. Sindaco			
	Fasc. personale che dura quanto il mandato	Permanente	
2. Vice-sindaco			
	Fasc. personale che dura quanto il mandato	Permanente	
3. Consiglio			
	Fasc. personali: un fasc. per ogni consigliere che dura quanto dura il mandato	Permanente	
	Convocazioni del Consiglio e OdG	1 anno	Purché riportati nei verbali
	Interrogazioni e mozioni consiliari	Permanente	dopo sfoltimento
	Bollettino della situazione patrimoniale dei titolari di cariche elettive e di cariche direttive	Permanente	
4. Presidente del Consiglio			
	Fasc. personale che dura quanto il mandato	Permanente	
5. Conferenza dei capigruppo e Commissioni del Consiglio			
	Verbali della Conferenza	Permanente	
	Verbali delle Commissioni	Permanente	
6. Gruppi consiliari			
	Accreditamento presso il Consiglio	Permanente	Scartare i materiali prodotti o raccolti dai Gruppi
7. Giunta			
	Nomine, revoche e dimissioni degli assessori	Permanente	
	Convocazioni della Giunta e OdG	1 anno	Purché riportati nei verbali
8. Commissario prefettizio e straordinario			
	Fasc. personale	Permanente	
9. Segretario e Vice-segretario			

	Fasc. personale (nomina, etc.) per la durata dell'incarico	Permanente	
10. Direttore generale e dirigenza			
	Fasc. personale	Permanente	
11. Revisori dei conti			
	Fasc. personale	Permanente	
12. Difensore civico			
	Fasc. personale	Permanente	
13. Commissario <i>ad acta</i>			
	Fasc. personale	Permanente	
14. Organi di controllo interni			
	Un fasc. per ogni organo	Permanente	
15. Organi consultivi			
	Un fasc. per ogni organo	Permanente	
16. Consigli circoscrizionali			
	Fasc. personali: un fasc. per ogni consigliere che dura quanto dura il mandato	Permanente	
	Convocazioni del Consiglio e OdG	1 anno	Purché riportati nei verbali
	Interrogazioni consiliari	Permanente	
17. Presidenti dei Consigli circoscrizionali			
	Fasc. personale che dura quanto il mandato	Permanente	
18. Organi esecutivi circoscrizionali			
	Nomine e dimissioni dei componenti	Permanente	
	Convocazioni e OdG delle riunioni	1 anno	Purché riportati nei verbali
19. Commissioni dei Consigli circoscrizionali			
	Un fasc. per ogni commissione	Permanente	
20. Segretari delle circoscrizioni			
	Fasc. personale (nomina, etc.) per la durata dell'incarico	Permanente	
21. Commissario <i>ad acta</i> delle circoscrizioni			

	Fasc. personale	Permanente	
22. Conferenza dei Presidenti di quartiere			
	Verbali della Conferenza	Permanente	

Titolo III. Risorse umane

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli personali dei dipendenti e assimilati (quindi anche collaboratori a contratto o a progetto)	Permanente previo sfoltimento da eseguire seguendo la tempistica prevista per le singole classi	
1. Concorsi, selezioni, colloqui			
	Criteri generali e normativa per il reclutamento del personale: un fasc. con eventuali sottofascicoli	Permanente	
	Procedimenti per il reclutamento del personale: un fasc. per ciascun procedimento (fasc. per affare), con i seguenti sottofascicoli: - Bando e manifesto - Domande - Allegati alle domande (ove previsti dal bando) - Verbali - Prove d'esame - Copie bando restituite al Comune	Permanente 1 anno dopo la scadenza dei termini per i ricorsi da restituire dopo la scadenza dei termini per i ricorsi permanente 1 anno dopo la scadenza dei termini per i ricorsi 1 anno dopo la scadenza dei termini per i ricorsi	Agli interessati
	<i>Curricula</i> inviati per richieste di assunzione	2 anni	
	Domande di assunzione pervenute senza indizione di concorso o selezione	1 anno	
2. Assunzioni e cessazioni			
	Criteri generali e normativa per le assunzioni e cessazioni	Permanente	
	Determinazioni di assunzione e cessazione dei singoli inserite nei singoli fascicoli personali	Permanente	
3. Comandi e distacchi; mobilità			

	Criteri generali e normativa per comandi, distacchi, mobilità	Permanente	
	Determinazioni di comandi, distacchi e mobilità inserite nei singoli fascicoli personali	Permanente	
4. Attribuzione di funzioni, ordini di servizio e missioni			
	Criteri generali e normativa per le attribuzioni di funzioni, ordini di servizio e missioni	Permanente	
	Determinazioni di attribuzione di funzioni inserite nei singoli fascicoli personali	Permanente	
	Determinazioni di missioni inserite nei singoli fascicoli personali	10 anni	
	Determinazioni di ordini di servizio inserite nei singoli fascicoli personali	Permanente	
	Ordini di servizio collettivi	Permanente	
	Autorizzazione allo svolgimento di incarichi esterni	2 anni	
5. Inquadramenti e applicazione contratti collettivi di lavoro			
	Criteri generali e normativa per gli inquadramenti e le applicazione dei contratti collettivi di lavoro	Permanente	
	Determinazione dei ruoli e contratti collettivi	Permanente	NB i contratti con il singolo confluiscono nel fasc. personale
	Determinazioni relative ai singoli	Permanente	
6. Retribuzioni e compensi			
	Criteri generali e normativa per le retribuzioni e compensi	Permanente	
	Anagrafe delle prestazioni: schede	5 anni	
	Determinazioni inserite nei singoli fascicoli personali	5 anni dalla cessazione dal servizio	
	Ruoli degli stipendi: base di dati/ tabulati	Permanente	
	Provvedimenti giudiziari di requisizione dello stipendio	5 anni	
7. Trattamento fiscale, contributivo e assicurativo			
	Criteri generali e normativa per gli adempimenti fiscali, contributivi e assicurativi	Permanente	

	Trattamento assicurativo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Trattamento contributivo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Trattamento fiscale inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Assicurazione obbligatoria inserita nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
8. Tutela della salute e sicurezza sul luogo di lavoro			
	Criteri generali e normativa per la tutela della salute e sicurezza sul luogo di lavoro	Permanente	
	Rilevazione dei rischi, ai sensi della 626/94: un fasc. per sede	Tenere l'ultima e scartare la precedente	
	Prevenzione infortuni	Permanente	
	Registro infortuni	Permanente	Per L. 626/94
	Verbali delle rappresentanze dei lavoratori per la sicurezza	Permanente	
	Denuncia di infortunio e pratica relativa, con referti, inserita nei singoli fascicoli personali	Permanente	
	Fascicoli relativi alle visite mediche ordinarie (medicina del lavoro)	10 anni	
9. Dichiarazioni di infermità ed equo indennizzo			
	Criteri generali e normativa per le dichiarazioni di infermità	Permanente	
	Dichiarazioni di infermità e calcolo dell'indennizzo inserite nel singolo fascicolo personale	Permanente	
10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza			
	Criteri generali e normativa per il trattamento di fine rapporto	Permanente	
	Trattamento pensionistico e di fine rapporto inserito nel singolo fascicolo personale	Permanente	
11. Servizi al personale su richiesta			
	Criteri generali e normativa per i servizi su richiesta	Permanente	

	Domande di servizi su richiesta (mensa, asili nido, colonie estive, soggiorni climatici, etc.)	2 anni	
12. Orario di lavoro, presenze e assenze			
	Criteri generali e normativa per le assenze	Permanente	
	Domande e dichiarazioni dei dipendenti sull'orario inserite nel singolo fascicolo personale: - 150 ore - permessi d'uscita per motivi personali - permessi per allattamento - permessi per donazione sangue - permessi per motivi sindacali - opzione per orario particolare e part-time	2 anni 2 anni 2 anni 2 anni 2 anni Permanente	
	Domande e dichiarazioni dei dipendenti sulle assenze (con allegati) inserite nel singolo fascicolo personale: - congedo ordinario - congedo straordinario per motivi di salute - congedo straordinario per motivi personali e familiari - aspettativa per infermità - aspettativa per mandato parlamentare o altre cariche elettive - aspettativa obbligatoria per maternità e puerperio - aspettativa facoltativa per maternità e puerperio - aspettativa per motivi di famiglia - aspettativa sindacale - certificati medici	2 anni 2 anni Alla cessazione dal servizio Permanente Permanente Permanente Permanente Permanente Permanente Alla cessazione dal servizio	
	Referti delle visite di controllo inseriti nel singolo fascicolo personale	Alla cessazione dal servizio	
	Fogli firma; cartellini marcatempo; tabulati elettronici di rilevazione presenze	2 anni	In assenza di pendenze disciplinari o giudiziarie
	Rilevazioni delle assenze per sciopero: - singole schede - prospetti riassuntivi	1 anno dopo la redazione dei prospetti riassuntivi Permanente	
13. Giudizi, responsabilità e provvedimenti disciplinari			
	Criteri generali e normativa per i provvedimenti disciplinari	Permanente	

	Provvedimenti disciplinari inseriti nel singolo fascicolo personale	Permanente	
--	---	------------	--

14. Formazione e aggiornamento professionale			
	Criteri generali e normativa per la formazione e l'aggiornamento professionale	Permanente	
	Organizzazione di corsi di formazione e aggiornamento: un fasc. per ciascun corso	Permanente previo sfoltimento dopo 5 anni	
	Domande/Invio dei dipendenti a corsi inseriti nel singolo fascicolo personale	Permanente previo sfoltimento dopo 5 anni	
15. Collaboratori esterni			
	Criteri generali e normativa per il trattamento dei collaboratori esterni	Permanente	
	Elenco degli incarichi conferiti: repertorio	Permanente	

Titolo IV. Risorse finanziarie e patrimoniali

Classi	Tipologie documentarie	Conservazione	Note
2. Bilancio preventivo e Piano esecutivo di gestione (PEG)			
	Bilancio preventivo e allegati, tra cui Relazione previsionale e programmatica	Permanente	
	PEG: articolato in fascicoli: un fasc. per ogni obiettivo	Permanente, previo sfoltimento	
	Carteggio prodotto dai differenti uffici del Comune per questioni afferenti alla formazione del bilancio e del PEG	10 anni	
2. Gestione del bilancio e del PEG (con eventuali variazioni)			
	Gestione del bilancio: un fasc. per ciascuna variazione	Permanente, previo sfoltimento	
3. Gestione delle entrate: accertamento, riscossione, versamento			
	Fascicoli personali dei contribuenti comunali: un fasc. per ciascun contribuente per ciascun tipo di imposte (ICI, TARSU, TOSAP, etc.), con eventuali sottofascicoli (variazioni, ricorsi, etc.)	10 dopo la cancellazione del contribuente dai ruoli	
	Ruolo ICI: base di dati/ stampe	10 anni	Prevedere una stampa periodica
	Ruolo imposta comunale sulla pubblicità: base di dati	10 anni	Prevedere una stampa periodica
	Ruolo diritti sulle pubbliche affissioni: base di dati	10 anni	Prevedere una stampa periodica
	Ruolo TARSU: base di dati	10 anni	Prevedere una stampa periodica
	Ruolo COSAP: base di dati	10 anni	Prevedere una stampa periodica
	Contratti di mutuo: un fasc. per ciascun mutuo	5 anni dall'estinzione del mutuo	
	Proventi da affitti e locazioni: un fasc. annuale per ciascun immobile locato	5 anni dal termine del contratto	

	Diritti di segreteria: registri annuali o pagamenti virtuali	5 anni	
	Matrici dei bollettari delle entrate: registri annuali	5 anni	
	Ricevute dei versamenti in banca delle somme riscosse nelle differenti UOR per diritti di segreteria	5 anni	
	Fatture emesse: repertorio annuale	10 anni	
	Reversali	5 anni	
	Bollettari vari	5 anni	
	Ricevute di pagamenti vari	5 anni	
4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento			
	Impegni di spesa (determinazioni dei dirigenti delle UOR): copie inviate dalle UOR alla Ragioneria: repertorio annuale	2 anni	
	Fatture ricevute: repertorio annuale	10 anni	
	Atti di liquidazione con allegati trasmessi da ciascuna UOR: repertorio annuale	2 anni	
	Mandati di pagamento con allegati emessi dalla Ragioneria e inviati alla Tesoreria: repertorio annuale	10 anni dall'approvazione del bilancio	Purché registrati in scritture contabili di sintesi
	Eventuali copie di mandati	2 anni	
5. Partecipazioni finanziarie			
	Gestione delle partecipazioni finanziarie: un fasc. per ciascuna partecipazione	Permanente, previo sfolgimento	
6. Rendiconto della gestione; adempimenti e verifiche contabili			
	Rendiconto della gestione, articolato in Conto del bilancio, Conto del patrimonio e Conto economico	Permanente	
7. Adempimenti fiscali, contributivi e assicurativi			
	Mod. 770	10 anni	Più se si ritiene opportuno
	Ricevute dei versamenti (IVA, IRPEF, etc.)	10 anni	
	Pagamento dei premi dei contratti assicurativi	5 anni dall'estinzione del contratto	
8. Beni immobili			
	Inventario dei beni immobili: registro o base di dati perenne	Permanente	

	Fascicoli dei beni immobili: un fasc. per ciascun bene immobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche, che possono anche essere di competenza di UOR diverse: - acquisizione - manutenzione ordinaria - gestione - uso - alienazione e dismissione	Permanente 20 anni 5 anni 5 anni Permanente	
	Concessioni di occupazione di spazi e aree pubbliche: repertorio	Permanente	
	Concessioni di beni del demanio statale: repertorio	Permanente	
	Concessioni cimiteriali: repertorio	Permanente	
	Fascicoli personali dei concessionari: un fasc. per ciascun concessionario	5 anni dalla cessazione del rapporto	
9. Beni mobili			
	Inventari dei beni mobili: uno per consegnatario	Permanente	
	Fascicoli dei beni mobili: un fasc. per ciascun bene mobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche, che possono anche essere di competenza di UOR diverse: - acquisizione - manutenzione - concessione in uso - alienazione e altre forme di dismissione	5 anni dalla dismissione 5 anni dalla dismissione 5 anni dalla dismissione 5 anni dalla dismissione	
10. Economato			
	Acquisizione di beni e servizi: un fasc. per ciascun acquisto	5 anni dalla dismissione del bene	
	Elenco dei fornitori: repertorio (in forma di base di dati)	Permanente	
11. Oggetti smarriti e recuperati			
	Verbal di rinvenimento: serie annuale repertoriata	2 anni	
	Ricevute di riconsegna ai proprietari: serie annuale repertoriata	2 anni	
	Vendita o devoluzione: un fasc. periodico (per attività)	2 anni	
12. Tesoreria			
	Giornale di cassa	Permanente	

	Mandati quietanzati, che vengono inviati in Ragioneria: repertorio periodico (mese/anno)	10 anni	
13. Concessionari ed altri incaricati della riscossione delle entrate			
	Concessionari: un fasc. per ciascuno dei concessionari	10 anni dalla cessazione del rapporto	
14. Pubblicità e pubbliche affissioni			
	Autorizzazioni alla pubblicità stabile: repertorio annuale	5 anni dalla scadenza dell'autorizzazione	Salvo non si rilevi qualche necessità particolare di conservazione a campione
	Autorizzazioni alla pubblicità circoscritta: repertorio annuale	5 anni dalla scadenza dell'autorizzazione	
	Richieste di affissione (con allegati da affiggere): un fasc. per richiesta	5 anni dalla scadenza dell'autorizzazione	

Titolo V. Affari legali

Classi	Tipologie documentarie	Conservazione	Note
1. Contenzioso			
	Fascicoli di causa	Permanente	Concentrare quelli presso gli studi professionali esterni
2. Responsabilità civile e patrimoniale verso terzi; assicurazioni			
	Contratti assicurativi	2 anni dalla scadenza	
	Richieste e pratiche di risarcimento	10 anni	
3. Pareri e consulenze			
	Pareri e consulenze	Permanente	

Titolo VI. Pianificazione e gestione del territorio
--

Classi	Tipologie documentarie	Conservazione	Note
1. Urbanistica: piano regolatore generale e varianti			
	PGR	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Pareri su piani sovracomunali	Permanente	Dopo sfoltimento
	Certificati di destinazione urbanistica	1 anno dopo la scadenza	
	Varianti al PRG	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
2. Urbanistica: strumenti di attuazione del piano regolatore generale			
	Piani particolareggiati del PRG	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piani di lottizzazione	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piani di edilizia economica e popolare – PEEP	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piano particolareggiato infrastrutture stradali - PPIS	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piano di riqualificazione urbana – PRU	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio

	Piano insediamenti produttivi - PIP	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Programma integrato di riqualificazione	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	programma di riqualificazione urbana e di sviluppo sostenibile del territorio	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
3. Edilizia privata			
	Autorizzazioni edilizie: repertorio	Permanente	
	Fascicoli dei richiedenti le autorizzazioni: un fasc. per ciascuna autorizzazione	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Accertamento e repressione degli abusi	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Denunce e relazioni finali delle opere in cemento armato	Fino a quando esiste l'edificio	
4. Edilizia pubblica			
	Costruzione di edilizia popolare	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
5. Opere pubbliche			
	Realizzazione di opere pubbliche	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Manutenzione ordinaria	5 anni	Salvo necessità particolari
	Manutenzione straordinaria	20 anni	Salvo necessità particolari

6. Catasto			
	Catasto terreni: mappe	Permanente	
	Catasto terreni: registri	Permanente	
	Catasto terreni: indice alfabetico dei possessori	Permanente	
	Catasto terreni: estratti catastali	Permanente	
	Catasto terreni: denunce di variazione (vulture)	Permanente	
	Catasto fabbricati: mappe	Permanente	
	Catasto fabbricati: registri	Permanente	
	Catasto fabbricati: indice alfabetico dei possessori	Permanente	
	Catasto fabbricati: estratti catastali	Permanente	
	Catasto terreni: denunce di variazione (vulture)	Permanente	
	Richieste di visure e certificazioni	1 anno	
7. Viabilità			
	Piano Urbano del Traffico: un fasc. per ciascun affare	Permanente sfoltimento	con
	Piano Urbano della Mobilità: un fasc. per ciascun affare	Permanente sfoltimento	con
	Autorizzazioni in deroga: serie annuale repertoriata	2 anni	
8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi			
	Approvvigionamento idrico (organizzazione e funzionamento)	Permanente sfoltimento	con
	Fascicoli relativi alle irregolarità	10 anni	
	Iniziative a favore dell'ambiente	Permanente sfoltimento	con
	Distribuzione dell'acqua: contratti con gli utenti	2 anni dalla cessazione del rapporto	Purché in assenza di contenzioso
	Produzione di energia elettrica o altre fonti energetiche (organizzazione e funzionamento)	Permanente sfoltimento	con
	Distribuzione di energia elettrica o altre fonti energetiche: contratti con gli utenti:	2 anni dalla cessazione del rapporto	Purché in assenza di contenzioso
	Trasporti pubblici (gestione)	Permanente sfoltimento	con
	Vigilanza sui gestori dei servizi: un fasc. annuale per attività	Permanente sfoltimento	con
	Fascicoli relativi alle irregolarità	10 anni	

	Iniziative di sensibilizzazione degli utenti per consumi razionali: un fasc. per ciascuna iniziativa	Permanente sfoltimento	con	
	Dichiarazioni di conformità degli impianti: repertorio annuale	1 anno		
9. Ambiente: autorizzazioni, monitoraggio e controllo				
	Valutazioni e pareri di impatto ambientale: un fasc. per ciascun parere	Permanente		
	Monitoraggi della qualità delle acque: fasc. annuale per attività	10 anni		
	Monitoraggi della qualità dell'aria: fasc. annuale per attività	10 anni		
	Monitoraggi della qualità dell'etere: un fasc. annuale per attività	10 anni		
	Altri eventuali monitoraggi: fasc. annuale per attività	10 anni		
	Fascicoli relativi alle irregolarità	10 anni		
	Controlli a campione sugli impianti termici dei privati: fasc. annuale per attività	2 anni		
	Fascicoli relativi alle irregolarità	10 anni		
10. Protezione civile ed emergenze				
	Segnalazioni preventive di condizioni metereologiche avverse: un fasc. annuale	2 anni		
	Addestramento ed esercitazioni per la protezione civile: un fasc. annuale	5 anni		
	Interventi per emergenze: un fasc. per ciascuna emergenza	Permanente sfoltimento	con	

Titolo VII. Servizi alla persona	
Osservazioni generali	<i>L'autonomia dei Comuni si può esplicitare in forme svariate soprattutto in questo titolo: perciò l'indicazione generica di evento o attività verrà riempita di contenuti concreti dalla singola amministrazione.</i>

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli per persona	Permanente, previo sfolto-mento del carteggio tempo-raneo e strumentale dopo 5 anni	
1. Diritto allo studio e servizi			
	Concessione di borse di studio: - bando - domande - graduatorie - assegnazioni	permanente 5 anni permanente 5 anni	
	Distribuzione buoni libro: un fasc. per scuola	2 anni	
	Gestione buoni pasto degli iscritti alle scuole: un fasc. per periodo	2 anni	
	Verbalì del comitato genitori per la mensa	3 anni	
	Azioni di promozione e sostegno del diritto allo studio: un fasc. per intervento	5 anni	
	Gestione mense scolastiche: un fasc. per mensa scolastica e per periodo	10 anni	
	Integrazione di neo-immigrati e nomadi: un fasc. per intervento	10 anni	
	Gestione trasporto scolastico: un fasc. per periodo e per tratta	2 anni	
2. Asili nido e scuola materna	Domande di ammissione agli asili nido e alle scuole materne: un fasc. per asilo/scuola	2 anni	
	Graduatorie di ammissione	2 anni	
	Funzionamento. degli asili e delle scuole materne: un fasc. per struttura	10 anni	

3. Promozione e sostegno delle istituzioni di istruzione e della loro attività			
	Iniziative specifiche: un fasc. per iniziativa	10 anni	
	Registri scolastici (del professore e della classe) prodotti dalle Scuole civiche (ove presenti)	Permanenti	
4. Orientamento professionale; educazione degli adulti; media-zione culturale			
	Iniziative specifiche: un fasc. per iniziativa	10 anni	
5. Istituti culturali			
	Funzionamento delle diverse istituzioni culturali: un fasc. per istituto	Permanente	
	Verbalì degli organi di gestione degli Istituti culturali	Permanente	
6. Attività ed eventi culturali			
	Attività ordinarie annuali: un fasc. per attività e per periodo)	10 anni	
	Eventi culturali: un fasc. per evento	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
	Feste civili e/o religiose: un fasc. per iniziativa	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative culturali. un fasc. per iniziativa	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
	Prestiti di beni culturali: un fasc. per affare	Permanente	
7. Attività ed eventi sportivi			
	Eventi e attività sportive: un fasc. per evento/attività	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 5 anni	
8. Pianificazione e accordi strate-gici con enti pubblici e privati e con il volontariato so-ciale			

	Piano sociale: un fasc. annuale eventualmente organizzato in sottofasc.	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Programmazione per settori: un fasc. per ciascun settore	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Accordi con i differenti soggetti: un fasc. per ciascun soggetto	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
9. Prevenzione, recupero e reintegrazione dei soggetti a rischio			
	Campagne di prevenzione: un fasc. per campagna	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Interventi di recupero e reintegrazione dei soggetti a rischio: un fasc. per intervento	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Ricognizione dei rischi: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
10. Informazione, consulenza ed educazione civica			
	Funzionamento e attività delle strutture (consultori, informagiovani, etc.): un fasc. per struttura	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative di vario tipo: un fasc. per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
11. Tutela e curatela di incapaci			

	Interventi per le persone sottoposte a tutela e curatela: un fasc. per intervento.	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
12. Assistenza diretta e indiretta, benefici economici			
	Funzionamento e attività delle strutture: un fasc. annuale per ciascuna struttura	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
13. Attività ricreativa e di socializzazione			
	Funzionamento e attività delle strutture (colonie, centri ricreativi, etc.): un fasc. annuale per ciascuna struttura	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
14. Politiche per la casa			
	Assegnazione degli alloggi: un fasc. per bando, organizzato in sottofascicoli: - bando - domande - graduatoria - assegnazione	permanente 5 anni permanente 5 anni	
	Fasc. degli assegnatari : un fasc. per assegnatario	5 anni dopo la scadenza del contratto	In assenza di contenzioso
15. Politiche per il sociale			
	Iniziative specifiche: un fasc. per iniziativa	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	

Titolo VIII. Attività economiche

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli individuali degli esercenti attività economiche: un fasc. per persona	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
1. Agricoltura e pesca			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
	Dichiarazioni raccolta e produzione: un fasc. per periodo	5 anni	
2. Artigianato			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
	Autorizzazioni artigiane: repertorio	Permanente	
3. Industria			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
4. Commercio			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
	Comunicazioni dovute: un fasc. per periodo	1 anno	
	Autorizzazioni commerciali: repertorio	Permanente	
5. Fiere e mercati			

	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
6. Esercizi turistici e strutture ricettive			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	
	Autorizzazioni turistiche: repertorio	Permanente	
7. Promozione e servizi			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteg-gio temporaneo e strumentale dopo 5 anni	

Titolo IX. Polizia locale e sicurezza pubblica

Classi	Tipologie documentarie	Conservazione	Note
1. Prevenzione ed educazione stradale			
	Iniziative specifiche di prevenzione: un fasc. per iniziativa	5 anni	
	Corsi di educazione stradale nelle scuole: un fasc. per corso	5 anni	
2. Polizia stradale			
	Direttive e disposizioni: un fasc. annuale	Permanente	
	Organizzazione del servizio di pattugliamento: un fasc. annuale	3 anni	
	Verbal di accertamento di violazioni al Codice della strada: repertorio annuale	10 anni	
	Accertamento di violazioni al Codice della strada e conseguente erogazione di sanzioni: un fasc. per accertamento	5 anni	
	Verbal di rilevazione incidenti: repertorio annuale	20 anni	In assenza di contenzioso (ai sensi dell'art. 157 del Codice penale)
	Statistiche delle violazioni e degli incidenti: un fasc. annuale	Permanente	
	Gestione veicoli rimossi: un fasc. per ciascun veicolo	2 anni	
3. Informative			
	Informative su persone residenti nel Comune: un fasc. per ciascuna persona	5 anni	
4. Sicurezza e ordine pubblico			
	Direttive e disposizioni generali: un fasc. annuale	Permanente	
	Servizio ordinario di pubblica sicurezza: un fasc. annuale	5 anni	
	Servizio straordinario di pubblica sicurezza, in caso di eventi particolari (manifestazioni, concerti, etc.): un fasc. per evento	5 anni	
	Autorizzazioni di pubblica sicurezza: repertorio annuale, organizzata in sottoserie	Permanente	

	Fascicoli dei richiedenti l'autorizzazione di pubblica sicurezza: un fasc. per richiedente	5 anni	
	Verbali degli accertamenti nei diversi settori (edilizio, sanitario, commerciale, anagrafico, sociale, etc.): un repertorio annuale per ciascun settore di accertamento	Permanente	

Titolo X. Tutela della salute

Classi	Tipologie documentarie	conservazione	Note
1. Salute e igiene pubblica			
	Emergenze sanitarie: un fasc. per ciascun evento	Permanente	
	Misure di igiene pubblica: un fasc. per ciascun affare	Permanente	
	Interventi di derattizzazione, dezzanarizzazione etc.: un fasc. per ciascun intervento	1 anno	
	Trattamenti fitosanitari e di disinfestazione: un fasc. per ciascun intervento	1 anno	
	Autorizzazioni sanitarie: repertorio annuale	Permanente	
	Fascicoli dei richiedenti autorizzazioni sanitarie: un fasc. per ciascuna persona/ditta	5 anni dalla cessazione dell'attività	
	Concessioni di agibilità: repertorio annuale	Permanente	
	Fascicoli dei richiedenti l'agibilità: un fasc. per ciascun richiedente	Permanente	
2. Trattamenti Sanitari Obbligatori			
	TSO: un fasc. per ciascun procedimento	Permanente	
	ASO: un fasc. per ciascun procedimento	Permanente	
	Fascicoli personali dei soggetti a trattamenti: un fasc. per ciascuna persona	Permanente	
3. Farmacie			
	Istituzione di farmacie: un fasc. per ciascuna farmacia	Permanente	
	Funzionamento delle farmacie: un fasc. per ciascun periodo (anno o mese)	2 anni	
4. Zooprofilassi veterinaria			
	Fasc. relativi a epizootie (epidemie animali): un fasc. per ciascun evento	Permanente	
5. Randagismo animale e ricoveri			
	Gestione dei ricoveri e degli eventi connessi: un fasc. per ciascun procedimento	3 anni	

Titolo XI. Servizi demografici

Classi	Tipologie documentarie	Conservazione	Note
1. Stato civile			
	Registro dei nati: repertorio annuale	Permanente	
	Registro dei morti: repertorio annuale	Permanente	
	Registro dei matrimoni: repertorio annuale	Permanente	
	Registro di cittadinanza: repertorio annuale	Permanente, se recanti registrazioni	
	Atti allegati per registrazioni	=	Trasmessi annualmente all'ufficio del governo competente per territorio
	Atti per annotazioni sui registri di stato civile: un fasc. per ciascun procedimento	10 anni	
	Comunicazione dei nati all'Agenzia per le entrate: un fasc. per ciascun periodo	1 anno	
2. Anagrafe e certificazioni			
	APR 4: iscrizioni anagrafiche: un fasc. per ciascuna persona	Permanente	
	AIRE: un fasc. per ciascuna persona	Permanente	
	Richieste certificati: un fasc. per ciascun periodo (mese o anno)	1 anno	
	Corrispondenza con altre amministrazioni per rilascio e trasmissione documenti: un fasc. per ciascun periodo (mese o anno)	1 anno	
	Cartellini per carte d'identità: uno per ciascuna persona	1 anno	Mediante incenerimento o triturazione
	Carte d'identità scadute e riconsegnate: un fasc. per ciascuna persona	5 anni	Mediante incenerimento o triturazione Circ. Min. interno – Direz. gen. PS 23 ott. 1950, n. 10-13070-12982-7-1
	Cambi di abitazione e residenza: un fasc. per ciascuna persona	10 anni	Salvo esigenze particolari
	Cancellazioni: un fasc. per ciascuna persona	10 anni	Salvo esigenze particolari
	Carteggio con la Corte d'appello per la formazione degli Albi dei giudici popolari: un fasc. per ciascun periodo	3 anni dall'ultima revisione	
	Registro della popolazione: su base di dati	Permanente	Salvataggi periodici per storicizzare la banca dati

3. Censimenti			
	Schedoni statistici del censimento	Si conservano quelli dell'ultimo censimento; quelli del precedente si scartano dopo 1 anno dall'ultimo	
	Atti preparatori e organizzativi	3 anni	
4. Polizia mortuaria e cimiteri			
	Registri di seppellimento	Permanente	
	Registri di tumulazione	Permanente	
	Registri di esumazione	Permanente	
	Registri di estumulazione	Permanente	
	Registri di cremazione	Permanente	
	Registri della distribuzione topografica delle tombe con annesse schede onomastiche	Permanente	
	Trasferimento delle salme: un fasc. per ciascun trasporto	50 anni	

Titolo XII. Elezioni e iniziative popolari	
Osservazioni	Ci si riferisca per i particolari a MINISTERO DELL'INTERNO-DIREZ. GEN. DELL'AMMINISTRAZIONE CIVILE –DIREZ CENTRALE PER I SERVIZI ELETTORALI, <i>Massimario per lo scarto degli atti elettorali</i> , Roma 1984

Classi	Tipologie documentarie	Conservazione	Note
1. Albi elettorali			
	Albo dei presidenti di seggio: un elenco per ciascuna elezione	5 anni	
	Albo degli scrutatori: un elenco per ciascuna elezione	5 anni	
2. Liste elettorali			
	Liste generali	1 anno dopo la redazione della successiva	
	Liste sezionali	1 anno dopo la redazione della successiva	
	Verballi della commissione elettorale comunale	Permanente	
	Copia dei verbali della Commissione elettorale mandamentale in ordine alle operazioni e deliberazioni adottate dalla Commissione elettorale comunale	5 anni	
	Schede dello schedario generale	5 anni dopo la redazione della successiva	
	Schede degli schedari sezionali	5 anni dopo la redazione della successiva	
	Fasc. personali degli elettori: un fasc. per ciascun elettore	5 anni dopo la cancellazione dalla lista	
	Elenchi recanti le proposte di variazione delle liste elettorali	5 anni dopo la redazione della lista successiva	
	Carteggio concernente la tenuta e la revisione delle liste elettorali	5 anni dopo la redazione della lista successiva	
3. Elezioni			
	Convocazione dei comizi elettorali: un fasc. per ciascuna elezione	Permanente	
	Presentazione delle liste: manifesto	Permanente	
	Presentazione delle liste: carteggio	5 anni	
	Atti relativi alla costituzione e arredamento dei seggi	5 anni	
	Verballi dei presidenti di seggio	=	Trasmessi al Min dell'interno
	Schede	=	Trasmesse al Min dell'interno

	Pacchi scorta elezioni	2 anni	
	Certificati elettorali non ritirati	2 anni	
	Istruzioni elettorali a stampa	2 anni	
4. Referendum			
	Atti preparatori	5 anni	
	Atti relativi alla costituzione e arredamento dei seggi	5 anni	
	Verbali dei presidenti di seggio	=	Trasmessi al Min dell'interno
	Schede	=	Trasmesse al Min dell'interno
5. Istanze, petizioni e iniziative popolari			
	Raccolta di firme per referendum previsti dallo statuto: un fasc. per ciascuna iniziativa	5 anni dopo il referendum	

Titolo XIII. Affari militari

Classi	Tipologie documentarie	Conservazione	Note
1. Leva e servizio civile sostitutivo			
	Liste di leva: una per anno	Permanente	
	Lista degli eliminati/esentati: una per anno	Permanente	
2. Ruoli matricolari			
	Uno per anno	Permanente	
3. Caserme, alloggi e servitù militari			
	Procedimenti specifici: un fasc. per ciascun procedimento	Permanente	
4. Requisizioni per utilità militari			
	Procedimenti specifici: un fasc. per ciascun procedimento	Permanente	

Elenco delle trasmissioni telematiche

Documento n. 7

Ente – soggetto - sistema	Tipologia trasmissione
Agenzia delle Entrate - piattaforma Sister	Dati catastali Portale dei Comuni Visure - estratti Trasmissione contratti digitali
Anagrafe Tributaria	Dati intestatari Denunce inizio attività e permessi di costruire
Ancitel/Sgate (Sistema gestione agevolazioni tariffe energetiche)	Richieste di ammissione al bonus luce e bonus gas
Aran	Trasmissione contratto decentrato Trasmissione deleghe sindacali
AVPC - Autorità di vigilanza sui contratti pubblici di lavori servizi e forniture	Richiesta codice CIG (in forma ordinaria SIMOG e semplificata) Certificati di esecuzione lavori Sistema AVCPass
Casellario Giudiziale	Comunicazione Decessi
CIPE	CUP
Corte dei Conti	Rendiconto, conto degli agenti contabili, revisione partecipazioni, debiti fuori bilancio, spese di rappresentanza, relazione di fine mandato
Entratel	F24EP F24 ORDINARIO 770S e 770O Ricezione mod. 730/4 Comunicazione contratti non registrati non superiori ad € 10.000,00
BDAP	Bilancio Rendiconto
Equitalia /Esatri /Agenzia Riscossione	Provvedimenti scarico Ruoli
Guce / Simap	Pubblicazione atti, avvisi e concorsi
Ifel	Dati contributo 0.8 per mille ICI
Inail	Denuncia annuale Denuncia Infortunio
Infocamere	Verifica autocertificazione imprese
Comunica Starweb	Verifica documentazione impresa

Impresainungiorno.gov	Verifica documentazione impresa
Inps – Gestione ex Inpdap	Mutui – piccoli prestiti – cessioni stipendi Variazioni anagrafiche Cartolarizzazione crediti
INPS Inps – Gestione ex Inpdap	Assegni di maternità nucleo familiare Gestione Malattie UNIEMENS LISTA POSTA Assegno nucleo familiare e maternità
Istat	Rilevazione permessi di costruire, DIA SCIA Statistiche demografiche Rilevazione cancellati dall'anagrafe per decesso
Cassa depositi e prestiti	Richieste somministrazione mutuo Gestione domande mutuo
Me.Pa.	Acquisizione beni e servizi e verifica inadempienze
Ministero Economia e Finanze	Dichiarazioni Delibere Aliquote IMU e Addizionali Comunali e regolamento Rilevazione partecipate
Ministero dell'Interno	ANAGAIRE Statistiche Elettorali Certificazioni TBEL (sanzioni codice della strada, CUP e questionari)
PERLAPA	GEDAP – Gestione distacchi e permessi sindacali e funzioni pubbliche elettive fruite dai dipendenti pubblici GEPAS – Gestione dichiarazioni di scioperi Rilevazione assenze retribuite del personale Permessi ex l.104/1992 Anagrafe delle prestazioni Monitoraggio lavoro flessibile
Prefettura “Portale Dait Servizi”	Dati e statistiche elettorali Incidenti Anagrafe Amministratori Locali
Ragioneria dello Stato	Monitoraggio trimestrale del personale Conto del personale e relazione allegata Certificazioni (covid)
AREA RGS - PCC	Conciliazione Debito scaduto e non pagato ITP Certificazione dei crediti
Regionali	Comunicazione relative ai lavori, servizi e forniture pubblici a norma di legge (superiori ad € 40.000,00) – Osservatorio Regionale Bandi di gara e relativi esiti – Osservatorio Regionale Rendicontazione Fondo sostegno affitti Rilevazione spesa sociale Trasmissione rendiconto elettorale per elezioni regionali Contributo Barriere Architettoniche

	Dote Scuola – Dote Sport VAS PIANO GOVERNO DEL TERRITORIO (P.G.T.) Trasmissione delle autorizzazioni paesaggistiche – piattaforma MAPEL Caricamento delle pratiche edilizie per impianti utilizzando fonti energetiche rinnovabili – SUAP Gestione impianti sportivi Comunicazione taglio boschi – piattaforma S.I.T.A.B.
Previmpresa	Notifiche preliminari cantieri pubblici
SIATEL	Accertamenti anagrafici vari Codice Fiscale
SINTEL	Acquisizione beni, servizi e lavori pubblici
SINTESI (Provincia)	Comunicazione relative al personale (assunzioni/cessazioni)
MEF-SOSE	Rilevazione spesa sociale dei comuni Rilevazione trasporto disabili Rilevazione asili nido Questionari sulle funzioni fondamentali
SISTER	Visure Portale dei Comuni – servizi catastali Conservatoria
SIVES	Gestione veicoli sequestrati
SPORTELO UNICO PREVIDENZIALE	DURC
TESORERIA COMUNALE	Flussi stipendi Flussi mandati / reversali F24

**Guida per l'attivazione del Registro di emergenza
art. 63 del DPR 445/2000**

Documento n. 8

Per attivare il registro di protocollo di emergenza si devono verificare tre condizioni, non necessariamente dipendenti una dall'altra:

- 1) guasto al software di protocollazione informatica;
- 2) guasto al sistema informatico di gestione;
- 3) mancanza di energia elettrica.

Quando si verifica la condizione numero 1 si deve attivare un protocollo di emergenza su supporto informatico.

Quando si verificano le condizioni numeri 2 e 3 si deve attivare un protocollo di emergenza su supporto cartaceo.

Per l'attivazione del protocollo di emergenza si deve:

- a) redigere il verbale di attivazione (documento n. 8.1)
- b) compilare il registro di emergenza [su supporto informatico; manuale (documento n. 8.2)];
- c) dare comunicazione alla struttura organizzativa dell'Amministrazione della attivazione dell'emergenza;
- d) comunicare alla Soprintendenza archivistica l'attivazione del registro di emergenza.

Al termine dell'emergenza si deve:

- a) revocare l'autorizzazione al protocollo di emergenza (documento n. 8.3)
- b) inserire le registrazioni di emergenza nel protocollo informatico attivando l'apposita funzione, come previsto dal manuale operativo del sistema integrato all'applicativo
- c) dare comunicazione alla struttura organizzativa dell'Amministrazione della revoca dell'emergenza;
- d) conservare il registro di emergenza;
- e) comunicare alla Soprintendenza archivistica il ripristino delle funzionalità del registro di protocollo informatico.

La numerazione del registro di emergenza è unica per l'intero anno. Ricomincia dal numero successivo all'ultimo generato per ogni attivazione.

Nel caso di attivazione del protocollo manuale (documento n. 8.2) si possono utilizzare fogli singoli con numerazione indicata nel margine destro, in modo che più operatori possano lavorare contemporaneamente. La numerazione indicata deve essere riportata per ogni documento registrato.

**Autorizzazione allo svolgimento delle operazioni di registrazione di protocollo
sul Registro di emergenza
(art. 63 DPR 445/2000)**

Documento 8.1

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445 preso atto che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa di interruzione	

non è possibile utilizzare la normale procedura informatica, si autorizza lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza.

Il Responsabile del Servizio archivistico per la tenuta del protocollo
informatico, della gestione dei flussi documentali e degli archivi

Registro di protocollo di emergenza

Documento 8.2

Numero Registro emergenza	Data	Tipo	Mittente/Destinatario	Oggetto	Classificazione	Fascicolo

**Revoca autorizzazione allo svolgimento delle operazioni di registrazione di protocollo
sul Registro di emergenza**

Documento 8.3

Ai sensi dell'art. 63 del DPR. 28 dicembre 2000 n. 445, ricordato che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa della interruzione	

non essendo possibile utilizzare la normale procedura informatica, è stato autorizzato lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;

preso atto che, dalla data ed ora sotto riportate:

Data ripristino	
Ora ripristino	

è stato ripristinato il normale funzionamento della procedura informatica;

- si revoca l'autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;
- si dispone il tempestivo inserimento delle informazioni relative ai documenti protocollati in emergenza nel sistema informatico, con automatica attribuzione della numerazione di protocollo ordinaria, mantenendo la correlazione con la numerazione utilizzata in emergenza.

Il Responsabile del Servizio per la tenuta del protocollo informatico, della
gestione dei flussi documentali
e degli archivi

Linee guida per le pubblicazioni all'Albo on-line

Documento n. 9

Pubblicità legale di documenti all'albo on-line di cui all'articolo 32 della legge 18 giugno 2009, n. 69

Vista la legge 7 agosto 1990, n. 241 e successive modifiche e integrazioni;
Visto il decreto legislativo 18 agosto 2000, n. 267 e successive modifiche e integrazioni;
Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e successive modifiche e integrazioni;
Visto il decreto legislativo 30 giugno 2003, n. 196 e successive modifiche e integrazioni;
Visto il decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni;
Vista la legge 18 giugno 2009, n. 69, in particolare gli articoli 32 e 67, in materia di pubblicità legale on-line;
Vista la Direttiva del Ministro della funzione pubblica 26 novembre 2009, n. 8;
Visto il decreto legislativo 14 marzo 2013, n. 33 e successive modifiche e integrazioni;
Vista la Deliberazione del Garante per la protezione dei dati personali 15 maggio 2014, n. 243;
Visto il regolamento del Parlamento europeo e del Consiglio 23 luglio 2014, n. 910, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, di seguito "eIDAS";
Visto il regolamento del Parlamento europeo e del Consiglio del 27 aprile 2016, n. 679, 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 generale sulla protezione dei dati);
Visto il decreto legislativo 25 maggio 2016, n. 97.

1 Oggetto e ambito di applicazione

Queste linee guida definiscono le regole tecniche, i criteri e le informazioni per la pubblicità legale di documenti, così come previsto dagli articoli 32 e 67 della legge 18 giugno 2009, n. 69.

2 Definizioni

Si definiscono:

- a) *albo on-line*: spazio accessibile senza formalità dalla pagina iniziale del sito informatico istituzionale nel quale sono pubblicati i documenti relativi ad atti e provvedimenti che, in base all'ordinamento o per scelta delle singole amministrazioni pubbliche, sono resi potenzialmente conoscibili a chiunque;
- b) *amministrazione pubblica*: ogni amministrazione indicata nel decreto legislativo 30 marzo 2001, n. 165 e successive modifiche e integrazioni, nonché le società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della amministrazione pubblica, come individuate dall'Istituto nazionale di statistica ai sensi dell'art. 1, comma 5, della legge 30 dicembre 2004, n. 311;
- c) *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;
- d) *Codice dei beni culturali*: il *Codice dei beni culturali e del paesaggio* contenuto nel decreto legislativo 22 gennaio 2004, n. 42 e successive modifiche e integrazioni;
- e) *Codice dell'amministrazione digitale*: il *Codice dell'amministrazione digitale* contenuto nel decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni;
- f) *Codice privacy*: il *Codice in materia di protezione dei dati personali* contenuto nel decreto legislativo 30 giugno 2003, n. 196 e successive modifiche e integrazioni e Regolamento generale sulla protezione dei dati, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
- g) *dati giudiziari*: dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del decreto del Presidente della Repubblica 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato previsti dagli articoli 60 e 61 del Codice di procedura penale;
- h) *dati identificativi*: dati personali che permettono l'identificazione diretta di un soggetto;
- i) *dati personali*: qualsiasi informazione relativa a persona fisica, persona giuridica, ente o associazione, che può identificarli o renderli identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- j) *dati sensibili*: dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, sindacale, lo stato di salute e la vita sessuale;
- k) *diffusione*: far conoscere dati personali a soggetti indeterminati, in qualsiasi forma, anche mediante la loro messa a disposizione o consultazione;

- l) *diritto all'informazione*: diritto di consultare informazioni, atti e documenti delle amministrazioni pubbliche;
- m) *diritto all'oblio*: diritto di non rimanere esposti a tempo indeterminato ai danni che la pubblicazione consecutiva o reiterata di una notizia, di un atto o di un provvedimento può arrecare, salvo che, per eventi sopravvenuti, il fatto ritorni di attualità e rinasca un nuovo interesse pubblico all'informazione o alla trasparenza;
- n) *diritto di accesso*: diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi, come previsto dall'articolo 22 della legge 7 agosto 1990, n. 241 e successive modifiche e integrazioni;
- o) *diritto di accesso civico*: obbligo in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati e comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione, come previsto dall'articolo 5 del decreto legislativo 14 marzo 2013, n. 33;
- p) *diritto di accesso generalizzato*: diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione, come previsto dall'articolo 5 del decreto legislativo 14 marzo 2013, n. 33;
- q) *estratto o "con ommissis"*: documento originale pubblicato con alcune parti omesse, con l'omissione resa evidente;
- r) *firma elettronica*: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
- s) *firma elettronica qualificata*: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
- t) *contrassegno*: sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico; i programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità;
- u) *impronta*: sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione di una funzione di hash;
- v) *manuale di gestione*: manuale di gestione del sistema di gestione informatica dei documenti, dei flussi documentali e degli archivi, previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid in vigore dal 10 settembre 2020
- w) *piano di conservazione ("massimario di selezione")*: strumento che, coordinato con il titolario d'archivio e la tabella dei procedimenti amministrativi, individua i tempi di selezione periodica (scarto o conservazione) delle tipologie di documenti, di serie o di unità archivistiche nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;
- x) *principio di temporaneità*: obbligo di eliminare dall'albo on-line dati, informazioni e documenti relativi a notizie, atti o provvedimenti non più necessari allo scopo per il quale sono stati pubblicati;
- y) *pubblicità legale*: forma di registrazione, pubblicazione e diffusione, con scopi di efficacia, di esecutività, di conoscenza piena e di trasparenza di atti e provvedimenti nella forma di documenti amministrativi, in luoghi fisici o digitali resi noti;
- z) *referta ("relata")*: certificazione di avvenuta pubblicazione di un documento all'albo on-line rilasciata da un pubblico ufficiale;
- aa) *repertorio dell'albo on-line*: insieme dei dati e delle registrazioni inerenti ai documenti pubblicati all'albo on-line;
- bb) *ritiro automatico*: rimozione del documento dalla pubblicazione all'albo on-line al termine del periodo di pubblicazione
- cc) *segnatura della pubblicazione all'albo on-line*: insieme di metadati contenente il numero di repertorio, la data di registrazione, la data iniziale e la data finale di pubblicazione, l'oggetto, l'impronta del documento o dei documenti pubblicati, la denominazione dell'ente e dell'area organizzativa omogenea responsabile del documento o dei documenti pubblicati;
- dd) *sistema di gestione informatica dei documenti*: insieme di procedure e di strumenti finalizzati ad assicurare un controllo sistematico sulla registrazione, classificazione, fascicolazione, gestione, assegnazione, reperimento, tenuta, selezione e conservazione dei documenti attraverso risorse di calcolo, apparati, reti di comunicazione e procedure informatiche;
- ee) *sito informatico istituzionale*: spazio informatico destinato all'informazione istituzionale e identificato da un indirizzo internet univoco, con le caratteristiche stabilite dall'articolo 53 del Codice dell'amministrazione digitale;
- ff) *unità organizzativa responsabile*: insieme di risorse umane e strumentali incaricate della responsabilità di un affare, di un'attività o di un procedimento amministrativo, così come previsto dagli articoli 4, 5 e 6 della legge 7 agosto 1990, n. 241.

3 Istituzione dell'albo on-line

L'amministrazione pubblica istituisce un unico albo on-line, valido per tutte le proprie aree organizzative omogenee e raggiungibile dalla pagina iniziale del sito web istituzionale.

Le registrazioni dell'albo on-line e i documenti pubblicati costituiscono una serie omogenea, così come

previsto dagli artt. 64 e 67 del TUDA.

Il repertorio dell'albo on-line è gestito esclusivamente e conservato permanentemente in ambiente digitale.

La pubblicazione all'albo on-line sostituisce ogni altra forma di pubblicità legale in altri siti informatici, salvo i casi espressamente previsti dall'ordinamento o dall'autorità giudiziaria.

La pubblicazione integrale di documenti con le procedure descritte nell'articolo 32, comma 7, della legge 18 giugno 2009, n. 69 soddisfa, nei casi previsti, il requisito di efficacia; in questo caso all'albo on-line, può essere pubblicato l'atto integrale oppure un avviso di avvenuta pubblicazione.

4 Sistema informatico dell'albo on-line

La registrazione e la pubblicazione di un documento all'albo on-line avvengono attraverso il sistema informatico di gestione dei documenti nella forma di registrazione particolare, così come previsto dall'articolo 53, comma 5, del TUDA oppure attraverso altro sistema informatico integrato con il sistema informatico di gestione dei documenti.

Il sistema informatico deve:

- a) registrare i documenti sequenzialmente e senza soluzione di continuità, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore;
- b) garantire la sicurezza e l'integrità del sistema stesso, mediante l'adozione di misure idonee al ripristino del sistema in caso di disservizi o temporanea indisponibilità dei dati e dei documenti, in tempi certi compatibili con i diritti degli interessati;
- c) consentire il reperimento delle informazioni che riguardano i documenti registrati;
- d) consentire l'accesso alle informazioni del sistema da parte di soggetti interessati in condizioni di sicurezza e nel rispetto delle disposizioni in materia di protezione dei dati personali;
- e) consentire la produzione del repertorio dell'albo on-line.

Il numero di repertorio dell'albo on-line è progressivo; la numerazione è rinnovata ogni anno solare.

5 Responsabilità dei dirigenti

Con atto adottato in base a quanto disposto dal proprio ordinamento, l'Amministrazione pubblica individua le responsabilità dei dirigenti, o dei loro delegati, riguardo a:

- a) redazione dei documenti da pubblicare, con riferimento alla completezza, correttezza, pertinenza, indispensabilità dei dati personali rispetto alle finalità della pubblicazione;
- b) pubblicazione dei documenti nel rispetto delle modalità e dei tempi previsti;
- c) conservazione del repertorio dell'albo on-line e dei documenti pubblicati, con riferimento all'autenticità, all'integrità, all'intelligibilità e dei rispettivi metadati.

6 Caratteristiche e organizzazione delle pubblicazioni

L'albo on-line è realizzato in modo da rispettare i principi di accessibilità, elevata usabilità, reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità e interoperabilità, così come previsto dall'articolo 53 del Codice dell'amministrazione digitale, dall'art. 6 del D.Lgs. 33/2013.

L'Amministrazione pubblica organizza l'albo on-line in modo da garantire:

- a) l'accessibilità alle registrazioni e ai documenti pubblicati, garantendo la ricerca delle informazioni, per testo libero, per tipologia documentale e per stato di pubblicazione;
- b) l'adeguata visibilità delle informazioni relative alle sanzioni civili e penali in cui si incorre mettendo in atto azioni che compromettano l'autenticità, la veridicità e l'integrità delle registrazioni e dei documenti pubblicati, oppure che limitino o impediscano, anche temporaneamente, l'accesso al servizio o ai documenti;
- c) l'esattezza e l'aggiornamento dei dati pubblicati;
- d) l'autenticità e l'integrità dei documenti pubblicati;
- e) l'inalterabilità dei documenti pubblicati da parte di terzi, per garantire l'immodificabilità degli atti.

L'indirizzo dell'albo on-line è reso accessibile dalla pagina iniziale del sito informatico istituzionale, a sua volta accreditato all'Indice PA, in una sezione dedicata del sito informatico istituzionale oppure in sottosezioni contenenti le pubblicazioni previste da norme speciali.

La pubblicazione del documento avviene in forma integrale, per estratto oppure mediante avviso.

I documenti sono elencati e visualizzati in ordine cronologico di pubblicazione con l'indicazione dello stato: "in corso di pubblicazione", "scaduto", "annullato" o equivalenti.

Limitatamente al periodo di pubblicazione, l'acquisizione in forma digitale dei documenti pubblicati da parte dell'utenza avviene gratuitamente e senza formalità.

Gli uffici relazioni con il pubblico indicano all'utenza con speciali necessità le modalità di accesso all'albo on-line, in uno dei seguenti modi:

- a) mettendo a disposizione di chiunque postazioni attrezzate per la consultazione dell'albo on-line, presso gli stessi uffici; in questo caso sono previsti solo i rimborsi dei costi per eventuali riproduzioni cartacee;
- b) indicando operatori a disposizione (oppure altri enti) in grado di supportare gli utenti impossibilitati alla consultazione dell'albo on-line.

7 Responsabile del procedimento amministrativo e responsabile della pubblicazione

Il responsabile del procedimento amministrativo o il soggetto esterno alla area organizzativa omogenea che chiede la pubblicazione di un documento lo conferisce per la pubblicità legale al responsabile della pubblicazione già predisposto per la protezione dei dati personali.

L'Amministrazione pubblica individua tra i propri dipendenti anche il responsabile della pubblicazione, che di norma coincide con il responsabile della gestione documentale, con il compito di:

- a) assicurare la regolarità e i tempi della pubblicazione;
- b) garantire l'immodificabilità, l'integrità e la leggibilità dei documenti pubblicati.

8 Diritto all'oblio e temporaneità della pubblicazione

La pubblicazione avviene limitatamente al periodo previsto dall'ordinamento, per rispettare il principio di temporaneità e nel rispetto del "diritto all'oblio".

Decorso il termine di pubblicazione, il sistema informatico di gestione dell'albo on-line impedisce la ricerca di qualsiasi esemplare del documento pubblicato tramite accesso alle proprie banche dati; inoltre, il sistema informatico segnala la temporaneità delle informazioni pubblicate ai motori di indicizzazione e di ricerca, anche attraverso formati idonei e accorgimenti tecnici di dialogo con sistemi esterni all'ente (ad es. no index, no archive del "robot exclusion protocol").

9 Periodo di pubblicazione

Il periodo di pubblicazione è di quindici giorni interi e consecutivi, salvo termini diversi previsti da norme speciali.

Il computo dei giorni inizia dal giorno successivo alla data di pubblicazione.

Per i propri documenti e con provvedimento espresso, l'Amministrazione pubblica può stabilire periodi più brevi fino a cinque giorni o periodi più lunghi fino a sessanta giorni.

L'Amministrazione pubblica può stabilire tempi di permanenza dei documenti sul sito informatico oltre il periodo di pubblicazione, nel rispetto dei principi di necessità, indispensabilità, pertinenza e non eccedenza.

La pubblicazione si intende soddisfatta se un documento è rimasto disponibile sul sito complessivamente per almeno dodici ore per ciascun giorno di pubblicazione.

Il periodo di pubblicazione è prorogato di un giorno per ciascun giorno di pubblicazione inferiore complessivamente a dodici ore, in base a un'attestazione del responsabile della pubblicazione o di un suo delegato.

10 Individuazione dei documenti soggetti a pubblicazione

Sono pubblicati all'albo on-line i documenti previsti dall'ordinamento, da provvedimenti dell'autorità giudiziaria e quelli dai quali possono nascere diritti, doveri, aspettative o interessi legittimi di terzi e dalla cui diffusione nei confronti di una indistinta pluralità di soggetti potenzialmente interessati dipende la loro efficacia.

11 Redazione dei documenti e obbligo della firma digitale

In armonia con quanto previsto dal Ministero dell'Interno - SSDD, Circolare 21 aprile 2011, n. 13 e dal Garante per la protezione dei dati personali, Deliberazione 15 maggio 2014, n. 243, sono pubblicati all'albo on-line:

- a) documenti informatici nativi, sottoscritti con firma digitale;
- b) documenti informatici in copia per immagine con annessa dichiarazione di conformità sottoscritta con firma digitale a cura del richiedente in armonia con quanto previsto dagli articoli 22 e 23 ter del Codice dell'amministrazione digitale; in questo caso, il documento è reso disponibile anche in formato testuale, in armonia con quanto previsto dalla legge 9 gennaio 2004, n. 4
- c) documenti informatici contenenti copie o avvisi o estratti sottoscritti con firma digitale a cura del richiedente in armonia con quanto previsto dagli articoli 23 bis e 23 ter del Codice dell'amministrazione digitale.

Il responsabile della pubblicazione accerta la validità del certificato di firma digitale sui documenti pubblicati.

12 Richiesta di pubblicazione

La richiesta di pubblicazione avviene esclusivamente in modalità informatica.

Le pubblicazioni e le richieste di pubblicazione cartacee sono nulle.

Le unità organizzative responsabili, le aree organizzative omogenee o enti esterni presentano, di norma almeno il giorno lavorativo precedente, richiesta di pubblicazione esclusivamente tramite il sistema per la gestione informatica dei documenti o altro sistema integrato, allegano il documento informatico sottoscritto o dichiarato conforme all'originale nei termini di legge e come previsto dal Codice dell'amministrazione digitale e indicano:

- a) la data iniziale di pubblicazione;
- b) la data finale di pubblicazione o, eventualmente, di proroga;
- c) l'oggetto del documento;

- d) descrizione degli allegati;
 - e) per le amministrazioni pubbliche, la denominazione dell'area organizzativa omogenea, l'unità organizzativa responsabile e il nominativo del responsabile del procedimento; per conto terzi, il richiedente;
 - f) se il documento è pubblicato nella forma integrale o di estratto;
- In caso di richiesta di pubblicazione da parte di terzi, il richiedente trasmette un documento informatico sottoscritto nei formati previsti dalle regole tecniche contenute nelle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid in vigore dal 10 settembre 2020, Allegato 2.

13 Elementi obbligatori della registrazione

Gli elementi obbligatori immodificabili della registrazione sono i seguenti:

- a) numero di repertorio, assegnato automaticamente dal sistema;
- b) data di registrazione, assegnata automaticamente dal sistema;
- c) data iniziale di pubblicazione;
- d) data finale di pubblicazione o, eventualmente, di proroga;
- e) denominazione del richiedente;
- f) oggetto del documento;
- g) numero degli allegati;
- h) descrizione degli allegati;
- i) documento o documenti informatici sottoscritti con firma digitale;
- l) impronta del documento o dei documenti informatici pubblicati;;
- m) denominazione dell'area organizzativa omogenea.

La modifica anche di una sola informazione immodificabile sopra descritte determina il contestuale annullamento dell'intera registrazione.

Il numero di repertorio, la data di registrazione, la data iniziale di pubblicazione, la data finale di pubblicazione, l'oggetto, l'impronta e la denominazione dell'ente e dell'area organizzativa omogenea costituiscono la segnatura del documento pubblicato all'albo.

La segnatura è associata ai documenti in forma permanente non modificabile ed è registrata nel repertorio dell'albo on line.

14 Integrazioni alla pubblicazione

Annotazioni immodificabili inserite da operatori abilitati possono integrare o prorogare i termini di pubblicazione.

Ogni integrazione dei campi della registrazione nel sistema di gestione informatica dei documenti aggiorna senza ritardo la pubblicazione on-line.

È ammessa la formula di «errata corrige» esclusivamente per mero errore materiale o refuso.

15 Annullamento di una pubblicazione

Con adeguata motivazione, il responsabile del procedimento amministrativo può richiedere l'annullamento di una pubblicazione.

In caso di errori od omissioni nel documento pubblicato, la registrazione del documento è annullata e il computo dei giorni è interrotto; se necessario, viene contestualmente pubblicato il documento corretto, con il computo dei giorni di pubblicazione che decorre nuovamente.

La registrazione è annullata nel repertorio dell'albo on-line esplicitando lo stato di «Annullato» in maniera tale da consentire la lettura delle informazioni registrate in precedenza.

In caso di annullamento sono indicati la data di annullamento, il nome dell'operatore e gli estremi della richiesta di annullamento, aggiornando senza ritardo la pubblicazione on-line.

Nello stesso tempo, nei dati di registrazione è associata la dicitura «Annullato» in maniera visibile e immodificabile, anche in caso di acquisizione del documento da parte di terzi.

Il documento annullato rimane pubblicato fino alla scadenza dei termini precedentemente assegnati, tranne nel caso in cui l'annullamento sia motivato da una possibile violazione di legge o per disposizione dell'autorità competente.

Le informazioni relative all'annullamento sono conservate nel repertorio dell'albo.

16 Ritiro e referta di pubblicazione

L'Amministrazione pubblica stabilisce modalità tecniche e organizzative che garantiscono, attraverso i propri sistemi informatici, il ritiro automatico dei documenti dall'albo on-line una volta terminato il rispettivo periodo di pubblicazione.

Al termine del periodo di pubblicazione, il sistema informatico consente di trasmettere una referta di pubblicazione al responsabile del procedimento o all'area organizzativa omogenea richiedente; nel caso di richiedente esterno, il responsabile della pubblicazione trasmette la referta al richiedente a corredo del documento pubblicato.

La referta contiene la dichiarazione di regolare avvenuta pubblicazione, l'indicazione del periodo di pubblicazione e il numero di registrazione a repertorio.

La referta è firmata digitalmente dal responsabile della pubblicazione.

17 Pubblicazione parziale di documenti e protezione dei dati personali

Fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute, la pubblicazione di documenti che contengono dati personali, compresi quelli sensibili e giudiziari, riferiti a persone fisiche, persone giuridiche, enti o associazioni, avviene nel rispetto dei principi di necessità, correttezza, esattezza, completezza, indispensabilità, pertinenza e non eccedenza, rispetto alle finalità della pubblicazione, previsti dal Codice della privacy.

I documenti da pubblicare devono essere già predisposti per la protezione dei dati personali a cura dell'ente richiedente o del responsabile del procedimento amministrativo.

Nel caso di pubblicazione di notifica di deposito di busta chiusa e sigillata ex art. 60, lett. e) del DPR 600/1973, l'avviso di deposito pubblicato all'albo on-line è sottoscritto con firma elettronica.

18 Conservazione ed eliminazione dei documenti pubblicati

Le modalità di conservazione del repertorio dell'albo on-line sono descritte nel manuale di conservazione.

19 Formati per la pubblicazione

L'amministrazione pubblica individua i formati dei file idonei alla pubblicazione dei documenti in armonia con quanto stabilito dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid in vigore dal 10 settembre 2020, Allegato 2.

I formati devono garantire la visualizzazione dei documenti mediante software di pubblico dominio, gratuiti e rispondenti a standard internazionali in modo da essere consultati attraverso qualsiasi sistema informatico.

La pubblicazione deve avvenire nel rispetto dei requisiti tecnici di accessibilità della legge 9 gennaio 2004, n. 4.

20 Formati per la conservazione

L'Amministrazione pubblica individua i formati idonei alla conservazione affidabile a lungo termine dei documenti pubblicati in armonia con quanto previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid in vigore dal 10 settembre 2020, Allegato 2.

L'Amministrazione pubblica utilizza formati non proprietari, aperti, ampiamente adottati, bene documentati, immuni da macroistruzioni o codici invasivi, indipendenti da soluzioni software e hardware e riconosciuti dagli organismi nazionali e internazionali di standardizzazione.

L'Amministrazione pubblica garantisce la conservazione a lungo termine dei documenti digitali pubblicati nei rispettivi fascicoli, in modo da mantenere nel tempo prova della loro autenticità, integrità, immodificabilità e intelligibilità, indipendentemente da soluzioni hardware e software adottate, scegliendo formati aperti e non proprietari, in armonia con quanto stabilito dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid in vigore dal 10 settembre 2020, Allegato 2.

Modelli per la riproduzione cartacea di documenti informatici

Documento n. 10

Nel caso della produzione di **copie cartacee conformi** di documenti informatici dovrà essere obbligatoriamente riportata l'indicazione:

Riproduzione cartacea del documento informatico sottoscritto digitalmente da <dati_firma> il <data_firma> ai sensi degli articoli 3 bis, 20, 21, e 23 del Dlgs.82/2005.

La presente copia, composta di n. _____ pagine è conforme al documento originale informatico, memorizzato, conservato digitalmente e rintracciabile nel sistema informativo del Comune di Sale.

Il sottoscritto _____

Responsabile dell'Area _____

Data _____

Firma _____

Nel caso della produzione di **copie cartacee semplici** di documenti informatici dovrà essere obbligatoriamente riportata l'indicazione:

Riproduzione cartacea del documento informatico sottoscritto digitalmente da <dati_firma> il <data_firma> ai sensi degli articoli 3 bis, 20, 21, e 23 del Dlgs.82/2005, memorizzato, conservato digitalmente e rintracciabile nel sistema informativo del Comune di Sale..

F.to <dati_firma>

Firma autografa sostituita dall'indicazione del nome ai sensi dell'art. 3, c. 2, del Dlgs n.39/1993.

Aruba PEC S.p.A.

Manuale di Conservazione

Versione: 1.9

Data approvazione: 16/03/2022

Redazione: Alessandro Capobianco

Verificato da: Nicole Mazzoni, Federico Ciofi

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
1.7	19/06/2020	Par.4.1: Aggiornati Ruoli e Responsabilità
1.8	22/12/2021	Par. 1: Aggiornamento Scopo e ambito del documento Par. 2: Revisione del Glossario Par. 3 Aggiornamento della normativa di riferimento e degli Standard di riferimento Par. 4: Revisione dei Ruoli e responsabilità Par. 5: Aggiornamento delle strutture organizzative Par. 6.3: Revisione dei formati attualmente gestiti Par. 7.1: Correzioni alle modalità di acquisizione dei pacchetti di versamento per la loro presa in carico. Par. 7.7.2: Rivedizioni relative alla produzione di copie Par. 7.8.2: Aggiunta di dettagli relativamente allo scarto dei pacchetti di archiviazione Par. 7.11: Aggiunta di dettagli relativamente alla produzione degli audit log Par. 9.2.2: Correzioni al mantenimento della firma per il periodo di conservazione Par. 10.1.1: Correzioni alla nomina di Aruba quale responsabile del servizio di conservazione e del trattamento dei dati
1.9	16/03/2022	Sommario: rivista la numerazione di alcuni paragrafi Par. 4.1: modificato il responsabile della sicurezza per il servizio di conservazione Par. 12.3.1: Aggiunto il capitolo

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	16
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.....	35
6.4 Metadati da associare alle diverse tipologie di documenti.....	36
6.5 Modalità di assolvimento dell'imposta di bollo sui documenti posti in conservazione.....	36
6.6 Pacchetto di versamento	36
6.6.1 Specifiche Pacchetto di Versamento	37
6.7 Pacchetto di Archiviazione.....	37
6.7.1 Specifiche Pacchetto di Archiviazione	37
6.8 Pacchetto di Distribuzione	37
6.9 Documenti rilevanti ai fini delle disposizioni tributarie.....	38
6.9.1 Modalità di assolvimento dell'imposta di bollo sui DIRT.....	39
6.10 Trattamento dei pacchetti di archiviazione contenenti documenti rilevanti ai fini delle disposizioni tributarie	39
7 Il processo di conservazione	40
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	40
7.1.1 Ricezione dell'indice del pacchetto di versamento.....	40
7.1.2 Ricezione documenti associati ad un pacchetto di versamento.....	41
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti.....	42

7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico	44
7.3.1	<i>Specifiche rapporto di versamento</i>	44
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie	44
7.5	Preparazione e gestione del Pacchetto di Archiviazione	44
7.5.1	<i>Chiusura anticipata (in corso d'anno) del Pacchetto di Archiviazione</i>	45
7.5.2	<i>Gestione dei Pacchetti di Archiviazione non validi o non completi</i>	45
7.5.3	<i>Rettifica dei pacchetti di archiviazione</i>	45
7.6	Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione	46
7.6.1	<i>Attività conseguenti alla cessazione del contratto</i>	46
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	47
7.7.1	<i>Produzione di duplicati</i>	47
7.7.2	<i>Produzione di copie</i>	47
7.7.3	<i>Produzione copie o duplicati su supporti rimovibili</i>	47
7.7.4	<i>Intervento del Pubblico Ufficiale</i>	48
7.8	Scarto dei pacchetti di archiviazione	48
7.8.1	<i>Trasferimento dei documenti informatici in conservazione</i>	48
7.8.2	<i>Scarto dei documenti informatici conservati</i>	48
7.8.3	<i>Richiesta di scarto immediato</i>	49
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	49
7.10	Tabella riepilogativa delle fasi del processo di conservazione	49
7.11	Audit Log	51
8	Il sistema di conservazione	51
8.1	Infrastruttura informatica datacenter	51
8.2	Caratteristiche generali della soluzione di conservazione	51
8.3	Componenti Logiche	52
8.4	Componenti tecnologiche	53
8.5	Componenti fisiche	54
8.5.1	<i>Sito Primario (Produzione)</i>	54
8.5.2	<i>Sito Secondario (DR)</i>	55
8.6	Procedure di gestione e di evoluzione	56
8.6.1	<i>Change management</i>	56
8.6.2	<i>Verifica periodica di conformità a normativa e standard di riferimento</i>	57
9	Monitoraggio e controlli	58
9.1	Procedure di monitoraggio	58
9.2	Verifiche sugli archivi	58
9.2.1	<i>Pianificazione delle verifiche periodiche da effettuare</i>	59
9.2.2	<i>Mantenimento della firma per il periodo di conservazione</i>	59
9.3	Soluzioni adottate in caso di anomalie	59
10	Specifiche contrattuali	60
10.1.1	<i>Nomina di Aruba quale responsabile del servizio di conservazione e del trattamento dei dati</i>	60

10.1.2	Scheda di conservazione	60
10.1.3	Elenco Persone	60
10.2	Modello di funzionamento del servizio	60
10.2.1	Obblighi del Cliente	61
10.2.2	Obblighi di ARUBA.....	62
10.2.3	Compiti organizzativi	62
10.2.4	Compiti di manutenzione e controllo	62
10.2.5	Compiti operativi.....	63
10.2.6	Fasi del processo di conservazione e responsabilità	63
11	Livelli di servizio (SLA)	64
12	Sicurezza del sistema di conservazione	65
12.1	Privacy e requisiti di sicurezza dei dati	65
12.2	Analisi dei Rischi.....	65
12.3	Controllo Accessi.....	65
12.4	Monitoraggio Eventi e Vulnerabilità di Sicurezza	66
12.5	Cifratura	66
12.6	Backup.....	66
12.7	Isolamento delle componenti critiche	66
12.8	Sicurezza fisica datacenter del Gruppo Aruba.....	67
12.8.1	Sicurezza Fisica Data Center Primario.....	67
12.8.2	Sicurezza fisica Data Center Secondario	69
12.9	Sicurezza organizzativa comune ai due data center.....	69
12.10	Sicurezza Logica dei sistemi e degli apparati	70
12.11	Piano di Disaster Recovery e Continuità operativa	71
12.11.1	Business Impact Analysis (BIA).....	72
12.11.2	Analisi dei Rischi.....	72
12.11.3	Classificazione dei Sistemi e delle Risorse	72
12.11.4	Modalità tecniche per la Business Continuity ed il Disaster Recovery	72
13	Disposizioni finali	73
13.1	Nullità o inapplicabilità di clausole	73
13.2	Interpretazione	73
13.3	Nessuna rinuncia.....	73
13.4	Comunicazioni.....	73
13.5	Intestazioni e Appendici e Allegati del presente Manuale Operativo	73
13.6	Modifiche del Manuale di conservazione.....	74
13.7	Violazioni e altri danni materiali	74
13.8	Norme Applicabili.....	74

1 Scopo e ambito del documento

Il presente documento è il Manuale del sistema di conservazione del Conservatore 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 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.

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) l'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
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
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	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici
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.
Linee Guida	Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate da AgID
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 del sistema di conservazione	Il presente documento, per brevità indicato anche come il "Manuale"
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;
Titolare dell'oggetto della conservazione	Soggetto produttore degli oggetti di conservazione.
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;
RdV	Rapporto di Versamento
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.
- **Linee Guida** sulla formazione, gestione e conservazione dei documenti informatici.

[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 11386:2020 Standard SInCRO** - Supporto all'interoperabilità nella conservazione e 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
Titolare dell'oggetto della conservazione	Cliente
Produttore dei PdV	Cliente
Responsabile della conservazione	Cliente
Referenti del Cliente	Cliente
Conservatore	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. 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.

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.

[Torna al sommario](#)

4.1 Profili professionali all'interno della struttura organizzativa ARUBA

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 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	David	Neumarker	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.	28/02/2022	
	Tacconi	Nicola	<i>Come sopra</i>	13/05/2020	28/02/2022
	Corsi	Matteo	<i>Come sopra</i>	06/09/2017	13/05/2020
	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:

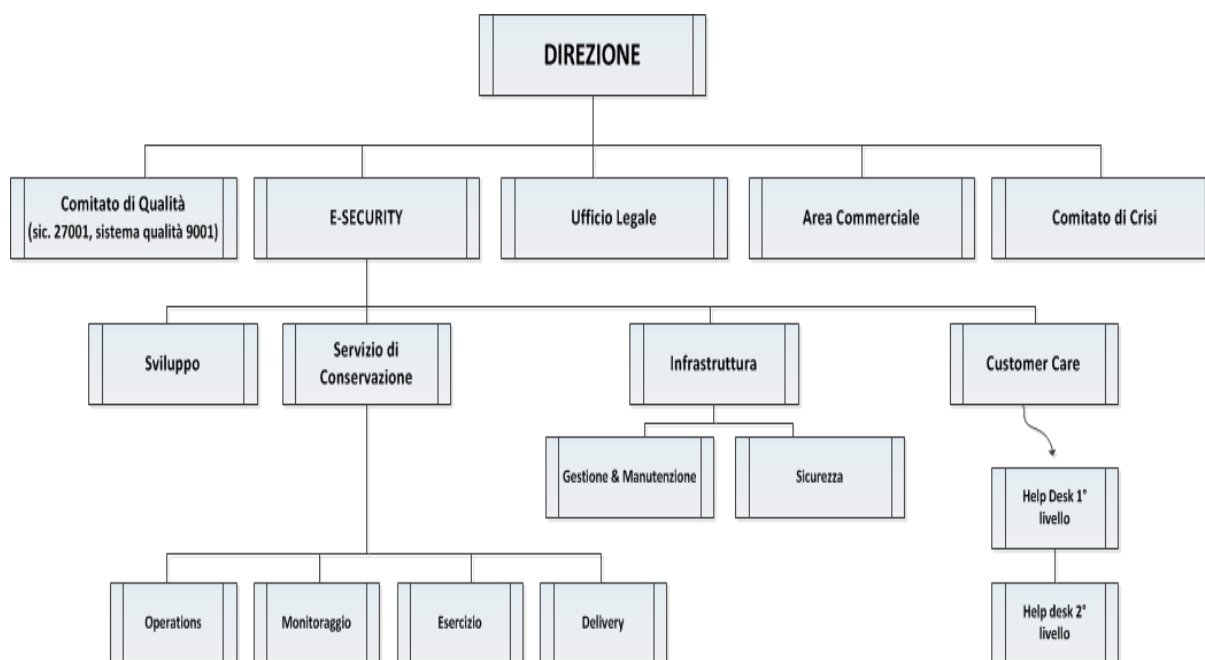


Figura 1: Rappresentazione delle strutture organizzative coinvolte nel servizio di conservazione

[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
- **Trust Service Regulatory & Design**
 - ✓ 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 di File e Riversamento" delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

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)	Offline 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>Sì</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	Sì	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	Sì																				
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>Sì</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	Sì	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	Sì																
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
---------	-------------

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

FORMATO	DESCRIZIONE	
ODT	Il formato OpenDocument Text (ODT) è una particolare implementazione del più generale formato OpenDocument	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Messaggi di testo
	Sviluppato da	Organization for the Advancement of Structured Information Standards
	Estensione	.odt
	Tipo MIME	application/vnd.oasis.opendocument.text
	Formato aperto	SI
	Specifiche tecniche	Famiglia di standard 26300 della ISO/IEC: • ISO/IEC 26300-1:2015, ODF for Office Applications v1.2 – Part 1: OpenDocument Schema • ISO/IEC 26300-3:2015, ODF for Office Applications v1.2 – Part 3: Packages • OASIS, Open Document Format for Office Applications (OpenDocument), v1.2 (2015)
	Altre caratteristiche	è un formato estendibile, de iure, binario.
Software necessario alla visualizzazione	Libre Office	

FORMATO	DESCRIZIONE	
DWG	Il formato DWG è proprietario ma ampiamente utilizzato per lo scambio di immagini vettoriali (prevalentemente bidimensionali) nel campo del disegno tecnico e dell'architettura	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Immagini vettoriali utilizzabili in ambito edile
	Sviluppato da	Autodesk
	Estensione	.dwg, .dwt
	Tipo MIME	application/acad, image/vnd.dwg
	Formato aperto	NO
	Specifiche tecniche	• Autodesk, AutoCAD .dwg file format • Open Design, Specification for .dwg, v5.4.1 (2018)
	Altre caratteristiche	è un formato libero, de facto, binario.
Software necessario alla visualizzazione	DWG TrueView	

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

XSLT	File per la descrizione del linguaggio di stile (in caso si tratti di un linguaggio diverso da XML) o del dialetto (in caso si tratti di una specializzazione di XML) — in XSL (.xsl).	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Messaggi di trasformazione XML di testo semplice.
	Sviluppato da	World Wide Web Consortium
	Estensione	.xslt
	Tipo MIME	application/xslt+xml, text/xml
	Formato aperto	SI
	Specifiche tecniche	W3C Recommendation XSL Transformations (XSLT) v2.0, 2007
	Altre caratteristiche	è un formato estendibile, de iure, testuale.
	Software necessario alla visualizzazione	Notepad++

FORMATO	DESCRIZIONE	
EXCEL 2007	File per la generazione e gestione di fogli di calcolo.	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Fogli di calcolo
	Sviluppato da	Microsoft Corporation
	Estensione	.xlsx
	Tipo MIME	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
	Formato aperto	SI
	Specifiche tecniche	- Microsoft, Excel (.xlsx) extensions to SpreadsheetML file format v16.0 (2018) - officeopenxml.com, Anatomy of a SpreadsheetML file
	Altre caratteristiche	proprietario (libero), estendibile, de facto
Software necessario alla visualizzazione	Excel viewer	

FORMATO	DESCRIZIONE	
MS-XLS	Il formato XLS è una specializzazione usata nei file di metadati all'interno di un pacchetto compresso in formato CFB (§2.3), specializzato per la rappresentazione di fogli di calcolo (estensione .xls).	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Fogli di calcolo
	Sviluppato da	Microsoft Corporation
	Estensione	.xls
	Tipo MIME	application/vnd.ms-excel
	Formato aperto	SI
	Specifiche tecniche	Microsoft, [MS-XLS]: Excel Binary file format (.xls) structure v8.0 (2018)
	Altre caratteristiche	è un formato proprietario (libero), estendibile, de facto, deprecato, binario
	Software necessario alla visualizzazione	Microsoft Office e visualizzatori open source

FORMATO	DESCRIZIONE	
PNG	Il formato PNG è particolarmente raccomandato per la rappresentazione di immagini raster che non hanno bisogno di essere accompagnate da metadati particolarmente complessi (come quelli colorimetrici, geometrico-fisico o ottici).	
	Caratteristiche e dati informativi	
	Informazioni gestibili	Immagini e fotografie
	Sviluppato da	ACME
	Estensione	.png
	Tipo MIME	image/png
	Formato aperto	SI

	Specifiche tecniche	ISO/IEC 15948:2004 • W3C Recommendation PNG Specification (2nd Ed.), 2003 • RFC-2083 • www.libpng.org
	Altre caratteristiche	è un formato aperto, <i>de iure</i> , binario, muto
	Software necessario alla visualizzazione	Image Glass

FORMATO	DESCRIZIONE
Word 2007	Documenti, prevalentemente di testo, impaginati.
	Caratteristiche e dati informativi
	Informazioni gestibili Fogli di lavoro di testo
	Sviluppato da Microsoft Corporation; ISO; ECMA
	Estensione .docx
	Tipo MIME application/vnd.openxmlformats-officedocument.wordprocessingml.document application/vnd.openxmlformats-officedocument.wordprocessingml.template
	Formato aperto SI
	Specifiche tecniche • Microsoft, Word extensions to OOXML (.docx) file format v11.1 (2018) • officeopenxml.com, Anatomy of a WordProcessingML file
	Altre caratteristiche è un formato di testo flessibile derivato da SGML (ISO 8879).
	Software necessario alla visualizzazione Word Mobile

FORMATO	DESCRIZIONE
HTML	Particolare dialetto di XML è HTML (ufficialmente codificato come XML puro a partire dalle sue versioni "XHTML" e "HTML5"), che serve a rappresentare il contenuto di pagine web.
	Caratteristiche e dati informativi
	Informazioni gestibili File di testo per gestione delle pagine html
	Sviluppato da World Wide Web Consortium
	Estensione .htm o .html
	Tipo MIME Text/html
	Formato aperto SI
	Specifiche tecniche • W3C Recommendation HTML 5.2, 2017 • validator.w3.org • W3C Recommendation XML 1.0 (5th Ed.), 2013
	Altre caratteristiche è un formato aperto, estendibile, <i>de iure</i> , testuale
	Software necessario alla visualizzazione Notepad++

FORMATO	DESCRIZIONE
JSON	Il formato JavaScript Object Notation (JSON) è un altro formato estremamente versatile ed estendibile che, come XML, è usato in moltissimi ambiti informatici e viene dunque impiegato per svariate applicazioni.
	Caratteristiche e dati informativi
	Informazioni gestibili File di testo semplici
	Sviluppato da Dominio pubblico
	Estensione .json
	Tipo MIME application/json
	Formato aperto SI

	Specifiche tecniche	• RFC-8259 • ECMA-404 • json.org • ISO/IEC 8825-8:2018, ASN.1 encoding rules, part 8: JSON
	Altre caratteristiche	è un formato di testo. aperto, estendibile, de iure
	Software necessario alla visualizzazione	Notepad++

FORMATO	DESCRIZIONE																
ZIP	Il formato consiste in un pacchetto di file, suddiviso in più cartelle, imbustato e compresso con un algoritmo ZIP e presentato come un unico file. Caratteristiche e dati informativi <table> <tr> <td>Informazioni gestibili</td><td>Archivio compresso</td></tr> <tr> <td>Sviluppato da</td><td>PKWARE</td></tr> <tr> <td>Estensione</td><td>.zip</td></tr> <tr> <td>Tipo MIME</td><td>application/zip</td></tr> <tr> <td>Formato aperto</td><td>NO</td></tr> <tr> <td>Specifiche tecniche</td><td> • ISO/IEC 21320-1:2015 • PKWARE, .ZIP File Format Specification, v6.3.5 (2018) </td></tr> <tr> <td>Altre caratteristiche</td><td>è un formato proprietario (libero), retrocompatibile, de iure, binario</td></tr> <tr> <td>Software necessario alla visualizzazione</td><td>7-zip</td></tr> </table>	Informazioni gestibili	Archivio compresso	Sviluppato da	PKWARE	Estensione	.zip	Tipo MIME	application/zip	Formato aperto	NO	Specifiche tecniche	• ISO/IEC 21320-1:2015 • PKWARE, .ZIP File Format Specification, v6.3.5 (2018)	Altre caratteristiche	è un formato proprietario (libero), retrocompatibile, de iure, binario	Software necessario alla visualizzazione	7-zip
Informazioni gestibili	Archivio compresso																
Sviluppato da	PKWARE																
Estensione	.zip																
Tipo MIME	application/zip																
Formato aperto	NO																
Specifiche tecniche	• ISO/IEC 21320-1:2015 • PKWARE, .ZIP File Format Specification, v6.3.5 (2018)																
Altre caratteristiche	è un formato proprietario (libero), retrocompatibile, de iure, binario																
Software necessario alla visualizzazione	7-zip																

FORMATO	DESCRIZIONE																
7Z	7-Zip compressed archive format Caratteristiche e dati informativi <table> <tr> <td>Informazioni gestibili</td><td>Archivio compresso</td></tr> <tr> <td>Sviluppato da</td><td>Igor Pavlov</td></tr> <tr> <td>Estensione</td><td>.7z</td></tr> <tr> <td>Tipo MIME</td><td>application/x-7z-compressed</td></tr> <tr> <td>Formato aperto</td><td>SI</td></tr> <tr> <td>Specifiche tecniche</td><td>Pavlov I., LZMA SDK (2018)</td></tr> <tr> <td>Altre caratteristiche</td><td>è un formato aperto (GNU LGPL), retrocompatibile, de facto, binario</td></tr> <tr> <td>Software necessario alla visualizzazione</td><td>7-zip</td></tr> </table>	Informazioni gestibili	Archivio compresso	Sviluppato da	Igor Pavlov	Estensione	.7z	Tipo MIME	application/x-7z-compressed	Formato aperto	SI	Specifiche tecniche	Pavlov I., LZMA SDK (2018)	Altre caratteristiche	è un formato aperto (GNU LGPL), retrocompatibile, de facto, binario	Software necessario alla visualizzazione	7-zip
Informazioni gestibili	Archivio compresso																
Sviluppato da	Igor Pavlov																
Estensione	.7z																
Tipo MIME	application/x-7z-compressed																
Formato aperto	SI																
Specifiche tecniche	Pavlov I., LZMA SDK (2018)																
Altre caratteristiche	è un formato aperto (GNU LGPL), retrocompatibile, de facto, binario																
Software necessario alla visualizzazione	7-zip																

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:
 - o metadato obbligatori
 - o 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.

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.”;

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

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

A tale fine, è necessario che, in relazione ad ogni classe documentale, il Cliente associ ad ogni DIRT i metadati previsti dal presente *Manuale* (ed, eventualmente, degli ulteriori previsti nell'apposito allegato del *Contratto*) necessari per adempiere agli obblighi imposti dalle disposizioni in materia.

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

Classificazione dei DIRT secondo aggregazioni per "Tipo documento"

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

[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.

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 slegata dall'architettura e dalla struttura del sistema di conservazione;
- ha una validità limitata nel tempo e pari al certificato emesso dalla CA;
- vede la propria sicurezza legata ad algoritmi soggetti ad obsolescenza tecnologica.

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 ogni caso il sistema di conservazione non consente l'invio dello stesso PdV per più di una volta. Una volta conclusa la fase di presa in carico del PdV e la conseguente creazione del RdV, così come descritto al cap. 7.1, non sarà possibile effettuare alcuna modifica e/o cancellazione.

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.

Il processo di scarto è composto di queste fasi:

1. l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato da Aruba PEC e trasmesso al responsabile della conservazione;
2. il responsabile della conservazione, verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale;
3. il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche

- solo su una parte dell'elenco proposto, provvede a trasmetterlo ad Aruba PEC;
4. Aruba PEC provvede alla distruzione dei pacchetti di archiviazione.

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di conservazione nel rispetto della normativa sui beni culturali.

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.

Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, il Titolare dell'oggetto di conservazione deve notificare l'esito della procedura di scarto agli organi preposti alla tutela come già indicato in precedenza. Analoga comunicazione è inviata al Ministero dell'interno in caso di eliminazione di pacchetti di archiviazione contenenti documenti e/o dati di carattere riservato.

[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 sintetica	Il sistema si mette in attesa dei documenti del PdV
FASE 6	Verifica dei documenti	
	Descrizione sintetica	In questa fase vengono condotti i controlli specifici del documento ricevuto
FASE 7	Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte	
	Descrizione sintetica	Una volta ricevuti correttamente, o con warning, tutti i documenti del PdV viene prodotto il PdV
FASE 8	Sottoscrizione del rapporto di versamento con firma digitale apposta da ARUBA	
	Descrizione sintetica	Il RdV viene firmato digitalmente dal Responsabile del servizio di Conservazione o da un suo delegato. Infine il RdV viene inviato al Cliente. 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.

Il Rapporto di Conservazione è l'attestazione di avvenuta conservazione da parte del Conservatore del/i PdV ricevuti e della loro effettiva conservazione nel sistema. Le evidenze del Rapporto di Conservazione vengono inviate via mail ordinaria.

[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:

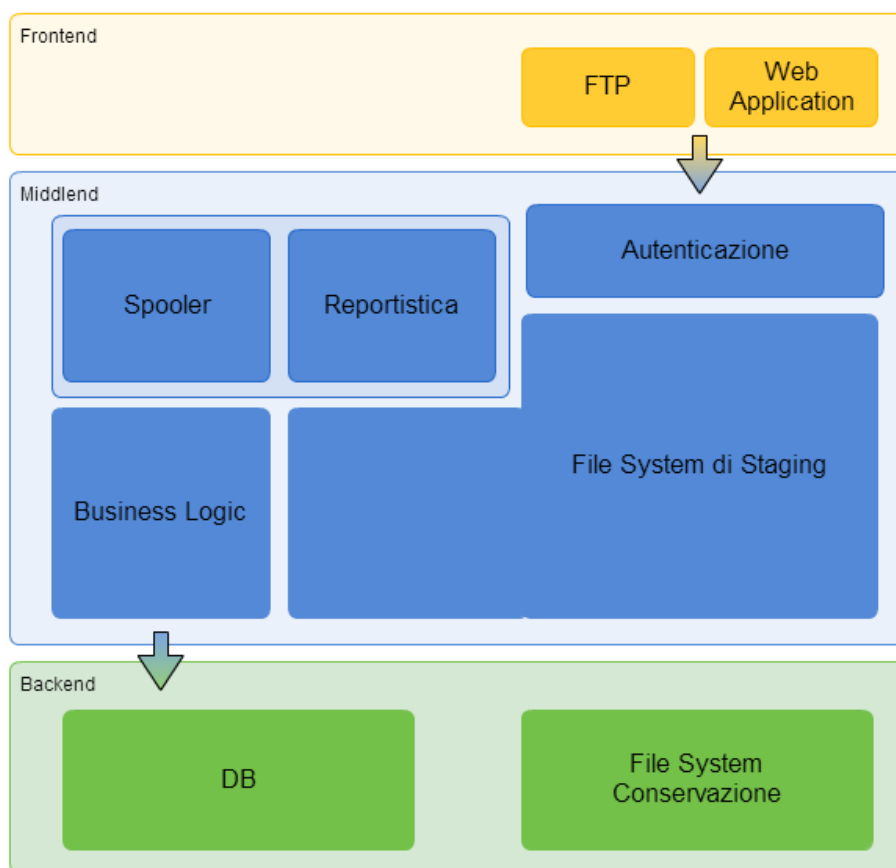


Figura 2: Rappresentazione delle componenti logiche

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 la 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.

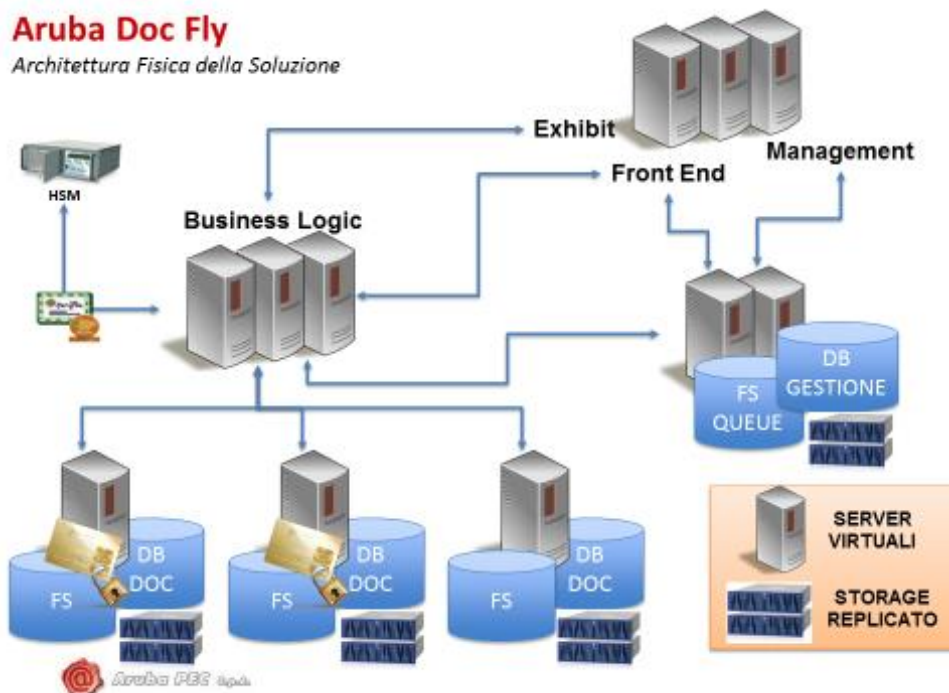


Figura 3: Rappresentazione architettura fisica della soluzione

[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.

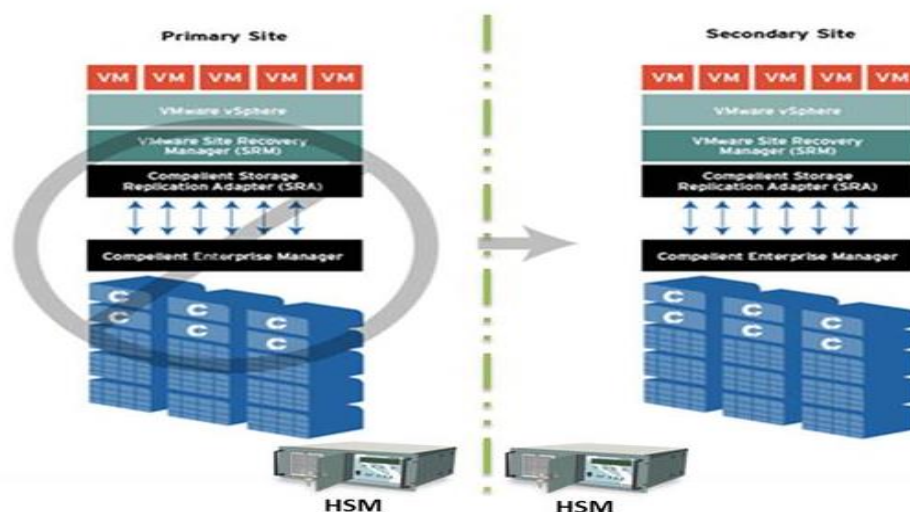


Figura 4 Schema logico della soluzione di Disaster Recovery

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 tracciatore 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 liste delle 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 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 3.9 delle Linee Guida. 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

12.3.1 Controlli sul personale non dipendente

Qualsiasi consulente indipendente o dipendente di una terza parte che partecipi al processo di conservazione è pienamente soggetto al presente Manuale, inclusi la conservazione dei documenti e la registrazione degli eventi (vedere il paragrafo 12.4).

Il personale non dipendente (es. consulenti) deve sottoscrivere un accordo di riservatezza (NDA) prima di iniziare a collaborare con Aruba PEC ed eventualmente accedere a dati confidenziali.

[Torna al sommario](#)

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

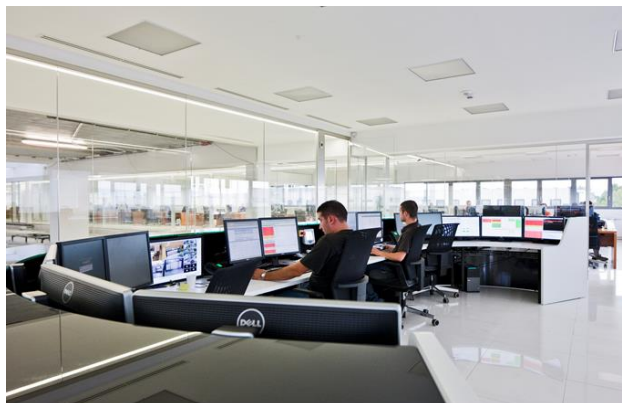


Figura 6: Immagine del Network Operations Center

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](#)

12.9 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](#)

12.10 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](#)

12.11 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](#)

12.11.1 **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](#)

12.11.2 **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](#)

12.11.3 **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](#)

12.11.4 **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. Andrea Sassetti.

[Torna al sommario](#)



UNIONE TERRE DI FIUME

tra i Comuni di
Molino dei Torti - Sale

VERBALE DI DELIBERAZIONE DELLA GIUNTA DELL'UNIONE

COPIA

DELIBERAZIONE N. 50

OGGETTO: NOMINA DEL RESPONSABILE DELLA GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE SOSTITUTIVA

L'anno **duemilaventitre** il giorno **ventinove** del mese di **Dicembre** alle ore **11:00**, nella Sala Giunta di Sale in Via Manzoni,1.

Previa l'osservanza di tutte le formalità prescritte dalla vigente legge vennero oggi convocati a seduta i componenti della Giunta dell'Unione.

All'appello risultano:

N.d'ord.	Cognome e Nome		Presente	Assente
1	ARZANI LAZZARINA	Presidente	X	
2	CAMPANELLA MARIO	Assessore	X	
3	CANOBBIO ENRICO	Assessore	X	
			Presenti: 3	Assenti: 0

Assiste e partecipa all'adunanza il **Segretario dell'Unione, MARIA MATRONE** il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti, il **Presidente, LAZZARINA ARZANI** assume la Presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

LA GIUNTA DELL'UNIONE

VISTO il D.P.R. 28 dicembre 2000, n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" che dispone:

-[...] Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse[...] (art. 50, comma 4);

-[...]in ciascuna delle grandi aree organizzative omogenee individuate ai sensi dell'articolo 50. Il servizio è posto alle dirette dipendenze della stessa area organizzativa omogenea[...] (art. 61, comma 1);

-[...]al servizio è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente[...] (art. 61, comma 2) **Ciascuna amministrazione istituisce un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi ;**

-[...]individua i compiti attribuiti al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, di seguito riepilogati (art. 61 comma 3):

a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;

b) garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni del presente testo unico;

c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53;

d) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;

e) conserva le copie di cui agli articoli 62 e 63, in luoghi sicuri differenti;

f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69;

g) autorizza le operazioni di annullamento di cui all'articolo 54;

h) vigila sull'osservanza delle disposizioni del presente testo unico da parte del personale autorizzato edegli incaricati;

Visto il D.lgs. 7/3/2005 n. 82 "Codice dell'amministrazione digitale" e, in particolare, l'art. 44 comma 1 bis in base al quale [...] il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza [...];

Visto altresì l'art. 71 del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 che all'art. 3 comma 1 lett. b) dispone che in ciascuna delle aree organizzative omogenee sia nominato il Responsabile della gestione documentale e un suo vicario, per i casi di vacanza, assenza o impedimento del primo;

Considerato che al Responsabile della gestione documentale sono demandate le attribuzioni definite da ciascuna P.A. in attuazione dell'art. 61 del D.P.R. n. 445/2000 e, in particolare, i compiti previsti in attuazione del citato D.Lgs. 82/2005;

Visti:

- il decreto del Presidente del Consiglio dei Ministri 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*»;

- il decreto del Presidente del Consiglio dei Ministri 13 novembre 2014, recante «*Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli artt. 20, 22, 23-bis, 23-ter, 40, comma 1, 41 e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*»;

Atteso che - ai sensi dell'art. 7/comma 3 del citato D.P.R. n. 3 dicembre 2013: "Nelle pubbliche amministrazioni, il ruolo del responsabile della conservazione è svolto da un dirigente o da un funzionario formalmente designato";

Considerato che il responsabile della conservazione, ai sensi dell'art. 7/comma 1 del D.P.R. n. 3 dicembre 2013, assolve in particolare ai seguenti compiti:

- a) definisce 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;*
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;*
- c) genera 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) assicura 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, 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) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;*
- 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) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;*
- m) predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.*

Considerate le Linee Guida dell'Agenzia "AGID" sulla formazione, gestione e conservazione dei documenti informatici, maggio 2021 ed in particolare:-la sezione 3.1.2, punto B, e la sezione 3.4, relativi rispettivamente alla nomina del responsabile della gestione documentale e ai compiti affidati a tale figura, e la sezione 3.1.2 relativamente alla nomina del Vicario del Responsabile;

-la sezione 4.4 e 4.5 in merito all'individuazione e al ruolo del Responsabile della conservazione;

Considerato che con deliberazione dell'Unione Terre di Fiume n. 29 del 2018 veniva approvato il manuale di gestione del protocollo, dei flussi documentali e della conservazione sostitutiva, nel quale si istituiva una sola Area Organizzativa Omogenea (AOO) ai fini del Protocollo Informatico, coincidente con l'intera Unione e, in seno ad essa ai sensi dell'art. 61 c.1 del DPR. 445/2000, si istituiva un unico Servizio per la tenuta del protocollo, per la gestione dei flussi documentali e degli archivi, riconducendolo al settore 4 - Settore Amministrativo;

Atteso che l'allora Responsabile del Servizio di Protocollo, flusso documentale e conservazione sostitutiva non è più dipendente dell'Unione dal 01/12/2019

Considerato che si rende necessario nominare un Responsabile della gestione documentale e della conservazione sostitutiva.

Visti:

- il Decreto del Presidente Unione Terre di Fiume n. 06 del 31/05/2021 di nomina della Dott.ssa Laura Ferrero a Responsabile del **“Servizio Amministrativo, Segreteria, U.R.P., Demografici, Servizi educativi e di promozione culturale e sportiva, Servizi sociali residuali”** dell'Unione “Terre di Fiume” e dei Comuni associati, con decorrenza dal 1° giugno 2021 a tutto il 31/12/2023, con istituto della *“prorogatio”*;
- il Decreto del Presidente Unione Terre di Fiume n. 14 del 22/12/2023 di nomina della Dott.ssa Laura Ferrero a Responsabile di elevata qualificazione del **“Servizio Amministrazione generale e Servizi alla Persona”** dell'Unione “Terre di Fiume” e dei Comuni associati, con decorrenza dal 1° gennaio 2024 a tutto il 31/12/2025, con istituto della *“prorogatio”*;

Ritenuto, pertanto, di individuare la dott.ssa Laura Ferrero, in qualità di Responsabile dei Servizi Amministrazione Generale e Servizi alla persona, come Responsabile della gestione documentale e della conservazione e pubblicazione dei documenti informatici;

Considerato che, in ottemperanza alle disposizioni di legge e alle linee guida Agid sulla formazione, gestione e conservazione dei documenti informatici, è necessario nominare un responsabile vicario del suddetto Responsabile della gestione documentale e della conservazione, in caso di vacanza, assenza o impedimento di questi;

Considerato altresì che in caso di temporanea assenza o impedimento del Responsabile di Servizio di E.Q. cui trattasi, la supplenza del Servizio Amministrazione Generale e Servizi alla Persona è attribuita al Responsabile del Servizio "Programmazione-Gestione Entrate Patrimoniali e Tributarie", nonché Responsabile della Transizione digitale, Dr.ssa Paola Brera;

DELIBERA

- 1) Di individuare - quale "Responsabile GESTIONE DOCUMENTALE E DELLA CONSERVAZIONE" la Dott.ssa Laura Ferrero in qualità di Responsabile dell'Area Servizi Amministrazione Generale e Servizi alla persona ;
- 2) - di nominare Responsabile vicario della Gestione Documentale e della Conservazione, la Dott.ssa Paola Brera;

ALLEGATO ALLA DELIBERA G.U. N. 50 del 29/12/2023

PARERE DI REGOLARITA' TECNICA E DI CONTROLLO PREVENTIVO
AMMINISTRATIVO DEL PARERE TECNICO SEGRETARIO.

(ai sensi e per gli effetti degli artt.li 49 e 147 bis del TUEL 267/2000 e dell'art. 4 del vigente
Regolamento comunale sulla disciplina dei Controlli interni)

FAVOREVOLE

F.to MARIA MATRONE

PARERE DI REGOLARITA' TECNICA E DI CONTROLLO PREVENTIVO
AMMINISTRATIVO DEL PARERE TECNICO.

(ai sensi e per gli effetti degli artt.li 49 e 147 bis del TUEL 267/2000 e dell'art. 4 del vigente
Regolamento comunale sulla disciplina dei Controlli interni)

FAVOREVOLE

F.to LAURA FERRERO

Letto, approvato e sottoscritto.

IL PRESIDENTE
F.to LAZZARINA ARZANI

IL SEGRETARIO DELL'UNIONE
F.to MARIA MATRONE

Copia conforme all'originale

Sale, _____

SEGRETARIO DELL'UNIONE
MARIA MATRONE

Unione Terre di Fiume

Provincia di Alessandria

Manuale di Conservazione

1 Introduzione al documento

- 1.1 *Scopo e campo di applicazione del documento*
- 1.2 *Principi del Manuale*
- 1.3 *Normativa e standard di riferimento, terminologia*

2 Modello organizzativo, ruoli e responsabilità

- 2.1 *Modello organizzativo*
- 2.2 *Ente, Titolare dell'oggetto della conservazione*
- 2.3 *Responsabile della conservazione*
- 2.4 *Conservatore*
- 2.5 *Produttore dei pacchetti di versamento*
- 2.6 *Utente*

3 Formazione e gestione dei documenti e dei fascicoli informatici

- 3.1 *Formazione e gestione dei documenti e dei fascicoli informatici da conservare*
- 3.2 *Controlli*
- 3.3 *Gestione delle anomalie*
- 3.4 *Formato dei documenti informatici*
- 3.5 *Metadati dei documenti informatici*
- 3.6 *Metadati dei fascicoli informatici*

4 Sistema di conservazione

- 4.1 *Descrizione generale del servizio di conservazione*
- 4.2 *Sistema di conservazione*
- 4.3 *Procedure di ricerca ed esibizione dei documenti conservati*
- 4.4 *Strategie adottate a garanzia della conservazione*

5 Documenti conservati

- 5.1 *Tipologie di documenti conservati*

6 Responsabilità del processo di conservazione

- 6.1 *Modello di funzionamento*

7 Misure di sicurezza

- 7.1 *Misure di sicurezza dell'Ente*
- 7.2 *Misure di sicurezza del sistema di conservazione*

8 Trattamento dei dati personali

- 8.1 *Misure per la protezione e il trattamento dei dati personali*

1 Introduzione al documento

1.1 Scopo e campo di applicazione del documento

Il presente documento è il Manuale di Conservazione come previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid, Determinazioni 407/2020 e 371/2021, in vigore dal 10 settembre 2020 (di seguito indicate come Linee Guida di Agid) e dal Codice dell'Amministrazione digitale DLgs 82/2005.

Come richiesto dalle Linee Guida di Agid, il presente documento “deve illustrare dettagliatamente l'Ente, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione”. In caso di ispezione da parte delle autorità di vigilanza preposte, il Manuale di Conservazione permette un agevole svolgimento di tutte le attività di controllo.

Il Manuale di Conservazione integra e dettaglia il Manuale di conservazione del conservatore esterno Aruba PEC, allegato al presente documento.

Si rimanda al Manuale di conservazione di Aruba PEC per indicazioni dettagliate circa:

- struttura organizzativa e ruoli di responsabilità del Conservatore
- formati e metadati associati agli oggetti conservati
- processo di conservazione e trattazione dei pacchetti di versamento, archiviazione e distribuzione
- dettaglio tecnico del sistema di conservazione
- monitoraggio e controlli effettuati dal Conservatore
- disposizioni in vigore nei luoghi dove sono conservati i documenti

Per quanto riguarda le tipologie degli oggetti sottoposti a conservazione, i rapporti con Aruba PEC che realizza il processo di Conservazione, la sicurezza delle informazioni e il trattamento dei dati, il presente Manuale è integrato con i documenti:

- specificità del contratto, allegato tecnico parte integrante e sostanziale del contratto per l'affidamento del Servizio di conservazione digitale di documenti informatici, che dettaglia le caratteristiche delle tipologie di documenti conservati
- politica aziendale della sicurezza delle informazioni
- Politica in materia di trattamento e protezione dei dati personali
- Politica della qualità

1.2 Principi del Manuale

Il Manuale di Conservazione mira a:

- fornire una chiara presentazione del sistema di conservazione e dei processi erogati
- descrivere l'insieme delle fasi del processo
- includere le informazioni rilevanti, con un livello di dettaglio sufficiente ad agevolare le ispezioni, evitando informazioni tecniche articolate e non necessarie

Il Manuale di Conservazione è adottato dall'Ente con provvedimento formale ed è pubblicato sul sito istituzionale, nella Sezione Amministrazione trasparente.

1.3 Normativa e standard di riferimento, terminologia

I principali riferimenti normativi relativi alla conservazione sono:

- Codice dell'Amministrazione digitale DLgs 82/2005
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di Agid, adottate con determinazione 407/2020 e in vigore dal 10 settembre 2020

Per ulteriori indicazioni e per quanto riguarda la terminologia (glossario e acronimi) e gli standard in uso si rimanda al Manuale di conservazione di Aruba PEC.

2 Modello organizzativo, ruoli e responsabilità

2.1 Modello organizzativo

Il modello organizzativo adottato è in outsourcing: l'Ente affida il servizio di conservazione a conservatore esterno, ai sensi dall'art. 34, c. 1-bis del Codice dell'Ente digitale DLgs 82/2005, fatte salve le competenze del Ministero della cultura, ai sensi del Codice dei beni culturali e del paesaggio DLgs 42/2004.

2.2 Ente, Titolare dell'oggetto della conservazione

L'Ente, Unione Terre di Fiume, è il Titolare dei documenti e dei fascicoli informatici posti in conservazione e, in relazione al modello organizzativo adottato, affida al Conservatore, Aruba PEC, la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia e specificato nel contratto di servizio.

Ente: Unione Terre di Fiume

Sede: Via Manzoni, 1, 15045 Sale (AL)

Sito web: <https://www.unioneterredifiume.it/it-it/home>

Codice Fiscale: 02525260069

Partita IVA: 02525260069

2.3 Responsabile della conservazione

Il Responsabile della conservazione opera secondo quanto previsto dall'art. 44, c. 1-quater, del Codice dell'Amministrazione digitale DLgs 82/2005.

Il Responsabile della conservazione:

- è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione
- è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche e archivistiche
- può essere svolto dal responsabile della gestione documentale

Il Responsabile della conservazione dell'Ente definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato.

Il Responsabile della conservazione è persona fisica inserita stabilmente nell'organico dell'Ente titolare dell'oggetto della conservazione; la normativa gli attribuisce compiti riguardanti le funzioni, gli adempimenti, le attività e le responsabilità del processo di conservazione. L'obiettivo principale del Responsabile della conservazione è definire e impostare le modalità di trattamento della documentazione soggetta a conservazione.

Le Linee guida di Agid enfatizzano il ruolo del Responsabile della conservazione che diviene fondamentale all'interno del processo di conservazione, insieme ai suoi delegati o ai terzi affidatari.

Quando il servizio di conservazione è affidato a un Conservatore, le attività in capo al Responsabile della conservazione sono demandate, tutte o in parte, al responsabile del servizio di conservazione del Conservatore, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al Responsabile della conservazione dell'Ente.

Il Responsabile della conservazione provvede a predisporre il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Le attività attribuite dalle Linee guida di Agid al Responsabile della conservazione ed eventualmente affidate al Conservatore sono:

- definire 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 e aggregazioni informatiche), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato
- gestire il processo di conservazione e garantire nel tempo la conformità alla normativa vigente
- generare e sottoscrivere il rapporto di versamento
- generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata
- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione
- effettuare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi
- 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, adottare analoghe misure con riguardo all'obsolescenza dei formati

- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico
- predisporre le misure necessarie per la sicurezza fisica e logica del sistema di conservazione
- assicurare 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
- assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Responsabile della conservazione: Laura Ferrero

Ente: Unione Terre di Fiume

Il Responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno dell'Ente, abbiano specifiche competenze ed esperienze.

2.4 Conservatore

Unione Terre di Fiume, avvalendosi di quanto previsto dal Codice dell'Amministrazione digitale D.Lgs 82/2005 e dalle Linee guida di Agid, ha affidato lo svolgimento delle attività di conservazione ad Aruba PEC che svolge tali attività tramite l'erogazione del servizio

Denominazione sociale Aruba PEC SpA

Sede legale e operativa Via S. Clemente 53, 24036 Ponte San Pietro (BG)

Sito web <https://www.pec.it>

E-mail info@arubapec.it

Telefono (centralino): +39 0575 050.350

Codice Fiscale / Partita IVA 01879020517

Numero REA 445886

Gli obiettivi di Aruba PEC tramite il servizio di conservazione sono:

- garantire conservazione, archiviazione e gestione dei documenti informatici e dei fascicoli informatici
- erogare servizi di accesso basati sui contenuti digitali conservati
- fornire supporto, formazione e consulenza al Titolare dell'oggetto di conservazione per i processi di dematerializzazione

Aruba PEC assume l'incarico di svolgere le attività affidate dal Responsabile della conservazione dell'Ente in accordo con quanto previsto dal contratto, dagli allegati tecnici contrattuali e dalle disposizioni delle Linee guida di Agid.

Aruba PEC provvede ad attribuire lo svolgimento delle attività al responsabile del servizio della conservazione e a più persone, che per competenza ed esperienza, garantiscano la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dal Manuale del sistema di conservazione. Per il dettaglio delle figure di responsabilità interne al Conservatore si rimanda al Manuale di conservazione di Aruba PEC.

Gli estremi identificativi del responsabile del servizio di conservazione di Aruba PEC (cognome, nome, codice fiscale) sono riportati anche nelle informazioni associate ai documenti conservati.

L'affidamento dello svolgimento delle attività del Responsabile della conservazione è stato conferito da Unione Terre di Fiume a Aruba PEC alla sottoscrizione del contratto di adesione al servizio di conservazione. La conservazione è svolta affidando ad Aruba PEC il ruolo e i compiti fissati nel documento di nomina a Responsabile del servizio di conservazione.

2.5 Produttore dei pacchetti di versamento

Il responsabile della gestione documentale svolge il ruolo di Produttore dei pacchetti di versamento e provvede a trasmettere i pacchetti al sistema di conservazione del Conservatore Aruba PEC.

Per pacchetto di versamento si intende: insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono collettivamente oltre che individualmente un contenuto informativo unitario e auto-consistente e che viene inviato dal Produttore al sistema di conservazione.

Unione Terre di Fiume provvede a:

- generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il Conservatore e descritti nel Manuale del sistema di conservazione di Aruba PEC
- verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa

visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

2.6 Utente

L'utente è il soggetto che può richiedere al sistema di conservazione l'accesso per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità definite nel Manuale del sistema di conservazione di Aruba PEC.

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un pacchetto di distribuzione direttamente acquisibile dai soggetti autorizzati.

Per pacchetto di distribuzione si intende: insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono collettivamente oltre che individualmente un contenuto informativo unitario e auto-consistente e che è inviato dal sistema di conservazione all'Utente in risposta a una sua richiesta di accesso a oggetti di conservazione.

Il Responsabile della conservazione è identificato come Utente del Sistema di conservazione. L'Ente può definire nel ruolo di Utente ulteriori operatori a tal fine abilitati.

L'abilitazione e l'autenticazione degli utenti avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione, e nel rispetto delle misure di sicurezza previste dal Codice in materia di protezione dei dati personali D.Lgs 196/2003 agg. 2018.

3 Formazione e gestione dei documenti e dei fascicoli informatici

3.1 Formazione e gestione dei documenti e dei fascicoli informatici da conservare

Unione Terre di Fiume forma e gestisce i documenti e i fascicoli informatici seguendo le disposizioni del Codice dell'Amministrazione digitale DLgs 82/2005 e delle Linee guida di Agid, utilizzando gli strumenti informatici a disposizione.

3.2 Controlli

Unione Terre di Fiume assicura che i documenti inviati in conservazione siano statici e non modificabili, in modo tale che il contenuto non possa essere alterabile durante le fasi di conservazione e accesso e sia quindi immutabile nel tempo.

3.3 Gestione delle anomalie

Il sistema di conservazione è configurato per accettare documenti in formati prestabiliti e con metadati definiti. Al venir meno di una di queste condizioni, sopraggiungendo l'impossibilità di accettare il documento, il sistema di conservazione lascia in attesa il documento in entrata senza immetterlo nel sistema di conservazione e contestualmente segnala l'anomalia all'Ente.

Il trattamento delle anomalie avviene mediante l'utilizzo di un'interfaccia web disponibile e accessibile alle risorse preposte al monitoraggio degli invii in conservazione.

3.4 Formato dei documenti informatici

Unione Terre di Fiume utilizza per formare i documenti destinati alla conservazione i formati idonei per la conservazione a lungo termine (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 2 Formati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 2 Formati di file e riversamento) e definiti nel Manuale di conservazione di Aruba PEC.

3.5 Metadati dei documenti informatici

Unione Terre di Fiume associa ai documenti i metadati previsti per il Documento amministrativo informatico (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati) e descritti nel Manuale di conservazione di Aruba PEC.

Eventuali ulteriori metadati aggiuntivi, sono individuati e specificati nell'allegato tecnico parte integrante e sostanziale del contratto per l'affidamento del Servizio di conservazione, che dettaglia le caratteristiche delle tipologie di documenti conservati dall'Ente.

3.6 Metadati dei fascicoli informatici

Unione Terre di Fiume associa ai fascicoli i metadati previsti per le Aggregazioni documentali informatiche (DPCM 3/12/2013 Regole tecniche per il protocollo informatico, Allegato 5 Metadati sino al 1° gennaio 2022 e successivamente Linee guida di Agid, Allegato 5 I metadati) e descritti nel Manuale di conservazione di Aruba PEC.

4 Sistema di conservazione

4.1 Descrizione generale del servizio di conservazione

Il servizio di conservazione permette di mantenere e garantire nel tempo le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità e la validità legale dei documenti informatici, nel rispetto della normativa vigente.

Il servizio è erogato in modalità SaaS (Software as a Service) tramite interfaccia web disponibile e accessibile alle risorse preposte individuate dall'Ente.

Il sistema di conservazione integra i sistemi e gli strumenti di produzione e gestione documentale in uso presso l'Ente, intervenendo solamente nella fase di conservazione per i documenti e i fascicoli che l'Ente sceglie di conservare.

Il versamento in conservazione dei documenti e dei fascicoli informatici è effettuato unicamente dagli operatori abilitati dall'Ente, utilizzando la modalità messe a disposizioni da Aruba PEC.

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.

Per la descrizione dettagliata del servizio di conservazione si rimanda al Manuale di conservazione di Aruba PEC.

4.2 Sistema di conservazione

Il sistema di conservazione 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
- architettura secondaria predisposta per consentire la doppia scrittura del dato

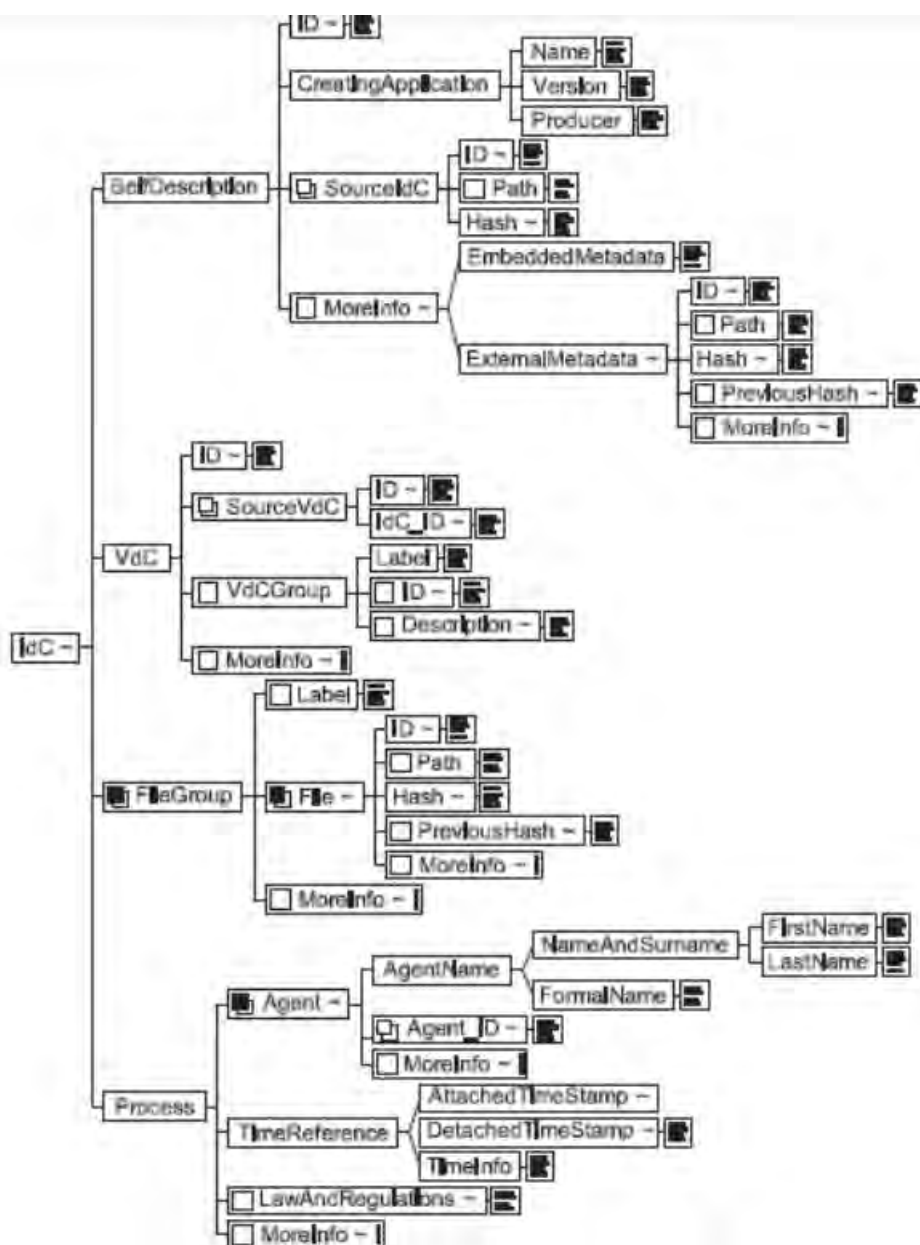
Il Sistema di Conservazione è sviluppato in modo modulare consentendo una facile scalabilità semplicemente aggiungendo unità e potenza elaborativa ai moduli sottoposti al maggior carico.

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.

Il processo di conservazione sostitutiva dei documenti verrà gestito secondo la norma UNI ISO 11386 – SInCRO (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali).

La conservazione dei dati sarà quindi gestita secondo il seguente schema XML:





Per la descrizione dettagliata delle componenti logiche, tecnologiche e fisiche e le procedure di gestione e di evoluzione si rimanda al Manuale di conservazione di Aruba PEC.

4.3 Procedure di ricerca ed esibizione dei documenti conservati

Le funzionalità messe a disposizione degli Utenti individuati dall'Ente consentono di richiedere in autonomia i pacchetti di distribuzione e di accedere ad apposite aree dell'applicazione web al fine di scaricare sulla propria postazione di lavoro i pacchetti messi a disposizione dal sistema.

Per pacchetto di distribuzione si intende: insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono collettivamente oltre che individualmente un contenuto informativo unitario e auto-consistente e che viene inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.

Per la descrizione dettagliata delle modalità di esibizione ed esportazione di pacchetti di distribuzione si rimanda al Manuale di conservazione di Aruba PEC.

4.4 Strategie adottate a garanzia della conservazione

Il conservatore Aruba PEC 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
- controllo di integrità, consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema

Per la descrizione dettagliata di procedure di monitoraggio, pianificazione delle verifiche periodiche da effettuare, mantenimento della firma per il periodo di conservazione e soluzioni adottate in caso di anomalie si rimanda al Manuale di conservazione di Aruba PEC.

5 Documenti conservati

5.1 Tipologie di documenti conservati

Unione Terre di Fiume concorda con Aruba PEC le tipologie di documenti (classi documentali) da conservare.

Sono inclusi anche i fascicoli informatici.

Le tipologie di documenti gestite dal sistema di conservazione sono dettagliatamente descritte nell'allegato tecnico parte integrante e sostanziale del contratto per l'affidamento del servizio di conservazione.

L'allegato tecnico per ciascuna tipologia di documento conservato definisce formati, metadati, sottoscrizione digitale, frequenza di versamento e software/altre informazioni per la visualizzazione dei documenti.

Unione Terre di Fiume conserva tramite il servizio di conservazione le seguenti tipologie di documenti:

Tipo di documento	Periodicità di conservazione	Formati ammessi
Registro giornaliero di repertorio	Giornaliera	Pdf/a Xml/eml Pdf
Fatture	Mensile	Pdf/a Xml/eml Pdf
Atti amministrativi	Mensile	Previsti dalla normativa
Documenti fascicolati	Mensile	Previsti dalla normativa
Registri	Annuale	Pdf/a Xml/eml Pdf

Per la descrizione e le caratteristiche delle tipologie di documenti conservati nel sistema di conservazione si rimanda al Manuale di conservazione di Aruba PEC.

6 Responsabilità del processo di conservazione

6.1 Modello di funzionamento

Il sistema di conservazione opera secondo i modelli organizzativi esplicitamente concordati dall'Ente con Aruba PEC.

La conservazione non viene svolta all'interno della struttura organizzativa dell'Ente, titolare dei documenti e dei fascicoli informatici da conservare, ma è affidata ad Aruba PEC, che svolge le attività per le quali ha ricevuto formale affidamento, nei limiti delle stesse 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 e dei fascicoli 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

Unione Terre di Fiume definisce con Aruba PEC la configurazione del servizio di conservazione in base alle specifiche esigenze, concordando le modalità di gestione e fruizione oltre alla quantità e tipologia di documenti da conservare.

Per la descrizione dettagliata del modello di funzionamento del servizio di conservazione e delle tipologie di compiti previsti si rimanda al Manuale di conservazione di Aruba PEC.

7 Misure di sicurezza

7.1 Misure di sicurezza dell'Ente

Unione Terre di Fiume provvede alle misure di sicurezza nelle fasi di trattamento, formazione e gestione dei documenti e dei fascicoli informatici definiti come da conservare.

All'interfaccia web per la gestione dei documenti inviati in conservazione (dedicata alle operazioni di verifica stato dei documenti, esibizione, ecc.) accedono solo gli utenti individuati dall'Ente e che possiedono i privilegi di accesso.

L'Ente si assicura preventivamente all'invio in conservazione che i documenti siano privi di qualsiasi agente di alterazione, pertanto i documenti da conservare non devono contenere virus, macroistruzioni corrispondenti in comandi interni che, al verificarsi di determinati eventi, possono generare automaticamente modifiche o variazione dei dati contenuti nel documento, né codici eseguibili corrispondenti in istruzioni, non sempre visibili all'operatore, che consentono all'elaboratore di modificare il contenuto del documento informatico.

Il Conservatore declina ogni responsabilità nel caso non sia rispettata la reciproca salvaguardia.

7.2 Misure di sicurezza del sistema di conservazione

Il sistema di conservazione di Aruba PEC è conforme ai requisiti di sicurezza prescritti dalla normativa.

Come previsto dalle norme vigenti in materia, Aruba PEC adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei documenti informatici
- danneggiamento delle risorse hardware su cui i documenti informatici sono registrati e dei locali ove i medesimi vengono custoditi
- accesso non autorizzato
- trattamenti non consentiti dalla legge o dai regolamenti aziendali

Le misure di sicurezza adottate assicurano:

- l'integrità dei documenti informatici, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati
- la disponibilità dei dati e dei documenti informatici da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei documenti informatici, evitando la perdita o la riduzione dei dati anche accidentale utilizzando un sistema di backup
- la riservatezza dei documenti informatici da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi

Per la descrizione delle misure di sicurezza e delle infrastrutture si rimanda al Manuale di conservazione di Aruba PEC.

8 Trattamento dei dati personali

8.1 Misure per la protezione e il trattamento dei dati personali

Nelle fasi di creazione, digitalizzazione, trattamento e invio in conservazione dei documenti informatici, l'Ente pone massima cura nel rispetto delle disposizioni previste dal Codice in materia di protezione dei dati personali DLgs 196/2003 agg. 2018.

In materia di trattamento dei dati personali Aruba PEC garantisce la tutela degli interessati in ottemperanza a quanto disposto dal Regolamento UE 2016/679, disciplinato in Italia dal DLgs 101/2018.

Ai fini dell'erogazione del servizio di conservazione digitale a norma, l'Ente nomina e affida ad Aruba PEC 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 DLgs. 196/2003 agg. 2018. Pertanto, i ruoli di Responsabile della conservazione e di Titolare del trattamento sono ricoperti dall'Ente, mentre i ruoli di Responsabile del servizio di conservazione e di Responsabile del trattamento dei dati saranno ricoperti da Aruba PEC.

Per l'illustrazione dettagliata del trattamento dei dati personali effettuato da Aruba PEC si rimanda al Manuale di conservazione di Aruba PEC e all'Informativa privacy pubblicata sul sito di Aruba PEC.



UNIONE TERRE DI FIUME

tra i Comuni di
Molino dei Torti - Sale

VERBALE DI DELIBERAZIONE DELLA GIUNTA DELL'UNIONE

COPIA

DELIBERAZIONE N. 3

OGGETTO: NOMINA DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITÀ OPERATIVA DIGITALE, AI SENSI DELL'ART. 17, COMMI 1 E 1 TER, DEL D. LGS 82/2005 (CODICE DELL'AMMINISTRAZIONE DIGITALE) – COSTITUZIONE DELL'UNITÀ DI PROGETTO.

L'anno **duemilaventuno** il giorno **due** del mese di **Febbraio** alle ore **12:00**, nella Sala Giunta di Sale in Via Manzoni,1.

Previa l'osservanza di tutte le formalità prescritte dalla vigente legge vennero oggi convocati a seduta i componenti della Giunta dell'Unione.

All'appello risultano:

N.d'ord.	Cognome e Nome		Presente	Assente
1	FANTATO ANNA	Presidente	X	
2	ARZANI LAZZARINA	Assessore	X	
3	BALDANZA ALESSANDRO	Assessore	X	
			Presenti: 3	Assenti: 0

Assiste e partecipa all'adunanza il **Segretario dell'Unione**, **MARIA MATRONE** il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti, il **Presidente**, **ANNA FANTATO** assume la Presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

LA GIUNTA DELL'UNIONE

Richiamato il decreto a firma del Presidente dell'Unione "Terre di Fiume" n. 5 in data 23.03.2020 ad oggetto: "Disposizioni organizzative per lo svolgimento delle sedute della Giunta e del Consiglio dell'Unione in videoconferenza a causa dell'emergenza Coronavirus Covid-19" in attuazione del Decreto Legge 17 marzo 2020 n. 18 c.d. "Cura Italia", laddove fra l'altro dispone che *"le sedute, in via convenzionale, si intendono effettuate sempre presso la sede istituzionale dell'Unione/Comune"*;

Premesso che L'Unione "Terre di Fiume", costituita tra i Comuni di Sale e Molino dei Torti, esercita in nome e per conto dei comuni associati tutte le funzioni fondamentali come di seguito riportate:

- a) organizzazione generale dell'amministrazione, gestione finanziaria e contabile e controllo;*
- b) organizzazione dei servizi pubblici di interesse generale di ambito comunale, ivi compresi i servizi di trasporto pubblico comunale;*
- c) catasto, ad eccezione delle funzioni mantenute allo Stato dalla normativa vigente;*
- d) la pianificazione urbanistica ed edilizia di ambito comunale nonché la partecipazione alla pianificazione territoriale di livello sovracomunale;*
- e) attività, in ambito comunale, di pianificazione di protezione civile e di coordinamento dei primi soccorsi;*
- f) edilizia scolastica ((per la parte non attribuita alla competenza delle province)), organizzazione e gestione dei servizi scolastici;*
- g) polizia municipale e polizia amministrativa locale;*
- h) i servizi in materia statistica e gli altri servizi demografici (anagrafe, stato civile, elettorale);*
- i) gestione residuale dei servizi sociali ed erogazione delle relative prestazioni ai cittadini (attività non svolte nella forma obbligatoria consortile, ai sensi della vigente normativa regionale);*
- l) funzioni e servizi attinenti la cultura, lo sport e il tempo libero.*

Considerato che:

- il decreto legislativo 179/2016, in attuazione della legge 124/2015 di riforma della pubblica amministrazione (cd. legge Madia), ha innovato in modo significativo il decreto legislativo 82/2005 (Codice dell'Amministrazione digitale);
- il nuovo CAD (ed. CAD 3.0), entrato in vigore il 14 settembre 2016, con i suoi principi generali e le collegate regole tecniche, in via di revisione, è l'asse portante e lo strumento operativo per rendere finalmente attuabile "la transizione alla modalità operativa digitale"; principio espressamente richiamato dall'art. 1, c.l. lett. n) della Legge 124/2015 e negli artt. 13 e 17, comma 1, dello stesso CAD, così come modificato dal D. Lgs. 179/2016;
- il D.Lgs. 13 dicembre 2017, n. 217, contiene le disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche;
- le importanti novità, introdotte nel testo del decreto legislativo 82/2005, sono improntate a principi di semplificazione normativa ed amministrativa così da rendere la codificazione digitale un comparto di regole e strumenti operativi capaci, da un lato, di relazionare la pubblica amministrazione ai continui mutamenti tecnologici della società, in una logica di costante work in progress e, dall'altro, di attuare la diffusione di una cultura digitale dei cittadini e delle imprese;

Vista la deliberazione di G.U. n. 30 del 12/09/2019, esecutiva ai sensi di legge, ad oggetto: "Nomina del Responsabile della transazione alla modalità digitale, ai sensi dell'art. 17, commi

1 e 1 ter, del D.Lgs. n. 82/2005 e s.m.i. (Codice dell'Amministrazione Digitale) nell'Unione "Terre di Fiume" e Comuni associati" ;

Dato atto che con il "decreto semplificazioni" – D.L. n. 76 del 16 luglio 2020, recante "Misure urgenti per la semplificazione e l'innovazione digitali", convertito con modificazioni in Legge 11 settembre 2020 n. 120, sono stati inseriti molti interventi relativi alla digitalizzazione che impattano in maniera diretta sugli enti locali;

Rilevato che:

- il processo di riforma pone in capo ad ogni amministrazione pubblica la funzione di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione, centralizzando in capo ad un ufficio unico il compito di conduzione del processo di transizione alla modalità operativa digitale ed altresì dei correlati processi di riorganizzazione, nell'ottica di perseguire il generale obiettivo di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;
- coerentemente, **il novellato articolo 17** (Strutture per l'organizzazione, l'innovazione e le tecnologie) del decreto legislativo 82/2005 e s.m.i. **disciplina puntualmente la figura del Responsabile della transizione alla modalità operativa digitale**: *"Le pubbliche amministrazioni garantiscono l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le regole tecniche di cui all'articolo 71. A tal fine, ciascuno dei già menzionati soggetti affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità."*

Al suddetto ufficio sono inoltre attribuiti i compiti relativi a:

- a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
- b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti ai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1 del decreto legislativo medesimo;
- d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4 (Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici);
- e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);

- g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
- i) promozione delle iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico e delle norme in materia di accessibilità e fruibilità.

Considerato che:

- la rilevanza dell'incarico di Responsabile della Transizione Digitale si connette necessariamente all'organizzazione dell'amministrazione, su cui esso deve poter agire in maniera trasversale, ed assume significato strategico, sia per le iniziative di attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie, sia per le responsabilità connesse;
- il responsabile della transizione alla modalità operativa digitale, ai sensi dell'articolo 17 comma 1 ter, è dotato di adeguate competenze tecnologiche, di informatica giuridica e gestionali e risponde, con riferimento ai compiti relativi alla transizione, alla modalità digitale direttamente all'organo di vertice politico;
- nell'ambito dell'assetto organizzativo dell'Unione "Terre di Fiume", il Responsabile del Servizio Programmazione e Gestione delle Entrate Patrimoniali e Tributarie, Dr.ssa Paola Brera, è la figura adatta a ricoprire tale ruolo, in relazione alla complessità delle competenze richieste, il Responsabile alla Transizione Digitale dovrà essere supportato da un adeguato Gruppo di Lavoro che possa permettere la copertura delle competenze richieste e lo svolgimento delle attività via via pianificate e risponderà funzionalmente al Responsabile della Transizione Digitale per le tematiche e i compiti relativi alla transizione alla modalità digitale;

Vista la circolare n. 3 del 1° ottobre 2018, adottata dal Ministro della Pubblica Amministrazione, che esorta le amministrazioni pubbliche a provvedere a tale adempimento centrale per il conseguimento degli obiettivi di trasformazione e passaggio al digitale, come previsto dal citato art. 17 del D.Lgs. n. 82/2005;

Visti:

- il D.Lgs. 18.08.2000, n. 267 e ss.mm.ii. e, in particolare, l'art. 48, comma 2, che attribuisce all'organo esecutivo la propria competenza a provvedere in merito;
- il D.Lgs. n. 82/2005;
- il D. Lgs. n. 179/2016 e le integrazioni del D.Lgs. n. 217/2017;

- il D.Lgs. n. 97/2016 (Decreto FOIA);
- il D.L. n. 76/2020, convertito con modificazioni in Legge n. 120/2020;

Acquisiti i pareri favorevoli in ordine alla regolarità tecnico amministrativa e in ordine alla regolarità contabile, ai sensi dell'art. 49, 1° comma, e dell'art. 147 bis del D. Lgs. 18.8.2000, n° 267 e s.m.i. e del Regolamento sui controlli interni, espressi per quanto di competenza dal Segretario dell'Unione e dal Responsabile del Servizio Gestione Bilancio Contabilità Finanziaria Economica Patrimoniale;

Con voti favorevoli e unanimi, espressi nei modi di legge,

DELIBERA

- 1. di approvare** le premesse quali parti integranti e sostanziale del presente atto;
- 2. di nominare** conseguentemente, ai sensi dell'articolo 17, comma 1 ter del rinnovato decreto legislativo 82/2005 (Codice dell'Amministrazione Digitale), il Responsabile del Servizio Gestione e Programmazione delle Entrate Patrimoniali e Tributarie, Dr.ssa Paola Brera, quale Responsabile della transizione alla modalità operativa digitale, cui sono affidati i compiti di conduzione del processo di transizione alla modalità operativa digitale e dei conseguenti processi di riorganizzazione, finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;
- 3. di precisare** che detto incarico è differenziato ed aggiuntivo rispetto a quello di Responsabile del Servizio Gestione e Programmazione delle Entrate Patrimoniali e Tributarie dell'Unione (ruolo ricoperto) e che a tale incarico non sono connessi ulteriori emolumenti retributivi;
- 4. di individuare** l'ufficio programmazione e gestione entrate patrimoniali e tributarie (ufficio scelto all'interno dell'Ente) come Ufficio Transizione al Digitale;
- 5. di costituire** l'Unità di Progetto, ai sensi dell'art. 5 quater del vigente Regolamento di Organizzazione degli Uffici e Servizi – Parte I°, per l'attuazione degli obiettivi definiti dal Codice per l'Amministrazione Digitale e dal Piano Triennale per l'Informatica nella Pubblica Amministrazione – Allegato A) al presente quale parte integrante e sostanziale;
- 6. di dare atto che** il Responsabile della Transizione alla modalità operativa digitale risponde all'organo di vertice politico con riferimento ai compiti relativi alla transizione, alla modalità digitale;
- 7. di incaricare** il Responsabile della Transizione digitale per provvedere all'inserimento dei dati sull'indice delle P.A.;
- 8. di pubblicare** il presente atto sul Sito Web - Amministrazione Trasparente e trasmettere il medesimo a tutti gli uffici dell'Unione "Terre di Fiume";
- 9. di dichiarare**, con successiva e separata votazione unanime e favorevole, espressa nei modi di legge, il presente provvedimento immediatamente eseguibile, ai sensi dell'art. 134 comma 4^a del T.U.E.L. n. 267/2000 e s.m.i., stante l'urgenza di provvedere.

ALLEGATO ALLA DELIBERA G.U. N. 3 del 02/02/2021

PARERE DI REGOLARITA' CONTABILE E DI CONTROLLO PREVENTIVO CONTABILE
DEL RESPONSABILE DEL SERVIZIO FINANZIARIO.

(ai sensi e per gli effetti degli artt.li 49 e 147 bis del TUEL 267/2000 e dell'art. 4 del vigente
Regolamento comunale sulla disciplina dei Controlli interni)

FAVOREVOLE

F.to OMBRETTA MARIA BAMBINA BUFFADOSSI

PARERE DI REGOLARITA' TECNICA E DI CONTROLLO PREVENTIVO
AMMINISTRATIVO DEL PARERE TECNICO SEGRETARIO.

(ai sensi e per gli effetti degli artt.li 49 e 147 bis del TUEL 267/2000 e dell'art. 4 del vigente
Regolamento comunale sulla disciplina dei Controlli interni)

FAVOREVOLE

F.to MARIA MATRONE

Letto, approvato e sottoscritto.

IL PRESIDENTE
F.to ANNA FANTATO

IL SEGRETARIO DELL'UNIONE
F.to MARIA MATRONE

Copia conforme all'originale

Sale, _____

IL SEGRETARIO DELL'UNIONE
MATRONE MARIA



UNIONE TERRE DI FIUME

tra i Comuni di
Molino dei Torti - Sale

VERBALE DI DELIBERAZIONE DELLA GIUNTA DELL'UNIONE

COPIA

DELIBERAZIONE N. 17

**OGGETTO: COSTITUZIONE DELL'UFFICIO VIRTUALE TRANSIZIONE AL DIGITALE
NELL'AMBITO DELL'UNIONE "TERRE DI FIUME".**

L'anno **duemilaventidue** il giorno **nove** del mese di **Maggio** alle ore **18:45**, nella Sala Giunta di Sale in Via Manzoni, 1.

Previo l'osservanza di tutte le formalità prescritte dalla vigente legge vennero oggi convocati a seduta i componenti della Giunta dell'Unione.

All'appello risultano:

N.d'ord.	Cognome e Nome		Presente	Assente
1	FANTATO ANNA	Presidente		X
2	ARZANI LAZZARINA	Vice Presidente	X	
3	CANOBBIO ENRICO	Assessore	X	
			Presenti: 2	Assenti: 1

Assiste e partecipa all'adunanza il **Segretario dell'Unione, MARIA MATRONE** il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti, il **Vice Presidente, LAZZARINA ARZANI** assume la Presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato.

LA GIUNTA DELL'UNIONE

Premesso che L'Unione "Terre di Fiume", costituita tra i Comuni di Sale e Molino dei Torti, esercita in nome e per conto dei comuni associati tutte le funzioni fondamentali come di seguito riportate:

- a) organizzazione generale dell'amministrazione, gestione finanziaria e contabile e controllo;*
- b) organizzazione dei servizi pubblici di interesse generale di ambito comunale, ivi compresi i servizi di trasporto pubblico comunale;*
- c) catasto, ad eccezione delle funzioni mantenute allo Stato dalla normativa vigente;*
- d) la pianificazione urbanistica ed edilizia di ambito comunale nonché la partecipazione alla pianificazione territoriale di livello sovracomunale;*
- e) attività, in ambito comunale, di pianificazione di protezione civile e di coordinamento dei primi soccorsi;*
- f) edilizia scolastica ((per la parte non attribuita alla competenza delle province)), organizzazione e gestione dei servizi scolastici;*
- g) polizia municipale e polizia amministrativa locale;*
- h) i servizi in materia statistica e gli altri servizi demografici (anagrafe, stato civile, elettorale);*
- i) gestione residuale dei servizi sociali ed erogazione delle relative prestazioni ai cittadini (attività non svolte nella forma obbligatoria consortile, ai sensi della vigente normativa regionale);*
- l) funzioni e servizi attinenti la cultura, lo sport e il tempo libero.*

Considerato che:

- il decreto legislativo 179/2016, in attuazione della legge 124/2015 di riforma della pubblica amministrazione (cd. legge Madia), ha innovato in modo significativo il decreto legislativo 82/2005 (Codice dell'Amministrazione digitale);
- il nuovo CAD (ed. CAD 3.0), entrato in vigore il 14 settembre 2016, con i suoi principi generali e le collegate regole tecniche, in via di revisione, è l'asse portante e lo strumento operativo per rendere finalmente attuabile "la transizione alla modalità operativa digitale"; principio espressamente richiamato dall'art. 1, c.l. lett. n) della Legge 124/2015 e negli artt. 13 e 17, comma 1, dello stesso CAD, così come modificato dal D. Lgs. 179/2016;
- il D.Lgs. 13 dicembre 2017, n. 217, contiene le disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche;
- le importanti novità, introdotte nel testo del decreto legislativo 82/2005, sono improntate a principi di semplificazione normativa ed amministrativa così da rendere la codificazione digitale un comparto di regole e strumenti operativi capaci, da un lato, di relazionare la pubblica amministrazione ai continui mutamenti tecnologici della società, in una logica di costante work in progress e, dall'altro, di attuare la diffusione di una cultura digitale dei cittadini e delle imprese;

Dato atto che con il "decreto semplificazioni" – D.L. n. 76 del 16 luglio 2020, recante "Misure urgenti per la semplificazione e l'innovazione digitali", convertito con modificazioni in Legge 11 settembre 2020 n. 120, sono stati inseriti molti interventi relativi alla digitalizzazione che impattano in maniera diretta sugli enti locali;

Rilevato che:

- il processo di riforma pone in capo ad ogni amministrazione pubblica la funzione di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione, centralizzando in capo ad un ufficio unico il compito di conduzione del processo di transizione alla modalità operativa digitale ed altresì dei correlati

processi di riorganizzazione, nell'ottica di perseguire il generale obiettivo di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;

- coerentemente, **il novellato articolo 17** (Strutture per l'organizzazione, l'innovazione e le tecnologie) del decreto legislativo 82/2005 e s.m.i. disciplina puntualmente la figura del Responsabile della transizione alla modalità operativa digitale: *"Le pubbliche amministrazioni garantiscono l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le regole tecniche di cui all'articolo 71. A tal fine, ciascuno dei già menzionati soggetti affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità."*

Al suddetto ufficio sono inoltre attribuiti i compiti relativi a:

- a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
- b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti ai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1 del decreto legislativo medesimo;
- d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4 (Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici);
- e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
- g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e partecipazione dei sistemi informativi cooperativi;
- i) promozione delle iniziative attinenti all'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- j) pianificazione e coordinamento del processo di diffusione, all'interno

dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico e delle norme in materia di accessibilità e fruibilità.

Richiamata la deliberazione G.U. n. 3 in data 02/02/2021 ad oggetto: *“Nomina del Responsabile della transazione alla modalità digitale, ai sensi dell'art. 17, commi 1 e 1 ter, del D.Lgs. n. 82/2005 e s.m.i. (Codice dell'Amministrazione Digitale) – Costituzione dell'Unità di Progetto”*, che ha confermato la Dr.ssa Paola Brera quale Responsabile alla Transizione al Digitale dell'Unione “Terre di Fiume” e dei Comuni associati” ;

Considerato che:

- nell'ambito dell'assetto organizzativo dell'Unione “Terre di Fiume”, il Responsabile del Servizio Programmazione e Gestione delle Entrate Patrimoniali e Tributarie, Dr.ssa Paola Brera, ricopre il ruolo di Responsabile alla Transizione Digitale che, in relazione alla complessità delle competenze richieste, dovrà essere supportato da un adeguato Gruppo di Lavoro che possa permettere la copertura delle competenze richieste e lo svolgimento delle attività via via pianificate e rispondere funzionalmente al Responsabile della Transizione Digitale per le tematiche e i compiti relativi alla transizione alla modalità digitale;

Ritenuto di costituire “l'Ufficio Virtuale Transizione al Digitale” nell'ambito dell'Unione “Terre di Fiume”, dando atto che il Gruppo di Lavoro è così formato:

- Dr.ssa Paola Brera – Responsabile del Servizio Programmazione e Gestione Entrate Patrimoniali e Tributarie e Responsabile alla Transizione Digitale;
- Dr.ssa Maria Matrone – Segretario Comunale/Unione;
- Dr.ssa Laura Ferrero – Responsabile del Servizio Amministrazione Generale e Servizio alla Persona;
- Simone Galiano, titolare della ditta Data Web Solution di Galiano Simone con sede in Sale – Amministratore di Sistema incaricato dell'assistenza tecnica alle reti in uso presso i Comuni dell'Unione;
- Andrea Marella di Si.Re Informatica con sede in Novi Ligure in qualità di supporto esterno al Responsabile per la Transizione al Digitale.

Visti:

il D.Lgs. 18.08.2000, n. 267 e ss.mm.ii. e, in particolare, l'art. 48, comma 2, che attribuisce all'organo esecutivo la propria competenza a provvedere in merito;

il D.Lgs. n. 82/2005 e s.m.i.;

il D. Lgs. n. 179/2016 e le integrazioni del D.Lgs. n. 217/2017;

il D.Lgs. n. 97/2016 (Decreto FOIA);

il D.L. n. 76/2020, convertito con modificazioni in Legge n. 120/2020 e s.m.i.;

Acquisiti i pareri favorevoli in ordine alla regolarità tecnico espressi dal Segretario dell'Unione e dal Responsabile del Servizio Programmazione e Gestione delle Entrate Patrimoniali e Tributarie, sensi dell'art. 49, 1° comma, e dell'art. 147 bis del D. Lgs. 18.8.2000, n° 267 e s.m.i. e

del Regolamento sui controlli interni;

Con voti favorevoli e unanimi, espressi nei modi di legge,

DELIBERA

1. di approvare le premesse quali parti integranti e sostanziale del presente atto;

2. di confermare la Dr.ssa Paola Brera quale Responsabile alla Transizione al Digitale dell'Unione “Terre di Fiume” e dei Comuni associati”, giusta deliberazione di G.U. n. 3/2021 adottata ai sensi dell'articolo 17, comma 1 ter del rinnovato decreto legislativo 82/2005 (Codice dell'Amministrazione Digitale);

3. di costituire l'Ufficio Virtuale Transizione al Digitale nell'ambito dell'Unione “Terre di Fiume”, dando atto che il Gruppo di Lavoro è così formato:

- Dr.ssa Paola Brera – Responsabile del Servizio Programmazione e Gestione Entrate Patrimoniali e Tributarie e Responsabile alla Transizione Digitale;
- Dr.ssa Maria Matrone – Segretario Comunale/Unione;
- Dr.ssa Laura Ferrero – Responsabile del Servizio Amministrazione Generale e Servizio alla Persona;
- Simone Galiano, titolare della ditta Data Web Solution di Galiano Simone con sede in Sale – Amministratore di Sistema incaricato dell'assistenza tecnica alle reti in uso presso i Comuni dell'Unione;
- Andrea Marella di Si.Re Informatica con sede in Novi Ligure in qualità di supporto esterno al Responsabile per la Transizione al Digitale.

4. di dare atto che il Responsabile della Transizione alla modalità operativa digitale risponde all'organo di vertice politico con riferimento ai compiti relativi alla transizione, alla modalità digitale;

5. di pubblicare il presente atto sul Sito Web - Amministrazione Trasparente e trasmettere il medesimo a tutti gli uffici dell'Unione “Terre di Fiume”;

6. di dichiarare, con successiva e separata votazione unanime e favorevole, espressa nei modi di legge, il presente provvedimento immediatamente eseguibile, ai sensi dell'art. 134 comma 4[^] del T.U.E.L. n. 267/2000 e s.m.i., stante l'urgenza di provvedere.

ALLEGATO ALLA DELIBERA G.U. N. 17 del 09/05/2022

PARERE DI REGOLARITA' TECNICA E DI CONTROLLO PREVENTIVO
AMMINISTRATIVO DEL PARERE TECNICO.

(ai sensi e per gli effetti degli artt.li 49 e 147 bis del TUEL 267/2000 e dell'art. 4 del vigente
Regolamento comunale sulla disciplina dei Controlli interni)

FAVOREVOLE

F.to PAOLA BRERA

PARERE DI REGOLARITA' TECNICA E DI CONTROLLO PREVENTIVO
AMMINISTRATIVO DEL PARERE TECNICO.

(ai sensi e per gli effetti degli artt.li 49 e 147 bis del TUEL 267/2000 e dell'art. 4 del vigente
Regolamento comunale sulla disciplina dei Controlli interni)

FAVOREVOLE

F.to MARIA MATRONE

Letto, approvato e sottoscritto.

IL VICE PRESIDENTE
F.to LAZZARINA ARZANI

IL SEGRETARIO DELL'UNIONE
F.to MARIA MATRONE

Copia conforme all'originale

Sale, _____

SEGRETARIO DELL'UNIONE
MARIA MATRONE

Spett.le Unione Terre di Fiume

La soluzione Golem Net s.r.l. fornisce i servizi via web, con modalità SAAS e in licenza d'uso, da parte dei soli utenti autorizzati dal Cliente, dei software applicativi indicati nel "Contratto di Assistenza e Manutenzione".

La memorizzazione dei dati inseriti o elaborati dal cliente, tramite i software applicativi di cui al punto precedente, su infrastrutture di terze parti autorizzate e certificate, presso sedi di terzi autorizzati da Golem Net, dotate di adeguati sistemi di protezione, sia per quanto riguarda la difesa contro accessi indesiderati, sia per quanto riguarda la salvaguardia dei dati del cliente (copie di salvataggio, ecc.), nei confronti di eventi imprevedibili;

Il software utilizzato non è installato localmente, ma viene messo a disposizione dei clienti tramite una connessione internet, pagando per l'utilizzo del software, non per il suo possesso. Per questo, si tratta per definizione di un servizio di cloud computing. Il servizio SaaS può esser definito come un insieme di mezzi, servizi e competenze che consente agli enti pubblici e privati di esternalizzare alcuni aspetti del loro sistema informatico e sostituirli con un costo di funzionamento piuttosto che con un investimento vero e proprio. La logica Software as a service (SaaS) è uno dei risultati pratici del paradigma service-oriented architecture (SOA). Il termine "SaaS" è diventato il termine di riferimento, rimpiazzando i precedenti termini Application service provider (ASP) e on-demand.

Servizi Saas Golem Net s.r.l.

I servizi Saas Golem Net s.r.l. sono conformi con quanto richiesto da ACN secondo quanto disposto nel Decreto direttoriale prot. N. 29 del 02/01/2023, come modificato dal Decreto prot. N. 20610 in data 28/07/2023.

Sul portale ACN sono riportate le schede tecniche di ogni servizio che mettono in evidenza il tipo di servizio e il relativo livello di qualifica visibili al seguente link: <https://catalogocloud.acn.gov.it/service/531> e <https://catalogocloud.acn.gov.it/service/1797>

Elenco degli standard tecnici utilizzati per la progettazione e gestione del servizio Cloud

- ITU-T Y.3502;
- ISO/IEC 17788:2014;
- ISO/IEC 17789:2014;
- Nist 800-145;
- ISO/IEC 27001;
- ISO/IEC 27017;
- ISO/IEC 27018;
- ISO/IEC 9001;
- ISO/IEC 27035;
- ISO/IEC 20000-1;
- ISO/IEC 22313

Elenco delle certificazioni ottenute relative all'organizzazione

- ISO 9001:2015
- ISO 27001:2013
- ISO/IEC 27017:2015

- ISO/IEC 27018:2019

Elenco delle certificazioni ottenute per il servizio cloud

- ANSI/TIA 942-A-2014 AS BUILT VALIDATION LEVEL IV (Solo DC IT1 e IT3);
- ISO 9001:2015 - Sistema di gestione per la qualità;
- ISO 27001:2013 - Sistema di gestione della sicurezza delle informazioni;
- ISO 27035-1/-2:2016 - Gestione degli incidenti di sicurezza delle informazioni;
- ISO 27017:2015 - Tecniche di sicurezza - controlli di sicurezza delle informazioni per i servizi cloud;
- ISO 27018:2014 - Tecniche di sicurezza - protezione dei dati personali per i CSP;
- ISO 14001:2015 - Sistema di gestione ambientale (Solo IT3);
- ISO 50001:2011 - Sistema di gestione dell'energia

Adozione modello organizzativo e gestione ai sensi del D.Lgs. 231/2001

La società **GOLEM NET S.r.l.**, in coerenza con i principi etici, di governance e le finalità dell'azienda ha adottato un Modello di Organizzazione, Gestione e Controllo e il Codice Etico.

Contestualmente all'adozione del "Modello di Organizzazione, Gestione e Controllo" e del "Codice Etico, la Società ha nominato un Organismo di Vigilanza (OdV) in forma monocratica.

Gestione della sicurezza

La società **GOLEM NET S.r.l.** adotta tutte le procedure aziendali consolidate ottimizzando il sistema (policy, procedure, regole) della sicurezza delle informazioni secondo ISO 27001

Supporto Tecnico

La **GOLEM NET S.r.l.** offre

- un servizio di assistenza tramite canale telefonico e mail;
- utilizza un sistema di ticketing online interno per la gestione RA, richieste di modifica, non conformità, livelli di servizio
- Offre un servizio di assistenza remota e on site