



Comune di Ollastra

Provincia di Oristano

Manuale di conservazione Documentale

Autore: Nazzarena Carrau

Redazione: giugno 2026



Indice

Sistema di Conservazione Digitale dei Documenti Informatici.....	4
I: INTRODUZIONE	4
Art. 1: Scopo del documento	4
Art. 2: Normativa di riferimento	4
Art. 3: Definizioni	6
II: ATTIVAZIONE DEL SERVIZIO E PROCESSI OPERATIVI	9
Art. 4: Affidamento del servizio	9
Art. 5: Accesso al servizio	9
Art. 6: Generalità processi operativi	9
III: SOGGETTI RUOLI E RESPONSABILITA'	10
Art. 7: Titolare dell'oggetto della Conservazione	10
Art. 9: Produttori dei PdV	10
Art. 10: Utente abilitato	11
Art. 11: Responsabile della conservazione	11
Art. 12: Delegato per l'attività di conservazione	13
Art. 13: Obblighi e responsabilità del delegato alla conservazione	13
IV: TIPOLOGIA DEL SERVIZIO (Processo di Conservazione)	14
Art. 14: Il sistema di conservazione	14
V: PROCESSO DI CONSERVAZIONE	15
Art. 17: Descrizione generale del Sistema di Conservazione	15
VI: INFRASTRUTTURA ARUBA.....	18
VII: TIPOLOGIE DEGLI OGGETTI DIGITALI SOTTOPOSTI A CONSERVAZIONE.....	19
Art. 22: Oggetti conservati	19
Art. 23: Metadati da associare	21
Art. 24: Tipologie documentali	22
VIII: MODALITA' DI ESIBIZIONE	22
Art. 25: Esibizione	22
IX: MISURE DI SICUREZZA DEL SISTEMA	23
Art. 26: Misure di sicurezza a tutela dei dati personali	23
X: SELEZIONE E SCARTO	24
Art. 27: LG per la selezione e scarto dei documenti informatici	24



Art. 28: Modalità adottata per la selezione e lo scarto	25
XI: DISPOSIZIONI FINALI	25
Art. 29: Pubblicità del presente manuale ed entrata in vigore	25
XII: Allegati	26
Art. 30: Allegati.....	26



Sistema di Conservazione Digitale dei Documenti Informatici

I: INTRODUZIONE

Art. 1: Scopo del documento

1. Il Comune di Ollastra ha scelto, per la conservazione dei documenti informatici prodotti, un modello in *outsourcing*, esternalizzando il servizio di conservazione alla società Aruba.
2. Il presente Manuale di Conservazione è adottato ai sensi delle nuove linee guida AGID del maggio 2021 concernente le “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici” di cui al decreto legislativo n. 82 del 2005, all’art. 71 e successive modificazioni e norme collegate entrate in vigore dal 01/01/2022 come indicato nella Determina 455 del 25 giugno 2021 adottata da AgID. Esso definisce, in particolare:
 - a. Il sistema di conservazione;
 - b. I pacchetti informativi;
 - c. Il modello organizzativo della conservazione;
 - d. i soggetti coinvolti nel processo di conservazione;
 - e. ruoli e responsabilità;
 - f. il processo di conservazione;
 - g. l’infrastruttura di conservazione a norma;
 - h. le modalità per ottenere l’esibizione di un documento conservato;
 - i. le misure di sicurezza adottate;
 - j. la selezione e lo scarto dei documenti informatici.

Art. 2: Normativa di riferimento

La normativa di riferimento del presente regolamento è la seguente:

- a. linee guida agid sulla formazione gestione e conservazione dei documenti informatici;
- b. Piano Triennale 2024-2026 per l’informatica nella Pubblica Amministrazione;
- c. [DPR 854/1975](#), Attribuzioni del Ministero dell’Interno in materia di documenti archivistici non ammessi alla libera consultabilità;
- d. [Legge 241/1990](#), Nuove norme sul procedimento amministrativo;



- e. [DPR 445/2000](#), Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- f. [DPR 37/2001](#), Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato;
- g. [D.lgs. 196/2003](#) recante il Codice in materia di protezione dei dati personali;
- h. [D.lgs. 42/2004](#), Codice dei beni culturali e del paesaggio, ai sensi dell'[articolo 10 della legge 6 luglio 2002, n. 137](#);
- i. [Legge 9 gennaio 2004, n. 4](#) aggiornata dal [decreto legislativo 10 agosto 2018, n. 106](#), disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici;
- j. [D.lgs. 82/2005](#) e s.m.i., Codice dell'amministrazione digitale;
- k. [D.lgs. 33/2013](#), Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- l. [DPCM 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;
- m. [DPCM 21 marzo 2013](#), Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente Linee Guida sulla formazione, gestione e conservazione dei documenti informatici 9 – 41 ed allegata al documento informatico, ai sensi dell' [22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82](#) e successive modificazioni;
- n. [UE 910/2014](#), in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;
- o. Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al [DPCM 13.11.2014](#) e conservati secondo le regole tecniche di cui al [DPCM 13.12.2013](#);



- p. UE 679/2016 (GDPR), 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;
- q. Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- r. Circolare n. 2 del 9 aprile 2018, recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
- s. Circolare n. 3 del 9 aprile 2018, recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
- t. UE 2018/1807, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea;
- u. [DPCM 19 giugno 2019, n. 76](#), Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.

Art. 3: Definizioni

1. **Archiviazione elettronica:** processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, così come individuati nella normativa vigente, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione.
2. **Blocco di conservazione:** raggruppamento di pacchetti informativi presi in carico per la conservazione dal sistema di conservazione.
3. **Conservazione:** processo che assicura, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, di documenti informatici, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità nel tempo.
4. **Delegato per l'attività di conservazione:** la persona fisica o giuridica tenuta a svolgere le attività di conservazione dei documenti in forza di apposita delega conferita dal responsabile della conservazione.
5. **Documento:** rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica
6. **Documento informatico:** documento elettronico che contiene la rappresentazione di atti, fatti o dati giuridicamente rilevanti ([Lgs. n. 82/05](#) e s.m.i. e norme collegate).
7. **Documento statico non modificabile:** documento informatico redatto adottando modalità che ne garantiscono l'integrità e l'immodificabilità durante le fasi di accesso e di



conservazione; a tal fine il documento informatico non deve contenere macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

8. **Esibizione:** operazione che consente di visualizzare un documento conservato o di ottenerne copia.
9. **Evidenza informatica:** una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
10. **Firma elettronica:** l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
11. **Firma elettronica qualificata:** la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.
12. **Firma digitale:** un particolare tipo di firma elettronica qualificata basata 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.
13. **Funzione di hash crittografica:** una funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest 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.
14. **Impronta crittografica:** la sequenza di simboli binari (bit) di lunghezza predefinita risultato dell'applicazione di una funzione di Hash crittografica ad una evidenza informatica.
15. **Marca temporale:** un'evidenza informatica che consente la validazione temporale.
16. **Pacchetto di archiviazione:** pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le modalità riportate nel manuale di conservazione del sistema di conservazione.
17. **Pacchetto di distribuzione:** pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
18. **Pacchetto di versamento:** pacchetto informativo inviato dall'utente al sistema di conservazione secondo un formato predefinito e concordato, descritto nel manuale di conservazione del sistema di conservazione.



19. **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.
20. **Responsabile della conservazione:** il soggetto che svolge le attività di conservazione avvalendosi del servizio offerto dal delegato per l'attività di conservazione, in conformità a quanto disposto dal presente manuale operativo e dalle disposizioni normative vigenti in materia.
21. **Riferimento temporale:** informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
22. **Riversamento diretto:** processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica. Per tale processo non sono previste particolari modalità.
23. **Riversamento sostitutivo:** processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica.
24. **Sistema di memorizzazione:** sistema tecnologico per la tenuta a lungo termine dei documenti conservati in modo non modificabile, in base agli ultimi standard tecnologici.
25. **Sistema di conservazione a norma:** l'unione dei sistemi di conservazione di cui sono responsabili i delegati su un'infrastruttura tecnologica qualificata.
26. **Utente abilitato:** il responsabile della conservazione o i soggetti espressamente abilitati dal medesimo ad accedere al sistema di conservazione o a fruire dei suoi servizi.
27. **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.
28. **Duplicato informatico:** il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;
29. **Copia informatica di documento analogico:** il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;
30. **Copia per immagine su supporto informatica di documento analogico:** il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;
31. **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



II: ATTIVAZIONE DEL SERVIZIO E PROCESSI OPERATIVI

Art. 4: Affidamento del servizio

1. Il responsabile della conservazione del Comune di Ollastra, verificata l'impossibilità di conservare in "casa" i documenti prodotti, affida il processo di conservazione ad Aruba attraverso la sottoscrizione del contratto o convenzione di servizio e atto di delega totale del processo stesso. Aruba è stata individuata tra l'elenco dei prestatori di servizi fiduciari qualificati e garantisce degli automatismi con i gestionali in uso (Siscom).

Art. 5: Accesso al servizio

L'accesso al servizio di conservazione avviene mediante un canale sicuro attivato dagli applicativi di gestione documentale Siscom oppure tramite SSH File Transfert Protocol e tramite canale Web service descritti dettagliatamente nel capitolo "Oggetti sottoposti in conservazione" paragrafo 6.3 del Manuale utente di Aruba, vedasi Allegato "Manuale di conservazione - Aruba"

Art. 6: Generalità processi operativi

1. Il processo di conservazione, nel dettaglio, secondo quanto previsto dalle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici", prevede:
 - a. l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;
 - b. la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione;
 - c. il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie;
 - d. la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti 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;
 - e. l'eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal responsabile della conservazione, ove prevista nel manuale di conservazione;
 - f. la preparazione, la sottoscrizione con firma digitale del responsabile della conservazione e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati e secondo le modalità riportate nel manuale della conservazione;
 - g. la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata, ove prevista nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;



- h. la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle Linee guida sulla formazione, gestione e conservazione dei documenti informatici.
- i. lo scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione, dandone informativa al produttore, previa autorizzazione della Soprintendenza Archivistica competente sul territorio.

III: SOGGETTI RUOLI E RESPONSABILITA'

Art. 7: Titolare dell'oggetto della Conservazione

- 1. Il titolare dell'oggetto di conservazione, soggetto produttore degli oggetti di conservazione è il comune di Ollastra.
- 2. Il titolare dell'oggetto della conservazione per definizione è la persona, fisica o giuridica, che ha la responsabilità di conservare per legge un documento.

Art. 8: Obblighi del Titolare nei confronti del conservatore

- 1. Il Comune di Ollastra ha l'obbligo di:
 - a. inviare esclusivamente documenti leggibili e conformi a quanto previsto dal presente manuale;
 - b. controllare che i certificati di firma digitale dei documenti non aventi un riferimento temporale certo (marca temporale o segnatura di protocollo o registrazione particolare) contenuti nel pacchetto di versamento siano validi almeno fino alla generazione del pacchetto di archiviazione, ovvero fino alla avvenuta memorizzazione e conservazione a norma;
 - c. archiviare il pacchetto di versamento inviato, se è disponibile la funzionalità nel sistema;
 - d. controllare che il pacchetto informativo indicato nella ricevuta di conservazione corrisponda a quello del pacchetto di archiviazione;
 - e. accettare o annullare il processo di conservazione (prenotazione automatizzata o manuale) avviato entro e non oltre il giorno stesso; in assenza di alcuna comunicazione entro l'indicato termine, il processo sarà considerato validamente concluso salvo cause di forza maggiore (interruzione del sistema di comunicazione, blackout, etc.);
- 2. In caso di esito negativo la procedura deve comunque essere ripetuta.

Art. 9: Produttori dei PdV

- 1. Nelle Pubbliche Amministrazioni, il ruolo di produttore del PdV è svolto da persona interna alla struttura organizzativa
- 2. Nelle PA il responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, svolge il ruolo di produttore di PdV e assicura la trasmissione del



pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione, vedasi definizione paragrafo 4.4 delle LG AgID sulla formazione, gestione e conservazione dei documenti informatici.

3. Nel comune di Ollastra il ruolo di produttore PDV è svolto dal responsabile di gestione documentale (vedasi allegato “Elenco delle figure Nominate”)
4. Il produttore PDV, responsabile del contenuto del pacchetto di versamento, provvede a generare e trasmettere al sistema di conservazione esterno i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore e descritti nel manuale di conservazione del sistema di conservazione. Provvede inoltre a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto da Aruba.

Art. 10: Utente abilitato

1. L'utente abilitato può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale di conservazione. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste dal presente manuale.

Art. 11: Responsabile della conservazione

1. Il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD, nello specifico il responsabile della conservazione opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, se presenti, e può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali.
2. Il responsabile della conservazione opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis.
3. Il Responsabile della conservazione viene nominato con atto formale dell'amministrazione, e a tal proposito vedasi l'allegato 1 “Elenco delle figure Nominate”.
4. Il responsabile della conservazione può essere svolto dal responsabile della gestione documentale ovvero dal coordinatore della gestione documentale.
5. Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
6. 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 della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.



7. In particolare, il responsabile della conservazione:

a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;

d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;

e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;

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 le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali;

m) predispone il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Avendo esternalizzato il servizio di conservazione, le attività suddette (dalla lettera: "a" alla "l" ad esclusione della lettera "m"), sono state affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della



conservazione del comune di Ollastra, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing dalle PA.

Art. 12: Delegato per l'attività di conservazione

1. Il delegato per l'attività di conservazione è, l'eventuale soggetto nominato dal responsabile della conservazione a cui viene affidata in modo totale o parziale la conservazione dei documenti.
2. Il delegato deve offrire idonee garanzie organizzative e tecnologiche per lo svolgimento delle funzioni.

Art. 13: Obblighi e responsabilità del delegato alla conservazione

1. Il delegato per l'attività di conservazione ha l'obbligo di:
 - a. predisporre un sistema atto alla conservazione dei documenti informatici per conto del Comune di Ollastra nel rispetto della normativa vigente;
 - b. archivia e rende disponibili, relativamente ad ogni pacchetto di archiviazione, le informazioni minime previste dalla normativa vigente;
 - c. fornisce un rapporto di versamento a fronte di ogni pacchetto di versamento generato dagli utenti produttori del pacchetto attraverso le soluzioni di gestione documentale adottate per gli specifici tipi di documenti;
 - d. mantiene e rende accessibile un archivio del software dei programmi di gestione e un archivio degli standard dei formati ammessi;
 - e. verifica la corretta funzionalità del sistema e dei programmi in gestione, delle logiche di tracciatura e documentazione del sistema stesso;
 - f. adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione e delle copie di sicurezza dei supporti di memorizzazione;
 - g. documenta le procedure di sicurezza rispettate per l'apposizione della marca temporale;
 - h. rende disponibili al Comune di Ollastra i documenti conservati nel caso di scadenza e/o risoluzione e/o cessazione del contratto di gestione secondo le clausole indicate nella convenzione/contratto sottoscritto tra le parti;
2. Il delegato per l'attività di conservazione verifica che il formato dei documenti trasmessi sia tra quelli ammessi rifiutando la conservazione di documenti in formati diversi da quelli fissati dal presente manuale operativo.



IV: TIPOLOGIA DEL SERVIZIO (Processo di Conservazione)

Art. 14: Il sistema di conservazione

1. il sistema di gestione informatica dei documenti (gestionali Siscom) trasferisce al sistema di conservazione, ai sensi dell'art. 44, comma 1-bis, del CAD
2. Il sistema di conservazione assicura, dalla presa in carico del produttore fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, degli oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, immutabilità e reperibilità dei seguenti:
 - a. documenti informatici e documenti amministrativi informatici con i metadati ad essi associati;
 - b. fascicoli informatici ovvero aggregazioni documentali informatiche con i metadati ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all' aggregazione documentale;
 - c. documenti analogici originali unici dei quali si intende adottare la conservazione sostitutiva informatica.
3. Le componenti funzionali del sistema di conservazione assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.
4. Il sistema di conservazione Aruba Docfly garantisce l'accesso all'oggetto conservato indipendentemente dall'evolversi del contesto tecnologico, a tempo indeterminato o fino al momento dell'eventuale scarto o cessazione del contratto, per maggiori dettagli vedasi allegato "Manuale di conservazione - Aruba".

Art. 15: Pacchetti Informativi

1. Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:
 - a) pacchetti di versamento;
 - b) pacchetti di archiviazione;
 - c) pacchetti di distribuzione.
2. L'interoperabilità tra i sistemi di conservazione dei soggetti che svolgono attività di conservazione è garantita dall'applicazione delle specifiche tecniche del pacchetto di archiviazione definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
3. Il Titolare dell'oggetto della conservazione utilizza, già al momento della formazione, le modalità e i formati individuati nel manuale di gestione e nel manuale di conservazione in



conformità con le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

4. Per un maggiore dettaglio, si veda il Manuale di Conservazione di Aruba, allegato “Manuale di conservazione - Aruba”.

Art. 16: Modello organizzativo della conservazione

1. Il comune di Ollastra realizza il processo di conservazione ai sensi dall’art. 34, comma 1-bis, del CAD, fatte salve le competenze del Ministero per i beni e le attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42.
2. Il processo di conservazione può essere pertanto svolto all’interno o all’esterno della struttura organizzativa dell’ente, si è scelta l’esternalizzazione del servizio ad Aruba.
3. I requisiti del processo di conservazione, le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione, e le loro modalità di interazione sono formalizzate nel presente manuale di conservazione, tali modalità trovano riscontro anche nel manuale di conservazione del conservatore (allegato “Manuale di conservazione - Aruba”).

V: PROCESSO DI CONSERVAZIONE

Art. 17: Descrizione generale del Sistema di Conservazione

Aruba mediante il proprio sistema di conservazione Docfly, sviluppato integralmente dalla società, è in grado di accettare e gestire, come richiesto ai sensi dell’art. 44, comma 1-bis, del CAD,

a) i fascicoli informatici chiusi e le serie informatiche chiuse;

b) i fascicoli informatici e le serie non ancora chiusi accettando i documenti in essi contenuti sulla base di specifiche esigenze del soggetto produttore. In particolare, in questo caso, il Titolare (Comune di Ollastra) e il Conservatore garantiscono specifico monitoraggio al fine di evitare rischi di obsolescenza tecnologica che possono sopravvenire prima della chiusura.

Aruba è predisposto per accettare aggregazioni documentali e tutte le tipologie di documenti informatici relativi a diversi ambiti applicativi.

In accordo con il soggetto produttore, Aruba si riserva infatti la facoltà di accettare qualsiasi tipologia documentale. L’indicazione delle tipologie documentali, compresa la gestione di queste, verrà indicata nella scheda cliente allegata al contratto stipulato con il soggetto produttore (vedasi allegato “Scheda richiesta attivazione docfly”).

Aruba accetta e conserva solo documenti informatici. Il sistema di conservazione permette l’acquisizione sia di documenti firmati digitalmente, sia di documenti non firmati. Entrambe le



tipologie entrano nel medesimo processo di Ingestion. Con l'ausilio del Responsabile del servizio di conservazione, è il Soggetto produttore a definire nella scheda cliente le modalità di trattamento dei documenti firmati o non firmati.

Art. 18: Processo di erogazione del servizio di conservazione

DocFly - Conservazione Digitale a Norma è un servizio in grado di garantire nel tempo la validità legale di un documento informatico, in conformità alle disposizioni normative delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici del 1 gennaio 2022. Grazie al rispetto dei più stringenti requisiti di gestione documentale, DocFly rappresenta uno strumento fondamentale per il processo di dematerializzazione anche all'interno dei settori più complessi e articolati, come la Pubblica Amministrazione. Il servizio può essere erogato con diverse caratteristiche di assistenza, livelli di servizio ed altri elementi accessori che non ne modificano le componenti tecniche di sicurezza

Caratteristiche funzionali del servizio

- Funzionalità di scarto
- Esibizione a norma dei documenti conservati
- Profilazione utenze in base al ruolo e ai permessi ad esse associate
- Accesso tramite web o web service
- Generazione e download di rapporto di versamento o rapporto di errore
- Multiutenza
- Consente il tracciamento dei log del sistema
- Monitoraggio de flusso di versamento
- Ricerca dei documenti e delle aggregazioni documentali
- Download dei documenti conservati
- Versamento dei documenti e delle aggregazioni documentali informatiche nella forma di pacchetti di versamento
- Verifiche sui metadati, formati, firme, integrità dei dati presenti nei pacchetti di versamento
- Creazione automatica del pacchetto di archiviazione

Connessione telematica rete internet Browser web per la ricerca, consultazione, scarico dei pacchetti informativi, scarto delle unità documentarie e archivistiche conservate, esibizioni

Il servizio offerto da Aruba ad ogni Soggetto produttore, (Comune di Ollastra) viene avviato al termine di un processo di attivazione che segue queste fasi fondamentali:



- condivisione di informazioni tecniche di richiesta configurazione e invio dei Pacchetti di versamento;
- verifiche sui Pacchetti di versamento e sugli oggetti in esso contenuti;
- accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico;
- rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie;
- preparazione e gestione del Pacchetto di archiviazione;
- preparazione e gestione del Pacchetto di distribuzione ai fini dell'esibizione;

Ognuno degli step sopra indicati viene eseguito per ogni tipologia di configurazione richiesta.

Art. 19: Acquisizione dei pacchetti di versamento per la loro presa in carico

In questa fase il Comune di Ollastra (Soggetto produttore) veicola al Responsabile del servizio di conservazione, al Privacy Manager e al Responsabile della funzione archivistica la richiesta di attivazione del servizio per l'invio di Pacchetti di versamento. Le tre figure responsabili sopracitate, con l'ausilio del Responsabile dello sviluppo e della manutenzione, incaricato di curare l'interfaccia con il Soggetto produttore relativamente alle modalità di trasferimento dei documenti, valuteranno la domanda di acquisizione del servizio affinché venga accertato che i requisiti del Soggetto produttore siano compatibili con le policy di Aruba.

L'attivazione del servizio avviene attraverso la compilazione del Modulo 'Scheda cliente' allegato "Scheda richiesta attivazione docfly". In particolare, tale modulo deve essere compilato con le seguenti informazioni:

- ragione sociale;
- indirizzo;
- partita iva;
- e-mail
- oggetti documentali gestiti
- tipo di protocollo da utilizzare per lo scambio dei Pacchetti.
- metadati specifici di tipologia
- utenze da abilitare per l'accesso al portale di distribuzione.

Per ogni Pacchetto di versamento dichiarato dal Soggetto produttore, è possibile definire:

- i volumi in termini di numero documenti annui previsti da gestire e spazio di occupazione previsto per i dati da Conservare (GB);
- la dimensione massima del Pacchetto di versamento;



- la frequenza di invio dei Pacchetti;

L'acquisizione dei Pacchetti di versamento avviene mediante due canali: tramite SSH File Transfert Protocol e tramite canale Web service descritti dettagliatamente nel paragrafo 7.1 del Manuale utente di Aruba, vedasi Allegato "Manuale di conservazione - Aruba"

Art. 20: Pacchetti di versamento

Per quanto concerne i seguenti argomenti puntati si fa direttamente riferimento al Manuale di Aruba "Manuale di conservazione - Aruba":

- le verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti;
- l'accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico;
- il rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie;
- la preparazione e gestione dei Pacchetti di archiviazione;
- la preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione;
- la produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento di un pubblico ufficiale;
- lo scarto dei Pacchetti di archiviazione;
- la predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori.

VI: INFRASTRUTTURA ARUBA

Art. 21: Descrizione Generale

Il Data Center di Aruba è qualificato ACN, ed è presente sul Marketplace al link: <https://www.acn.gov.it/portale/w/sa-3158>, di seguito

- 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 necessita.

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

L’architettura modulare del sistema è implementata al 100% su infrastruttura di virtualizzazione con hypervisor VMware e garantisce in sintesi i seguenti vantaggi:

Affidabilità - Totale ridondanza ai guasti HW

- Funzionalità di HA implementata dall’architettura virtuale.
- Almeno due moduli con il medesimo ruolo posizionati su server fisici separati.
- DBMS in configurazione Master-Master.
- 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

VII: TIPOLOGIE DEGLI OGGETTI DIGITALI SOTTOPOSTI A CONSERVAZIONE

Art. 22: Oggetti conservati

1. La selezione conservativa dei documenti informatici deve riguardare tutti i documenti informatici prodotti dall'Amministrazione. Un elenco delle tipologie di documenti conservate è indicato all'allegato 3 “Tipologie documentali e Metadati minimi”.
2. I documenti informatici devono essere statici, non modificabili e possono essere anche muniti di sottoscrizione elettronica e/o di marca temporale.
3. Sono accettati, per la conservazione, i formati che soddisfino caratteristiche di apertura, sicurezza, portabilità, funzionalità, diffusione, leggibilità nel tempo e supporto allo sviluppo.
4. Sono privilegiati i formati che siano standard internazionali (de jure e de facto) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche.



5. Ulteriore elemento di valutazione nella scelta del formato è il tempo di conservazione previsto dalla normativa per le singole tipologie di documenti informatici.
6. I formati indicati nel seguente elenco rappresentano l'insieme dei formati utilizzabili anche ai fini della conservazione previsti dall'allegato n. 2 "Formati di File e riversamento" delle LG sulla formazione, gestione e conservazione dei documenti informatici. Per maggiori dettagli si rimanda all'allegato "Formati di file adottati, interoperabilità e procedura di riversamento", contenuto nel Manuale di Gestione Documentale e richiamato anche nel presente Manuale di Conservazione.
 - **Documenti impaginati** — PDF, Microsoft® OOXML (.docx) e Word (.doc), OpenDocument Text (.odt), Rich-Text Format (.rtf), EPUB, PostScript™ (.ps), Adobe® InDesign® Markup Language (.idml);
 - **Ipertesti** — XML, dialetti e schemi XML (.xsd, .xsl), HTML (.html, .htm), fogli di stile per XML/HTML (.xsl, .xslt, .css), Markdown (.md);
 - **Dati strutturati** — SQL, CSV, Microsoft® OOXML (.accdb) e Access (.mdb), OpenDocument Database (.odb), JSON, Linked OpenData (.json-ld), JWT4;
 - **Posta elettronica** — .eml, .mbox;
 - **Fogli di calcolo** — Microsoft® OOXML (.xlsx) e Excel (.xls), OpenDocument Spreadsheet (.ods);
 - **Presentazioni multimediali** — Microsoft® OOXML (.pptx) e PowerPoint (.ppt), OpenDocument Presentation (.odp);
 - **Immagini raster** — JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), PNG, GIF, OpenEXR (.exr), JPEG2000 (.jp2k, .jp2c, .jp2), DICOM, Adobe® DNG, Adobe® Photoshop® (.psd), DPX, ARRIRAW (.ari);
 - **Immagini vettoriali e modellazione digitale** — SVG, Adobe® Illustrator® (.ai), Encapsulated PostScript™ (.eps);
 - **Modelli digitali** — StereoLithography (.stl); Autodesk® DWG™, DXF™, DWF™, FBX™.
 - **Caratteri tipografici** — OpenType (.otf), TrueType (.ttf), Web Open Font (.woff, .woff2);
 - **Suono** — Waveform RIFF / Broadcast Wave (.wav, .bwf), MP3, audio RAW (.pcm, .raw, .snd), AIFF (.aiff, .aifc, .aif), FLAC, MusicXML™ (.music.xml), MIDI (.mid); molteplici



codec audio;

- **Video** — formati video delle famiglie MPEG2 e MPEG4; molteplici codec video;
- **Sottotitoli** — TTML/IMSC/EBU-TT (.ttml, .dfxp, .xml), EBU STL;
- **Contenitori multimediali** — MP4, MXF, MPEG2 Transport/Program Stream (.vob, .ts, .ps), AVI RIFF (.avi), Matroska (.mkv), QuickTime (.mov, .qt), WebM;
- **Pacchetti multimediali** — pacchetto di master interoperabile (IMF, IMP); pacchetto per il cinema digitale (DCP); master per la distribuzione cinematografica (DCDM); pacchetti Digital Intermediate basati su sequenze di fotogrammi (.exr/.dpx; .wav), ACES metadata file (.amf); pacchetto XDCAM;
- **Archivi compressi** — TAR, ZIP, GZIP, 7-Zip (.7z), RAR, TAR compresso (.tgz, .t7z, ...), ISO9660 (.iso), VMware® Disk (.vmdk), Apple Disk Image (.dmg);
- **Documenti amministrativi** — fattura elettronica, fascicolo sanitario elettronico, response SAML SPID, segnatura di protocollo;
- **Applicazioni e codice sorgente** — eseguibili Microsoft® (.exe, .com), applet Java (.jar); pacchetti applicativi Windows® (.msi), Android (.apk), macOS® (.pkg), iOS® (.ipa); librerie statiche (.a, .lib) e dinamiche (.so, .dll, .dylib); script interpretabili (.sh, .?sh, .bat, .cmd, .py, .perl, .js, .go, .r, ...); codice sorgente in vari linguaggi di programmazione (.c, .cpp, .h, .java, .asm, ...).
- **Applicazioni crittografiche** — certificati elettronici (.cer, .crt, .pem), chiavi crittografiche (.pkix, .pem), marcature temporali elettroniche (.tsr, .tsd, .tst), impronte crittografiche (.sha1, .sha2, .md5, ...); per le firme e i sigilli elettronici avanzati: buste crittografiche XAdES (.xml), CAdES (.p7m, .p7s), PAdES (.pdf), contenitori ASiC (.zip); KDM (.kdm.xml).

Art. 23: Metadati da associare

1. I metadati costituiscono gli insiemi di dati da associare a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto, la struttura, nonché per permetterne la gestione e la ricerca nel tempo nel sistema di conservazione.
2. I metadati generali od oggettivi da associare a tutte le tipologie di documenti da conservare devono fornire le informazioni base relative al pacchetto di archiviazione, al suo contenuto e al processo di produzione dello stesso.



3. In ogni caso i metadati minimi da associare devono essere quelli previsti, dall'allegato n. 2 "Formati di File e riversamento" delle LG sulla formazione, gestione e conservazione dei documenti informatici. Un elenco dettagliato dei metadati inviati in conservazione per ciascuna delle tipologie documentali è indicato all'allegato 3 "Tipologie documentali e Metadati minimi".
4. I metadati devono essere inclusi nel pacchetto di archiviazione ottenuto dalla trasformazione del pacchetto di versamento all'atto della messa in conservazione.

Art. 24: Tipologie documentali

1. Il sistema di gestione documentale e il sistema di conservazione utilizzati dall'Ente, sono organizzati in classi documentali.
2. Le tipologie documentali sono definite nel contratto di convenzione con l'ente conservatore Aruba all'atto della stipula.
3. La classe documentale specifica tutte le caratteristiche relative ad una tipologia di documento da sottoporre a conservazione, individuando le informazioni necessarie a qualificare e identificare univocamente ogni singolo documento. Ha parametri propri di comportamento ed attributi o metadati caratteristici, vedasi allegato "Scheda richiesta attivazione docfly"

VIII: MODALITA' DI ESIBIZIONE

Art. 25: Esibizione

1. Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettiva.
2. L'adozione di formati standard consolidati e riconosciuti a livello internazionale nella rappresentazione dei dati conservati ne garantiscono l'accesso attraverso sistemi esterni o software di terzi basati sui medesimi standard.
3. La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'utente, il conservatore Aruba, attraverso il sistema Docfly, prevedendo la conservazione dei Pacchetti di archiviazione firmati, implementa un formato di composizione delle marche tale da permettere l'esibizione probatoria di un singolo documento. Quindi, ogni singolo file può essere esibito insieme ai suoi metadati, registrati nel data base, e alle sue prove di conservazione in maniera assolutamente indipendente dagli altri documenti.
4. I livelli di accesso vengono definiti in base alle esigenze delle richieste effettuate, rendendo disponibile soltanto il materiale richiesto grazie all'utilizzo di filtri predefiniti che selezionano i canali previsti per la visualizzazione di un determinato pacchetto.
5. È possibile visualizzare i documenti tramite triplice canale come descritto nell'allegato "Manuale di conservazione - Aruba" che di seguito riportiamo fedelmente:



- via web: i Soggetti produttori titolari dei documenti potranno ricercare e visualizzare tutti i documenti conservati direttamente sul portale di Aruba attraverso l'apposita funzionalità. L'accesso avviene tramite il portale al quale è demandata la sicurezza e la gestione della sessione. I documenti saranno disponibili per l'esibizione on-line per tutto il periodo di conservazione. Per la ricerca dei documenti è possibile utilizzare dei filtri valorizzando gli appositi campi delle maschere di ricerca con i metadati dichiarati in fase di versamento. L'accesso al portale può avvenire tramite credenziali nominali fornite al momento dell'attivazione delle utenze o tramite SPID. Vengono inoltre resi disponibili servizi web (Web Services) per le eventuali integrazioni con i portali dei Soggetti produttori.
- copia del documento su supporto removibile. La descrizione dettagliata circa la visualizzazione dei Pacchetti di distribuzione mediante supporto removibile è presente nel capitolo 6 Oggetti sottoposti a conservazione, paragrafo 6.5 del "Manuale di conservazione - Aruba".
- restituzione via canale SFTP. In questo caso viene richiesto al soggetto produttore di generare una coppia di chiavi (pubblica e privata) in formato OpenSSH RSA, di lunghezza minima 2048 bit e di fornirci la chiave pubblica della coppia per l'apertura del canale. La struttura architeturale di Aruba consente di definire diversi livelli operativi e garantisce che ciascuna Azienda/Ente, Area Organizzativa, Agenzia, Ufficio, Dipartimento, ecc. possa accedere solo ed esclusivamente ai propri documenti, in base alle credenziali e alle politiche di accesso attivate.

IX: MISURE DI SICUREZZA DEL SISTEMA

Art. 26: Misure di sicurezza a tutela dei dati personali

1. Nell'attuazione delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della conservazione, di concerto con il responsabile per la transizione digitale, con il responsabile della gestione documentale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.
2. L'adozione delle predette misure è in capo al titolare (Comune di Ollastra) che ha provveduto ad individuare sulla base dell'art.28 del Regolamento UE 679/2016 il responsabile del trattamento (Aruba) essendo quest'ultimo il conservatore.



3. Le misure di sicurezza sono descritte nell'allegato "Piano di Sicurezza Relativo alla Formazione, alla Gestione, alla Trasmissione, all'interscambio all'accesso ai documenti informatici" e nel cap 12 dell'allegato "Manuale di conservazione - Aruba".

X: SELEZIONE E SCARTO

Art. 27: LG per la selezione e scarto dei documenti informatici

1. 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.
2. Nel caso degli archivi pubblici con il solo riferimento a quelli dichiarati di interesse storico particolarmente importante l'autorizzazione è rilasciata ai sensi della normativa vigente in materia di beni culturali.
3. il Comune di Ollastra una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore Aruba affinché provveda alla distruzione dei pacchetti di archiviazione.
4. Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, il Comune di Ollastra 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, tale operazione avrà completa efficacia solo al momento del completo aggiornamento delle copie di sicurezza del sistema.
5. Nel sistema di conservazione, la selezione e lo scarto dei pacchetti di archiviazione sono definiti dal Comune (Titolare dell'oggetto di conservazione) e secondo quanto indicato dal piano di conservazione. Nel nostro caso, avendo affidato all'esterno il servizio di conservazione le modalità operative sono concordate dal Comune di Ollastra e dal Conservatore Aruba.
6. Il responsabile della conservazione genera l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e, dopo aver verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale.
7. In caso di affidamento esterno del servizio di conservazione (come nel nostro caso) l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione e trasmesso al responsabile della conservazione che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale.
8. I documenti e le aggregazioni documentali informatiche sottoposti a scarto nel sistema di conservazione devono essere distrutti anche in tutti i sistemi gestiti dal Comune di Ollastra.



Art. 28: Modalità adottata per la selezione e lo scarto

1. Nel sistema di conservazione, la selezione e lo scarto dei pacchetti di archiviazione sono definiti dal Comune di Ollastra secondo quanto indicato dal piano di conservazione adottato dall'Ente.
2. Se non diversamente indicato dal Responsabile della conservazione e dal Responsabile della gestione documentale del Comune, tutti gli oggetti trasmessi in conservazione digitale sono considerati "a conservazione PERMANENTE".
3. Il Responsabile della conservazione genera l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e, dopo aver verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al Responsabile della gestione documentale del Comune di Ollastra.
4. Il Responsabile della conservazione del Comune, una volta ricevuta l'autorizzazione del responsabile della gestione documentale (autorizzazione comunicata necessariamente a seguito dell'acquisizione del nulla osta vincolante della competente Soprintendenza Archivistica), provvede a trasmetterlo al conservatore, Aruba, affinché disponga la distruzione dei pacchetti di archiviazione.
5. Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, il Comune notifica l'esito della procedura di scarto alla Soprintendenza Archivistica, tale operazione avrà completa efficacia solo al momento del completo aggiornamento delle copie di sicurezza del sistema.
6. I documenti e le aggregazioni documentali informatiche sottoposti a scarto nel sistema di conservazione devono essere distrutti anche in tutti i sistemi gestiti dal Comune, come detto in precedenza al p.to 8 dell'art. 27.
7. Per qualsiasi altro dettaglio si faccia riferimento all'allegato 4 denominato "Piano di conservazione, selezione e scarto" ed al cap. 7.8 "Scarto dei Pacchetti di archiviazione" dell'allegato "Manuale di conservazione - Aruba".

XI: DISPOSIZIONI FINALI

Art. 29: Pubblicità del presente manuale ed entrata in vigore

1. Il presente documento ed i rispettivi allegati vengono pubblicati sul sito istituzionale dell'Ente nell'apposita sezione di Amministrazione Trasparente, come previsto dal piano triennale per l'informatica per la PA (PT 2024-2026 OB. 3.3.1/B | Cap. 3 PA 18) e dall'art. 9 del D.Lgs. 33/2013.
2. Il presente manuale è predisposto su proposta del Responsabile della conservazione documentale, d'intesa con il Responsabile della gestione documentale, il Responsabile dei sistemi informativi, il Responsabile per la transizione al digitale e trasmesso, per quanto di



competenza, al Responsabile della protezione dei dati personali. L'approvazione del manuale da parte della Giunta comunale è subordinata, ai sensi dell'art. 21, commi 4 e 5, del D.Lgs. 42/2004, alla preventiva autorizzazione della Soprintendenza Archivistica della regione Sardegna.

3. Il presente Regolamento entra in vigore il giorno successivo alla data di esecutività della delibera di adozione.
4. Ogni qualvolta si renderà necessario un aggiornamento (derivante da un cambio normativo, un cambio nell'organigramma dell'Ente o un cambio nel software o del software gestionale), questo dovrà essere effettuato con il medesimo iter utilizzato per l'approvazione ed adozione originaria, le figure preposte sono: il Responsabile della conservazione; il Responsabile della gestione documentale; il Responsabile dei sistemi informativi, se presente; il Responsabile per la transizione al digitale ed il DPO (responsabile protezione dei dati) per quanto di competenza.

XII: Allegati

Art. 30: Allegati

1. Al presente regolamento si allegano gli schemi:
 - Allegato 1 – Elenco delle figure Nominate;
 - Allegato 2 – Formati di file adottati dall'Ente;
 - Allegato 3 – Tipologie documentali e Metadati minimi;
 - Allegato 4 – Piano di conservazione, selezione e scarto;
 - Allegato Piano di Sicurezza Informatica;
 - Allegato Scheda richiesta attivazione docfly;
 - Allegato Manuale di conservazione - Aruba



Comune di Ollastra

Provincia di Oristano

Allegato 1

Elenco delle figure Nominate

Manuale di Conservazione

FUNZIONI E RESPONSABILITÀ NELLA PUBBLICA AMMINISTRAZIONE

INTRODUZIONE

Nell'ambito della Pubblica Amministrazione (PA), la gestione documentale, la conservazione dei documenti digitali e la transizione digitale sono aspetti fondamentali per garantire trasparenza, efficienza e conformità normativa. Diverse figure professionali assumono ruoli chiave in questi processi, assicurando che le informazioni siano archiviate, gestite e protette secondo le normative vigenti.

Di seguito vengono descritte le principali funzioni e responsabilità di alcune delle figure più rilevanti in questo contesto seguito dalle AOU

1. Responsabile della Conservazione

Il Responsabile della Conservazione è la figura incaricata di garantire che il sistema di conservazione dei documenti digitali della PA sia conforme a quanto riportato nel D.Lgs. 82/2005 art. 44, 1-quater:

- Opera d'intesa con il DPO, con il Responsabile della Transizione Digitale che è referente per la Sicurezza e con l'Amministratore di Sistema per garantire l'integrità e l'accessibilità dei documenti, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali.
 - opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis.
-

2. Incaricato alla Conservazione

L'Incaricato alla Conservazione supporta il Responsabile della Conservazione nello svolgimento delle attività operative. Tra i suoi compiti principali ci sono:

- Attuazione delle procedure di conservazione stabilite dal Responsabile.
 - Monitoraggio dell'integrità e della leggibilità dei documenti digitali nel tempo.
 - Gestione delle operazioni quotidiane relative al sistema di conservazione.
-

3. Responsabile del Servizio di Protocollazione

Questa figura è responsabile della gestione del protocollo informatico, un sistema fondamentale per la registrazione e la tracciabilità dei documenti all'interno della PA. I suoi compiti comprendono:

- Garantire la corretta registrazione, classificazione e archiviazione dei documenti protocollati.
 - Assicurare la conformità del sistema di protocollazione alle norme vigenti.
 - Coordinare le attività degli incaricati alla gestione del protocollo.
-

4. Incaricato alla Gestione del Servizio di Protocollazione

L'Incaricato alla Gestione del Servizio di Protocollazione svolge attività operative sotto la direzione del Responsabile del Servizio di Protocollazione. Le sue funzioni principali sono:

- Registrazione e gestione del protocollo informatico quotidiano.
 - Smistamento e archiviazione dei documenti protocollati.
 - Verifica della corretta associazione dei documenti all'interno dei fascicoli amministrativi.
-

5. Responsabile della Gestione Documentale

Questa figura ha il compito di garantire la gestione efficace dei documenti della PA, con particolare attenzione alla digitalizzazione e all'organizzazione delle informazioni. Le sue responsabilità includono:

- Definizione delle regole di classificazione e archiviazione dei documenti.
 - Coordinamento delle attività di gestione documentale e conservazione.
 - Supporto alla transizione digitale attraverso l'adozione di strumenti innovativi.
-

6. Responsabile della Transizione Digitale

Il Responsabile della Transizione Digitale (RTD) ha un ruolo strategico nella modernizzazione della PA e nell'attuazione delle politiche digitali previste dall'art. 17 del D.Lgs. 7 marzo 2005, n. 82 (CAD), di seguito riportiamo quanto indicato nel suddetto art.17:

Le pubbliche amministrazioni garantiscono l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le Linee guida. A tal fine, ciascuna pubblica amministrazione 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 dai 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;
- 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](#);
- 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 identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo

di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis. j-bis) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).

1-ter. Il **responsabile dell'ufficio di cui al comma 1** è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali e risponde, con riferimento ai compiti relativi alla transizione, alla modalità digitale direttamente all'organo di vertice politico.

7. Responsabile della Privacy

Il Responsabile della Privacy, spesso identificato con il Data Protection Officer (DPO), ha il compito di garantire che il trattamento dei dati personali avvenga nel rispetto delle normative sulla protezione dei dati (come il GDPR). Le sue principali attività comprendono:

- Monitoraggio della conformità dell'ente alle normative sulla protezione dei dati.
- Consulenza e formazione del personale sulle tematiche della privacy.
- Gestione delle richieste relative ai diritti degli interessati in materia di dati personali.

AREA ORGANIZZATIVA OMOGENEA (Codice univoco: A377665 denominata in IPA: COMUNE DI OLLASTRA)

L'art. 50, comma 4, del DPR 445/00 stabilisce che all'interno di ciascuna amministrazione siano create delle Aree Organizzative Omogenee, in modo da assicurare criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna delle stesse.

L'art. 61 del DPR 445/00 stabilisce, altresì, che si costituisca per ciascuna AOO un Servizio responsabile della tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Al detto Servizio deve essere preposto un dirigente ovvero funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica.

Le Linee guida AgID sul documento informatico ribadiscono l'obbligo di individuare le suddette Aree Organizzative Omogenee e di nominare, al loro interno, un Responsabile della gestione documentale nonché un suo vicario per casi di vacanza, assenza o impedimento ed un Responsabile della conservazione, a tal riguardo si faccia riferimento all'art. 3 del presente manuale di gestione documentale.

Di seguito si elencano gli estremi degli atti di nomina per ciascuna figura precedentemente menzionata:

Responsabile della Conservazione	
Nominativo	Nazzarena Carrau
Tipologia di atto per la nomina	Decreto Sindacale
Numero dell'atto di nomina	N°2
Data dell'atto di nomina	15.04.2024

Vicario o Delegato della Conservazione	
Nominativo	Alice Ghiani
Tipologia di atto per la nomina	Decreto Sindacale
Numero dell'atto di nomina	N°2
Data dell'atto di nomina	15.04.2024

Responsabile del Servizio di Protocollazione	
Nominativo	Alice Ghiani
Tipologia di atto per la nomina	Decreto Sindacale
Numero dell'atto di nomina	N°27
Data dell'atto di nomina	30.12.2021

Responsabile della Gestione Documentale	
Nominativo	Nazzarena Carrau
Tipologia di atto per la nomina	Decreto Sindacale
Numero dell'atto di nomina	N°2
Data dell'atto di nomina	15.04.2024

Vicario della Gestione Documentale	
Nominativo	Alice Ghiani
Tipologia di atto per la nomina	Decreto Sindacale
Numero dell'atto di nomina	N°2
Data dell'atto di nomina	15.04.2024

Responsabile per la Transizione Digitale - RTD	
Nominativo	Alice Ghiani
Tipologia di atto per la nomina	Deliberazione della Giunta Comunale
Numero dell'atto di nomina	N°70
Data dell'atto di nomina	25.11.2019

Responsabile Protezione Dati Personali - DPO	
Nominativo	Avv. Alessandra Etzo
Tipologia di atto per la nomina	Determinazione Responsabile Area Tecnica dell'Unione dei Comuni della Bassa Valle del Tirso e del Grighine
Numero dell'atto di nomina	N°15
Data dell'atto di nomina	03.04.2024

ARTICOLAZIONE DELL'ENTE IN UNITÀ ORGANIZZATIVE RESPONSABILI

Il Comune di Ollastra è strutturato nelle seguenti unità organizzative responsabili (UOR); tali UOR per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato:

Denominazione UOR	Responsabile UOR
Area Amministrativo-Contabile	Alice Ghiani
UOR collegate	
Ufficio Amministrativo	Istruttore Amministrativo: Dr. Nicola Delogu
Ufficio Ragioneria	Istruttore Amministrativo: Dr.ssa Alice Ghiani
Ufficio Servizi Demografici	Istruttore Amministrativo: Nazzarena Carrau
Ufficio Tributi	Istruttore di Vigilanza: Valentina Pirastu
Ufficio Servizi Sociali	Assistente Sociale: Dr.ssa Claudia Defraia
Ufficio Amministrativo-Contabile	Istruttore Amministrativo: Rag. Pierangelo Trogu
Area Tecnica	Ing. Riccardo Meli
UOR collegate	
Ufficio Tecnico	Istruttore tecnico: Geom. Giovanni Canoppia
Ufficio Polizia Municipale	Istruttore di Vigilanza: Valentina Pirastu



Comune di Ollastra
Provincia di Oristano

Allegato 2
Formati di files adottati, Interoperabilità e
Procedura di Riversamento
Manuale di Conservazione

FORMATI ELETTRONICI ADOTTATI

Tipologie di Formati

Il comune di Ollastra, al fine di produrre, gestire e mandare in conservazione i documenti informatici in modo conforme a quanto indicato nell'allegato n. 2 "Formati di File e riversamento" delle LG sulla formazione, gestione e conservazione dei documenti informatici, utilizza i formati elettronici, obbligatori, previsti nel suddetto allegato 2 che di seguito riportiamo:

- **Documenti impaginati** — PDF, Microsoft® OOXML (.docx) e Word (.doc), OpenDocument Text (.odt), Rich-Text Format (.rtf), EPUB, PostScript™ (.ps), Adobe® InDesign® Markup Language (.idml);
- **Ipertesti** — XML, dialetti e schemi XML (.xsd, .xsl), HTML (.html, .htm), fogli di stile per XML/HTML (.xsl, .xslt, .css), Markdown (.md);
- **Dati strutturati** — SQL, CSV, Microsoft® OOXML (.accdb) e Access (.mdb), OpenDocument Database (.odb), JSON, Linked OpenData (.json-ld), JWT4;
- **Posta elettronica** — .eml, .mbox;
- **Fogli di calcolo** — Microsoft® OOXML (.xlsx) e Excel (.xls), OpenDocument Spreadsheet (.ods);
- **Presentazioni multimediali** — Microsoft® OOXML (.pptx) e PowerPoint (.ppt), OpenDocument Presentation (.odp);
- **Immagini raster** — JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), PNG, GIF, OpenEXR (.exr), JPEG2000 (.jp2k, .jp2c, .jp2), DICOM, Adobe® DNG, Adobe® Photoshop® (.psd), DPX, ARRIRAW (.ari);
- **Immagini vettoriali e modellazione digitale** — SVG, Adobe® Illustrator® (.ai), Encapsulated PostScript™ (.eps);
- **Modelli digitali** — StereoLithography (.stl); Autodesk® DWG™, DXF™, DWF™, FBX™.
- **Caratteri tipografici** — OpenType (.otf), TrueType (.ttf), Web Open Font (.woff, .woff2);
- **Suono** — Waveform RIFF / Broadcast Wave (.wav, .bwf), MP3, audio RAW (.pcm, .raw, .snd), AIFF (.aiff, .aifc, .aif), FLAC, MusicXML™ (.music.xml), MIDI (.mid); molteplici codec audio;
- **Video** — formati video delle famiglie MPEG2 e MPEG4; molteplici codec video;
- **Sottotitoli** — TTML/IMSC/EBU-TT (.ttml, .dfxp, .xml), EBU STL;
- **Contenitori multimediali** — MP4, MXF, MPEG2 Transport/Program Stream (.vob, .ts, .ps), AVI RIFF (.avi), Matroska (.mkv), QuickTime (.mov, .qt), WebM;
- **Pacchetti multimediali** — pacchetto di master interoperabile (IMF, IMP); pacchetto per il cinema digitale (DCP); master per la distribuzione cinematografica (DCDM); pacchetti Digital Intermediate

basati su sequenze di fotogrammi (.exr/.dpx; .wav), ACES metadata file (.amf); pacchetto XDCAM;

- **Archivi compressi** — TAR, ZIP, GZIP, 7-Zip (.7z), RAR, TAR compresso (.tgz, .t7z, ...), ISO9660 (.iso), VMware® Disk (.vmdk), Apple Disk Image (.dmg);
- **Documenti amministrativi** — fattura elettronica, fascicolo sanitario elettronico, response SAML SPID, segnature di protocollo;
- **Applicazioni e codice sorgente** — eseguibili Microsoft® (.exe, .com), applet Java (.jar); pacchetti applicativi Windows® (.msi), Android (.apk), macOS® (.pkg), iOS® (.ipa); librerie statiche (.a, .lib) e dinamiche (.so, .dll, .dylib); script interpretabili (.sh, .?sh, .bat, .cmd, .py, .perl, .js, .go, .r, ...); codice sorgente in vari linguaggi di programmazione (.c, .cpp, .h, .java, .asm, ...).
- **Applicazioni crittografiche** — certificati elettronici (.cer, .crt, .pem), chiavi crittografiche (.pkix, .pem), marcature temporali elettroniche (.tsr, .tsd, .tst), impronte crittografiche (.sha1, .sha2, .md5, ...); per le firme e i sigilli elettronici avanzati: buste crittografiche XAdES (.xml), CAdES (.p7m, .p7s), PAdES (.pdf), contenitori ASiC (.zip); KDM (.kdm.xml), i file con estensione (.enc) sono buste telematiche criptate utilizzate per il Processo Civile Telematico (PCT), Il formato (.sgp) è un tipo di file specifico utilizzato dai Comuni italiani per l'aggiornamento degli albi dei Giudici Popolari (Corti d'Assise e Corti d'Assise d'Appello) da inviare ai Tribunali competenti.

Nel successivo prospetto si indicano in maniera riassuntiva alcune caratteristiche più significative di cui godono i file con i rispettivi formati individuati nell'elenco soprastante, abbiamo riportato esclusivamente i formati ed i tipi di file più utilizzati dal nostro Ente:

FORMATO ADOTTATO	PROPRIETÀ RILEVANTI AI FINI DELLA GESTIONE E CONSERVAZIONE DEI DOCUMENTI
(Documenti impaginati) PDF	Il formato PDF è il “principe” dei formati per documenti impaginati. Nato come formato proprietario (sviluppato da Adobe Corporation), è stato rapidamente adottato come standard de facto per la produzione digitale del cartaceo; nel 2008 è diventato uno standard de iure, con il nome di ISO 32000-1 (PDF versione 1.7); successivamente rivisto nel 2017, con il nome di ISO 32000-2 (PDF versione 2.0). Il formato PDF è estremamente versatile in quanto è stato continuamente aggiornato nel tempo aggiungendo nuove funzionalità.
(Documenti impaginati) PDF/A	Profilo particolarmente adatto alla creazione di documenti di cui deve essere garantita la leggibilità in caso di archiviazione a lungo termine e conservazione.
(Documenti impaginati) Microsoft® OOXML	La suite di applicativi Microsoft® Office®, dalla versione 2007 in poi, utilizza un formato di file unico per i suoi applicativi principali, chiamato Open Office XML. 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.

(Documenti impaginati) Word	Il formato binario Word, ® utilizzato come formato principale fino alla versione 2003 da codesto applicativo di videoscrittura, è una variante specializzata del formato Compound File Binary, proprietario di Microsoft Corporation (cfr. §2.5); utilizza l'estensione .doc per i documenti impaginati normale, e la cambia in caso di varianti, quali ad esempio i modelli di documento (estensione .dot). Il formato contiene in un unico file i metadati, i contenuti testuali, ipertestuali e gli allegati dell'impaginato, senza offrire efficaci meccanismi di controllo dell'integrità.
(Documenti impaginati) Rich-Text Format	Rich Text Format (RTF) è un formato di proprietà di Microsoft utilizzato come formati interoperabile di documenti impaginati. Il formato supporta un numero molto ridotto di caratteristiche grafiche e tipografiche, e una possibilità limitata relativamente a ipertesti e allegati multimediali, a fronte di una semplicità strutturale conforme con lo scopo della sua introduzione
(Ipertesti) XML	Il principale tipo di sintassi ipertestuale è costituito dall'Extensible Markup Language (XML), la cui caratteristica aggiuntiva è di essere facilmente human readable.
(Ipertesti) HTML	HTML (ufficialmente codificato come XML puro a partire dalle sue versioni "XHTML" e "HTML5"), serve a rappresentare il contenuto di pagine web. In questo caso HTML (.htm, .html) è affiancato dal CSS, linguaggio specifico per descrivere i fogli di stile che trasformano i componenti logici di una pagina in elementi grafici (la cosiddetta "presentazione" della pagina).
(Dati strutturati) SQL	I file SQL servono a contenere configurazioni e tabelle per basi di dati relazionali, complete o parziali, sotto forma del loro linguaggio di programmazione comune. A tale scopo bisogna dunque specificare che SQL è in realtà un ceppo linguistico, da cui sono derivati molteplici dialetti di SQL, differenziati a seconda dell'applicativo –commerciale o meno– che funge da gestore di basi di dati. È raccomandato quindi, per l'archiviazione a lungo termine e l'interscambio.
(Dati strutturati) OpenDocument	<u>Il formato OpenDocument è utilizzato per la rappresentazione di basi di dati. ODP è un formato deprecato e va perciò evitata la produzione di nuovi file.</u>
(Dati strutturati) 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. Un vantaggio di JSON rispetto a XML è la semplicità della sintassi che, pur non offrendo capacità avanzate quali i namespace o la possibilità di "attraversare" la struttura ad albero (offerte da XML), dispone di una struttura più semplice da interpretare –soprattutto da parte di processi automatici– senza perdere la caratteristica fondamentale della leggibilità da parte dell'uomo.

(Posta elettronica) EML / MBOX	Il formato EML rappresenta interamente l'evidenza informatica costituente un singolo messaggio di posta elettronica MIME, così come definito negli standard RFC-5322 e RFC-2822. Così come EML rappresenta, integralmente un singolo messaggio di posta elettronica, il formato MBOX può usarsi per contenerci diversi messaggi di posta elettronica, organizzati su più livelli.
(Fogli di calcolo) XLS	Il formato XLS è specializzato per la rappresentazione di fogli di calcolo (estensione .xls). È stato utilizzato, come formato principale per tali documenti fino alla versione 2003 di Microsoft® Office®, ma è compatibile con moltissimi altri applicativi. Nonostante l'obbligo per le PP.AA. di accettare e aprire documenti in questo formato, <u>si raccomanda di non formarne altri esemplari e di valutare il riversamento di fogli di calcolo preesistenti in altro formato della stessa tipologia</u>: in quest'ordine, OpenDocument Spreadsheet (.ods) ovvero SpreadsheetML (.xlsx).
(Presentazioni multimediali) PPT /PPTX	Il formato PPT è specializzato per la rappresentazione di presentazioni multimediali (estensione .ppt). È stato utilizzato, come formato principale per tali documenti fino alla versione 2003 di Microsoft® Office®, ma è compatibile con moltissimi altri applicativi. Nonostante l'obbligo per le PP.AA. di accettare e aprire documenti in questo formato, <u>si raccomanda di non formarne altri esemplari e di valutare il riversamento di presentazioni preesistenti in altro formato della stessa tipologia</u>: in quest'ordine, OpenDocument Presentation (.odp) ovvero PresentationML (.pptx).
(Presentazioni multimediali) ODP	Il formato OpenDocument Presentation è usato per rappresentare fogli di calcolo (estensione .odp). È attualmente utilizzato dalla suite open source di applicativi da ufficio LibreOffice, anche se è pienamente utilizzabile in Microsoft® Office, ® in OpenOffice.org e in altri applicativi che elaborano documenti di questo tipo.
(Immagini raster) JPEG	Il formato JPEG è un altro "pilastro" storico per le immagini raster, permettendo una loro rappresentazione generica e, soprattutto, estremamente compatta per via dell'uso di un algoritmo di compressione lossy, in cui alcuni parametri algoritmici sono selezionabili in fase di formazione del file, permettendo così un bilanciamento tra "qualità" dell'immagine e dimensione del file.
(Immagini raster) TIFF	Il formato TIFF è il capostipite dei formati raster professionali, pur essendo ancora considerato appartenente alla categoria dei formati generali per le immagini raster. Nato con poche varianti e metadati prevalentemente per rappresentare immagini pronte sia per l'invio telematico (tramite fax) che per la stampa professionale –monocromatica o "offset" – è stato successivamente esteso dalla Adobe, fino a diventare uno standard aperto e de iure.

(Immagini raster) GIF	Il formato GIF venne introdotto nella fine degli anni '80 per rappresentare immagini fotorealistiche quando le capacità dei computer di visualizzare simultaneamente molti colori erano limitate. Alcune delle novità tecniche di questo formato sono sopravvissute sino ad oggi, tanto che vi sono ancora molti casi d'uso soprattutto nelle pagine web. Anche se oggi esistono formati molto più adeguati alle immagini fotorealistiche, il formato, implementando fra le altre cose una compressione lossless, è ancora tecnicamente valido per immagini con bassissimi requisiti di animazione, trasparenza e numero di colori (tipicamente loghi o porzioni di elementi grafici minimalisti), come quelle che si trovano in diversi siti web che spesso vengono salvate in questo formato.
(Immagini raster) JPEG2000	Il formato JPEG2000 utilizza una compressione basata su trasformata wavelet, cosiddetta multi-risoluzione, poiché l'evidenza informatica ivi rappresentata codifica prima i dettagli "grossolani" (cd. a bassa frequenza) dell'immagine, poi i dettagli via via più "fini" (cd. ad alte frequenze). A fronte di una maggiore complessità nella produzione (i.e. nella compressione) dell'immagine, il vantaggio tecnologico offerto da questo formato risiede nel fatto che la decodifica successiva dell'immagine (i.e. la sua decompressione) può avvenire anche non integralmente e interrompersi a un certo livello.
(Immagini vettoriali) SVG	Il formato SVG, basato su XML, descrive un'immagine vettoriale componente per componente, utilizzando l'estendibilità del linguaggio per "etichettare" opzionalmente alcune parti di queste componenti affinché possano essere referenziate da altri documenti o applicativi (ad es., una pagina web in HTML e il suo foglio di stile CSS allo scopo di migliorare l'interattività con le immagini vettoriali). Data la sua versatilità e l'apertura dello standard è il formato fortemente raccomandato per l'uso, la trasmissione e la conservazione di tutte le immagini vettoriali. <u><i>C'è una nuova versione proposta per essere la futura SVG 2.0; essa supporta alcune caratteristiche quali l'animazione dei componenti. Tale versione, tuttavia, non è allo stato attuale raccomandata.</i></u>
(Modelli digitali) DWF	Il formato DWF è stato specificatamente pensato per l'interoperabilità; è infatti basato, dalla versione 6.0, sullo standard ISO/IEC 29500-2 dell'open packaging (lo stesso usato da OOXML), e dunque costituito da un file ZIP contenente più file differenti (XML per la descrizione del modello; PNG per le preview e le texture). Pur trattandosi di un formato testuale (che descrive gli oggetti che compongono il modello o l'immagine mediante primitive grafiche) il medesimo formato permette anche la compressione allo scopo di ridurre l'occupazione digitale del file. È spesso utilizzato come formato di interscambio e, tra tutti i formati imparentati, è quello con le specifiche più aperte; perciò, è utilizzabile anche per archiviazione e conservazione.

(Suono) WAV / MP3	I campioni audio di una forma d'onda possono subire una compressione digitale allo scopo di ridurre le dimensioni occupate. I formati più noti per la memorizzazione di tali segnali audio sono il Waveform RIFF (.wav), MP3, FLAC, OGG e Broadcast Wave (.bwf).
(Video) MPEG-2 / MPEG-4	Un file (ovvero un flusso) video <i>strictu sensu</i> rappresenta una sequenza ordinata di immagini raster (dette fotogrammi — frame in inglese) riprodotte ad una velocità temporale fissa, espressa in numero di fotogrammi al secondo. Gli algoritmi di compressione inter-frame largamente diffusi sono MPEG-2, MPEG-4.
(Archivi compressi) TAR / 7-Zip / RAR	Nota Bene: Alcuni dei pacchetti di file oggetto dell'Allegato 2 delle LG AgID "Formati di File e Riversamento" sono di fatto creati, come ultimo passaggio, impacchettando una porzione di filesystem in un unico file compresso, utilizzando formati descritti. Tali documenti sono dunque rappresentati, grazie a questo stratagemma tecnico, da un unico file anziché da un pacchetto. Alcuni di questi formati mantengono l'estensione file del formato di archiviazione sopra descritto (e.g. .zip, .tar, .7z, ...); altri utilizzano estensioni proprie (e.g. .docx/.xlsx/.pptx, .od?, .woff/.woff2, .jar, .apk, .ipa).
(Documenti amministrativi) fatturazione elettronica XML	La fattura elettronica è creata, trasmessa, elaborata e conservata centralmente dal Sistema di Interscambio (SdI) dell'Agenzia delle Entrate, ovvero da altri applicativi ad esso interconnessi. Il formato della fattura elettronica è costituito da un file XML nel dialetto FatturaPA, che comprende tutte le varianti di processo della fatturazione convenzionale.
(Documenti amministrativi) SPID	Le asserzioni legate al Sistema Pubblico di Identità Digitale (SPID), siano esse in linguaggio SAML (basato su XML), ovvero in formato JWT (basato su JSON, sono da considerarsi un formato a sé stante in quanto possono trasportate e, se adeguatamente gestite, conservare a lungo termine dati personali o sensibili di persone fisiche o giuridiche.
(Applicazioni e codice sorgente) EXE / COM / MSI / PKG	Esistono una miriade di formati per codificare le applicazioni (altrimenti dette, impropriamente anche se a causa di una forzatura storica, binari). Tipicamente, tali formati dipendono dall'architettura dell'hardware e dal SO impiegato. Per tale motivo figurano tanto gli eseguibili Microsoft® (.exe, .com, .msi), quanto quelli macOS® (.pkg), quanto le app per dispositivi mobili, sia Android (.apk), che iOS® (.ipa). Oltre agli eseguibili, le porzioni di codice statico (.a, .lib) e dinamico (.so, .dll, .dylib) sono anch'esse dotate di formati specifici, largamente dipendenti dal SO.
(Applicazioni crittografiche) certificati elettronici CAdES / PAdES	Per meglio chiarire il contesto, si premette che i servizi fiduciari elettronici sono normati da fonti di livello pari o superiore a quello delle presenti Linee guida, le quali contengono obblighi e raccomandazioni anche in merito ai formati di file utilizzati per tali servizi. Tali fonti, includenti le loro successive modificazioni, sono: • Regolamento (UE) No 910/2014 del Parlamento europeo e del Consiglio

	(regolamento “eIDAS”); • Decisioni di Esecuzione (UE) collegate con il regolamento eIDAS; • articoli 20, 21, 24, 28, 35 e 36 del CAD; • Linee Guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate, emanate con Determinazione AgID No 121/2019; • D.P.C.M. del 21 maggio 2013 (Nuove Regole Tecniche Firma Elettronica Avanzata).
--	--

Raccomandazioni sui formati dei FILE:

I formati da utilizzare sopra inseriti sono stati riportati e descritti nell’ambito delle LG AgID sulla formazione, gestione e conservazione dei documenti informatici, sono quelli previsti nel capitolo 2 dell’Allegato 2 “Formati di File e riversamento”. Nello scegliere tali formati di file, da utilizzare per i propri documenti informatici, il Comune può effettuare la valutazione di interoperabilità che prediliga formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo al fine di:

- prevenire il rischio della loro obsolescenza tecnologica (rischio che incrementa con il divergere delle caratteristiche del formato da quelle sopraelencate);
- mitigare il rischio del *vendor lock-in*, che sussiste soprattutto per i formati proprietari, non codificati in standard *de iure*, o per quelli dipendenti dal dispositivo;
- facilitare il più possibile un loro futuro riversamento in altro formato, prediligendo caratteristiche quali l’estendibilità, la codifica testuale, la compatibilità in avanti e, in misura minore, la robustezza.

Di seguito riportiamo la metodologia adottata per la gestione dei documenti accettati “in entrata” dal pubblico ovvero da altre organizzazioni, pubblicati, ovvero prodotti “in uscita” verso altre organizzazioni e archiviati ovvero mandati in conservazione.

- i documenti informatici prodotti dall’Ente, al fine di essere sottoscritti con firma digitale, vengono migrati in PDF/A prima di essere sottoscritti e registrati nel Sistema;
- per l’acquisizione in formato digitale di documenti, nativamente prodotti in formato cartaceo, mediante l’attività di scansione, l’Ente utilizzerà il formato PDF e successivamente lo trasformerà e conserverà con il formato PDF/A;
- per l’acquisizione di immagini sul Sistema di Gestione Informatica dei Documenti vengono utilizzati i formati TIFF e JPG; l’utilizzo di quest’ultimo formato, tuttavia, avviene preferibilmente nella versione JPEG2000 (.jp2) perché può utilizzare una compressione senza perdita di informazioni e dunque senza pregiudicare la qualità dell’immagine;
- per l’acquisizione di documenti sottoscritti con firma digitale o altra sottoscrizione elettronica inviati all’AOO da parte di utenti esterni, il Comune richiede l’utilizzo del formato PDF/A; costituiscono eccezione le fatture elettroniche, le quali sono in formato XML;
- per l’acquisizione sul sistema di documenti che non necessitano di firma digitale o altra sottoscrizione

elettronica il Comune accetta, a seconda delle finalità per cui i documenti sono utilizzati, tutti i formati previsti dall'allegato n. 2 "Formati di File e riversamento", adatti ai fini della conservazione digitale; in tal caso possono essere utilizzati anche i formati ODF, OOXML (es. DOCX) e TXT;

- ai fini della conservazione dei messaggi di posta elettronica lo standard a cui fare riferimento è RFC 2822/MIME, mentre per quanto riguarda il formato degli allegati al suddetto messaggio si utilizzeranno, a seconda della tipologia del documento trattato e delle esigenze, i formati elettronici precedentemente indicati;
- al fine della pubblicazione di documenti sul proprio sito istituzionale l'Ente utilizza esclusivamente il formato PDF/A;
- per la produzione del registro giornaliero di protocollo da inviare al conservatore accreditato l'Ente utilizza il formato PDF/A.

VALUTAZIONE INTEROPERABILITA' FORMATI DEI DATI

Il Comune di Ollastra effettua una valutazione periodica dell'interoperabilità e dell'idoneità dei formati utilizzati per la produzione, gestione e conservazione dei documenti informatici, al fine di garantire nel tempo l'accessibilità, l'autenticità, l'integrità e la leggibilità degli stessi. Il comune non dispone di strutture o risorse dedicate allo sviluppo di Software interno e si avvale esclusivamente di soluzioni esterne, previa valutazione dell'interoperabilità dei formati dati, privilegiando in maniera esclusiva i formati standard.

Cadenza della valutazione

La verifica viene svolta con cadenza annuale, e comunque ogniqualvolta si verificano:

- modifiche normative o aggiornamenti delle Linee Guida AgID che incidano sui formati ammessi;
- aggiornamenti tecnologici che possano compromettere la leggibilità dei documenti;
- necessità di riversamento dovute a obsolescenza o dismissione di software/hardware.

Il Responsabile della gestione documentale, il Responsabile della conservazione e l'RTD effettuano un'analisi dei formati correntemente in uso, confrontandoli con:

- l'elenco dei formati aperti e raccomandati da AgID;
- le indicazioni provenienti dal sistema di conservazione adottato (Doc-Fly Aruba);
- le indicazioni tecniche provenienti dalla Software House (Siscom).

Questa analisi viene sottoposta al DPO per verificarne la conformità dal punto di vista del GDPR (Regolamento UE 2016/679).

Se vengono riscontrati formati differenti rispetto a quelli adottati l'Ente valuterà la presenza sul mercato di alternative aperte e interoperabili e ne valuterà il rischio di obsolescenza tecnologica adottando eventuali azioni correttive (riversamento in altro formato).

PROCEDURA DI RIVERSAMENTO

Il riversamento di formato comporta il trasferimento di un documento informatico in un formato di file diverso: contestualmente, ciò può comportare anche una duplicazione da un sistema di storage ad un altro (volume, disco, nastro, filesystem, storage ad oggetti o altri). Quando si parla di riversamento di file, s'intende un riversamento di almeno il suo formato.

Quando si effettua un riversamento finalizzato alla conservazione del file si può e, in certi casi previsti dalla legge, si deve, conservare anche la copia del file nel formato originario. In entrambe questi casi il file originario è conservato indipendentemente dal suo formato di file originario, purché sia conservata anche una copia conforme del medesimo in un formato adatto alla conservazione.

Quando si effettua un riversamento finalizzato alla conservazione, il file riversato è una copia digitale di un documento digitale e, come tale, la conformità della copia è attestata in base alla normativa vigente, inclusa la certificazione di processo come riportata nell'Allegato 3 delle LG AgID sulla formazione, gestione e conservazione dei documenti informatici.

Qualora dall'analisi di riversamento emerga la necessità di sostituire un formato non più idoneo, l'Amministrazione avvierà una procedura di riversamento che prevede:

- ✓ individuazione del formato di destinazione tra quelli aperti e raccomandati;
- ✓ definizione delle modalità tecniche di conversione (riversamento sostitutivo o migratorio);
- ✓ verifica di corrispondenza tra il documento originario e quello riversato in termini di contenuto, metadati e leggibilità;
- ✓ aggiornamento dei metadati di gestione e conservazione, registrando l'operazione di riversamento.

Tutte le attività di valutazione e riversamento verranno documentate in appositi verbali, i quali saranno fascicolati e archiviati presso l'Ente di conservazione a norma Doc-Fly Aruba.



Comune di Ollastra
Provincia di Oristano

Allegato 3

Tipologie Documentali e Metadati Associati dal Sistema di Gestione Documentale

Manuale di Conservazione

Tipologie documentali e Metadati

La codifica dell'informazione digitale, a differenza di altre, non è mai né autosufficiente né auto-esplicativa, ma deve sempre e necessariamente documentare sé stessa al livello minimo del singolo *atomo* di informazione, aggiungendo al dato/contenuto vero e proprio molte informazioni necessarie per la decodifica, l'identificazione, il recupero, l'accesso e l'uso di ciascun oggetto digitale. Tali informazioni sono dette "metadati".

Ai documenti informatici prodotti o gestiti dal Comune è sempre associato, ai fini della conservazione, almeno il set di metadati previsto dall'allegato n. 5 delle Linee guida AgID. Ai documenti informatici prodotti o gestiti attraverso i software della Siscom sono associati i metadati elencati nel presente allegato.

Elenco delle classi documentali

1. Sono state individuate 15 tipologie documentali denominate:
 1. Registro Giornaliero di Protocollo.
 2. Allegati al Protocollo
 3. Deliberazioni.
 4. Determinazioni.
 5. Ordinanze.
 6. Decreti.
 7. Atti di Liquidazione
 8. Contratti
 9. Contratti liberi (per chi non utilizza la procedura contratti)
 10. Liste elettorali.
 11. Fattura ricevuta PA.
 12. Fattura emessa PA.
 13. Fascicolo Elettorale elettronico.
 14. Documenti Generali
 15. Documenti Fiscali.
 16. Documenti Risorse Umane.
2. Per ognuna di queste è previsto un insieme minimo di metadati elencati nelle tabelle di seguito riportate.

REGISTRO GIORNALIERO DI PROTOCOLLO

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
id_class_s	Indice di classificazione
num_fine_s	Numero fine
num_inizio_s	Numero inizio
oggetto_s	Oggetto
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
modform_s	Modalità di formazione
formid_s	Identificativo del formato
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

ALLEGATI AL PROTOCOLLO

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
oggetto_s	Oggetto
cod_aoo_s	Codice identificativo AOO
num_prot_i	Numero protocollo
data_prot_dt	Data protocollo
classificazione_s	Indice di classificazione
tipo_prot_s	Tipo protocollo
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
modform_s	Modalità di formazione
formid_s	Identificativo del formato
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

DELIBERAZIONI

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
dirigente_s	Dirigente
id_class_s	Indice di classificazione
num_repertorio_s	Numero di repertorio
oggetto_s	Oggetto
responsabile_s	Responsabile procedimento
organo_delib_s	Organo deliberante
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
modform_s	Modalità di formazione
formid_s	Identificativo del formato
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
datregid_s	Dati di registrazione - Id registro
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

DETERMINAZIONI

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
dirigente_s	Dirigente
id_class_s	Indice di classificazione
nr_reg_s	Numero registro particolare
oggetto_s	Oggetto
responsabile_s	Responsabile procedimento
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
modform_s	Modalità di formazione
formid_s	Identificativo del formato
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
datregid_s	Dati di registrazione - Id registro
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

ORDINANZE

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
dirigente_s	Dirigente
id_class_s	Indice di classificazione
nr_reg_s	Numero registro particolare
oggetto_s	Oggetto
responsabile_s	Responsabile procedimento
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
datregid_s	Dati di registrazione - Id registro
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
modform_s	Modalità di formazione
formid_s	Identificativo del formato
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

DECRETI

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
responsabile_s	Responsabile procedimento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
dirigente_s	Dirigente
id_class_s	Indice di classificazione
nr_reg_s	Numero registro particolare
oggetto_s	Oggetto
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
modform_s	Modalità di formazione
formid_s	Identificativo del formato
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
datregid_s	Dati di registrazione - Id registro
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

ATTI DI LIQUIDAZIONE

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
dirigente_s	Dirigente
id_class_s	Indice di classificazione
nr_reg_s	Numero registro particolare
oggetto_s	Oggetto
responsabile_s	Responsabile procedimento
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
modform_s	Modalità di formazione
formid_s	Identificativo del formato
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
datregid_s	Dati di registrazione - Id registro
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

CONTRATTI

Nome Campo Metadato	Descrizione campo Metadato
Importo_registrazione_d	reg_importo
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
contraente_s	Contraente
data_stipula_dt	Data stipula
id_class_s	Indice di classificazione
num_repertorio_s	Numero di repertorio
oggetto_s	Oggetto
reg_data_dt	Data registrazione
reg_num_s	Numero registrazione
reg_serie_s	Serie registrazione
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
modform_s	Modalità di formazione
formid_s	Identificativo del formato
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

CONTRATTI LIBERI

Nome Campo Metadato	Descrizione campo Metadato
Importo_registrazione_d	reg_importo
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
contraente_s	Contraente
data_stipula_dt	Data stipula
id_class_s	Indice di classificazione
num_repertorio_s	Numero di repertorio
oggetto_s	Oggetto
reg_data_dt	Data registrazione
reg_num_s	Numero registrazione
reg_serie_s	Serie registrazione
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
modform_s	Modalità di formazione
formid_s	Identificativo del formato
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

LISTE ELETTORALI

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
destinatario_s	Destinatario
nr_verb_s	Numero verbale
oggetto_s	Oggetto
produttore_s	Soggetto produttore
responsabile_s	Responsabile procedimento
sezzo_s	sezzo
sezione_s	Numero sezione
tipo_s	tipo
tipologia_s	tipologia
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
allegdesc_s	Allegati - Descrizione
modform_s	Modalità di formazione
formid_s	Identificativo del formato
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento
note_s	Note

FATTURE PASSIVE

Nome Campo Metadato	Descrizione campo Metadato
__anno_fiscale_i	Periodo di imposta
__data_documento_dt	Data documento
cig_s	Codice Identificativo Gara
codice_fiscale_emittente_s	Codice fiscale emittente
codice_fiscale_s	Codice Fiscale
codice_pa_s	Codice Ufficio IPA
cup_s	Codice Unitario Progetto
data_protocollo_dt	Data protocollo
denominazione_emittente_s	Denominazione emittente
denominazione_s	Denominazione
identificativoSdi_s	Identificativo univoco dato da SDI
nome_file_sogei_s	Nome file SOGEI
numero_documento_s	Numero documento - Numero Fattura
numero_protocollo_s	Numero protocollo attribuito dal
partita_iva_emittente_s	Partita IVA emittente
partita_iva_s	Partita IVA
token_flusso_s	Parametro interno per identificare il
alleg_i	Allegati - Numero
allegdesc_s	Allegati - Descrizione
cop_b	Verifica conformità copie
datregdata_dt	Dati di registrazione - Data registrazione
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregnum_s	Dati di registrazione - Numero
datregtipreg_s	Dati di registrazione - Tipo registro
firm_b	Verifica firma digitale
formid_s	Identificativo del formato
iddocalg_s	ID doc algoritmo
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
marc_b	Verifica marca temporale
modform_s	Modalità di formazione
ogg_s	Chiave descrittiva Oggetto
sig_b	Verifica sigillo
soggcod_s	Soggetti - Codice
soggnom_s	Soggetti - Nominativo
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
tipdoc_s	Tipologia documentale
vers_i	Versione del documento

FATTURE ATTIVE

Nome Campo Metadato	Descrizione campo Metadato
__anno_fiscale_i	Periodo di imposta
__data_documento_dt	Data documento
__data_inizio_numerazione_dt	Data inizio periodo di imposta
__serie_s	Serie numerazione
alleg_i	Allegati - Numero
allegdesc_s	Allegati - Descrizione
codice_cig_s	Codice CIG
codice_cup_s	Codice CUP
codice_fiscale_emittente_s	Codice fiscale emittente
codice_fiscale_s	Codice fiscale
codice_pa_s	Codice PA
cop_b	Verifica conformità copie
datregdata_dt	Dati di registrazione - Data registrazione
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregnum_s	Dati di registrazione - Numero
datregtipreg_s	Dati di registrazione - Tipo registro
denominazione_emittente_s	Denominazione emittente
denominazione_s	Denominazione
firm_b	Verifica firma digitale
formid_s	Identificativo del formato
iddocalg_s	ID doc algoritmo
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
identificativoSdi_s	Identificativo SDI
marc_b	Verifica marca temporale
modform_s	Modalità di formazione
nome_file_sogei_s	Nome file SOGEI
numero_documento_s	Numero documento
ogg_s	Chiave descrittiva Oggetto
partita_iva_emittente_s	Partita IVA emittente
partita_iva_s	Partita IVA
sig_b	Verifica sigillo
soggcod_s	Soggetti - Codice
soggnom_s	Soggetti - Nominativo
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
tipdoc_s	Tipologia documentale
token_flusso_s	Parametro interno per identificare il
totale_importo_d	Totale importo
vers_i	Versione del documento

FASCICOLO ELETTORALE

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
dest_s	Destinatario
el_cne_s	Cognome e Nome elettore
el_dce_dt	Data di cancellazione elettore
el_dce_s	Data di cancellazione elettore
el_dne_dt	Data di nascita elettore
el_dne_s	Data di nascita elettore
id_class_s	Indice di classificazione
mitt_s	Mittente
num_prot_s	Numero protocollo
prot_data_dt	Data protocollo
oggetto_s	Oggetto
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
modform_s	Modalità di formazione
formid_s	Identificativo del formato
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento

DOCUMENTI GENERALI

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
destinatario_s	Destinatario
oggetto_s	Oggetto
produttore_s	Soggetto produttore
responsabile_s	Responsabile procedimento
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
modform_s	Modalità di formazione
formid_s	Identificativo del formato
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento
note_s	Note

DOCUMENTI FISCALI

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
denominazione_s	Denominazione
codice_fiscale_s	Codice Fiscale
repertorio_i	N. Progressivo
data_prot_dt	Data Protocollo
mitt_s	Mittente
dest_s	Destinatario
_indice_fascicolo_s	Indice Fascicolo
tipo_documento_s	Tipo Documento
partita_iva_s	Partita iva
__anno_fiscale_i	Anno Imposta
mese_fiscale_i	Mese Imposta
tipo_allegato_s	Tipo Documento
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
modform_s	Modalità di formazione
formid_s	Identificativo del formato
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
datregid_s	Dati di registrazione - Id registro
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcd_s	Soggetti - Codice
alleg_i	Allegati - Numero
allegdesc_s	Allegati - Descrizione
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento
note_s	Note

DOCUMENTI RISORSE UMANE

Nome Campo Metadato	Descrizione campo Metadato
__data_documento_dt	Data documento
cod_amm_s	Codice identificativo amministrazione
cod_aoo_s	Codice identificativo AOO
denominazione_s	Denominazione
codice_fiscale_s	Codice Fiscale
data_prot_dt	Data Protocollo
mitt_s	Mittente
dest_s	Destinatario
_indice_fascicolo_s	Indice Fascicolo
tipo_documento_s	Tipo Documento
nominativo_s	Nominativo
__anno_fiscale_i	Anno Imposta
mese_fiscale_i	Mese Imposta
tipo_allegato_s	Tipo Documento
iddocid_s	ID doc identificativo
iddocimp_s	ID doc Impronta
iddocalg_s	ID doc algoritmo
tipdoc_s	Tipologia documentale
datregflusso_s	Dati di registrazione - Tipologia di flusso
datregtipreg_s	Dati di registrazione - Tipo registro
datregdata_dt	Dati di registrazione - Data registrazione
datregnum_s	Dati di registrazione - Numero
datregid_s	Dati di registrazione - Id registro
ogg_s	Chiave descrittiva Oggetto
soggru_s	Soggetti - Ruolo
soggtip_s	Soggetti - Tipo soggetto
soggnom_s	Soggetti - Nominativo
soggcod_s	Soggetti - Codice
alleg_i	Allegati - Numero
allegdesc_s	Allegati - Descrizione
modform_s	Modalità di formazione
formid_s	Identificativo del formato
firm_b	Verifica firma digitale
marc_b	Verifica marca temporale
sig_b	Verifica sigillo
cop_b	Verifica conformità copie
vers_i	Versione del documento
note_s	Note

METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE

L'idAgg:

È una sequenza di caratteri alfanumerici associata in modo univoco all'aggregazione documentale informatica in modo da consentirne l'identificazione, indica se si tratta di un Fascicolo o di una Serie Documentale o di una serie fascicoli.

Il fascicolo è una 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.

Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.

Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

Tipologia fascicolo:

I fascicoli sono organizzati per tipo:

- **Tipo 1 - fascicolo per affare:** conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta.
- **Tipo 2 - fascicolo per persona fisica o giuridica:** comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona (fisica o giuridica). Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.
- **Tipo 3 - fascicolo per attività:** comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.
- **Tipo 4 - fascicolo per procedimento amministrativo:** conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo

Di seguito riportiamo un insieme minimo di metadati elencato nella tabella di seguito riportata.

Nome Campo Metadato	Descrizione campo Metadato
Idagg_soggru_a	Soggetti - Ruolo
Idagg_soggtip_a	Soggetti - Tipo soggetto
Idagg_soggnom_a	Soggetti - Nominativo
Idagg_soggcod_a	Soggetti - Codice
Idagg_sogguor_a	Soggetti - UOR
Idagg_asstip_a	Assegnazione - Tipo assegnazione
Idagg_assru_a	Assegnazione - Ruolo
Idagg_assog_a	Assegnazione - Tipo soggetto
Idagg_asscod_a	Assegnazione - Codice
Idagg_assdatain_a	Assegnazione - Data inizio assegnazione
Idagg_assfin_a	Assegnazione - Data fine assegnazione
Idagg_datap_a	Data apertura
Idagg_classind_a	Classificazione - Indice di classificazione

Idagg_classdescr_a	Classificazione - Descrizione
Idagg_prog_a	Progressivo
Idagg_deskey_a	Chiave descrittiva - Oggetto
Idagg_datch_a	Data chiusura
Idagg_ammproc_a	Procedimento amministrativo - Procedimento
Idagg_ammcatproc_a	Procedimento amministrativo - Catalogo procedimenti
Idagg_ammfasi_a	Procedimento amministrativo - Fasi
Idagg_posdoc_a	Posizione fisica Aggregazione Documentale
Idagg_cons_a	Tempo conservazione



Comune di Ollastra
Provincia di Oristano

Allegato 4
Piano di conservazione, selezione e scarto
Manuale di Conservazione

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 Titolario 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 titolare 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.

Documenti originari 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.

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

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	7
Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia	12
Titolo III. Risorse umane	15
Titolo IV. Risorse finanziarie e patrimoniali	20
Titolo V. Affari legali	24
Titolo VI. Pianificazione e gestione del territorio	25
Titolo VII. Servizi alla persona	29
Titolo VIII. Attività economiche	33
Titolo IX. Polizia locale e sicurezza pubblica	35
Titolo X. Tutela della salute	36
Titolo XI. Servizi demografici	37
Titolo XII. Elezioni e iniziative popolari	39
Titolo XIII. Affari militari	41

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	
	Verbali e deliberazioni della Commissione comunale per la toponomastica: repertorio annuale	Permanente	
3. Statuto			
	Redazione, modifiche e interpretazioni dello statuto	Permanente, dopo sfoltoimento del materiale informativo relativo ad altri Comuni	
4. Regolamenti			
	Regolamenti emessi dal Comune: repertorio annuale	Permanente	
	Redazione dei regolamenti: un fascicolo per ciascun affare	Permanente, previo sfoltoimento 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: fascicolo 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	

	Verballi degli 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 fascicolo per ciascun affare	Permanente, dopo sfolgimento 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 fascicolo per ciascuna definizione dell'organigramma	Permanente	
	Organizzazione degli uffici: un fascicolo 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 fascicolo per ciascuna iniziativa	Permanente	
	Onorificenze (concesse e ricevute): un fascicolo per ciascun evento	Permanente	
	Concessione dell'uso del sigillo: un fascicolo annuale	Permanente	
14. Interventi di carattere politico e umanitario; rapporti istituzionali			
	Iniziative specifiche (ad esempio, adesione a movimenti di opinione): un fascicolo per ciascun affare	Permanente	
	Gemellaggi	Permanente	
	Promozione di comitati: un fascicolo 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 sfoltoimento del carteggio di carattere transitorio	
	Partecipazione del Comune a enti e associazioni (comprensivo della nomina dei rappresentanti)	Permanente, previo sfoltoimento 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			
	Fascicolo personale che dura quanto il mandato	Permanente	
2. Vicesindaco			
	Fascicolo personale che dura quanto il mandato	Permanente	
3. Consiglio			
	Fascicolo personali: un fascicolo 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			
	Fascicolo 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			
	Fascicolo personale	Permanente	
9. Segretario e Vicesegretario			
	Fascicolo personale (nomina, etc.) per la durata dell'incarico	Permanente	
10. Direttore generale e dirigenza			
	Fascicolo personale	Permanente	
11. Revisori dei conti			
	Fascicolo personale	Permanente	
12. Difensore civico			
	Fascicolo personale	Permanente	
13. Commissario <i>ad acta</i>			
	Fascicolo personale	Permanente	
14. Organi di controllo interni			
	Un fascicolo per ogni organo	Permanente	
15. Organi consultivi			
	Un fascicolo per ogni organo	Permanente	
16. Consigli circoscrizionali			
	Fascicolo personali: un fascicolo 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			
	Fascicolo 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 fascicolo per ogni commissione	Permanente	
20. Segretari delle circoscrizioni			
	Fascicolo personale (nomina, etc.) per la durata dell'incarico	Permanente	
21. Commissario <i>ad acta</i> delle circoscrizioni			
	Fascicolo 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 fascicolo con eventuali sottofascicoli	Permanente	
	Procedimenti per il reclutamento del personale: un fascicolo per ciascun procedimento (fascicolo 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 indicazione 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 applicazioni dei contratti collettivi di lavoro	Permanente	
	Determinazione dei ruoli e contratti collettivi	Permanente	NB i contratti con il singolo confluiscono nel fascicolo 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 fascicolo 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 fascicolo 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 fascicolo per ogni obiettivo	Permanente, previo sfoltoimento	
	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 fascicolo per ciascuna variazione	Permanente, previo sfoltoimento	
3. Gestione delle entrate: accertamento, riscossione, versamento			
	Fascicoli personali dei contribuenti comunali: un fascicolo 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 fascicolo per ciascun mutuo	5 anni dall'estinzione del mutuo	
	Proventi da affitti e locazioni: un fascicolo 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 fascicolo per ciascuna partecipazione	Permanente, previo sfoltoimento	
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 fascicolo 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 fascicolo 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 fascicolo 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 fascicolo 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			
	Verballi di rinvenimento: serie annuale repertoriata	2 anni	
	Ricevute di riconsegna ai proprietari: serie annuale repertoriata	2 anni	

	Vendita o devoluzione: un fascicolo 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 fascicolo 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 fascicolo 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 fascicolo 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 fascicolo per ciascun affare	Permanente con sfoltimento	
	Piano Urbano della Mobilità: un fascicolo per ciascun affare	Permanente con sfoltimento	
	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 con sfoltimento	
	Fascicoli relativi alle irregolarità	10 anni	
	Iniziative a favore dell'ambiente	Permanente con sfoltimento	
	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 con sfoltimento	
	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 con sfoltimento	
	Vigilanza sui gestori dei servizi: un fascicolo annuale per attività	Permanente con sfoltimento	
	Fascicoli relativi alle irregolarità	10 anni	

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

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 sfoltimento del carteggio temporaneo 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 fascicolo per scuola	2 anni	
	Gestione buoni pasto degli iscritti alle scuole: un fascicolo per periodo	2 anni	
	Verbalì del comitato genitori per la mensa	3 anni	
	Azioni di promozione e sostegno del diritto allo studio: un fascicolo per intervento	5 anni	
	Gestione mense scolastiche: un fascicolo per mensa scolastica e per periodo	10 anni	
	Integrazione di neo-immigrati e nomadi: un fascicolo per intervento	10 anni	
	Gestione trasporto scolastico: un fascicolo per periodo e per tratta	2 anni	
2. Asili nido e scuola materna			
	Domande di ammissione agli asili nido e alle scuole materne: un fascicolo per asilo/scuola	2 anni	
	Graduatorie di ammissione	2 anni	

	Funzionamento. degli asili e delle scuole materne: un fascicolo per struttura	10 anni	
3. Promozione e sostegno delle istituzioni di istruzione e della loro attività			
	Iniziative specifiche: un fascicolo 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 fascicolo per iniziativa	10 anni	
5. Istituti culturali			
	Funzionamento delle diverse istituzioni culturali: un fascicolo per istituto	Permanente	
	Verbali degli organi di gestione degli Istituti culturali	Permanente	
6. Attività ed eventi culturali			
	Attività ordinarie annuali: un fascicolo per attività e per periodo)	10 anni	
	Eventi culturali: un fascicolo per evento	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
	Feste civili e/o religiose: un fascicolo per iniziativa	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative culturali. un fascicolo per iniziativa	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 10 anni	
	Prestiti di beni culturali: un fascicolo per affare	Permanente	
7. Attività ed eventi sportivi			

	Eventi e attività sportive: un fascicolo per evento/attività	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 5 anni	
8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale			
	Piano sociale: un fascicolo annuale eventualmente organizzato in sotto fascicolo.	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 5 anni	
	Programmazione per settori: un fascicolo per ciascun settore	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 5 anni	
	Accordi con i differenti soggetti: un fascicolo per ciascun soggetto	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 5 anni	
9. Prevenzione, recupero e reintegrazione dei soggetti a rischio			
	Campagne di prevenzione: un fascicolo per campagna	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 5 anni	
	Interventi di recupero e reintegrazione dei soggetti a rischio: un fascicolo per intervento	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 5 anni	
	Ricognizione dei rischi: un fascicolo per affare	Permanente, previo sfoltoimento del carteggio temporaneo e strumentale dopo 5 anni	
10. Informazione, consulenza ed educazione civica			

	Funzionamento e attività delle strutture (consultori, informagiovani, etc.): un fascicolo per struttura	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative di vario tipo: un fascicolo 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 fascicolo per intervento.	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
12. Assistenza diretta e indiretta, benefici economici			
	Funzionamento e attività delle strutture: un fascicolo annuale per ciascuna struttura	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative specifiche: un fascicolo per ciascuna iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
13. Attività ricreativa e di socializzazione			
	Funzionamento e attività delle strutture (colonie, centri ricreativi, etc.): un fascicolo annuale per ciascuna struttura	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative specifiche: un fascicolo per ciascuna iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
14. Politiche per la casa			
	Assegnazione degli alloggi: un fascicolo per bando, organizzato in sottofascicoli: - bando - domande - graduatoria	permanente 5 anni permanente	

	- assegnazione	5 anni	
	Fascicolo degli assegnatari: un fascicolo per assegnatario	5 anni dopo la scadenza del contratto	In assenza di contenzioso
15. Politiche per il sociale			
	Iniziative specifiche: un fascicolo per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	

Titolo VIII. Attività economiche

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli individuali degli esercenti attività economiche: un fascicolo per persona	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
1. Agricoltura e pesca			
	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Dichiarazioni raccolta e produzione: un fascicolo per periodo	5 anni	
2. Artigianato			
	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Autorizzazioni artigiane: repertorio	Permanente	
3. Industria			

	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfortimento del carteggio temporaneo e strumentale dopo 5 anni	
4. Commercio			
	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfortimento del carteggio temporaneo e strumentale dopo 5 anni	
	Comunicazioni dovute: un fascicolo per periodo	1 anno	
	Autorizzazioni commerciali: repertorio	Permanente	
5. Fiere e mercati			
	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfortimento del carteggio temporaneo e strumentale dopo 5 anni	
6. Esercizi turistici e strutture ricettive			
	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfortimento del carteggio temporaneo e strumentale dopo 5 anni	
	Autorizzazioni turistiche: repertorio	Permanente	
7. Promozione e servizi			
	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfortimento del carteggio 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 fascicolo per iniziativa	5 anni	
	Corsi di educazione stradale nelle scuole: un fascicolo per corso	5 anni	
2. Polizia stradale			
	Direttive e disposizioni: un fascicolo annuale	Permanente	
	Organizzazione del servizio di pattugliamento: un fascicolo annuale	3 anni	
	Verballi 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 fascicolo per accertamento	5 anni	
	Verballi 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 fascicolo annuale	Permanente	
	Gestione veicoli rimossi: un fascicolo per ciascun veicolo	2 anni	
3. Informative			
	Informative su persone residenti nel Comune: un fascicolo per ciascuna persona	5 anni	
4. Sicurezza e ordine pubblico			
	Direttive e disposizioni generali: un fascicolo annuale	Permanente	
	Servizio ordinario di pubblica sicurezza: un fascicolo annuale	5 anni	
	Servizio straordinario di pubblica sicurezza, in caso di eventi particolari (manifestazioni, concerti, etc.): un fascicolo per evento	5 anni	
	Autorizzazioni di pubblica sicurezza: repertorio annuale, organizzata in sottoserie	Permanente	
	Fascicoli dei richiedenti l'autorizzazione di pubblica sicurezza: un fascicolo per richiedente	5 anni	
	Verballi 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 fascicolo per ciascun evento	Permanente	
	Misure di igiene pubblica: un fascicolo per ciascun affare	Permanente	
	Interventi di derattizzazione, dezanarizzazione etc.: un fascicolo per ciascun intervento	1 anno	
	Trattamenti fitosanitari e di disinfestazione: un fascicolo per ciascun intervento	1 anno	
	Autorizzazioni sanitarie: repertorio annuale	Permanente	
	Fascicoli dei richiedenti autorizzazioni sanitarie: un fascicolo per ciascuna persona/ditta	5 anni dalla cessazione dell'attività	
	Concessioni di agibilità: repertorio annuale	Permanente	
	Fascicoli dei richiedenti l'agibilità: un fascicolo per ciascun richiedente	Permanente	
2. Trattamenti Sanitari Obbligatori			
	TSO: un fascicolo per ciascun procedimento	Permanente	
	ASO: un fascicolo per ciascun procedimento	Permanente	
	Fascicoli personali dei soggetti a trattamenti: un fascicolo per ciascuna persona	Permanente	
3. Farmacie			
	Istituzione di farmacie: un fascicolo per ciascuna farmacia	Permanente	
	Funzionamento delle farmacie: un fascicolo per ciascun periodo (anno o mese)	2 anni	
4. Zooprofilassi veterinaria			
	Fascicolo relativi a epizootie (epidemie animali): un fascicolo per ciascun evento	Permanente	
5. Randagismo animale e ricoveri			

	Gestione dei ricoveri e degli eventi connessi: un fascicolo 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 fascicolo per ciascun procedimento	10 anni	
	Comunicazione dei nati all'Agenzia per le entrate: un fascicolo per ciascun periodo	1 anno	
2. Anagrafe e certificazioni			
	APR 4: iscrizioni anagrafiche: un fascicolo per ciascuna persona	Permanente	
	AIRE: un fascicolo per ciascuna persona	Permanente	
	Richieste certificati: un fascicolo per ciascun periodo (mese o anno)	1 anno	
	Corrispondenza con altre amministrazioni per rilascio e trasmissione documenti: un fascicolo 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 fascicolo 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 fascicolo per ciascuna persona	10 anni	Salvo esigenze particolari
	Cancellazioni: un fascicolo per ciascuna persona	10 anni	Salvo esigenze particolari
	Carteggio con la Corte d'appello per la formazione degli Albi dei giudici popolari: un fascicolo 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 fascicolo 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	
	Fascicolo personali degli elettori: un fascicolo 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 fascicolo 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	

	Verbali 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 fascicolo 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 fascicolo per ciascun procedimento	Permanente	
4. Requisizioni per utilità militari			
	Procedimenti specifici: un fascicolo per ciascun procedimento	Permanente	



Comune di Ollastra
Provincia di Oristano

Allegato

Piano di Sicurezza Relativo alla Formazione, alla Gestione, alla Trasmissione, all'Interscambio, all'Accesso ai Documenti Informatici

Manuale di Conservazione

Premessa

Il presente Piano di Sicurezza è adottato ai sensi dell'art. 3.4 e 3.9 delle LG AgID “sulla formazione, gestione e conservazione dei documenti informatici”;

Il responsabile della gestione documentale è preposto al servizio di cui all'articolo 61 del TUDA e, d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale di cui all'art. 17 del CAD e acquisito il parere del responsabile della protezione dei dati personali di cui, agli artt. 37 “Designazione del responsabile della protezione dei dati” e 39 “Compiti del Responsabile della protezione dei dati” del Regolamento UE 679/2016, predispone:

- il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione.

Tale manuale conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:

- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.

Il comune di Ollastra ha implementato le misure minime di sicurezza ICT (*Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015*) emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017.

Il comune di Ollastra ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR), anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso prevede opportune misure tecniche e organizzative per garantire un livello di sicurezza *adeguato* al rischio in materia di protezione dei dati personali.

In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è eventualmente delegata la tenuta del sistema di gestione informatica dei documenti sono individuati come Responsabili del trattamento dei dati e devono presentare (in fase di procurement) garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Piano di Sicurezza

Il piano di sicurezza, si basa sui risultati dell'analisi dei rischi cui sono esposti i dati (personali, particolari e/o giudiziari), e/o i documenti trattati, esso definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno del Comune di Ollastra;
- le modalità di accesso al Sistema di Gestione Informatica dei Documenti;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza e alle misure adeguate al rischio calcolato per ciascun trattamento dati effettuato;
- la formazione dei dipendenti;
- le modalità con le quali viene effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza adottate.

Tale Piano di Sicurezza è soggetto a revisione con cadenza annuale; a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche, potrà essere modificato anticipatamente.

Elementi di rischio cui sono soggetti i documenti informatici

I principali elementi di rischio individuati cui sono soggetti i documenti informatici e i dati trattati con l'ausilio delle tecnologie informatiche sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al Sistema di Gestione Informatica dei Documenti (SGID) o come accesso ai documenti, dati e unità archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati, includendo a tale proposito tutti i dati presenti sul Sistema di Gestione Informatica dei Documenti;
- perdita dei documenti e dei dati contenuti nel Sistema;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con il trattamento dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, il Comune di Ollastra adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Sicurezza e misure adottate per la protezione della rete Comunale

Firewall e VPN: nella LAN della sede Comunale è installato un sistema firewall come protezione perimetrale relativo alla messa in sicurezza delle comunicazioni Untrusted (non affidabili) che avvengono tra l'esterno della rete (tipicamente Internet/Extranet) ed il resto dell'infrastruttura.

Le comunicazioni che avvengono all'interno dell'organizzazione e l'accesso ai computer sono attuate tramite l'adozione di un Server di dominio di Active Directory (gestisce l'autenticazione e le autorizzazioni di accesso al dato) inoltre è stato implementato un sistema di Antivirus centralizzato.

Da un punto di vista generale, qualsiasi accesso esterno alla rete comunale può costituire una minaccia, tuttavia, la necessità di avere costantemente a disposizione i dati, anche quando non è possibile fisicamente accedere al sistema informativo dall'interno, impone l'utilizzo di tecnologie in grado di fornire un accesso diretto ai sistemi interni attraverso una connessione dati, da qualsiasi punto del mondo ed indipendentemente dall'orario locale, per questa ragione l'accesso esterno alla rete LAN avviene esclusivamente previo passaggio autenticato su VPN (Virtual Private Network).

Il sistema gestionale Siscom è in cloud qualificato ACN presente al link: <https://www.acn.gov.it/portale/w/sa-143>, questo permette di avere una adeguata sicurezza non avendo più nessuna banca dati in locale.

Accesso al Sistema di Gestione Informatica da parte di utenti interni all'AOO

L'accesso al Sistema di Gestione Informatica dei Documenti, da parte degli utenti interni all'AOO, avviene attraverso l'utilizzo di credenziali di autenticazione. L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al livello di riservatezza degli stessi.

Le credenziali di autenticazione consistono in un codice (User-Id), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (Password), conosciuta solamente dal medesimo; tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione/autenticazione, il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente, memorizzando, ai fini di controllo, l'User-Id corrispondente, ma non la Password dello stesso.

Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della Password; quest'ultima è composta da almeno dieci caratteri, tra cui lettere maiuscole e minuscole, almeno un numero e un carattere speciale e non contiene riferimenti agevolmente riconducibili al titolare.

La Password deve essere modificata dall'incaricato al suo primo utilizzo e, successivamente, con cadenza trimestrale. L'User-Id non può essere assegnato a nessun altro incaricato per nessuna motivazione. Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica; tali credenziali sono altresì disattivate anche nel caso di perdita della qualità (intesa come efficacia sulla sicurezza) che consente all'incaricato l'accesso ai dati personali.

Nel comune di Ollastra il compito di gestire le credenziali d'accesso è affidato all'Amministratore di Sistema, lo stesso AdS non è in grado di conoscere la Password dell'utente; qualora l'utente dimenticasse la propria Password esso stesso procederà ad effettuare un password recovery.

Accesso al trattamento di dati personali comuni, particolari o giudiziari e politiche di sicurezza previste

L'accesso ai documenti contenenti dati personali, sensibili o giudiziari e ai dati medesimi avviene per mezzo dell'individuazione di specifici profili di autorizzazione, stabiliti sulla base del livello di riservatezza di ciascun documento, fascicolo, sotto fascicolo o inserto, tali profili, per ciascun autorizzato o per classi omogenee di autorizzati, sono individuati e configurati anteriormente

all'inizio del trattamento.

Periodicamente, e comunque con cadenza almeno annuale, deve essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Gli autorizzati al trattamento di dati personali, particolari o giudiziari non devono lasciare incustodita e accessibile la propria postazione di lavoro durante il trattamento degli stessi.

Ai fini del trattamento dei dati personali, sensibili o giudiziari, agli autorizzati sono state impartite istruzioni scritte da parte del Responsabile per il trattamento dei dati personali, relative alle modalità delle operazioni, del controllo e della custodia di atti e documenti. Questo avviene sia per i dati nativi digitali, svolto per mezzo di strumenti elettronici, che per quelli ricevuti ed archiviati in forma cartacea, le suddette istruzioni avvengono con cadenza almeno annuale.

I suddetti documenti cartacei sono controllati e custoditi dagli autorizzati del trattamento per tutto il tempo di svolgimento dei relativi compiti, trascorso il quale provvederanno alla restituzione; nell'arco di tale periodo gli autorizzati si assicureranno che a tali documenti non accedano persone prive di autorizzazione.

L'accesso agli archivi contenenti dati particolari o giudiziari è consentito solo previa autorizzazione; le persone ammesse sono identificate e registrate.

Sicurezza delle registrazioni nel sistema di gestione documentale

Eventuali modifiche autorizzate, vengono registrate per mezzo di log di sistema che mantengano traccia dell'autore, della modifica effettuata, nonché della data e dell'ora; il Sistema mantiene leggibile la precedente versione dei dati, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione.

I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano imm modificabili e non eliminabili; l'accesso ad essi, da parte degli utenti interni all'AOO, avviene soltanto attraverso il Sistema medesimo, previa la suddetta procedura di identificazione informatica e nel rispetto dei profili di autorizzazione di ciascun utente.

Il Sistema consente l'attuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il Sistema effettua, inoltre, il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il Sistema e tutti i documenti e/o dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici dannosi in quanto il Comune di Ollastra si impegna a rendere ragionevolmente sicuri gli accessi al Sistema e tutti i documenti e dati in esso contenuti.

Ai fini di ridurre la vulnerabilità dei sistemi informativi, i sistemi operativi utilizzati dall'AOO per l'accesso ai dati ed il Sistema di Gestione Informatica dei Documenti, vengono costantemente tenuti aggiornati, per mezzo dell'installazione degli aggiornamenti (patch) periodici che i fornitori rendono disponibili.

Backup e ripristino dell'accesso ai dati

Il comune di Ollastra avendo il sistema primario di gestione dei dati in cloud qualificato, non ha più in casa i Backup dei dati, questo garantisce una maggior sicurezza ed anche dei costi minori nella gestione degli stessi, il livello di sicurezza è garantito dal contratto stipulato tra l'Ente e la Software house, la quale viene, sempre per contratto, individuata come Responsabile del trattamento e deve garantire la Continuità del Servizio come da clausole contrattuali.

La stessa Software House garantisce un piano di Disaster Recovery che è stato preventivamente accettato tra le parti.

Per il trattamento di dati che non avviene mediante il Cloud (cartelle condivise tra gli uffici), è stato incaricato l'AdS di implementare tutte le misure adeguate a evitare l'accesso non desiderato di persone non autorizzate, a tal fine i dati sono stati sottoposti a crittografia e solo le persone autorizzate possono accedervi tramite ulteriore pwd che decrittografa il contenuto.

Trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno del Comune di Ollastra avviene esclusivamente per mezzo del Sistema di Gestione Informatica dei Documenti; nessun'altra modalità è consentita, al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati. La trasmissione di documenti informatici al di fuori del Comune avviene tramite PEC o mediante i meccanismi dell'interoperabilità e della cooperazione applicativa di cui al Sistema Pubblico di Connettività, utilizzando le informazioni contenute nella segnatura di protocollo. I messaggi di posta elettronica certificata prodotti del Comune sono compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045 e 2049 e successive modificazioni.

Piani formativi del personale

In conformità a quanto disposto dalle LG AgID, ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, l'Ente predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del Sistema di Gestione Informatica dei Documenti;
- fascicolazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione in materia di protezione dei dati personali;

Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

L'Amministrazione comunale ha nominato l'amministratore di Sistema in conformità al Provvedimento Generale dell'Autorità Garante per la Protezione dei dati personali: "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente

alle attribuzioni delle funzioni di amministratore di sistema", del 27 novembre 2008), la stessa amministrazione può controllare periodicamente i log di sistema dell'AdS e li mantiene per 6 mesi, al fine di verificare eventuali violazioni del Sistema.

Il Responsabile della gestione documentale insieme al Responsabile della Conservazione, al DPO ed al Responsabile per la Transizione al Digitale del Comune effettuano periodiche verifiche sul corretto funzionamento del Sistema di Gestione Informatica dei Documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale.

Piano di violazione dei Dati (data breach)

Il comune di Ollastra ha implementato il piano di violazione dei dati (data breach) in ottemperanza a quanto previsto degli artt. 33-34 del Regolamento UE 679/201640, è stato redatto nell'ambito del piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente e permette di includere e registrare nel dettaglio tutti gli elementi della violazione, corrispondenti a quelli che il Garante per la Protezione dei Dati Personali richiede a fini di notifica.

Il piano prevede i seguenti passaggi da compiere in caso di violazione dei dati:

1. Registrazione del "nome" e della "data" dell'avvenuta violazione;
2. Riporta la persona individuata per la registrazione dell'evento;
3. Riporta eventuali ulteriori titolari del trattamento coinvolti (oltre il comune);
4. Riporta la descrizione dell'evento e tipo di violazione, indicare la modalità con le quali si è venuti a conoscenza della violazione
5. Indica l'eventuale causa della violazione;
6. Riporta Descrizione della violazione;
7. Indica il numero (anche approssimativo) di interessati coinvolti nella violazione;
8. Indica le categorie di soggetti a cui si riferiscono i dati personali coinvolti nell'evento di violazione;
9. Riporta le categorie di dati coinvolti;
10. Specifica i potenziali effetti negativi per gli interessati;
11. Indica se la violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo;
12. Descrive l'area di impatto (Integrità, Riservatezza e Disponibilità);
13. Riporta una descrizione delle possibili conseguenze della violazione;
14. Descrive le misure di sicurezza adottate al momento della violazione;
15. Descrive le misure di sicurezza adottate successivamente alla violazione al fine di contenere la medesima;
16. Descrive una valutazione della gravità;
17. Indica se l'incidente è stato notificato o comunicato;
18. Riporta una descrizione delle ragioni e delle modalità relative alla notifica o comunicazione della violazione oppure relative alla mancata notifica o comunicazione della medesima.

Se si dovesse verificare una violazione o presunta tale, la persona che ne viene a conoscenza deve immediatamente avvisare il referente privacy che provvederà in urgenza a contattare il DPO.

RICHIESTA DI EROGAZIONE DEI SERVIZI DOCFLY CONSERVAZIONE SOSTITUTIVA E FATTURAZIONE ELETTRONICA - TITOLARE

Il/La sottoscritto/a, Nome Oswaldo Cognome Congiu
C.F. CNGSLD70C20G043X nella sua qualità di titolare, legale rappresentante o soggetto delegato della
Comune di Ollastra con sede in Via G.M. Angioy, 25 CAP
09088 Comune Ollastra () C.F. azienda 80005470952 P.IVA 00475880951
email info@comune.ollastra.or.it in ragione del contratto di fornitura dei Servizi DocFly Conservazione Sostitutiva e Fatturazione
protocollo@pec.comunediolllastra.it
Elettronica concluso con il PARTNER di Aruba Pec S.p.A. Siscom S.p.A., con la
sottoscrizione del presente atto, nella sua qualità di Titolare dell'oggetto di Conservazione (di seguito anche Titolare)

CHIEDE

alla società Aruba Pec S.p.A l'erogazione dei Servizi DocFly Conservazione Sostitutiva e Fatturazione Elettronica come previsti dal contratto di fornitura e

DICHIARA

di essere munito dei necessari poteri per impegnare la ditta/società/ente quivi indicato come Titolare dell'oggetto di Conservazione sottoscrivendo il presente atto ed i relativi allegati e di accettare integralmente, sempre con la sottoscrizione della presente richiesta dopo averne presa espressa ed attenta visione, le Condizioni di Erogazione dei Servizi DocFly Conservazione sostitutiva e Fatturazione Elettronica – Titolare versione 3.6 con gli altri documenti ivi richiamati e quindi in dettaglio:

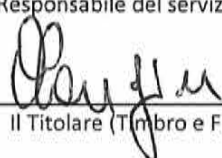
- Scheda Prodotto DocFly – Conservazione, Titolare;
- Scheda Prodotto Fatturazione Elettronica, Titolare;
- Manuale della Conservazione;
- Informativa privacy Aruba Pec S.p.A. – disponibile al link http://www.pec.it/Policy_Privacy.aspx;
- Scheda di conservazione;
- Elenco Persone¹.

La suddetta documentazione forma e disciplina il "Contratto" avente ad oggetto l'erogazione dei Servizi DocFly Titolare. Sempre ai fini dell'erogazione dei Servizi DocFly avvalendosi delle facoltà previste dal Contratto, il sottoscritto

NOMINA E DELEGA

la società Aruba PEC S.p.A., con sede legale in Ponte San Pietro (BG), Via San Clemente n. 53, assegnataria del codice fiscale e numero di iscrizione al Registro Imprese: 01879020517, indirizzo e-mail - conservazione@arubapec.it, nr. Telefono: +390575/0500 "Responsabile del servizio di conservazione" dei documenti informatici della tipologia riportata nelle Schede di conservazione allegata al Contratto, secondo quanto ivi previsto ed a norma di quanto riportato all'art. 22 delle Condizioni di erogazione Servizi DocFly Conservazione sostitutiva e Fatturazione Elettronica – Titolare ("Nomina di Aruba PEC a Responsabile del servizio di conservazione").

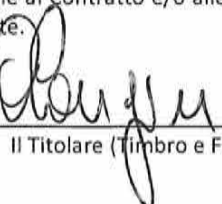
Luogo Ollastra, data 19.12.2023


Il Titolare (Timbro e Firma)



Ai sensi e per gli effetti degli art. 1341 e 1342 c.c., il Sottoscritto dichiara di aver preso chiara ed esatta visione e di approvare espressamente ed in modo specifico le seguenti clausole delle Condizioni di erogazione Servizi DocFly Conservazione sostitutiva e Fatturazione Elettronica Titolare versione 3.6: 2) Struttura del Contratto e ordine di prevalenza; 3) Oggetto del Contratto; 4) Perfezionamento del Contratto; 5) Attivazione del Servizio; 6) Durata del Contratto e cessazione; 7) Obblighi e limitazioni di responsabilità di Aruba Pec; 8) Obblighi e diritti del Titolare; 9) Servizio: modalità di utilizzo, configurazione assistenza e manutenzione; 10) Sospensione del Servizio; 11) Clausola risolutiva espressa; 12) Recesso; 13) Modifiche al Contratto e/o alle Policy Aruba Pec; 16) Miscellanea; 17) SLA e indennizzi; 18) Ultrattività; 21) Legge applicabile e foro competente.

Luogo Ollastra, data 19.12.2023


Il Titolare (Timbro e Firma)



¹ Questo documento può essere compilato online se è previsto dalla procedura del Servizio in questione.

Il Sottoscritto dichiara di aver preso visione dell'informativa fornita da Aruba PEC S.p.A., ai sensi dell'art. 13 del Regolamento UE 2016/679 richiamata all'art. 19 delle Condizioni di erogazione sopra indicate e pubblicata al link <https://www.pec.it/partner-documentazione.aspx>,

Fermo quanto sopra ai fini dell'erogazione dei Servizi DocFly, il sottoscritto nella sua qualità di legale rappresentante del Titolare, tra quelli sopra menzionati, compila, sottoscrive e consegna al Partner, affinché li consegni ad Aruba Pec S.p.A, quando previsto dal Contratto, i seguenti documenti:

- Scheda di conservazione;
- Elenco Persone;

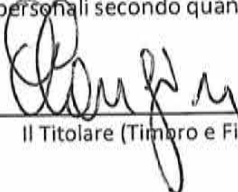
Luogo Ollastra, data 19.12.2023


Il Titolare (Timbro e Firma)



☐ dichiara di accettare integralmente i contenuti delle Condizioni di Erogazione sopra indicate, facendoli propri in ogni sua parte, e di nominare Aruba PEC S.p.a. Responsabile del trattamento dei dati personali secondo quanto previsto dall'art. 20 del documento sopra indicato.

Luogo Ollastra, data 19.12.2023


Il Titolare (Timbro e Firma)



☐ **DELEGA FATTURA**

In relazione all'Opzione **Fatturazione Elettronica**, il sottoscritto nella sua qualità di legale rappresentante del Titolare delega Aruba Pec all'emissione della fattura ed all'apposizione della firma digitale sulla medesima, secondo quanto previsto dal Contratto o ad inoltrare al Titolare le rispettive fatture, se passive. A tal proposito il sottoscritto prende atto e dichiara che rimangono a suo carico, in via esclusiva, tutte le responsabilità in sede civile, penale ed amministrativa in relazione al contenuto delle Fatture emesse, trasmesse o ricevute da e verso la Pubblica Amministrazione o i privati interessati attraverso il Sistema di Interscambio e per l'effetto, si impegna, ora per allora, a manlevare e tenere indenne Aruba Pec da qualsiasi pretesa di terzi o conseguenza pregiudizievole che possa comunque alla stessa derivare dal compimento delle attività delegate.

RICHIESTA DI EROGAZIONE SERVIZI DOCFLY CONSERVAZIONE SOSTITUTIVA E FATTURAZIONE ELETTRONICA - TITOLARE

Il/La sottoscritto/a, Nome Oswaldo Cognome Congiu C.F. _____
CNGSLD70C20G043X Indirizzo Via G.M. Angioy, 25
Cap 09088 Comune Ollastra (OR) E-Mail info@comune.ollastra.or.it

in ragione del contratto di fornitura dei **Servizi DocFly** Conservazione sostitutiva e Fatturazione Elettronica concluso con il PARTNER di Aruba Pec S.p.A. **Siscom spa**, con l'accettazione presente atto, nella sua qualità di **TITOLARE** dell'oggetto di Conservazione (di seguito anche Titolare)

CHIEDE

alla società Aruba Pec S.p.A l'erogazione dei Servizi DocFly Conservazione sostitutiva e Fatturazione Elettronica.
A tal proposito

DICHIARA

di essere munito dei necessari poteri per impegnare la ditta/società/ente quivi indicato come Titolare accettando il presente atto ed i relativi allegati.

Sempre ai fini dell'erogazione dei Servizi DocFly avvalendosi delle facoltà previste dal Contratto, il sottoscritto

NOMINA E DELEGA

la società Aruba PEC S.p.A., con sede legale in Ponte San Pietro (BG), Via San Clemente n. 53, assegnataria del codice fiscale e numero di iscrizione al Registro Imprese: 01879020517, indirizzo e-mail - conservazione@arubapec.it, nr. Telefono: 0575/0500, "Responsabile del servizio di conservazione" dei documenti informatici della tipologia riportata nelle Schede di conservazione allegate al Contratto, secondo quanto ivi previsto ed a norma di quanto riportato all'art. 22 delle Condizioni di erogazione Servizi DocFly Conservazione sostitutiva e Fatturazione Elettronica - Titolare vers. 3.7 ("Nomina di Aruba PEC a Responsabile del servizio di conservazione").

Ai sensi e per gli effetti degli art. 1341 e 1342 c.c., il Sottoscritto dichiara di aver preso chiara ed esatta visione e di approvare espressamente ed in modo specifico le seguenti clausole delle Condizioni di erogazione Servizi Docfly Conservazione sostitutiva e Fatturazione Elettronica - Titolare vers. 3.7: 2) Struttura del Contratto e cessazione; 3) Oggetto del Contratto; 4) Perfezionamento del Contratto; 5) Attivazione del Servizio; 6) Durata del Contratto e cessazione; 7) Obblighi e limitazioni di responsabilità di Aruba Pec e/o del Partner; 8) Obblighi e diritti del Titolare; 9) Servizio: modalità di utilizzo, configurazione assistenza e manutenzione; 10) Sospensione del Servizio; 11) Clausola risolutiva espressa; 12) Recesso; 13) Modifiche al Contratto e/o alle Policy Aruba Pec; 16) Miscellanea; 17) SLA e indennizzi; 18) Ultrattività; 21) Legge applicabile e foro competente.

DELEGA FATTURA

In relazione all'Opzione Fatturazione Elettronica, il sottoscritto nella sua qualità di titolare o legale rappresentante o soggetto delegato del Titolare delega Aruba Pec all'emissione della fattura ed all'apposizione della firma digitale sulla medesima, secondo quanto previsto dal Contratto o ad inoltrare al Titolare le rispettive fatture, se passive. A tal proposito il sottoscritto prende atto e dichiara che rimangono a suo carico, in via esclusiva, tutte le responsabilità in sede civile, penale ed amministrativa in relazione al contenuto delle Fatture emesse, trasmesse o ricevute da e verso la Pubblica Amministrazione o i privati interessati attraverso il Sistema di interscambio e per l'effetto, si impegna, ora per allora, a manlevare e tenere indenne Aruba Pec da qualsiasi pretesa di terzi o conseguenza pregiudizievole che possa comunque alla stessa derivare dal compimento delle attività delegate.

NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

in applicazione del "Regolamento (UE) 2016/679" ai sensi e per gli effetti degli artt. 4, 1° comma n. 8 e 28

Comune di Ollastra _____, con sede e domicilio fiscale in Ollastra _____ (____),
Via G.M. Angioy _____ n. 25 _____ ed assegnatario del codice fiscale 80005470952 _____,
in persona del Sindaco pro tempore _____ Sig. Osvaldo Congiu _____, munito di
tutti i necessari poteri per la firma del presente atto, in qualità di Titolare del trattamento, come previsto dall'art. 4 del
Regolamento (UE) 2016/679, di seguito, per brevità, definito "Titolare del trattamento";

- preso atto che l'art. 4, comma 1, numero 8 del suddetto Regolamento definisce quale *"responsabile del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*;
- considerato che è stato con Voi stipulato, ed è tuttora in corso di validità, il Contratto per l'erogazione del servizio di conservazione digitale di documenti informatici di cui il Cliente Partner è Titolare e/o Produttore, di seguito per brevità chiamato anche *"Contratto"*, perfezionatosi tra il sottoscritto Titolare del trattamento e la società ARUBA PEC Spa;
- considerato che il perfezionamento del Contratto di cui al punto precedente comporta la necessità di trattare, in nome e per conto del suddetto Titolare, dati personali che, come tali, sono soggetti all'applicazione
- del Regolamento (UE) 2016/679 (di seguito anche "Regolamento UE");

NOMINA

La società **ARUBA PEC S.P.A.**, in appresso denominata anche "**Aruba PEC**", con sede legale in Ponte San Pietro (BG), 24036, Via San Clemente n 53, C.F. e P.IVA 01879020517, iscritta al Registro delle Imprese di Bergamo REA BG-445886, **Responsabile esterno del Trattamento dei dati**, in relazione al trattamento dei dati personali effettuato in occasione dell'erogazione dei servizi di cui al Contratto. Pertanto Aruba PEC effettuerà il trattamento dei dati personali in qualità di Responsabile esterno del trattamento (ai sensi dell'art. 4, 1° comma n. 8 del Regolamento UE) ed il Cliente opererà in qualità di Titolare del trattamento dei dati personali (ai sensi dell'art. 4, primo comma, n. 7 del Regolamento UE).

Ciascuna parte osserverà gli obblighi ad essa applicabili ai sensi del Regolamento UE e della legislazione nazionale applicabile in relazione al trattamento dei dati personali del Cliente.

In particolare il Responsabile è tenuto al rispetto dei compiti e degli oneri impartiti dal Titolare, come di seguito specificati, per tutta la durata del Contratto e sino all'eventuale ulteriore termine se previsto.

Per effetto della predetta nomina, Aruba PEC è autorizzata esclusivamente al trattamento dei dati personali nella misura e nei limiti necessari all'esecuzione delle attività ad essi assegnate. Aruba PEC ha il potere di compiere tutte le attività necessarie per assicurare il rispetto delle vigenti disposizioni in materia nonché il compito di organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali ad essi comunicati dai Titolari ai fini dell'esecuzione delle attività oggetto del presente Servizio. In conformità a quanto prescritto dal Regolamento EU e dalla legislazione nazionale applicabile relativamente ai dati personali ed alle modalità di trattamento, si precisa che è dovere di Aruba PEC:

- trattare i dati personali soltanto per l'esecuzione dei Servizi oggetto del Contratto, con le caratteristiche tecniche e di sicurezza stabilite sulla base di quanto previsto nello stesso, nei Manuali e negli appositi Allegati Tecnici che li disciplinano, che ai fini del presente articolo devono intendersi quale documentazione contenente le istruzioni di trattamento dei dati che il Cliente accetta. Nel caso in cui il Cliente manifesti necessità particolari che richiedano un trattamento diverso rispetto a quanto descritto nella documentazione sopra richiamata, deve manifestare tale necessità ad Aruba PEC e descrivere le misure che richiede vengano implementate, le quali verranno quotate con una specifica offerta;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure richieste ai sensi dell'articolo 32 del Regolamento EU;
- rispettare le condizioni di cui ai paragrafi 2 e 4 del Regolamento EU per ricorrere a un altro responsabile del trattamento;
- assistere il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile;
- assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento EU, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti;

h) mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consentire e contribuire alle attività di revisione, previo accordo sui tempi e sulle modalità di dette verifiche e purché le stesse non contrastino con obblighi di riservatezza assunti da Aruba e con le policy della medesima Aruba. I costi di tali verifiche saranno a carico del Titolare.

Nel caso in cui Aruba PEC si avvalga della collaborazione di Incaricati per lo svolgimento delle attività sopra descritte, provvede alla loro assegnazione specifica al trattamento dando loro le istruzioni necessarie e rendendoli edotti delle modalità convenute e di quelle prescritte dal Regolamento EU e della legislazione nazionale applicabile. Aruba PEC, pertanto, effettua il trattamento dei dati nel rispetto delle istruzioni sopra riportate, delle indicazioni del Manuale che disciplina il Servizio, degli eventuali allegati e delle prescrizioni contenute nel Regolamento EU e nella legislazione nazionale applicabile, nonché nel rispetto dei requisiti di sicurezza stabiliti per l'erogazione dei singoli servizi. Nel caso in cui si verificano situazioni anomale o di emergenza, Aruba PEC avviserà immediatamente il Titolare.

Il Titolare del Trattamento nulla più pretenderà rispetto a quanto previsto nel presente atto di nomina e considererà assolto l'adempimento da parte del Responsabile esterno del trattamento con l'applicazione delle procedure sopra indicate. Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Ollastra, li 19.12.2023

Il Cliente Partner



ELENCO PERSONE CLIENTE

Ruolo	Titolare dell'oggetto di Conservazione		
Ragione sociale	COMUNE DI OLLASTRA		
Partita iva	00475880951	Codice Fiscale	80005470952

Di seguito l'elenco delle persone designate dal Cliente ad operare in suo nome, conto e interesse con Aruba Pec per l'esecuzione del contratto in funzione del ruolo:

Ruolo	Responsabile della Conservazione / Delegato ¹	Riceve tutte le notifiche del processo di conservazione
Cognome e Nome Incaricato/Ragione Sociale	Carrau Nazzarena	
Codice Fiscale/Partita IVA	CRRNZR78M52G113U	
Indirizzo PEC	protocollo@pec.comunediol्लाstra.it	
Indirizzo e-mail	demografici@comune.ollastra.or.it	

Ruolo	Responsabile Produttore dei Pacchetti di Versamento	Riceve tutte le notifiche del processo di versamento
Selezionare se uguale a	☒ Responsabile della Conservazione / Delegato	
Cognome e Nome incaricato		
Codice Fiscale		
Indirizzo PEC		
Indirizzo e-mail		

Ai sensi del presente modulo si intende per:

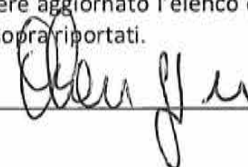
- **Responsabile della Conservazione:** il Titolare del servizio, od il soggetto dal medesimo nominato, il quale ha facoltà di affidare a terzi, in tutto o in parte, l'esecuzione delle attività previste a suo carico dalla vigente normativa. Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia;
- **Responsabile Produttore dei Pacchetti di Versamento:** la 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. Qualora il Cliente sia una Pubblica Amministrazione, il Produttore dei pacchetti di versamento si identifica con il responsabile della gestione documentale;

Il Cliente dichiara che i suddetti soggetti sono stati dallo stesso valutati come persone esperte ed affidabili ed in grado di interagire autonomamente con Aruba Pec ed il sistema di conservazione dalla stessa fornito.

Il Cliente dichiara inoltre di aver sottoscritto con i suddetti soggetti un accordo volto far rispettare quanto previsto dal Contratto inclusi i relativi allegati, e che i medesimi a loro volta hanno dichiarato ed accettato di essere informati circa il contenuto dei richiamati documenti e di conoscere quanto previsto dalla Normativa regolante la conservazione di documenti informatici ivi inclusa quella relativa alla privacy. Il Cliente si assume la responsabilità in ordine all'operato dei suddetti soggetti impegnandosi a manlevare e/o tenere indenne Aruba Pec da ogni e qualsiasi responsabilità per eventuali richieste danni, diretti o indiretti, da chiunque avanzate per fatti imputabili a detti soggetti. Il Cliente si obbliga a tenere aggiornato l'elenco dei suddetti incaricati nonché a comunicare tempestivamente ad Aruba ogni variazione rispetto ai dati sopra riportati.

Luogo Ollastra Data 19.12.2023

Firma (timbro)



Scheda conservazione – Documento amministrativo informatico

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

Dati identificativi	Cognome, nome o ragione sociale	Codice fiscale o partita IVA
Archivio Cliente	Comune di Ollastra	80005470952 - 00475880951

Definizione Documenti											
Classe Documentale	Formati Accettati						Anno di conservazione	Verifica sull'apposizione della Firma Digitale ¹	Verifica sulla validità della Firma Digitale ²	Firma Massiva	Username Firma
	Previsti dalla Normativa e idonei alla conservazione		Previsti dalla Normativa e NON idonei alla conservazione		Altri Formati non previsti dalla normativa ¹						
atti, provvedimenti e verbali	PDF	PDF/A	[selezione]	[selezione]	[selezione]	[selezione]	99	NO	NO	NO	[Username]
	XML	EML	[selezione]	[selezione]	[selezione]	[selezione]					
	ZIP	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
contratti	PDF	PDF/A	[selezione]	[selezione]	[selezione]	[selezione]	99	NO	NO	NO	[Username]
	XML	EML	[selezione]	[selezione]	[selezione]	[selezione]					
	ZIP	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
registri	PDF	PDF/A	[selezione]	[selezione]	[selezione]	[selezione]	99	NO	NO	NO	[Username]
	XML	EML	[selezione]	[selezione]	[selezione]	[selezione]					
	ZIP	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
comunicazioni	PDF	PDF/A	[selezione]	[selezione]	[selezione]	[selezione]	99	NO	NO	NO	[Username]
	XML	EML	[selezione]	[selezione]	[selezione]	[selezione]					
	ZIP	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					

METADATI

METADATI OBBLIGATORI PREVISTI DA NORMATIVA

Elenco dei metadati previsti da normativa, la cui compilazione è obbligatoria in fase di formazione del documento informatico. Presenti nell'Indice di Versamento (IPdV) e nell'Indice di Conservazione (IdC) in valorizzati.

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Modalità di formazione	NO	NO
Oggetto Documento	SI	NO
Nome del documento	NO	NO
Segnatura ⁴	NO	NO
Dati di registrazione		
Tipologia di flusso	NO	NO
Tipo registro	NO	NO
Data registrazione del protocollo	SI	NO
Numero Protocollo	SI	NO
Codice registro ⁵	NO	NO

1 Selezionando "SI", verranno accettati solo documenti firmati con firma digitale. Selezionando "NO", verranno accettati anche documenti non firmati.

2 Selezionando "SI", verranno accettati solo documenti con firma digitale valida al momento dell'invio presso il sistema di conservazione (in caso di marca temporale valida, la verifica della firma verrà fatta alla data della marca). La verifica della validità della firma è possibile solo se si è selezionato "SI" nella "verifica sull'apposizione della firma". Selezionando "NO", verranno accettati anche documenti con firma non valida o scaduta, con le limitazioni di responsabilità e con le obbligazioni descritte nelle Condizioni di erogazione Servizi DocFly Conservazione Sostitutiva e Fatturazione Elettronica.

3 Per gli altri formati, non potrà essere garantita la disponibilità nel tempo di un visualizzatore del file: i documenti versati con tali estensioni verranno pertanto accettati da Aruba alle Condizioni di erogazione Servizi DocFly Conservazione Sostitutiva e Fatturazione Elettronica.

4 SI, nel caso di documento protocollato.

5 SI, nel caso in cui il tipo registro sia protocollo ordinario/protocollo emergenza, o Repertorio/Registro.

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
<i>Soggetti</i>		
Ruolo Autore⁶	NO	NO
Tipo soggetto	NO	NO
<i>Se persona fisica valorizzare:</i>		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Organizzazione valorizzare:</i>		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Amministrazioni Pubbliche Italiane valorizzare:</i>		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento	NO	NO
<i>Se Amministrazioni Pubbliche estere valorizzare:</i>		
Denominazione Amministrazione	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Ruolo Mittente⁶	NO	NO
Tipo soggetto	NO	NO
<i>Se persona fisica valorizzare:</i>		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Organizzazione valorizzare:</i>		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Amministrazioni Pubbliche Italiane valorizzare:</i>		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento	NO	NO
<i>Se Amministrazioni Pubbliche estere valorizzare:</i>		
Denominazione Amministrazione	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Ruolo Operatore⁷	NO	NO
Tipo soggetto	NO	NO
Cognome	NO	NO
Nome	NO	NO

⁶ Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.

⁷ Sì, solo nel caso in cui venga compilato il metadato "Tracce di modifica documento".

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Soggetti		
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Amministrazione che effettua la registrazione	NO	NO
Tipo soggetto	NO	NO
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Allegati		
Numero Allegati	NO	NO
Id Doc Allegati ⁸	NO	NO
Descrizione Allegati ⁸	NO	NO
Identificativo del formato		
Formato	NO	NO
Prodotto Software	NO	NO
Prodotto Software_Nome prodotto	NO	NO
Prodotto Software_Versione prodotto	NO	NO
Prodotto Software_Produttore	NO	NO
Verifica		
Firmato digitalmente ⁹	NO	NO
Sigillato elettronicamente ⁹	NO	NO
Marcatura temporale ⁹	NO	NO
Conformità copie immagine su supporto informatico ¹⁰	NO	NO
Tracciatura modifiche documento		
Tipo modifica ¹¹	NO	NO
Soggetto autore della modifica ¹¹	NO	NO
Data modifica/Ora modifica ¹¹	NO	NO
IdDoc versione precedente ¹¹	NO	NO
Altri dati		
Riservato	NO	NO
Identificativo Documento Primario ¹²	NO	NO
Versione del documento	NO	NO
Documenti contenuti nel procedimento	SI	NO

8 Se numero allegati > 0.

9 SI, obbligatorio nel caso di modalità di formazione doc = a/b.

10 SI, obbligatorio nel caso di modalità di formazione doc = b.

11 Nel caso di versione > 1 o in caso di annullamento.

12 SI, nel caso in cui sia presente un documento primario.

METADATI PREVISTI DA NORMATIVA NON OBBLIGATORI		
Elenco dei metadati previsti da normativa, la cui COMPILAZIONE NON È OBBLIGATORIA IN FASE DI FORMAZIONE del documento informatico. Presenti nell'Indice di Versamento (IPdV) o nell'Indice di Conservazione (IdC) se valorizzati		
Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Classificazione		
Indice di classificazione	NO	NO
Descrizione classificazione	NO	NO
Piano di classificazione	NO	NO
Soggetti		
Ruolo Assegnatario	NO	NO
Tipo soggetto	NO	NO
Cognome (non obbligatorio)	NO	NO
Nome (non obbligatorio)	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR	NO	NO
Indirizzo digitali di riferimento	NO	NO
Ruolo Destinatario	NO	NO
Tipo soggetto	NO	NO
Se persona fisica valorizzare:		
Nome	NO	NO
Cognome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Se Organizzazione valorizzare:		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
Se Amministrazioni Pubbliche italiane valorizzare:		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento	NO	NO
Se Amministrazioni Pubbliche estere valorizzare:		
Denominazione Amministrazione	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Ruolo Produttore	NO	NO
Tipo soggetto	NO	NO
Denominazione sistema	NO	NO
Ruolo Responsabile della Gestione Documentale	NO	NO
Tipo soggetto	NO	NO
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Responsabile del Servizio di Protocollo	NO	NO
Tipo soggetto	NO	NO

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Classificazione		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Responsabile Unico del Procedimento	NO	NO
Tipo soggetto	NO	NO
Cognome	NO	NO
Nome	NO	NO
Codice Fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione /Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR	NO	NO
Indirizzi digitali di riferimento	NO	NO
Ruolo Amministrazione titolare	NO	NO
Tipo soggetto	NO	NO
Denominazione Amministrazione /Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Ruolo Amministrazione partecipanti	NO	NO
Tipo soggetto	NO	NO
Se Amministrazioni Pubbliche italiane valorizzare:		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Se Amministrazioni Pubbliche estere valorizzare:		
Denominazione Amministrazione	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Altri dati		
Parole chiave	NO	NO
Tempo di conservazione	NO	NO
Numero documento	NO	NO
Materia\ Argomento\ Struttura procedimento	NO	NO
Data di registrazione ¹³	NO	NO
Soggetto Produttore ¹³	NO	NO
Destinatario ¹³	NO	NO
Soggetto Mittente ¹³	NO	NO
Amministrazione titolare del procedimento ¹³	NO	NO
Amministrazioni partecipanti ¹³	NO	NO
AOO di riferimento ¹³	NO	NO
Responsabile del procedimento ¹³	NO	NO
Oggetto del procedimento ¹³	NO	NO

¹³ Metadati che garantiscono la retrocompatibilità con il passato.

INFORMAZIONI AGGIUNTIVE, NON PREVISTE DA NORMATIVA		
Elenco di metadati aggiuntivi disponibili, valorizzazione non obbligatoria Presenti nell'Indice di Versamento (IPdV) e nell'Indice di Conservazione (IdC) se valorizzati		
Identificazione del Sistema versante	Identificativo del documento nel sistema di origine	Applicativo di produzione del documento
Livello di riservatezza	Condizioni di accesso	Codice fiscale del titolare del certificato di firma
ID fascicolo	ID pacchetto di versamento	Numero di altra registrazione
Serie	Data di altra registrazione	Registro
Repertorio	Classificazione Archivistica	Ufficio produttore
Esistenza di originale analogico	Identificativo della unità archivistica	Annotazione
Annesso	Note 1	Note 2
Allegato 1	Allegato 2	

EXTRAINFO AGGIUNTIVE[illegible]

NOTE:

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

Altresì, con la sottoscrizione del presente documento, il Cliente concede ad Aruba PEC, in via temporanea, per la durata del Contratto ed a titolo gratuito, i diritti di proprietà intellettuale necessari al regolare svolgimento delle prestazioni previste nel Contratto medesimo, senza che ciò faccia scaturire alcun obbligo per Aruba PEC e ferma restando la titolarità di detta proprietà intellettuale in capo al Cliente.

Luogo Ollastra Data 19.12.2023

Firma (timbro)

Manifestazione del consenso al trattamento dei dati personali

Il sottoscritto dichiara di aver preso attenta visione dell'Informativa resa da Aruba S.p.A. ed Aruba PEC S.p.a. ai sensi dell'Art. 13 del Regolamento (UE) n. 2016/679 ("GDPR") e disponibile al link https://www.aruba.it/informativa_arubaspa.pdf, e di rilasciare il proprio consenso al trattamento dei dati personali per le finalità ivi indicate finalizzate alla corretta esecuzione delle obbligazioni contrattuali. Il Cliente dichiara, altresì, di essere consapevole che in mancanza di rilascio del consenso a tale trattamento potranno trovare applicazione le disposizioni indicate nella predetta Informativa.

Luogo Ollastra Data 19.12.2023

Firma (timbro)

Scheda conservazione – Documento Fiscale

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

Dati Identificativi	Cognome, nome o ragione sociale	Codice fiscale o partita IVA
Archivio Cliente	Comune di Ollastra	80005470952 - 00475880951

Definizione Documenti											
Classe Documentale	Formati Accettati						Anno di conservazione si consiglia di inserire almeno 10 anni	Verifica sull'apposizione della Firma Digitale ¹	Verifica sulla validità della Firma Digitale ²	Firma Massiva	Username Firma
	Previsti dalla Normativa e idonei alla conservazione		Previsti dalla Normativa e NON idonei alla conservazione		Altri Formati non previsti dalla normativa ³						
fattura pa	XML	ZIP	[selezione]	[selezione]	[selezione]	[selezione]	15				[Username]
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]		NO	NO	NO	
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
notifica pa	XML	ZIP	[selezione]	[selezione]	[selezione]	[selezione]	15				[Username]
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]		NO	NO	NO	
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
[Inserisci TIPO 3]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[Inserisci anno]				[Username]
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]		[selezione]	[selezione]	[selezione]	
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
[Inserisci TIPO 4]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[Inserisci anno]				[Username]
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]		[selezione]	[selezione]	[selezione]	
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					
	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]	[selezione]					

1

METADATI

METADATI OBBLIGATORI PREVISTI DA NORMATIVA

Elenco dei metadati previsti da normativa, la cui compilazione è obbligatoria in fase di formazione del documento informatico. Presenti nell'Indice di Versamento (IPdV) o nell'Indice di Conservazione (IdC) se valorizzati.

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Modalità di formazione	NO	NO
Oggetto Documento	SI	NO
Nome del documento	NO	NO
Dati di registrazione		
Tipologia di flusso	NO	NO
Tipo registro	NO	NO
Data registrazione	NO	NO
Numero Documento	NO	NO
Codice registro ⁴	NO	NO

¹ Selezionando "SI", verranno accettati solo documenti firmati con firma digitale. Selezionando "NO", verranno accettati anche documenti non firmati.

² Selezionando "SI", verranno accettati solo documenti con firma digitale valida al momento dell'invio presso il sistema di conservazione (in caso di marca temporale valida, la verifica della firma verrà fatta alla data della marca). La verifica della validità della firma è possibile solo se si è selezionato "SI" nella "verifica sull'apposizione della firma". Selezionando "NO", verranno accettati anche documenti con firma non valida o scaduta, con le limitazioni di responsabilità e con le obbligazioni descritte nelle Condizioni di erogazione Servizi DocFly Conservazione Sostitutiva e Fatturazione Elettronica.

³ Per gli altri formati, non potrà essere garantita la disponibilità nel tempo di un visualizzatore del file: i documenti versati con tali estensioni verranno pertanto accettati da Aruba alle Condizioni di erogazione Servizi DocFly Conservazione Sostitutiva e Fatturazione Elettronica.

⁴ SI, nel caso in cui il tipo registro sia protocollo ordinario/protocollo emergenza, o Repertorio/Registro.

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Soggetti		
Ruolo Autore⁵	NO	NO
Tipo soggetto	NO	NO
<i>Se persona fisica valorizzare:</i>		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Organizzazione valorizzare:</i>		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Amministrazioni Pubbliche Italiane valorizzare:</i>		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (non obbligatorio)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Amministrazioni Pubbliche estere valorizzare:</i>		
Denominazione Amministrazione	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Mittente⁶		
Tipo soggetto	NO	NO
<i>Se persona fisica valorizzare:</i>		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Organizzazione valorizzare:</i>		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Amministrazioni Pubbliche Italiane valorizzare:</i>		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Amministrazioni Pubbliche estere valorizzare:</i>		
Denominazione Amministrazione (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Operatore⁶	NO	NO
Tipo soggetto	NO	NO
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Allegati		
Numero Allegati	NO	NO
Id Doc Allegati ⁷	NO	NO

⁵ Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.

⁶ Sì, solo nel caso in cui venga compilato il metadato "Tracce/modifica documento".

⁷ Se numero allegati > 0.

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Allegati		
Descrizione Allegati ⁷	NO	NO
Identificativo del formato		
Formato	NO	NO
Prodotto Software	NO	NO
Prodotto Software_Nome prodotto	NO	NO
Prodotto Software_Versione prodotto	NO	NO
Prodotto Software_Produttore	NO	NO
Verifica		
Firmato digitalmente ⁸	NO	NO
Sigillato elettronicamente ⁹	NO	NO
Marcatura temporale ⁸	NO	NO
Conformità copie immagine su supporto informatico ⁹	NO	NO
Tracciatura modifiche documento		
Tipo modifica ¹⁰	NO	NO
Soggetto autore della modifica ¹¹	NO	NO
Data modifica/Ora modifica ¹¹	NO	NO
IdDoc versione precedente ¹¹	NO	NO
Altri dati		
Riservato	NO	NO
Identificativo Documento Primario ¹¹	NO	NO
Versione del documento	NO	NO

METADATI PREVISTI DA NORMATIVA NON OBBLIGATORI

Elenco dei metadati previsti da normativa, la cui compilazione non è obbligatoria in fase di formazione del documento informatico. Presenti nell'Indice di Versamento (IPdV) e nell'Indice di Conservazione (IdC) se Valorizzati

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Classificazione		
Indice di classificazione	NO	NO
Descrizione classificazione	NO	NO
Piano di classificazione	NO	NO
Soggetti		
Ruolo Assegnatario	NO	NO
Tipo soggetto	NO	NO
Cognome (non obbligatorio)	NO	NO
Nome (non obbligatorio)	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Organizzazione	NO	NO
Denominazione Ufficio	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Destinatario	NO	NO
Tipo soggetto	NO	NO
Se persona fisica valorizzare:		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Se Organizzazione valorizzare:		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO

8 Sì, obbligatorio nel caso di modalità di formazione doc = a/b.

9 Sì, obbligatorio nel caso di modalità di formazione doc = b.

10 Nel caso di versione > 1 o in caso di annullamento.

11 Sì, nel caso in cui sia presente un documento primario.

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Soggetti		
<i>Se Amministrazioni Pubbliche Italiane valorizzare:</i>		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Amministrazioni Pubbliche estere valorizzare:</i>		
Denominazione Amministrazione (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Produttore	NO	NO
Tipo soggetto	NO	NO
Denominazione sistema	NO	NO
Ruolo Responsabile della Gestione Documentale	NO	NO
Tipo soggetto	NO	NO
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Responsabile del Servizio di Protocollo	NO	NO
Tipo soggetto	NO	NO
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Soggetto che effettua la registrazione	NO	NO
Tipo soggetto	NO	NO
<i>Se persona fisica valorizzare:</i>		
Nome	NO	NO
Cognome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Organizzazione valorizzare:</i>		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Altro	NO	NO
Tipo soggetto	NO	NO
<i>Se persona fisica valorizzare:</i>		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Organizzazione valorizzare:</i>		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
<i>Se Amministrazioni Pubbliche Italiane valorizzare:</i>		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Soggetti		
<i>Se Amministrazioni Pubbliche estere valorizzare:</i>		
Denominazione Amministrazione (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Altri dati		
Parole chiave	NO	NO
Tempo di conservazione	NO	NO
Soggetto Produttore ¹²	NO	NO
Destinatario ¹²	NO	NO
Data documento tributario ¹²	NO	NO
Soggetto Tributario ¹²	NO	NO

INFORMAZIONI AGGIUNTIVE, NON PREVISTE DA NORMATIVA

Elenco di metadati aggiuntivi disponibili, valorizzazione non obbligatoria
Presenti nell'Indice di Versamento (IPdV) e nell'Indice di Conservazione (IdC) se valorizzati

Soggetto Produttore	Destinatario	Identificazione del Sistema versante
Identificativo del documento nel sistema di origine	Applicativo di produzione del documento	Livello di riservatezza
Condizioni di accesso	Codice fiscale del titolare del certificato di firma	
ID fascicolo	ID pacchetto di versamento	Note 1
Note 2	Allegato 1	Allegato 2
Nota Accredito	Ddt	Codice Tipologia
Soggetto Imposta	Nome Sezionale	Sezionale
Numero Fattura	Tipologia	Progressivo

¹² Metadati che garantiscono la retrocompatibilità con il passato

EXTRAINFO AGGIUNTIVE[illegible]

NOTE:

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

Altri, con la sottoscrizione del presente documento, il Cliente concede ad Aruba PEC, in via temporanea, per la durata del Contratto ed a titolo gratuito, i diritti di proprietà intellettuale necessari al regolare svolgimento delle prestazioni previste nel Contratto medesimo, senza che ciò faccia scaturire alcun obbligo per Aruba PEC e ferma restando la titolarità di detta proprietà intellettuale in capo al Cliente.

Luogo Ollastra Data 19.12.2023

Firma (timbro)

[Handwritten signature]



Manifestazione del consenso al trattamento dei dati personali

Il sottoscritto dichiara di aver preso attenta visione dell'Informativa resa da Aruba S.p.A. ed Aruba PEC S.p.a. ai sensi dell'Art. 13 del Regolamento (UE) n. 2016/679 ("GDPR") e disponibile al link https://www.aruba.it/informativa_arubasp.pdf, e di rilasciare il proprio consenso al trattamento dei dati personali per le finalità ivi indicate finalizzate alla corretta esecuzione delle obbligazioni contrattuali. Il Cliente dichiara, altresì, di essere consapevole che in mancanza di rilascio del consenso a tale trattamento potranno trovare applicazione le disposizioni indicate nella predetta Informativa.

Luogo Ollastra Data 19.12.2023

Firma (timbro)

Don J



Scheda conservazione – Registro giornaliero di protocollo

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

Dati identificativi Archivio Cliente	Cognome, nome o ragione sociale Comune di Ollastra	Codice fiscale o partita IVA 80005470952 - 00475880951
---	---	---

Definizione Documenti											
Classe Documentale	Formati Accettati						Anno di conservazione	Verifica sull'apposizione della Firma Digitale ¹	Verifica sulla validità della Firma Digitale ²	Firma Massiva	Username Firma
	Previsti dalla Normativa e idonei alla conservazione		Previsti dalla Normativa e NON idonei alla conservazione		Altri Formati non previsti dalla normativa ¹						
Registro Giornaliero di Protocollo	PDF	PDF/A	[seleziona]	[seleziona]	[seleziona]	[seleziona]	gg	NO	NO	NO	{Username}
	JPG	TIFF	[seleziona]	[seleziona]	[seleziona]	[seleziona]					
	XML	DOCX	[seleziona]	[seleziona]	[seleziona]	[seleziona]					
	EML	ZIP	[seleziona]	[seleziona]	[seleziona]	[seleziona]					
	[seleziona]	[seleziona]	[seleziona]	[seleziona]	[seleziona]	[seleziona]					

METADATI

METADATI OBBLIGATORI PREVISTI DA NORMATIVA		
Elenco dei metadati previsti da normativa, la cui COMPILAZIONE È OBBLIGATORIA IN FASE DI FORMAZIONE del documento informatico Presenti nell'Indice di Versamento (IPdV) e nell'Indice di Conservazione (IdC) se valorizzati		
Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Modalità di formazione	NO	NO
Oggetto Documento	SI	NO
Nome del documento	NO	NO
Segnatura ⁴	NO	NO
Dati di registrazione		
Tipologia di flusso	NO	NO
Tipo registro	NO	NO
Data registrazione del protocollo	SI	NO
Numero Protocollo	SI	NO
Codice identificativo del registro	SI	NO
Numero progressivo del registro ⁵	SI	NO
Soggetti		
Ruolo Autore ⁶	NO	NO
Tipo soggetto	NO	NO
Se persona fisica valorizzare:		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Se Organizzazione valorizzare:		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO

1 Selezionando "SI", verranno accettati solo documenti firmati con firma digitale. Selezionando "No", verranno accettati anche documenti non firmati.

2 Selezionando "SI", verranno accettati solo documenti con firma digitale valida al momento dell'invio presso il sistema di conservazione (in caso di marca temporale valida, la verifica della firma verrà fatta alla data della marca). La verifica della validità della firma è possibile solo se si è selezionato "SI" nella "verifica sull'apposizione della firma". Selezionando "No", verranno accettati anche documenti con firma non valida o scaduta, con le limitazioni di responsabilità e con le obbligazioni descritte nelle Condizioni di erogazione Servizi DocFly Conservazione Sostitutiva e Fatturazione Elettronica.

3 Per gli altri formati, non potrà essere garantita la disponibilità nel tempo di un visualizzatore dei file: i documenti versati con tali estensioni verranno pertanto accettati da Aruba alle Condizioni di erogazione Servizi DocFly Conservazione Sostitutiva e Fatturazione Elettronica.

4 SI, nel caso di documento protocollato.

5 SI, nel caso in cui il tipo registro sia protocollo ordinario/protocollo emergenza, o Repertorio/Registro.

6 Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Soggetti		
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
Se Amministrazioni Pubbliche italiane valorizzare:		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento	NO	NO
Se Amministrazioni Pubbliche estere valorizzare:		
Denominazione Amministrazione	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento	NO	NO
Ruolo Mittente⁶	NO	NO
Tipo soggetto	NO	NO
Se persona fisica valorizzare:		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicata l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicata l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
Se Organizzazione valorizzare:		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatorio)	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
Se Amministrazioni Pubbliche italiane valorizzare:		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Se Amministrazioni Pubbliche estere valorizzare:		
Denominazione Amministrazione	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento	NO	NO
Ruolo Operatore⁷	NO	NO
Tipo soggetto	NO	NO
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicata l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicata l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Amministrazione che effettua la registrazione		
Tipo soggetto	NO	NO
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzo digitali di riferimento	NO	NO
Allegati		
Numero Allegati	NO	NO
Id Doc Allegati ⁸	NO	NO

⁷ Sì, solo nel caso in cui venga compilato il metadato "Tracciatore modifica documento".
⁸ Se numero allegati > 0.

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
<i>Allegati</i>		
Descrizione Allegati ⁹ :	NO	NO
<i>Identificativo del formato</i>		
Formato	NO	NO
Prodotto Software	NO	NO
Prodotto Software_Nome prodotto	NO	NO
Prodotto Software_Versione prodotto	NO	NO
Prodotto Software_Produttore	NO	NO
<i>Verifica</i>		
Firmato digitalmente ⁹	NO	NO
Sigillato elettronicamente ⁹	NO	NO
Marcatura temporale ⁹	NO	NO
Conformità copie immagine su supporto informatico ¹⁰	NO	NO
<i>Tracciatura modifiche documento</i>		
Tipo modifica ¹¹	NO	NO
Soggetto autore della modifica ¹¹	NO	NO
Data modifica/Ora modifica ¹¹	NO	NO
IdDoc versione precedente ¹¹	NO	NO
<i>Altri dati</i>		
Riservato	NO	NO
Identificativo Documento Primario ¹²	NO	NO
Versione del documento	NO	NO
Documenti contenuti nel procedimento	SI	NO

⁹ SI, obbligatorio nel caso di modalità di formazione doc = a/b.

¹⁰ SI, obbligatorio nel caso di modalità di formazione doc = b.

¹¹ Nel caso di versione > 1 o in caso di annullamento.

¹² SI, nel caso in cui sia presente un documento primario.

METADATI PREVISTI DA NORMATIVA NON OBBLIGATORI

Elenco dei metadati previsti da normativa, la cui COMPILAZIONE NON È OBBLIGATORIA IN FASE DI FORMAZIONE del documento informatico. Presenti nell'Indice di Versamento (IPdV) e nell'Indice di Conservazione (IdC) se valorizzati

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Classificazione		
Indice di classificazione	NO	NO
Descrizione classificazione	NO	NO
Piano di classificazione	NO	NO
Soggetti		
Ruolo Assegnatario		
Tipo soggetto	NO	NO
Cognome (non obbligatoria)	NO	NO
Nome (non obbligatoria)	NO	NO
Codice fiscale (non obbligatoria)	NO	NO
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR	NO	NO
Indirizzo digitali di riferimento	NO	NO
Ruolo Destinatario		
Tipo soggetto	NO	NO
Se persona fisica valorizzare:		
Nome	NO	NO
Cognome	NO	NO
Codice fiscale (non obbligatoria)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatoria)	NO	NO
Indirizzi digitali di riferimento (non obbligatoria)	NO	NO
Se Organizzazione valorizzare:		
Denominazione Organizzazione	NO	NO
Codice fiscale/partita IVA (non obbligatoria)	NO	NO
Denominazione Ufficio (non obbligatoria)	NO	NO
Indirizzo digitali di riferimento (non obbligatoria)	NO	NO
Se Amministrazioni Pubbliche Italiane valorizzare:		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR (non obbligatoria)	NO	NO
Indirizzo digitali di riferimento	NO	NO
Se Amministrazioni Pubbliche estere valorizzare:		
Denominazione Amministrazione	NO	NO
Denominazione Ufficio (non obbligatoria)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Ruolo Produttore		
Tipo soggetto	NO	NO
Denominazione sistema	NO	NO
Ruolo Responsabile della Gestione Documentale		
Tipo soggetto	NO	NO
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatoria)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatoria)	NO	NO
Indirizzi digitali di riferimento (non obbligatoria)	NO	NO
Ruolo Responsabile del Servizio di Protocollo		
Tipo soggetto	NO	NO

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
Classificazione		
Cognome	NO	NO
Nome	NO	NO
Codice fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione/Codice IPA (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione AOO/Codice IPA AOO (obbligatorio solo se si è indicato l'AOO o l'UOR)	NO	NO
Denominazione Amministrazione UOR/Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento (non obbligatorio)	NO	NO
Ruolo Responsabile Unico del Procedimento		
Tipo soggetto	NO	NO
Cognome	NO	NO
Nome	NO	NO
Codice Fiscale (non obbligatorio)	NO	NO
Denominazione Amministrazione /Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR	NO	NO
Indirizzi digitali di riferimento	NO	NO
Ruolo Amministrazione titolare		
Tipo soggetto	NO	NO
Denominazione Amministrazione /Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Ruolo Amministrazione partecipanti		
Tipo soggetto	NO	NO
Se Amministrazioni Pubbliche italiane valorizzare:		
Denominazione Amministrazione/Codice IPA	NO	NO
Denominazione Amministrazione AOO /Codice IPA AOO	NO	NO
Denominazione Amministrazione UOR /Codice IPA UOR (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Se Amministrazioni Pubbliche estere valorizzare:		
Denominazione Amministrazione	NO	NO
Denominazione Ufficio (non obbligatorio)	NO	NO
Indirizzi digitali di riferimento	NO	NO
Altri dati		
Parole chiave	NO	NO
Tempo di conservazione	NO	NO
Numero documento	NO	NO
Materia\ Argomento\ Struttura procedimento	NO	NO
Data di registrazione ¹³	NO	NO
Soggetto Produttore ¹³	NO	NO
Destinatario ¹³	NO	NO
Soggetto Mittente ¹³	NO	NO
Amministrazione titolare del procedimento ¹³	NO	NO
Amministrazioni partecipanti ¹³	NO	NO
AOO di riferimento ¹³	NO	NO
Responsabile del procedimento ¹³	NO	NO
Oggetto del procedimento ¹³	NO	NO
Codice identificativo amministrazione (IPA)	NO	NO
Anno	NO	NO
Numero prima registrazione effettuata sul registro	NO	NO
Numero ultima registrazione effettuata sul registro	NO	NO

¹³ Metadati che garantiscono la retrocompatibilità con il passato.

Nome	Obbligatorio inserire il TAG all'interno dell'IPdV se inviato dal cliente	Controllo del Servizio sulla presenza di valorizzazione
<i>Altri dati</i>		
Data prima registrazione effettuata sul registro	NO	NO
Data ultima registrazione effettuata sul registro	NO	NO
Denominazione dell'amministrazione	NO	NO
Cognome soggetto produttore 2	NO	NO
Nome soggetto produttore 2	NO	NO
Codice fiscale soggetto produttore 2	NO	NO
Cognome responsabile gestione documentale	NO	NO
Nome responsabile gestione documentale	NO	NO
Codice fiscale responsabile gestione documentale	NO	NO

INFORMAZIONI AGGIUNTIVE, NON PREVISTE DA NORMATIVA

Elenco di metadati aggiuntivi disponibili, valorizzazione non obbligatoria
 Presenti nell'Indice di Versamento (IPdV) e nell'Indice di Conservazione (IdC) se valorizzati

Identificazione del Sistema versante	Identificativo del documento nel sistema di origine	Applicativo di produzione del documento
Livello di riservatezza	Condizioni di accesso	Codice fiscale del titolare del certificato di firma
ID fascicolo	ID pacchetto di versamento	Numero di altra registrazione
Serie	Data di altra registrazione	Registro
Repertorio	Classificazione Archivistica	Ufficio produttore
Esistenza di originale analogico	Identificativo della unità archivistica	Annotazione
Annesso	Note 1	Note 2
Allegato 1	Allegato 2	

6

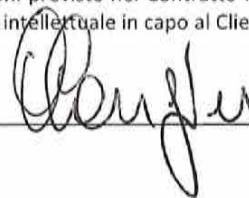
NOTE:

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

Altresì, con la sottoscrizione del presente documento, il Cliente concede ad Aruba PEC, in via temporanea, per la durata del Contratto ed a titolo gratuito, i diritti di proprietà intellettuale necessari al regolare svolgimento delle prestazioni previste nel Contratto medesimo, senza che ciò faccia scaturire alcun obbligo per Aruba PEC e ferma restando la titolarità di detta proprietà intellettuale in capo al Cliente.

Luogo Ollastra Data 19.12.2023

Firma (timbro)

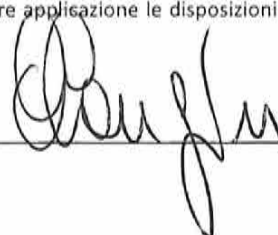


Manifestazione del consenso al trattamento dei dati personali

Il sottoscritto dichiara di aver preso attenta visione dell'Informativa resa da Aruba S.p.A. ed Aruba PEC S.p.A. ai sensi dell'Art. 13 del Regolamento (UE) n. 2016/679 ("GDPR") e disponibile al link https://www.aruba.it/informativa_arubaspa.pdf, e di rilasciare il proprio consenso al trattamento dei dati personali per le finalità ivi indicate finalizzate alla corretta esecuzione delle obbligazioni contrattuali. Il Cliente dichiara, altresì, di essere consapevole che in mancanza di rilascio del consenso a tale trattamento potranno trovare applicazione le disposizioni indicate nella predetta Informativa.

Luogo Ollastra Data 19.12.2023

Firma (timbro)




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>	<i>44</i>
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>	<i>45</i>
7.5.2	<i>Gestione dei Pacchetti di Archiviazione non validi o non completi</i>	<i>45</i>
7.5.3	<i>Rettifica dei pacchetti di archiviazione</i>	<i>45</i>
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>	<i>46</i>
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>	<i>47</i>
7.7.2	<i>Produzione di copie</i>	<i>47</i>
7.7.3	<i>Produzione copie o duplicati su supporti rimovibili</i>	<i>47</i>
7.7.4	<i>Intervento del Pubblico Ufficiale</i>	<i>48</i>
7.8	Scarto dei pacchetti di archiviazione	48
7.8.1	<i>Trasferimento dei documenti informatici in conservazione</i>	<i>48</i>
7.8.2	<i>Scarto dei documenti informatici conservati</i>	<i>48</i>
7.8.3	<i>Richiesta di scarto immediato</i>	<i>49</i>
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>	<i>54</i>
8.5.2	<i>Sito Secondario (DR)</i>	<i>55</i>
8.6	Procedure di gestione e di evoluzione	56
8.6.1	<i>Change management</i>	<i>56</i>
8.6.2	<i>Verifica periodica di conformità a normativa e standard di riferimento</i>	<i>57</i>
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>	<i>59</i>
9.2.2	<i>Mantenimento della firma per il periodo di conservazione</i>	<i>59</i>
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>	<i>60</i>

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:

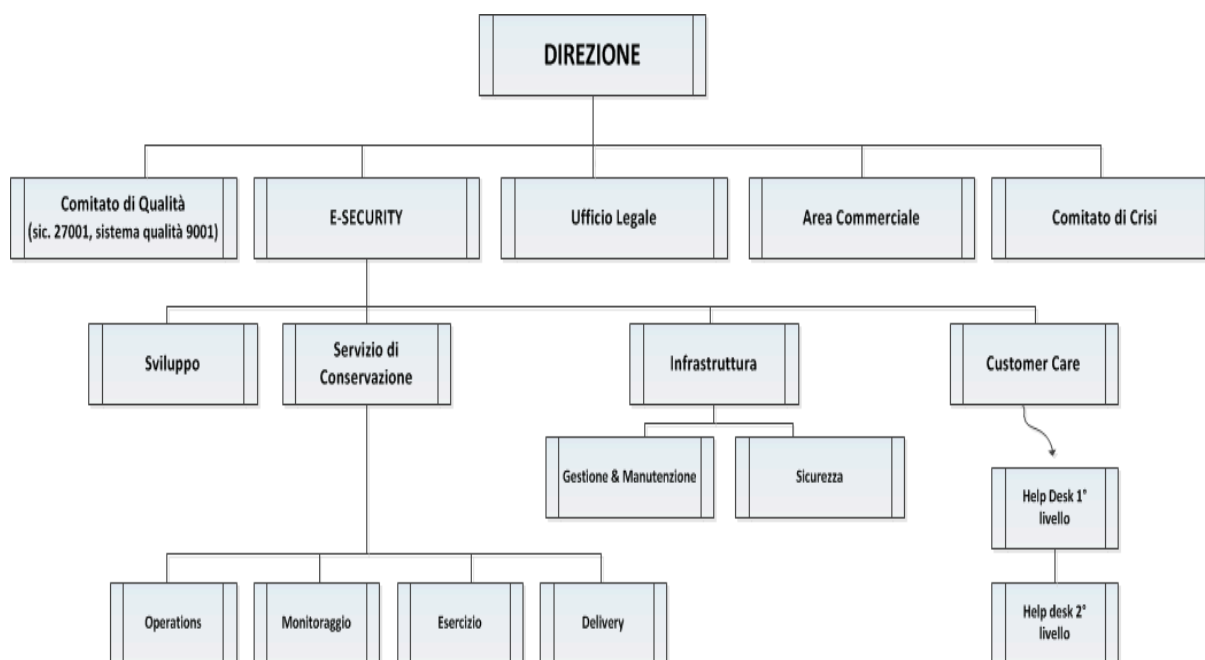


Figura 1: Rappresentazione delle strutture organizzative coinvolte nel servizio di conservazione

[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'adequatezza e la completezza delle specifiche stesse. In relazione a questo aspetto, ARUBA ha privilegiato formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e OASIS.
2	SICUREZZA	La sicurezza di un formato dipende da due elementi: - il grado di modificabilità del contenuto del file; - la capacità di essere immune dall'inserimento di codice maligno.
3	PORTABILITÀ	Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto si ottiene mediante l'impiego fedele di standard documentati e accessibili e dalla loro diffusione sul mercato.
4	FUNZIONALITÀ	Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione del Cliente per la formazione e gestione del documento informatico.
5	SUPPORTO ALLO SVILUPPO	Il supporto allo sviluppo è la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).
6	DIFFUSIONE	La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici. Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.

[Torna al sommario](#)

6.3.2 Formati consigliati per la conservazione

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

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

FORMATO	DESCRIZIONE
PDF - PDF/A	Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. Questo formato è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A.
	Caratteristiche e dati informativi
	Informazioni gestibili Testo formattato, immagini, grafica vettoriale 2D e 3D, filmati.
	Sviluppato da Adobe Systems - http://www.adobe.com/
	Estensione .pdf
	Tipo MIME Application/pdf
	Formato aperto SI
	Specifiche tecniche Pubbliche
	Standard ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
	Altre caratteristiche Assenza di collegamenti esterni Assenza di codici eseguibili Assenza di contenuti crittografati Il file risulta indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo Le più diffuse suite d'ufficio permettono di salvare direttamente i file nel formato PDF/A Sono disponibili prodotti per la verifica della conformità di un documento PDF al formato PDF/A.
	Software necessario alla visualizzazione Adobe Reader

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

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

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

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

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

FORMATO	DESCRIZIONE																				
Open Document Format	ODF (Open Document Format, spesso referenziato con il termine OpenDocument) è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni. Caratteristiche e dati informativi <table> <tr> <td>Informazioni gestibili</td><td>Documenti di testo, fogli di calcolo, presentazioni e grafici.</td></tr> <tr> <td>Sviluppato da</td><td>OASIS</td></tr> <tr> <td>Estensioni principali</td><td>.ods, .odp, .odg, .odb</td></tr> <tr> <td>Tipo MIME</td><td>application/vnd.oasis.opendocument.text</td></tr> <tr> <td>Formato aperto</td><td>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
	Sviluppato da
	Estensione
	Tipo MIME
	Formato aperto
	Specifiche tecniche
	Altre caratteristiche
	Software necessario alla visualizzazione

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
	Sviluppato da
	Estensione
	Tipo MIME
	Formato aperto
	Specifiche tecniche
	Altre caratteristiche
	Software necessario alla visualizzazione

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
	Sviluppato da
	Estensione
	Tipo MIME
	Formato aperto

	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:

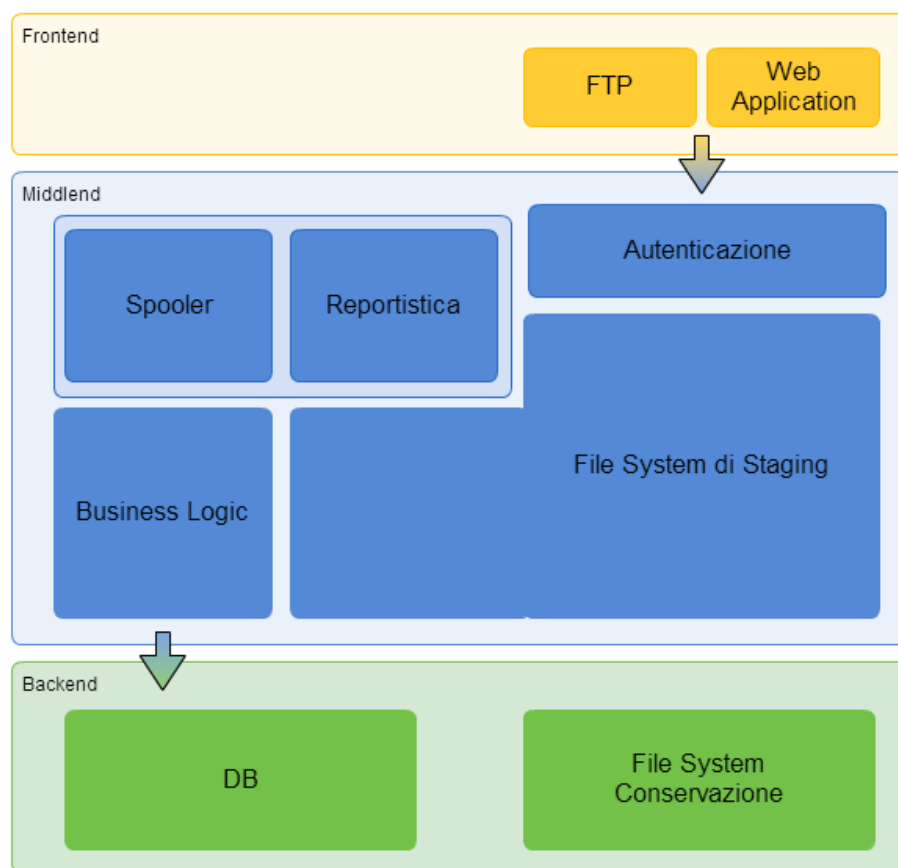


Figura 2: Rappresentazione delle componenti logiche

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.

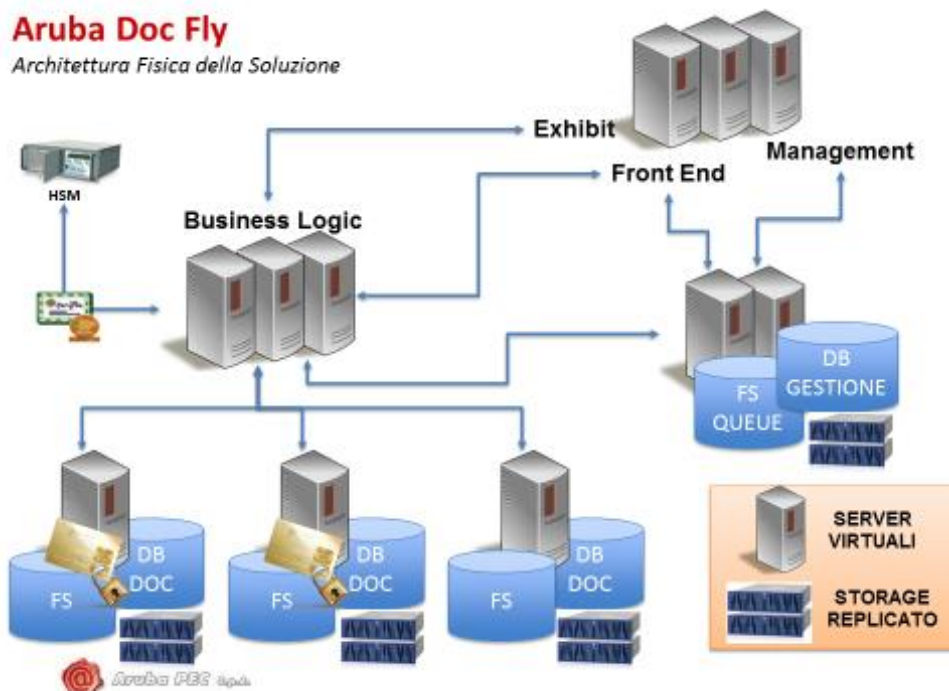


Figura 3: Rappresentazione architettura fisica della soluzione

[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.

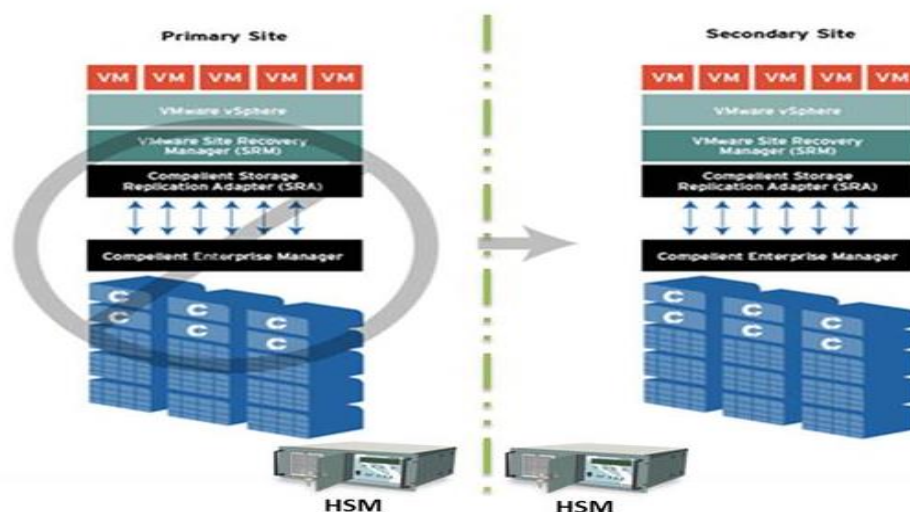


Figura 4 Schema logico della soluzione di Disaster Recovery

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 tracciate che vengono effettuate a livello di database. Tutte le operazioni eseguite determinano infatti la creazione di apposite revisioni che registrano tutte le modifiche intervenute sul sistema permettendo eventualmente di ripristinare i dati a seguito di situazioni anomale.

[Torna al sommario](#)

9.2 Verifiche sugli archivi

ARUBA assicura la verifica periodica, con cadenza non superiore a 36 mesi, dell'integrità degli archivi e della leggibilità degli stessi; assicura, inoltre, agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

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

Il controllo eseguito è di due tipologie:

- **controllo di leggibilità:** consiste nel rendere disponibile attraverso una macchina virtuale un viewer per la visualizzazione dei documenti conservati. Il viewer specifico viene fornito sulla base dell'estensione del documento (mime type) e della versione del formato associato. Il dettaglio di tutte le 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](#)