COMUNE DI DUALCHI
PROVINCIA di NUORO

Manuale di conservazione Documentale

Autore: Emanuele Uda
Redazione: maggio 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 11
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 Unimatica) 14
Art. 14: Il sistema di conservazione 14
V: PROCESSO DI CONSERVAZIONE UNIMATICA 15
Art. 17: Descrizione generale del Sistema di Conservazione Unimatica 15
VI: INFRASTRUTTURA UNIMATICA 19
VII: TIPOLOGIE DEGLI OGGETTI DIGITALI SOTTOPOSTI A CONSERVAZIONE 20
Art. 22: Oggetti conservati 20
Art. 23: Metadati da associare 22
Art. 24: Tipologie documentali 22
VIII: MODALITA' DI ESIBIZIONE 23
Art. 25: Esibizione 23
IX: MISURE DI SICUREZZA DEL SISTEMA 24
Art. 26: Misure di sicurezza a tutela dei dati personali 24
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 26
Art. 29: Pubblicità del presente manuale ed entrata in vigore 26
XII: Allegati 27
Art. 30: Allegati 27

Sistema di Conservazione Digitale dei Documenti Informatici

I: INTRODUZIONE

Art. 1: Scopo del documento

1. Il Comune di Dualchi ha scelto, per la conservazione dei documenti informatici prodotti, un modello in *outsourcing,* esternalizzando il servizio di conservazione alla società Unimatica.

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 a 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 Dualchi, verificata l'impossibilità di conservare in "casa" i documenti prodotti, affida il processo di conservazione ad Unimatica attraverso la sottoscrizione del contratto o convenzione di servizio e atto di delega totale del processo stesso. Unimatica è stata individuata tra l'elenco dei prestatori di servizi fiduciari qualificati e garantisce degli automatismi con i gestionali in uso (Halley Informatica).

Art. 5: Accesso al servizio

L'accesso al servizio di conservazione avvenire mediante un canale sicuro attivato dagli applicativi di gestione documentale Halley 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 Unimatica, vedasi Allegato "Manuale del sistema di conservazione - Unimatica S.p.A._v.20"

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 Dualchi.
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 Unimatica

1. Il Comune 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 Dualchi il ruolo di produttore PDV è svolto dala 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 Unimatica 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 Unimatica.

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 Dualchi, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sul 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 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 Dualchi 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 Unimatica)

Art. 14: Il sistema di conservazione

1. il sistema di gestione informatica dei documenti (gestionali Halley) 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, immodificabilità 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 Unimatica by Namirial 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 del sistema di conservazione - Unimatica S.p.A._v.20".

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 Unimatica, allegato "Manuale del sistema di conservazione - Unimatica S.p.A._v.20".

Art. 16: Modello organizzativo della conservazione

1. Il comune di Dualchi 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 Unimatica.

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 del sistema di conservazione - Unimatica S.p.A._v.20").

V: PROCESSO DI CONSERVAZIONE UNIMATICA

Art. 17: Descrizione generale del Sistema di Conservazione Unimatica

Unimatica mediante il proprio sistema di conservazione Unistorage, 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 Dualchi) e il Conservatore garantiscono specifico monitoraggio al fine di evitare rischi di obsolescenza tecnologica che possono sopravvenire prima della chiusura.

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

In accordo con il soggetto produttore, Unimatica 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_Cliente_HALLEY_ rev20".

Unimatica 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

Il processo di conservazione eseguito da Unimatica adotta il modello standard OAIS - Open Archival Information System (è lo standard ISO per la conservazione a lungo termine di archivi digitali) che definisce concetti e funzionalità degli archivi digitali. Lo schema seguente illustra brevemente gli aspetti principali di un generico processo di conservazione: il Soggetto produttore invia il Pacchetto di versamento, di cui ha piena responsabilità, al Soggetto conservatore, il quale provvede a trasformarlo in Pacchetto di archiviazione. Ai fini dell'esibizione e della distribuzione richiesti dalla comunità di riferimento (il sottoinsieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dall'OAIS), il Soggetto conservatore provvederà a creare i Pacchetti di distribuzione in una forma tale che venga garantita la corretta visualizzazione di questi.

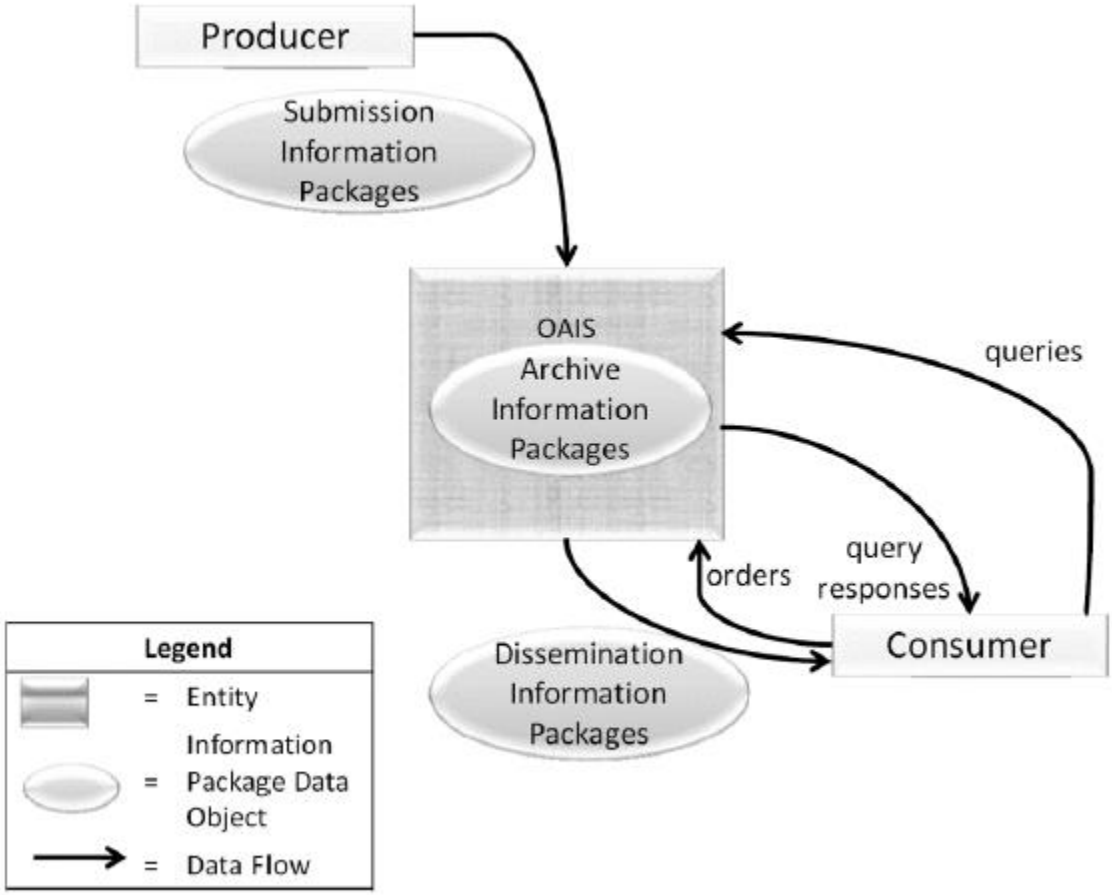


Figura 1 - Modello OAIS

Il servizio offerto da Unimatica ad ogni Soggetto produttore, 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 Dualchi (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 Unimatica.

L'attivazione del servizio avviene attraverso la compilazione del Modulo 'Scheda cliente' allegato "Scheda_Cliente_HALLEY_ rev20". 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 capitolo "Oggetti sottoposti in conservazione" paragrafo 6.3 del Manuale utente di Unimatica, vedasi Allegato "Manuale del sistema di conservazione - Unimatica S.p.A._v.20"

Art. 20: Pacchetti di versamento
Per quanto concerne i seguenti argomenti puntati si fa direttamente riferimento al Manuale di unimatica "Manuale del sistema di conservazione - Unimatica S.p.A._v.20":

- 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 UNIMATICA

Art. 21: Descrizione Generale

Il Data Center di Unimatica è qualificato ACN, ed è presente sul Marketplace al link: https://www.acn.gov.it/portale/w/in-330, di seguito

I Data Center hanno livello di classificazione TIA-942 (TIER III) e sono dotati di Certificazione ISO/IEC 27001:2022. Unimatica si avvale delle soluzioni di aziende leader nel settore: Cisco Systems, Hewlett-Packard, Hitachi Data Systems, IBM, EMC, VMWARE, ORACLE e di funzionalità quali:

• Politiche di servizio con dislocazioni multiple dei dati e singoli punti di ingresso e ricerca.

• L'innovativo servizio di Enterprise Application Services for Business Continuity (EASBC) che, nel caso estremamente remoto di failure contemporaneo dei DataCenter primario e secondario, permette di attivare i servizi essenziali per l'invio dei documenti sulla seconda coppia di Data Center ai fini di garantire una totale garanzia di Business Continuity.

• Piattaforma di memorizzazione storage multilivello UCP (Unimatica Content Platform) compatibile a livello di servizi con Amazon Web Services – S3

• 4 HSM (Hardware Security Module) in alta affidabilità e D/R per la gestione delle firme massive e automatiche. Tutti i server applicativi di produzione, oggetto del servizio di outsourcing, sono implementati su una infrastruttura virtuale, utilizzando la tecnologia VMWare ESXi 5.5.

L'infrastruttura virtuale è composta da sei sistemi Blade lame IBM HS23, ognuno dotato di 2 CPU con 6 Core XeonE5-2620 e 256 GB RAM. L'infrastruttura Database Server è implementata su due sistemi Blade NON virtualizzati, con 2 processori Quad-core e 96 GB Ram ciascuno, configurati in modalità Cluster "Active / Stand-by". Entrambi i sistemi sono dotati di schede (1 Gbit/s) ridondate e doppio percorso verso la Storage Area Network.

È disponibile, in entrambi i siti, una Storage Area Network EMC VMax, con adeguati livelli di espandibilità, switch Brocade a 24 porte e moduli per la replica sincrona o asincrona dei dati.

Per garantire la scalabilità degli Application Server di front-end è previsto l'utilizzo di un componente hardware (Alteon) per il bilanciamento degli accessi web.

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 Unimatica 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_Cliente_HALLEY_ rev20"

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 Unimatica, attraverso il sistema UniStorage, 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 del sistema di conservazione - Unimatica S.p.A._v.20" 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 Unimatica 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 del sistema di conservazione - Unimatica S.p.A._v.20".

    - 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 architetturale di UniStorage 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 Dualchi) che ha provveduto ad individuare sulla base dell'art.28 del Regolamento UE 679/2016 il responsabile del trattamento (Unimatica) 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 8 dell'allegato "Manuale del sistema di conservazione - Unimatica S.p.A._v.20".

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 una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore 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 Dualchi 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 Dualchi e dal Conservatore Unimatica.

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 Dualchi.

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 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 di Dualchi, 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.

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, Unimatica, 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. 7.9 "Scarto dei Pacchetti di archiviazione" dell'allegato "Manuale del sistema di conservazione - Unimatica S.p.A._v.20"

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_Cliente_ rev20;
   - Allegato Manuale del sistema di conservazione - Unimatica S.p.A._v.20

COMUNE DI DUALCHI
PROVINCIA di NUORO

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 l'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 IPA = ADDC696; Denominazione = Area Amministrativa)

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	**Emanuele Uda**
Tipologia di atto per la nomina	**Decreto del Sindaco**
Numero dell'atto di nomina	**n.9**
Data dell'atto di nomina	**30/06/2025**

Vicario o Delegato della Conservazione	
Nominativo	**Isabella Miscali**
Tipologia di atto per la nomina	**Decreto del Sindaco**
Numero dell'atto di nomina	**n. 9**
Data dell'atto di nomina	**30/06/2025**

Responsabile del Servizio di Protocollazione	
Nominativo	**Emanuele Uda**
Tipologia di atto per la nomina	**Decreto**
Numero dell'atto di nomina	**n. 15**
Data dell'atto di nomina	**23/12/2025**

Responsabile della Gestione Documentale	
Nominativo	**Emanuele Uda**
Tipologia di atto per la nomina	**Decreto del Sindaco**
Numero dell'atto di nomina	**n.9**
Data dell'atto di nomina	**30/06/2025**

Vicario della Gestione Documentale	
Nominativo	**Isabella Miscali**
Tipologia di atto per la nomina	**Decreto del Sindaco**
Numero dell'atto di nomina	**n.9**
Data dell'atto di nomina	**30/06/2025**

Responsabile per la Transizione Digitale - RTD	
Nominativo	**Emanuele Uda**
Tipologia di atto per la nomina	**Decreto**
Numero dell'atto di nomina	**4**
Data dell'atto di nomina	**03/03/2026**

Responsabile Protezione Dati Personali - DPO	
Nominativo	**Alessandra Sebastiana Etzo**
Tipologia di atto per la nomina	**Determinazione**
Numero dell'atto di nomina	**n.36**
Data dell'atto di nomina	**03/04/2023**

ARTICOLAZIONE DELL'ENTE IN UNITÀ ORGANIZZATIVE RESPONSABILI

Il Comune di Dualchi 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 Amministrativa e sociale	**Emanuele Uda**
Area Economico Finanziaria	**Antonella Masala**
Area Tecnica	**Luigi Podda**

COMUNE DI DUALCHI
PROVINCIA di NUORO

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

Manuale di Conservazione

FORMATI ELETTRONICI ADOTTATI

Tipologie di Formati

Il comune di Dualchi, 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, 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), 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**	*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*.
(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 contenervi diversi messaggi di posta elettronica, organizzati su più livelli.
(Fogli di calcolo) **XLS**	Il foramto 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, *si raccomanda di non formarne altri esemplari e di valutare il riversamento di fogli di calcolo preesistenti in altro formato della stessa tipologia*: in quest'ordine, OpenDocument Spreadsheet (.ods) ovvero SpreadsheetML (.xlsx).
(Presentazioni multimediali) **PPT /PPTX**	Il foramto 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, *si raccomanda di non formarne altri esemplari e di valutare il riversamento di presentazioni preesistenti in altro formato della stessa tipologia*: in quest'ordine, OpenDocument Presentation (.odp) ovvero PresentationML (.pptx).
(Presentazioni multimediali) **ODP**	Il foramto 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. *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*.
(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 ridurne 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 *strictu sensu* 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 Dualchi 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 verifichino:

- 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 (Unimatica);
- le indicazioni tecniche provenienti dalla Software House (Halley Informatica).

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 Unimatica.

COMUNE DI DUALCHI
PROVINCIA di NUORO

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 di Halley informatica 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 Halley)
    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
sesso_s	sesso
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
soggcod_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 DUALCHI
PROVINCIA di NUORO

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 titolario è strettamente connesso.

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

I fondamenti della conservazione permanente

- In genere, salvo poche eccezioni, tutti i repertori devono essere conservati permanentemente.
- Il Comune non deve scartare i documenti considerati "vitali" (quelli che – mutuando una definizione formulata da Luciana Duranti[1] – 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 sfoltimento 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 sfoltimento 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 titolario 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	

	Verbali 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'elimina-zione dei materiali prepara-tori	
8. Informazioni e relazioni con il pubblico			
	Iniziative specifiche dell'URP: un fascicolo per ciascun affare	Permanente, dopo sfoltimento 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'organi-gramma	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	
	Verbali 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 sfoltimento del carteggio di carattere transitorio	
	Partecipazione del Comune a enti e associazioni (comprensivo della nomina dei rappresentanti)	Permanente, previo sfoltimento del carteggio di carattere transitorio	
16. Area e città metropolitana			
	Costituzione e rapporti istituzionali	Permanente	
17. Associazionismo e partecipazione			
	Politica di incoraggiamento e appoggio alle associazioni	Permanente	
	Albo dell'associazionismo: elenco delle associazioni accreditate	Permanente	
	Fascicoli delle associazioni che chiedono l'iscrizione all'albo	Permanente	

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

Classi	Tipologie documentarie	Conservazione	Note
1. Sindaco			
	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 *ad acta*			
	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 *ad acta* 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
	Curricula inviati per richieste di assunzione	2 anni	
	Domande di assunzione pervenute senza indizione di concorso o selezione	1 anno	
2. Assunzioni e cessazioni			
	Criteri generali e normativa per le assunzioni e cessazioni	Permanente	
	Determinazioni di assunzione e cessazione dei singoli inserite nei singoli fascicoli personali	Permanente	
3. Comandi e distacchi; mobilità			

	Criteri generali e normativa per comandi, distacchi, mobilità	Permanente	
	Determinazioni di comandi, distacchi e mobilità inserite nei singoli fascicoli personali	Permanente	
4. Attribuzione di funzioni, ordini di servizio e missioni			
	Criteri generali e normativa per le attribuzioni di funzioni, ordini di servizio e missioni	Permanente	
	Determinazioni di attribuzione di funzioni inserite nei singoli fascicoli personali	Permanente	
	Determinazioni di missioni inserite nei singoli fascicoli personali	10 anni	
	Determinazioni di ordini di servizio inserite nei singoli fascicoli personali	Permanente	
	Ordini di servizio collettivi	Permanente	
	Autorizzazione allo svolgimento di incarichi esterni	2 anni	
5. Inquadramenti e applicazione contratti collettivi di lavoro			
	Criteri generali e normativa per gli inquadramenti e le 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 sfoltimento	
	Carteggio prodotto dai differenti uffici del Comune per questioni afferenti alla formazione del bilancio e del PEG	10 anni	
2. Gestione del bilancio e del PEG (con eventuali variazioni)			
	Gestione del bilancio: un fascicolo per ciascuna variazione	Permanente, previo sfoltimento	
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 sfoltimento	
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			
	Verbali 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 (volture)	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 (volture)	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	*L'autonomia dei Comuni si può esplicare in forme svariate soprattutto in questo titolo: perciò l'indicazione generica di evento o attività verrà riempita di contenuti concreti dalla singola amministrazione.*

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	
	Verbali 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 sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Feste civili e/o religiose: un fascicolo per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative culturali. un fascicolo per iniziativa	Permanente, previo sfoltimento 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 sfoltimento 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 sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Programmazione per settori: un fascicolo per ciascun settore	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Accordi con i differenti soggetti: un fascicolo per ciascun soggetto	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
9. Prevenzione, recupero e reintegrazione dei soggetti a rischio			
	Campagne di prevenzione: un fascicolo per campagna	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Interventi di recupero e reintegrazione dei soggetti a rischio: un fascicolo per intervento	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Ricognizione dei rischi: un fascicolo per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
10. Informazione, consulenza ed educazione civica			

	Funzionamento e attività delle strutture (consultori, informagiovani, etc.): un 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 sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
4. Commercio			
	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfoltimento 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 sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
6. Esercizi turistici e strutture ricettive			
	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Autorizzazioni turistiche: repertorio	Permanente	
7. Promozione e servizi			
	Iniziative specifiche: un fascicolo per affare	Permanente, previo sfoltimento 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	
	Verbali 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	
	Verbali 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	
	Verbali degli accertamenti nei diversi settori (edilizio, sanitario, commerciale, anagrafico, sociale, etc.): un repertorio annuale per ciascun settore di accertamento	Permanente	

Titolo X. Tutela della salute

Classi	Tipologie documentarie	conservazione	Note
1. Salute e igiene pubblica			
	Emergenze sanitarie: un fascicolo per ciascun evento	Permanente	
	Misure di igiene pubblica: un fascicolo per ciascun affare	Permanente	
	Interventi di derattizzazione, dezanzarizzazione 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 epizoozie (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, *Massimario per lo scarto degli atti elettorali,* 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	
	Verbali 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 DUALCHI
PROVINCIA di NUORO

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 Dualchi 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 Dualchi 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 dell'Ente;
- 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 Dualchi 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 Halley è in cloud qualificato ACN presente al link: https://www.acn.gov.it/portale/w/pa-918, 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.

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 immodificabili 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 Dualchi 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'istallazione degli aggiornamenti (patch) periodici che i fornitori rendono disponibili.

Backup e ripristino dell'accesso ai dati

Il comune 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 è 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 sato 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 accederci 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 Dualchi 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 Dualchiha 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.

Servizio di Conservazione a norma

Scheda Cliente

Titolare dell'oggetto della conservazione

Comune di Dualchi – Gestionali HALLEY

Storia delle versioni del modello Unimatica SpA

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
01	03/10/2009	Emissione	RSGQ	Silvano Ghedini
02	05/10/2010	Aggiornamento	RSGQ	Silvano Ghedini
03	06/12/2010	Aggiornamento	RSGQ	Silvano Ghedini
04	22/02/2016	Aggiornamento	RSGQ	Silvano Ghedini
05	29/10/2017	Aggiornamento Informativa	RSGQ	Silvano Ghedini
06	03/10/2019	Aggiornamento logo e dicitura informativa cliente	Cecilia Canova	Paolo Vandelli
07	07/10/2019	Esplicitati metadati minimi documento informatico	Paolo Vandelli	Paolo Vandelli
08	10/10/2019	Esplicitati metadati minimi fattura elettronica	Paolo Vandelli	Paolo Vandelli
09	16/10/2019	Esplicitati metadati minimi documento amministrativo informatico (cap. 2.1.1), esplicitati vincoli legati ai formati idonei alla conservazione (cap. 2), aggiunta sottoscrizione da parte del cliente e per accettazione da parte di Unimatica	Cecilia Canova	Paolo Vandelli
10	18/10/2019	Aggiunta possibilità di evidenziare per ogni tipologia documentale, la presenza di dati personali (cap. 2.1.2)	Anna Veltri	Paolo Vandelli
11	07/11/2019	Rimossi alcuni criteri di chiusura dei PDA, non significativi	Paolo Vandelli	Paolo Vandelli
12	14/01/2020	Aggiunta dichiarazione per esercizio fiscale (in coda al capitolo 2)	Cecilia Canova	Paolo Vandelli
13	28/11/2020	Adeguamento alle Linee guida sulla formazione, gestione e conservazione dei documenti informatici (AgID 10-09-2020)	Eleonora Luzi	Paolo Vandelli
14	28/11/2021	Adeguamento alla revisione delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici	Eleonora Luzi, Andrea Grilli, Paolo Vandelli	Paolo Vandelli
15	06/05/2022	Aggiornamento Responsabile del Servizio di Conservazione	Eleonora Luzi	Paolo Vandelli
16	19/09/2022	Aggiunta colonna *email* alla tabella del paragrafo *5.1. Esigenze di accessibilità e fruizione*	Eleonora Luzi	Paolo Vandelli
17	21/12/2022	Aggiornamento logo certificazioni ISO9001-ISO14001-27001-37001	Eleonora Luzi	Paolo Vandelli
18	26/01/2023	Aggiunta indicazione implicita del responsabile della conservazione in caso di mancata indicazione del	Eleonora Luzi	Paolo Vandelli

		nominativo nella relativa tabella (§1.1)		
19	27/04/2023	Modifiche apportate ai §§ 1 e 2	Eleonora Luzi	Cecilia Canova
20	20/12/2023	Aggiornamento logo Unimatica – a Namirial Company	Eleonora Luzi	Cecilia Canova

Storia delle versioni della presente scheda cliente:

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
16.01	19/09/2022	Prima stesura Modello specifico	Eleonora Luzi	Paolo Vandelli
17.01	21/12/2022	Allineamento al template rev. 17 del modello specifico	Eleonora Luzi	Paolo Vandelli
19.01	20/06/2023	Allineamento al template rev. 19 del modello specifico	Eleonora Luzi	Cecilia Canova
20.01	27/12/2023	Allineamento al template rev. 20 del modello specifico	Eleonora Luzi	Cecilia Canova

INDICE

1 INFORMAZIONI 5

1.1 CLIENTE 5

1.2 GLOSSARIO 7

2 MATERIALE DOCUMENTARIO DA CONSERVARE 8

2.1 METADATI 10

2.1.1 Metadati specifici per le tipologie documentali oggetto di conservazione 10

2.1.2 Controlli da effettuare sui set di metadati obbligatori 57

2.2 MODALITÀ DI TRASMISSIONE DEGLI OGGETTI DOCUMENTALI AL SISTEMA DI CONSERVAZIONE 57

3 CONFIGURAZIONE VERIFICA INIZIALE 58

3.2 TABELLA CONTENENTE I CONTROLLI EFFETTUATI PER LE VARIE TIPOLOGIE DI DOCUMENTO 59

4 GESTIONE PACCHETTI DI ARCHIVIAZIONE (PDA) 60

4.1 REGOLE CREAZIONE PDA 60

4.2 REGOLE CHIUSURA PACCHETTI DI ARCHIVIAZIONE 61

5 VARIE 62

5.1 ESIGENZE DI ACCESSIBILITÀ E FRUIZIONE 62

1 Informazioni

Il presente modello viene consegnato al cliente (Titolare dell'oggetto di conservazione) per il censimento di tutte le informazioni necessarie all'attivazione ed erogazione del servizio di conservazione Unistorage di Unimatica SpA. Il documento deve essere compilato dal Titolare dell'oggetto di conservazione in tutte le sue parti. Ogni variazione al presente documento (tipologie documenti, metadati, formati di file, controlli all'accesso, regole di creazione e di chiusura dei PdA) dovrà essere concordata fra le parti attraverso la sottoscrizione di una nuova revisione dello stesso oppure ad un addendum che richiama questo documento.

1.1 Cliente

Cliente		
Comune di DUALCHI		
Attributo	Descrizione	
Tipo Attività	Conservazione Documenti Informatici	
Dati Anagrafici del Cliente	Indirizzo	**Via Parini n. 1**
	C.F./P.IVA	**00155030919**
	Codice IPA	**c_d376**
	Indirizzo Pec	***protocollo@pec.comune.dualchi.nu.it***
Informativa	Unimatica SpA non è responsabile dei documenti versati dal cliente in ambiente di collaudo e del loro contenuto; pertanto, si raccomanda di non riportare dati personali reali all'interno dei documenti versati o dei relativi metadati.	
	Unimatica SpA, a fronte di dichiarazioni da parte del cliente, si impegna a gestire i documenti coperti da proprietà intellettuale o restrizioni di utilizzo secondo la normativa vigente.	

Il Titolare dell'oggetto di conservazione affida la conservazione dei propri documenti informatici e delle aggregazioni documentali informatiche al Responsabile della conservazione. Il Responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Ruolo	Nome e Cognome	Atto di nomina
Responsabile della conservazione*	*Emanuele Uda*	Decreto del Sindaco n. 9 del 30.06.2025

In assenza di tale nominativo si assume che il ruolo di Responsabile della Conservazione sia ricoperto dal legale rappresentante firmatario di questo documento.

Il Responsabile della conservazione, sotto la propria responsabilità, delega lo svolgimento delle proprie attività o parte di esse ai seguenti soggetti:

Ruolo	Nome e cognome	Funzioni e competenze delegate
Vicario	*Isabella Miscali*	Decreto del Sindaco n. 9 del 30.06.2025

Restano ferme le deleghe a Unimatica SpA sottoscritte nel documento di delega, che eroga il servizio di conservazione sulla base delle indicazioni ricevute dal Responsabile della Conservazione, come di seguito descritto.

1.2 Glossario

In merito alla terminologia specifica e agli acronimi usati nel presente documento si rimanda all'Allegato 1 delle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici[1].

[1] https://www.agid.gov.it/sites/default/files/repository_files/allegato_1_glossario_dei_termini_e_degli_acronimi.pdf

2 Materiale documentario da conservare

Di seguito vengono elencate le diverse tipologie documentali inviati al servizio di conservazione da parte del Titolare dell'oggetto della conservazione o suo delegato.

In sintesi, le tipologie documentarie per le quali viene richiesto il servizio di conservazione digitale sono di seguito elencate nelle due tabelle e riguardano i formati indicati nell'allegato 2 Formati di file e riversamento delle Linee guida.

Tabella 2.1 – Formati idonei alla conservazione

(Riportare in questa tabella i formati dei file individuati come idonei alla conservazione nelle specifiche dell'allegato 2 alle Linee Guida, che il Titolare intende inviare in conservazione)

Tipo Documento	Formato file (*)	Periodicità invio in conservazione (**)
Deliberazione	PDF/PDFA/P7M	Giornaliera /settimanale
Determinazione Liquidazione	PDF/PDFA/P7M	Giornaliera /settimanale
Ordinanza - Decreto	PDF/PDFA/P7M	Giornaliera /settimanale
Atto interno	PDF/PDFA/P7M	Giornaliera /settimanale
Allegato Deliberazione	PDF/PDFA/P7M	Giornaliera /settimanale
Allegato Determinaz-Liquidaz	PDF/PDFA/P7M	Giornaliera /settimanale
Allegato Ordinanza - Decreto	PDF/PDFA/P7M	Giornaliera /settimanale
Allegato Atto interno	PDF/PDFA/P7M	Giornaliera /settimanale
Verbale di adunanza	PDF/PDFA/P7M	Giornaliera /settimanale
Allegato Verbale di adunanza	PDF/PDFA/P7M	Giornaliera /settimanale
Contratto	PDF/PDFA/P7M	Giornaliera /settimanale
Allegato del contratto	PDF/PDFA/P7M	Giornaliera /settimanale
Documento protocollato	PDF/PDFA/P7M	Giornaliera /settimanale
Documento riservato	PDF/PDFA/P7M	Giornaliera /settimanale
Registro protocollo	PDF/PDFA/P7M	Giornaliera /settimanale
Email protocollo	EML	Giornaliera /settimanale
Allegato email protocollo	PDF/PDFA/P7M	Giornaliera /settimanale
Allegato comunicazione	PDF/PDFA/P7M	Giornaliera /settimanale
Allegato fascicolo	PDF/PDFA/P7M	Giornaliera /settimanale
Allegato carteggio	PDF/PDFA/P7M	Giornaliera /settimanale
Fattura attiva	XML	Giornaliera /settimanale
Fattura passiva	XML	Giornaliera /settimanale
Allegato Fattura Attiva	XML	Giornaliera /settimanale
Allegato Fattura Passiva	XML	Giornaliera /settimanale
Protocollo Ricevuta PEC	PDF/PDFA/P7M	Giornaliera /settimanale
Protocollo Email in Arrivo	PDF/PDFA/P7M	Giornaliera /settimanale
Protocollo Email in Partenza	PDF/PDFA/P7M	Giornaliera /settimanale
Protocollo Fattura	PDF/PDFA/P7M	Giornaliera /settimanale

(*) I formati di file devono presentare, come da Allegato 2 delle Linee Guida sulla formazione gestione e conservazione dei documenti informatici, caratteristiche di formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo.
(**) giornaliera, settimanale, mensile, bimestrale, trimestrale, semestrale, annuale, altro…

Tabella 2.2 – Formati non idonei alla conservazione

(Riportare in questa tabella i formati dei file individuati come **non idonei** alla conservazione nelle specifiche dell'allegato 2 alle Linee Guida, che il Titolare chiede comunque di conservare).

Tipo Documento	Formato file	N° file per periodicità	Dimensioni medie file (KB)	Periodicità invio in conservazione (**)

(**) giornaliera, settimanale, mensile, bimestrale, trimestrale, semestrale, annuale, altro…

Tabella 2.3 – Formati non presenti nell'allegato 2

(Riportare in questa tabella i formati dei file non censiti nell'allegato 2, che l'ente chiede di conservare)

Tipo Documento	Formato file	N° file per periodicità	Dimensioni medie file (KB)	Periodicità invio in conservazione (**)

(**) giornaliera, settimanale, mensile, bimestrale, trimestrale, semestrale, annuale, altro…

Il soggetto produttore conferma la necessità di conservare file nei formati riportati nelle tabelle 2.2 e 2.3. Consapevole del fatto che tali formati potrebbero non presentare le caratteristiche di formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo ai sensi del paragrafo 3.6 delle Linee guida, chiede ad Unimatica SpA di procedere comunque all'accettazione di questi formati in fase di ingestion. Solleva inoltre Unimatica SpA da possibili complicazioni che dovessero emergere nella produzione di copie o duplicati, nonché nell'eventuale azione di riversamento dei file stessi su nuovo formato.

In caso di conservazione di documenti di natura fiscale il soggetto produttore dichiara che il proprio esercizio fiscale:	
☒	Coincide con l'anno solare
☐	Non coincide con l'anno solare e si chiude il: _____

2.1 Metadati

Così come illustrato nell'Allegato 1 alle LLGG AgID sulla formazione, gestione e conservazione dei documenti informatici, i metadati sono dei *"Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo – in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017".*

Per la mappatura di metadati specifici delle varie marco categorie individuate dall'Allegato 5 alle LLGG AgID si rimanda al documento "*All.SchedaCliente_metadatiAGID_rev1.1*", parte integrante della presente "Scheda cliente".

2.1.1 Metadati specifici per le tipologie documentali oggetto di conservazione

Di seguito si riportano i metadati specifici che il sistema mittente trasmette al servizio di conservazione.

Oltre ai metadati indicati nelle tabelle seguenti, i sistemi gestionali Halley riportano i metadati obbligatori all'interno di un file XML allegato ad ogni documento versato. Il file, generato solo per documenti prodotti dopo il 1/1/2022, è formato nel rispetto degli *schemi XSD* riportati all'interno dell'allegato 5 alle Linee guida. Pertanto, si richiede che venga opportunamente conservato assieme agli altri file che descrivono il documento.

Tipo Documento	Metadati specifici	Dati personali
Deliberazione	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documentomirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione • at_pubbl_datainiz : Data inizio pubblicazione • at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica

	• at_partec_data : Data parere regolarità tecnica • at_partcon_nome : Parere regolarità contabile • at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione • at_CIG : CIG • at_importo : Importo	
Determinazione Liquidazione	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione • at_pubbl_datainiz : Data inizio pubblicazione • at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica • at_partec_data : Data parere regolarità tecnica • at_partcon_nome : Parere regolarità contabile • at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione

	• at_CIG : CIG • at_importo : Importo	
Ordinanza - Decreto	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione • at_pubbl_datainiz : Data inizio pubblicazione • at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica • at_partec_data : Data parere regolarità tecnica • at_partcon_nome : Parere regolarità contabile • at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione • at_CIG : CIG • at_importo : Importo	
Atto interno	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione	

	• at_pubbl_datainiz : Data inizio pubblicazione • at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica • at_partec_data : Data parere regolarità tecnica • at_partcon_nome : Parere regolarità contabile • at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione • at_CIG : CIG • at_importo : Importo	
Allegato Deliberazione	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione • at_pubbl_datainiz : Data inizio pubblicazione • at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica • at_partec_data : Data parere regolarità tecnica	

	• at_partcon_nome : Parere regolarità contabile • at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione • at_CIG : CIG • at_importo : Importo	
Allegato Determinaz-Liquidaz	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione • at_pubbl_datainiz : Data inizio pubblicazione • at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica • at_partec_data : Data parere regolarità tecnica • at_partcon_nome : Parere regolarità contabile • at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione • at_CIG : CIG • at_importo : Importo	

Allegato Ordinanza - Decreto	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione • at_pubbl_datainiz : Data inizio pubblicazione • at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica • at_partec_data : Data parere regolarità tecnica • at_partcon_nome : Parere regolarità contabile • at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione • at_CIG : CIG • at_importo : Importo	
Allegato Atto interno	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione • at_pubbl_datainiz : Data inizio pubblicazione	

	• at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica • at_partec_data : Data parere regolarità tecnica • at_partcon_nome : Parere regolarità contabile • at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione • at_CIG : CIG • at_importo : Importo	
Verbale di adunanza	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione • at_pubbl_datainiz : Data inizio pubblicazione • at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica • at_partec_data : Data parere regolarità tecnica • at_partcon_nome : Parere regolarità contabile	

	• at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione • at_CIG : CIG • at_importo : Importo	
Allegato Verbale di adunanza	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • at_organo_atto : Descrizione organo • at_pubbl_num : Numero pubblicazione • at_pubbl_anno : Anno pubblicazione • at_pubbl_datainiz : Data inizio pubblicazione • at_pubbl_datafine : Data fine pubblicazione • at_pubbl_esecut : Data esecutività • at_data_seduta : Data seduta • at_partec_nome : Parere regolarità tecnica • at_partec_data : Data parere regolarità tecnica • at_partcon_nome : Parere regolarità contabile • at_partcon_data : Data parere regolarità contabile • at_settore_des : Descrizione settore • at_settore_num : Numero registro settore • at_settore_anno : Anno registro settore • at_settore_datareg : Data registrazione • at_CIG : CIG • at_importo : Importo	

Contratto	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • ct_data_stipula : Data stipula contratto • ct_uffic_rogante : Dati ufficio rogante • ct_anagr_contr : Dati contraenti • ct_data_scadenza : Data scadenza contratto	
Allegato del contratto	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • ct_data_stipula : Data stipula contratto • ct_uffic_rogante : Dati ufficio rogante • ct_anagr_contr : Dati contraenti • ct_data_scadenza : Data scadenza contratto	
Documento protocollato	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione	

	• pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Documento riservato	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Registro protocollo	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO	

	• pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Email protocollo	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione	

	• pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Allegato email protocollo	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Allegato comunicazione	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici	

	• pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Allegato fascicolo	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente	

	• pi_mail_dest: Indirizzo email destinatario	
Allegato carteggio	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Fattura attiva	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pf_tipdo: Tipo Documento • pf_importo: Importo • pf_data_scadenza: Data Scadenza • pf_tip_reg_iva: tipo registro IVA • pf_rif_reg_iva: riferimento registro IVA • pf_rif_cont_cap: riferimento contabile capitolo	

	• pf_rif_cont_acc: riferimento contabile accertamento • pf_ufficio_sdi: Ufficio SDI • pf_ident_sdi: Identificativo SDI • pf_num_ruf: numero RUF • pf_anno_ruf: anno RUF • pf_cig: CIG • pf_cup: CUP • pf_rif_cont_imp: riferimento contabile impegno • pf_ril_iva: rilevante IVA • pf_aliq_iva_rc: aliquota IVA reverse charge • pf_importo_iva_rc: totale IVA reverse charge • pf_tipno: tipo notifica	
Fattura passiva	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pf_tipdo: Tipo Documento • pf_importo: Importo • pf_data_scadenza: Data Scadenza • pf_tip_reg_iva: tipo registro IVA • pf_rif_reg_iva: riferimento registro IVA • pf_rif_cont_cap: riferimento contabile capitolo • pf_rif_cont_acc: riferimento contabile accertamento • pf_ufficio_sdi: Ufficio SDI • pf_ident_sdi: Identificativo SDI • pf_num_ruf: numero RUF • pf_anno_ruf: anno RUF • pf_cig: CIG • pf_cup: CUP • pf_rif_cont_imp: riferimento contabile impegno • pf_ril_iva: rilevante IVA • pf_aliq_iva_rc: aliquota IVA reverse charge	

	• pf_importo_iva_rc: totale IVA reverse charge • pf_tipno: tipo notifica	
Allegato Fattura Attiva	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pf_tipdo: Tipo Documento • pf_importo: Importo • pf_data_scadenza: Data Scadenza • pf_tip_reg_iva: tipo registro IVA • pf_rif_reg_iva: riferimento registro IVA • pf_rif_cont_cap: riferimento contabile capitolo • pf_rif_cont_acc: riferimento contabile accertamento • pf_ufficio_sdi: Ufficio SDI • pf_ident_sdi: Identificativo SDI • pf_num_ruf: numero RUF • pf_anno_ruf: anno RUF • pf_cig: CIG • pf_cup: CUP • pf_rif_cont_imp: riferimento contabile impegno • pf_ril_iva: rilevante IVA • pf_aliq_iva_rc: aliquota IVA reverse charge • pf_importo_iva_rc: totale IVA reverse charge • pf_tipno: tipo notifica	
Allegato Fattura Passiva	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pf_tipdo: Tipo Documento • pf_importo: Importo • pf_data_scadenza: Data Scadenza • pf_tip_reg_iva: tipo registro IVA	

	• pf_rif_reg_iva: riferimento registro IVA • pf_rif_cont_cap: riferimento contabile capitolo • pf_rif_cont_acc: riferimento contabile accertamento • pf_ufficio_sdi: Ufficio SDI • pf_ident_sdi: Identificativo SDI • pf_num_ruf: numero RUF • pf_anno_ruf: anno RUF • pf_cig: CIG • pf_cup: CUP • pf_rif_cont_imp: riferimento contabile impegno • pf_ril_iva: rilevante IVA • pf_aliq_iva_rc: aliquota IVA reverse charge • pf_importo_iva_rc: totale IVA reverse charge • pf_tipno: tipo notifica	
Protocollo Ricevuta PEC	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione	

	• pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Protocollo Email in Arrivo	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Protocollo Email in Partenza	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento • org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici	

	• pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente • pi_mail_dest: Indirizzo email destinatario	
Protocollo Fattura	• org_ente_codice : Codice ente • org_ente_nome : Nome ente • org_docum_riser : Regole accesso • org_docum_inidc : Documento indicizzabile • org_docum_visua : Documento visualizzabile • apl_sigla : Sigla procedura • apl_sigla_sezio : Sezioni procedura • apl_sigla_tipdo : Nome documento • org_oper_codice : Codice operatore • org_oper_nome : Nome operatore • org_do_area : Area struttura • org_do_sett : Settore struttura • org_do_uff : Ufficio struttura • org_do_serv : Servizio struttura • org_do_uoc : Uoc struttura • org_prot_num : Numero identificativo documento • org_prot_rifer : Anagrafica di riferimento documento • org_prot_codcc : Codice univoco classificazione • org_prot_categ : Codice categoria documento	☒ Contiene dati personali ☐ Contiene dati particolari ☐ Contiene dati relativi a condanne penali o reati ☒ Le informazioni sopra classificate possono essere presenti anche sui file oggetto della conservazione

	• org_prot_class : Codice classe • org_prot_sottoc : Codice sottoclasse • org_docum_data : Data produzione documento • org_docum_ogg : Contenuto documento • org_docum_filor : Nome documento originale • org_regis_tipo : Tipo registro/repertorio • org_regis_num : Numero registro/repertorio • org_regis_anno : Anno registro/repertorio • org_regis_data : Data registro/repertorio • org_docum_aggreg : Chiave aggregazione univoca • org_fascic_cod : Codice univoco fascicolo • org_fascic_num : Numero fascicolo • org_fascic_data : Data apertura fascicolo • org_fascic_den : Denominazione fascicolo • org_docum_mirror : Documento mirrorato • pi_ente_ipa : Codice IPA titolare • pi_ente_aoo : Codice AOO • pi_proto_tipo : Protocollo tipo • pi_proto_uffi : Protocollo uffici • pi_proto_mezzo : Protocollo mezzo ricezione/spedizione • pi_mitte_num : Protocollo numero mittente • pi_mitte_data : Protocollo data mittente • pi_regis_tipo : Registro tipo • pi_regis_anno: Registro anno • pi_regis_nump : Registro numero prima registrazione • pi_regis_numu : Registro numero ultima registrazione • pi_regis_datap : Registro data prima registrazione • pi_regis_datau: Registro data ultima registrazione • pi_mail_mitt: Indirizzo email mittente	

	• pi_mail_dest: Indirizzo email destinatario	

2.1.2 Controlli da effettuare sui set di metadati obbligatori

Il sistema di conservazione, sulla base delle indicazioni recepite dalla normativa, effettua un controllo[2] sulla presenza dei metadati obbligatori versati a corredo dei documenti amministrativi informatici e dei documenti informatici. Il Titolare dell'oggetto di conservazione richiede che questo controllo venga effettuato a livello di:

☒	**WARNING NON BLOCCANTE (*modalità Permissive*)**: il titolare dell'oggetto di conservazione dichiara di non essere in grado di produrre i metadati obbligatori previsti dall'allegato 5 delle Linee Guida, pertanto chiede ad Unimatica SpA di procedere con la conservazione delle tipologie documentali elencate con i soli metadati riportati nella tabella di cui sopra. Il sistema di conservazione, in assenza di uno o più metadati obbligatori, deve segnalare tramite un warning che il versamento non è conforme alla normativa vigente ma deve comunque procedere con la conservazione del contenuto del Pacchetto di Versamento ricevuto.
☐	**ERRORE BLOCCANTE (*modalità Strict*):** il sistema di conservazione deve rifiutare il versamento di documenti privi di anche uno solo dei metadati obbligatori previsti dall'allegato 5 delle Linee Guida.
☐	**NESSUN ERRORE (*modalità Skip*):** applicato a tutti i soggetti produttori stranieri, non vincolati alla normativa italiana (Codice dell'Amministrazione Digitale e Linee Guida). In questo caso i metadati obbligatori sono concordati con il soggetto produttore in base alle buone prassi o ai vincoli normativi del paese di origine.

2.2 Modalità di trasmissione degli oggetti documentali al sistema di conservazione

Vengono elencate, per ogni tipologia documentale riportata precedentemente, le relative modalità di trasmissione: (es.: Upload Manuale tramite interfaccia web, Web Services, SFTP.)

Tipo Documento	Trasmissione
Tutti	Web Services

2 Il controllo viene effettuato verificando la presenza dei metadati versati con le label riportate nelle tabelle richiamate al capitolo 2.1.1 del presente documento.

3 Configurazione verifica iniziale

Vengono elencate le modalità con le quali i documenti in ingresso vengono verificati; i parametri possibili sono:

- **Permetti il versamento di un documento con certificato non ancora valido**: se abilitato si accettano certificati non ancora validi
- **Permetti il versamento di un documento con certificato non *trusted***: se abilitato si accettano certificati con catena *trusted* non valida
- **Permetti il versamento di un documento con certificato revocato**: se abilitato si accettano certificati revocati
- **Permetti il versamento di un documento con certificato scaduto**: se abilitato si accettano certificati scaduti
- **Permetti il versamento di un file alterato**: se abilitato si accettano file alterati
- **Permetti il versamento di documenti non firmati digitalmente**: indica se accettare nel sistema di conservazione documenti informatici privi di firma elettronica
- **Effettua le verifiche sui certificati di firma dei documenti versati**: indica se effettuare tutti i controlli di validità (inizio validità, scadenza, usage, revoca, trust...) dei certificati di firma digitale durante le verifiche prima di accettare un versamento.
- **Effettua le verifiche relative ai controlli di revoca dei certificati di firma dei documenti versati**: indica se effettuare o meno i soli controlli di revoca relativi alle Certificate Revocation List (CRL) dei certificati di firma digitale durante le verifiche prima di accettare un versamento.
- **Effettua le verifiche sulla catena *trusted* dei certificati di firma dei documenti versati**: indica se effettuare o meno il controllo di affidabilità del certificato per una firma digitale durante le verifiche prima di accettare un versamento.

3.2 Tabella contenente i controlli effettuati per le varie tipologie di documento

Tipo documento	Controlli disponibili	Stato
TUTTI	Permetti il versamento di un documento con certificato non ancora valido	☐
	Permetti il versamento di un documento con certificato non *trusted*	☐
	Permetti il versamento di un documento con certificato revocato	☐
	Permetti il versamento di un documento con certificato scaduto	☐
	Permetti il versamento di un documento alterato	☐
	Permetti il versamento di documenti non firmati digitalmente	☒
	Effettua le verifiche sui certificati di firma dei documenti versati	☒
	Effettua le verifiche relative ai controlli di revoca dei certificati di firma dei documenti versati	☒
	Effettua le verifiche sulla catena *trusted* dei certificati di firma dei documenti versati	☒

Se non diversamente specificato la configurazione di default prevede che vengano attivate le seguenti opzioni:

- Permetti il versamento di documenti non firmati digitalmente
- Effettua le verifiche sui certificati di firma dei documenti versati
- Effettua le verifiche relative ai controlli di revoca dei certificati di firma dei documenti versati
- Effettua le verifiche sulla catena *trusted* dei certificati di firma dei documenti versati

4 Gestione Pacchetti di Archiviazione (PdA)

4.1 Regole Creazione PdA

I criteri per la creazione dei PdA si determinano impostando dei criteri sia sui metadati del documento sia sui dati sia sulle proprietà, elenchiamo di seguito le proprietà disponibili:

- Formato File
- Stato Archiviazione (Non Conservato)
- Tipo Documento
- Dalla Data Scadenza Firma
- Alla Data Scadenza Firma
- Dalla Data Inserimento
- Alla Data Inserimento
- Firma (Tutti, Firmati Validi e Invalidi, Firmati Validi, Firmati Invalidi, Non Firmati e Firmati Invalidi, Non Firmati e Firmati Validi)
- Forza Conservazione valori possibili: Attivo, Disattivo
- Forza Accettazione valori possibili: Attivo, Disattivo

esempio di una regola per la creazione dei blocchi

- Formati file= Tutti
- Stato Conservazione =Non Conservato
- Firma=Tutti
- Forza Conservazione=Attivo
- Forza Accettazione=Attivo

Nome regola	Criteri regola
Tipo documento	Tutti, suddivisi per tipologia
Stato archiviazione	NON_CONSERVATO
Firma	TUTTI

Se non diversamente specificato la regola è:

- Stato Conservazione =Non Conservato
- Formati file= Tutti
- Suddivisi per *Tipo documento*

4.2 Regole Chiusura Pacchetti di Archiviazione

La chiusura dei PdA può avvenire o per raggiunta dimensione massima o per tempo di apertura.

Esempio regola chiusura: *Chiudi il PdA quando ha una dimensione di 30 MB o al raggiungimento del 6° giorno di apertura*.

Nome regola	Criteri Chiusura
Tipologia documento	Tutti (suddivisi per tipologia documentale)
Soglia massima	60 MB
Anzianità dei documenti in PDA aperti	10 giorni

Nome regola	Criteri Chiusura
Tipologia documento	REGISTRODIPROTOCOLLO
Soglia massima	30 MB
Anzianità dei documenti in PDA aperti	1 giorno

5 Varie

5.1 Esigenze di accessibilità e fruizione

Il soggetto titolare dell'oggetto di conservazione ha la facoltà di consultare, tramite un applicativo web, l'insieme dei documenti archiviati, con possibilità di ricerca sulla base di metadati trasmessi al sistema di archiviazione.

Per questo motivo vengono definite le seguenti figure:

Utente	Ruolo	Email
Emanuele Uda	Operatore del portale	
Isabella Miscali	Visitatore del portale	

I ruoli ammessi sono:

Ruolo	Autorizzazioni
Visitatore del portale	• Ricerca documenti generici
Operatore del portale	• Upload manuale da interfaccia web

Luogo, data

Comune di _____
Ruolo
Nome e Cognome
_____

Per accettazione:
Bologna,

Unimatica SpA
f.to dal Responsabile del servizio di conservazione o
dal suo Delegato

_____

☒	Documento informatico firmato digitalmente ai sensi del Testo Unico D.P.R. 28 dicembre 2000 n. 445 e del D.Lgs 7 marzo 2005 n. 82 e norme collegate.

MANUALE DEL SISTEMA DI CONSERVAZIONE

Sommario

Registro delle versioni 4
1. Scopo e ambito del documento 6
1.1. Trattamento dei dati personali 6
1.2. Trasparenza 8
2. Terminologia 10
3. Normativa e standard di riferimento 15
3.1. Normativa di Riferimento 15
3.2. Standard di Riferimento 16
4. Ruoli e responsabilità 18
4.1. Ruoli di ausilio al processo di conservazione 21
4.2. Precedenti responsabili 22
5. Struttura organizzativa per il servizio di conservazione 23
5.1. Organigramma 23
5.2. Strutture organizzative 24
6. Oggetti sottoposti a conservazione 27
6.1. Metadati 27
6.1.1 Metadati del documento informatico 28
6.1.2 Metadati del documento amministrativo informatico 30
6.1.3 Metadati delle aggregazioni documentali informatiche 32
6.1.4 Metadati del documento informatico di natura fiscale e contabile 36
6.2 Formati 36
6.2.1 Riversamento 36
6.3 Struttura dati del Pacchetto di versamento 37
6.4 Struttura dati del Pacchetto di archiviazione 37
6.5 Struttura dati del Pacchetto di distribuzione 37
7. Il processo di erogazione del servizio di conservazione 39
7.1. Il processo di conservazione 39
7.2. Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico 40
7.3. Verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti 41
7.4. Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico 42
7.5. Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie 43
7.6. Preparazione e gestione dei Pacchetti di archiviazione 43
7.7. Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione 44
7.8. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento di un pubblico ufficiale 45
7.9. Scarto dei Pacchetti di archiviazione 45
7.10. Predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori 46
7.11. Chiusura del contratto 47
8. Procedure di gestione e di evoluzione 48
8.1. Misure di sicurezza logica 48
8.1.1 Gestione utenze 48
8.1.2 Gestione sistemi di protezione 49
8.1.3 Gestione degli incidenti di sicurezza 49
8.1.4 Gestione dei backup e Disaster Recovery 50
8.1.4.1 Siti Settimo Torinese (TO) e Firenze 50
8.1.4.2 Siti di Cornaredo (MI) e Roma 51
8.1.4.3 Disaster Recovery 52
8.1.5 Gestione dei supporti di memorizzazione 52
8.2. Procedure di evoluzione e Change management 53
8.3. Cessazione del Servizio di conservazione 53
9. Monitoraggio e controlli 54
9.1 Audit interni e Verifica dell'integrità degli archivi 54

9.2 Reportistica di servizio 55
10. La server farm di Unimatica 56
Appendice A 57

Indice delle figure

Figura 1 - Modello OAIS 38

Registro delle versioni

Revisione	Data	Motivo Revisione	Redatto da	Approvato da
1.0	03/10/2009	Emissione	AA	SG
2.0	12/02/2010	Aggiornamento funzionalità	AA	SG
3.0	20/06/2010	Aggiornamento funzionalità	AA	SG
4.0	28/09/2010	Aggiornamento funzionalità	AA	SG
5.0	15/10/2010	Aggiornamento funzionalità	AA	SG
6.0	10/02/2011	Modifica gestione anomalie – Ampliamento funzionalità Unistorage	AA	SG
7.0	20/05/2011	Aggiornamento composizione societaria Unimatica	AA	SG
8.0	30/11/2012	Aggiornamento Data Center	AA	SG
8.1	11/12/2012	Personalizzazioni	AA	SG
8.2	20/06/2013	Aggiornamento compiti e responsabilità della conservazione	SF	AA
8.3	04/07/2013	Aggiornamento normative	SF	AA
8.4	05/02/2014	Aggiornamento normative	SF	AA
8.5	11/02/2014	Aggiornamento Data Center	SF	AA
8.6	05/03/2014	Adeguamento normative	SF	AA
8.7	17/02/2015	Adeguamento DPCM 03/12/2013	RR	SG
8.8	15/10/2015	Passaggio alla ISO 27001:2013	RR	SG
8.9	20/01/2016	Adeguamento Schema Manuale della conservazione AgID	RR	SG
9.0	11/04/2017	Modifica ruolo Responsabile della Funzione Archivistica	RR	SG
9.1	14/06/2017	Aggiornamento definizioni per termine “Produttore”	RR	SG
9.2	05/10/2017	· Aggiornamento Server farm · Visualizzazione di 200 risultati da portale	RR	SG
9.3	20/10/2017	· Capitolo Trasparenza · Aggiornamento elenco formati · Aggiunto testo alternativo mancante su alcune immagini · Sostituita immagine 7 precedentemente con parti nascoste	RR	SG
9.4	25/10/2018	· Aggiornamento par. 1.1 adeguamento GDPR · Modifica ruolo Privacy Manager cap. 4 · Aggiornamento tabella normativa par. 3.1 · Aggiunto ruolo DPO al par.4.1	RR	SG
9.5	29/01/2019	· Recepimento N.C. AgID Recepimento Oss. Audit interno · Aggiornamento Nomina ad Interim Responsabile della funzione archivistica · Aggiornamento proc. Gestione Incident par. 8.1.3	RR	SG
9.6	19/04/2019	· Revoca nomina ad Interim per la Responsabilità della funzione archivistica · Aggiornamento nomina ad interim DPO	RR	SG
9.7	27/09/2019	· Aggiornamento Ruoli (Delegato Responsabile del servizio di conservazione – Responsabile dello sviluppo e della manutenzione – Responsabile dei sistemi informative – DPO) · Aggiornamento proc. Gestione Incident par. 8.1.3 · Aggiornamento estensioni ISO 27017 – 27018 · Aggiornamento descrizione par. 7.5 Rifiuto PDV	RR PV	SG
9.8	20/12/2019	· Aggiornamento capp. 4 e 5 a seguito della sostituzione del Delegato alla Responsabilità del servizio di conservazone, della Responsabile della funzione archivistica e della Responsabile dello sviluppo e manutenzione · A seguito delle NC ricevute in fase di audit è stato eliminato il par. 9.2 ed aggiornato il par. 8.1.3 sulla Gestione degli incident di sicurezza.	RR PV	SG

9.9	13/01/2021	· Aggiornamento cap. 4 a seguito di Oss da Audit interno. Aggiunto nominativo Resp. dello sviluppo in carica. · Aggiornamento tabella formati par. 6.2	RR	SG
10	13/09/2021	· Aggiornamenti a seguito del cambio ragione sociale · Aggiornamento par. 1.1 sulla privacy · Aggiornamento par. 1.2 per certificazione ISO 14001 · Aggiornamento modifica sito d/r secondario Acilia (RM)	RR	SG
11	30/12/2021	· Aggiornamento a seguito dell'adeguamento alle Linee guida per la formazione, gestione e conservazione del documento informatico (revisionati cap. 1-2-3-4-6-7)	EL	PV
12	21/06/2022	· Capitolo 4.1.: riportato nuovo responsabile del servizio; rimossa evidenza della delega assegnata a PV dal precedente responsabile del servizio; · Aggiunto capitolo '4.2. Precedenti responsabili' · Rivisto capitolo '5.1. Organigramma' in funzione della nuova nomina	EL	PV
13	01/09/2022	· Indicazione socio unico a piede pagina	EL	PV
14	30/01/2023	· Aggiornamento logo RINA alla ISO 37001	EL	PV
15	22/08/2023	· Aggiornamento nominativi organigramma; · Aggiornamento paragrafo 4.2 "Precedenti resposabili"	EL	PV
16	22/12/2023	· Aggiornamento logo Unimatica – a Namirial Company · Aggiornamento cap. 1.1 Trattamento dei dati personali	EL	PV
17	12/06/2024	· Aggiornamento Ruolo Responsabile del Servizio di Conservazione; · Aggiornamento logo Unimatica	EL	CC
18	04/07/2024	· Revisione dei processi di scarto, di produzione PdD e di fine contratto	CC EL	CC
19	02/12/2024	· Specifica sulle modalità di accesso al portale di conservazione	CC	CC
20	05/05/2025	· Aggiornamento dati sede legale Unimatica; · Aggiornamento logo RINA alla UNI PdR 125 Parità di Genere; · Aggiunta Allegato " Unimatica Data Center"	EL	CC

1. Scopo e ambito del documento

Il presente documento costituisce il Manuale del servizio di conservazione erogato da Unimatica ed ha lo scopo di illustrare la struttura del sistema di conservazione descrivendone analiticamente gli oggetti sottoposti a conservazione, il processo di conservazione e le componenti logiche, tecnologiche e fisiche relative al suo funzionamento. Delinea, inoltre, i soggetti che sono coinvolti nelle attività e nei processi di conservazione i quali hanno la responsabilità del sistema.

Il Manuale del servizio unitamente alla Scheda cliente predisposta da Unimatica, al fine di personalizzare il rapporto contrattuale con il Cliente Soggetto produttore (da ora in poi Soggetto produttore), costituiscono parte integrante del contratto di fornitura del servizio e mira a garantire e illustrare formalmente ai propri clienti il sistema di conservazione e le sue caratteristiche di disponibilità nel tempo di documenti integri, autentici, legalmente validi e facilmente consultabili.

Questo documento è reso disponibile a tutte le parti interessate a seguito di apposita richiesta.

Torna al sommario

1.1. Trattamento dei dati personali

Ai sensi e per gli effetti dell'articolo 28 del Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora innanzi anche "GDPR" o "Regolamento") e del D.lgs. 30 giugno 2003 n. 196, relativamente e limitatamente ai trattamenti riguardanti la conservazione degli oggetti digitali affidati a Unimatica, a partire dalla data di sottoscrizione del contratto, il Soggetto produttore, nella sua qualità di Titolare del trattamento, affida a Unimatica, che diventa Responsabile del trattamento dei dati personali trattati in esecuzione del contratto, i seguenti compiti e impartisce le seguenti istruzioni per il trattamento dei dati cui Unimatica deve attenersi:

1. Unimatica per espletare le attività pattuite per conto del Soggetto produttore potrebbe trattare direttamente o anche solo indirettamente una o più delle seguenti categorie di dati:

   - dati personali,
   - dati rientranti nelle categorie "particolari" di dati personali,
   - dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza,

   di cui è Titolare il Soggetto produttore. Per i dettagli, occorre fare riferimento a quanto pattuito nel contratto/ordine/accordo.
2. I dati trattati da Unimatica si riferiscono potenzialmente, a titolo esemplificativo, ma non esaustivo, alle seguenti categorie di interessati: clienti, dipendenti, utenti, fornitori, richiedenti impiego, soci, etc.
3. Il trattamento dei dati in questione è effettuato da Unimatica esclusivamente per lo svolgimento del servizio di Conservazione a norma, in modo lecito e secondo correttezza, attenendosi alle prescrizioni della normativa sulla protezione dei dati personali nonché alle previsioni della specifica delega a Responsabile del Servizio di Conservazione o successivamente concordate tra le parti; è fatto esplicito divieto di diffondere o comunicare i dati in questione a soggetti che siano estranei all'esecuzione del trattamento.
4. Unimatica, nella sua qualità di Responsabile del trattamento, in particolare è tenuta a:
   a) trattare direttamente, o per il tramite dei propri dipendenti, collaboratori, consulenti - designati incaricati del trattamento - i dati personali del Titolare, per le sole finalità connesse allo svolgimento delle attività previste dal contratto/ordine/accordo, in modo lecito e secondo correttezza, nonché nel pieno rispetto delle disposizioni impartite dal GDPR e delle presenti istruzioni;

b) non diffondere o divulgare o rendere noti a terzi -per alcuna ragione ed in alcun momento, presente o futuro ed anche una volta cessati i trattamenti oggetto del contratto/ordine/accordo- i dati personali ricevuti dal Titolare o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, se non previamente autorizzato per iscritto dal Titolare, fatti salvi eventuali obblighi di legge o ordini dell'Autorità Giudiziaria e/o di competenti Autorità amministrative;

c) collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;

d) non creare banche dati nuove senza espressa autorizzazione del Titolare, fatto salvo quando ciò risulti strettamente indispensabile ai fini dell'esecuzione degli obblighi assunti;

e) in caso di ricezione di richieste specifiche avanzate dall'Autorità Nazionale per la protezione dei dati personali o altre Autorità, coadiuvare il Titolare per quanto di propria competenza;

f) segnalare eventuali criticità al Titolare che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;

g) vigilare affinché i dati personali degli interessati vengano comunicati solo a quei soggetti preventivamente autorizzati dal Titolare che presentino garanzie sufficienti secondo le procedure di autorizzazione disposte e comunicate dal Titolare. Sono altresì consentite le comunicazioni richieste per legge nei confronti di soggetti pubblici.

5. Istruzioni specifiche per il trattamento dati particolari e/o relativi a condanne penali e reati. Il Titolare indica al Responsabile la presenza nei propri documenti di tali categorie di dati nel contratto/ordine/accordo e nella scheda cliente/scheda tecnica/scheda di attivazione. Nel caso di trattamento di tali dati, il Responsabile, oltre a quanto già sopra garantito, si impegna a:

a) prestare particolare attenzione al trattamento di tali dati conosciuti in esecuzione dell'incarico affidato, procedendo al loro trattamento solo ove ciò si renda necessario per lo svolgimento delle attività di competenza e istruendo in tal senso le persone autorizzate che operano all'interno della propria struttura;

b) gestire la documentazione contenente tali dati adottando, implementando e aggiornando misure di sicurezza adeguate e idonee, concordate con il Titolare, al fine di evitare accessi non autorizzati, distruzione, perdita e/o qualunque violazione dei dati.

6. Il trattamento dei dati deve intendersi effettuato sotto la vigilanza del Soggetto produttore il quale, in ogni momento e con congruo preavviso, potrà operare controlli e impartire eventuali ulteriori specifiche istruzioni per il suo svolgimento, nonché chiederne la cessazione se imposta dalla necessità di adempiere a divieti od obblighi di legge, ovvero a provvedimenti dell'Autorità Garante e/o Giudiziaria.

7. Sicurezza dei dati personali. Il Responsabile, ai sensi dell'art. 32 del GDPR, deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio (di distruzione, di perdita, di modifica, di divulgazione non autorizzata o dell'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati) di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

   Il Titolare concorda sulle misure di sicurezza adottate dal Responsabile e le ritiene adeguate. Il Responsabile, su richiesta, fornirà al Titolare l'elenco aggiornato delle misure di sicurezza adottate, in particolare, in merito alle Politiche di crittografia si rimanda al documento di dettaglio presente al seguente link: https://www.unimaticaspa.it/it/trasparenza-dei-servizi.

8. Unimatica si impegna a notificare al Titolare, senza ingiustificato ritardo e, ove possibile, entro 24 ore dal momento in cui è venuto a conoscenza, con comunicazione da inviarsi all'indirizzo PEC del Titolare ogni violazione dei dati personali (data breach) che riguardi il trattamento di cui in argomento. Ulteriori informazioni possono essere fornite dal Responsabile, su richiesta, anche successivamente e appena disponibili senza giustificato ritardo. Il Responsabile si

impegna a prestare assistenza al Titolare al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32 - 34 del GDPR.

9. In esecuzione degli accordi in essere, il Titolare del trattamento concede al Responsabile l'autorizzazione generale ad affidare l'attività -parziale o totale- a soggetti terzi, dei quali garantisce il possesso dei requisiti di esperienza, capacità ed affidabilità, ivi compreso il profilo relativo alla sicurezza. Ove ricorra tale ipotesi, il Responsabile provvede personalmente a designare Responsabili del trattamento ai sensi dell'art. 28 del GDPR i suddetti soggetti terzi (nel seguito anche "Sub-Responsabile del trattamento") con idoneo atto giuridico e ne dà notizia al Titolare tramite la pubblicazione dell'elenco sul proprio sito web al seguente link: https://www.unimaticaspa.it/it/gdpr-elenco-sub-responsabili. Il Titolare può opporsi entro e non oltre 14 giorni dalla pubblicazione.
10. Unimatica assicura che nessun dato personale potrà essere trasferito all'esterno dell'Area Economica Europea (EEA).
11. Premesso che l'accesso ai dati personali da parte degli interessati esercitato ai sensi degli artt. 15 e seguenti del GDPR sarà gestito direttamente dal Soggetto produttore, Unimatica si rende disponibile a collaborare con il Soggetto produttore stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.
12. Unimatica – ove tale obbligo si applichi anche alla stessa, nella sua qualità di Responsabile del trattamento e in base alle disposizioni del comma 5 dell'art. 30 del GDPR - mantiene un registro di tutte le categorie di attività relative al trattamento svolte per conto del Soggetto produttore.
13. Unimatica si impegna a mettere a disposizione del Soggetto produttore tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di sicurezza descritti nel presente documento e, in generale, il rispetto delle obbligazioni assunte in forza del GDPR, consentendo e, su richiesta, contribuendo alle attività di audit, comprese le ispezioni, realizzate dal Soggetto produttore o da altro soggetto da esso incaricato.
14. L'autorizzazione al trattamento dei dati personali avrà la medesima validità ed efficacia della durata della conservazione legale dei documenti, stabilita dalla normativa.

Torna al sommario

1.2. Trasparenza

La conservazione a norma di Unimatica è rivolta a Pubbliche amministrazioni, banche, assicurazioni, strutture sanitarie ed ai privati in genere.
Al fine di rendere tali servizi agevoli ed accessibili ad un pubblico variegato e disomogeneo, Unimatica rende disponibili una serie di strumenti ed informazioni utili a garantire una totale trasparenza delle proprie attività mediante canali diretti ed indiretti.
In generale, nel sito internet aziendale www.unimaticaspa.it sono disponibili:

- i contatti principali quali telefono, fax, email ed indirizzo.
- La certificazione per la Qualità ISO 9001:2015 (Unimatica è certificata dal 2006)
- La certificazione per il Sistema di Gestione Ambientale ISO 14001:2015
- La certificazione per la Sicurezza delle Informazioni ISO 27001:2013 (Unimatica è certificata dal 2014) con estensioni alle Linee guida ISO 27017:2015, ISO 27018:2019 ed ISO 27701:2019
- Il Codice Etico aziendale

- Il Modello di Organizzazione, Gestione e Controllo (MOG), ai sensi della L. 231/01 (consultabile a richiesta)
- La Politica Aziendale (consultabile a richiesta)
- L'elenco delle Associazioni di cui l'azienda fa parte e delle Partnership tecnico/commerciali
- La descrizione dei servizi e prodotti offerti dall'azienda e le modalità attraverso cui ottenere informazioni dettagliate su di essi e su come richiederli
- Le informazioni sulle principali attività svolte o in corso

Oltre alle certificazioni sopra elencate, Unimatica ha implementato un sistema di gestione anticorruzione ISO 37001:2016.
Tale certificazione, obbligatoria ai fini dell'adeguamento alle Linee guida per la formazione, gestione e conservazione dei documenti informatici in vigore dal 1° gennaio 2022, è stata aggiunta alle altre presenti nella sezione Trasparenza.

Negli anni, il settore Conservazione di Unimatica ha ottemperato a tutti gli obblighi normativi applicabili. Nello specifico, infatti, da marzo del 2015 ha mantenuto l'accreditamento presso l'Agenzia per l'Italia Digitale (AgID) con la pubblicazione del Manuale della conservazione nell'apposita area a ciò dedicata sul sito web di AgID.
Dall'ottobre del 2017 fino ad abrogazione, in continuità con le disposizioni normative, ha ottenuto e mantenuto la certificazione in conformità all'art. 24 del Regolamento eIDAS e alla check list "*Lista di riscontro per la visita ispettiva AgID e la certificazione di conformità*".
Tali strumenti, oltre ad essere sinonimo di eccellenza, sono risultati negli anni passi indispensabili per la crescita dell'azienda, del team e per migliorare continuamente il prodotto Unistorage e il servizio offerto ai clienti.

Unimatica considera altrettanto importante il concetto di trasparenza rivolto ai propri dipendenti. Sull'intranet aziendale, infatti, ogni dipendente ha a disposizione strumenti e materiali informativi relativi al sistema di gestione integrato della Qualità, della Sicurezza, dell'Ambiente, della Privacy e dell'Anticorruzione (ISO/IEC 27001, ISO 9001, ISO 14001, ISO 37001) e a tutte le Procedure di conservazione. L'impegno, l'attenzione, la formazione e le competenze di tutta l'azienda sulla tematica specifica ed i risultati raggiunti nel corso degli anni di attività hanno permesso ad Unimatica di ottenere l'iscrizione quale socio sostenitore presso l'associazione ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale).

Per dimostrare trasparenza ed affidabilità, inoltre, Unimatica garantisce da sempre la propria disponibilità ad ospitare audit finanziari e/o di seconda parte, rispettando così le disposizioni delle autorità di controllo e, previo accordo, anche gli accordi stabiliti con clienti per i quali presta servizi.

Torna al sommario

2. Terminologia

TERMINE	DEFINIZIONE
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
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, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti.
Convenzioni di denominazione del file	Anche detta *Naming convention*, è l'insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato.
Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva

Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
Esibizione	Operazione che consente di visualizzare un documento conservato.
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di *bit* che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
Firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare; (art.3 del Regolamento eIDAS).
Firma elettronica avanzata	Per essere definite tale una FEA deve soddisfare I seguenti requisiti: essere connessa unicamente al firmatario; essere idonea a identificare il firmatario; essere creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; essere collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati; (artt. 3 e 26 del Regolamento eIDAS).
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche; (art. 3 del Regolamento eIDAS).
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzione di *hash* crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
Hash	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.

Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture. Con l'entrata in vigore delle LLGG AgID sulla formazione, gestione e conservazione dei documenti informatici (1 gennaio 2022) vengono sancite due forme distinte di manuale di conservazione: uno proprio del soggetto conservatore e uno proprio del Titolare dell'oggetto di conservazione.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
Pacchetto di archiviazione (PdA)	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione (PdD)	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di file (*file package*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
Pacchetto di versamento (PdV)	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
Pathname	Concatenazione ordinata del percorso di un file e del suo nome.
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso. Detto anche *path.*
Periodo di conservazione dei documenti	La durata temporale per ciascuna tipologia documentale, espressa in anni, per la quale il Soggetto produttore richiede il servizio di conservazione. Tale durata temporale sarà riportata all'interno del piano di conservazione, qualora redatto dal Soggetto produttore,
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio,

	di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Piano di organizzazione delle aggregazioni documentali	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione
Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Responsabile del servizio di conservazione	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. Nella PA il ruolo deve essere rivestito da un soggetto interno all'organigramma; negli enti privati può essere rivestito da un soggetto interno all'organigramma o da un soggetto esterno, purchè diverso dal Conservatore a cui si è affidato il servizio di conservazione dei documenti informatici.
Responsabile della funzione archivistica di conservazione	Soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.

Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Termine del contratto del servizio di conservazione	Termine contrattualmente previsto per il servizio di conservazione occorso il quale il Titolare dell'oggetto di conservazione può decidere se estendere il contratto o optare per la restituzione dei documenti conservati..
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione e per estensione eventuali soggetti terzi delegati.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Torna al sommario

3. Normativa e standard di riferimento

Il sistema di conservazione sviluppato da Unimatica è conforme alla normativa e agli standard elencati nei successivi paragrafi.

Periodicamente vengono effettuate verifiche per l'aggiornamento dei requisiti normativi al fine di assicurare una puntuale conformità alle disposizioni legislative. Eventuali ulteriori riferimenti normativi non direttamente riconducibili alla conservazione, ma comunque applicabili per via di servizi correlati ad essa, sono elencati in uno specifico documento facente parte del sistema di gestione integrato, denominato SIC040 – Monitoraggio.

Torna al sommario

3.1. Normativa di Riferimento

Notazione abbreviata	Riferimento
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], art. 2215 bis – Documentazione informatica.
RD 1163/1911	Regolamento per gli archivi di Stato
DPR 1409/1963	Norme relative all'ordinamento ed al personale degli archivi di Stato
Legge 241/1990	Nuove norme sul procedimento amministrativo
DPR 445/2000	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
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
D.lgs 196/2003	Recante il Codice in materia di protezione dei dati personali
D.lgs 42/2004	Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n.137
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
D.lgs 82/2005 e ss.mm.ii.	Codice dell'amministrazione digitale
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
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
DPCM 21 marzo 2013	Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
Reg. 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;
Circolare 40 e 41 del 14 dicembre 2015 della	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;

Direzione generale degli archivi	
Reg. 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;
Circolare 18 aprile 2017 n. 2/2017 dell'Agenzia per l'Italia Digitale	Recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
Circolare n. 2 del 9 aprile 2018	Recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
Circolare n. 3 del 9 aprile 2018	Recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
Reg. UE 2018/1807	Relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;
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.
Linee guida AgID ed Allegati	Linee guida sulla Formazione, Gestione, Conservazione dei documenti informatici Allegato 1 Glossario dei termini e degli acronimi Allegato 2 Formati di File e Riversamento Allegato 3 Certificazione di processo Allegato 4 Standard e specifiche tecniche Allegato 5 Metadati
Regolamento AgID ed Allegati	Regolamento sui criteri di conservazione Allegato A Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni Allegato B Piano di cessazione del servizio di conservazione dei documenti informatici

Torna al sommario

3.2. Standard di Riferimento

Sigla	Titolo standard
UNI 11386	Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
ISO 14721	OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.
ISO 15836	Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core
ISO/TR 18492	Long-term preservation of electronic document-based information.
ISO 20652	Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard.
ISO 20104	Space data and information transfer systems — Producer-Archive Interface Specification (PAIS).
ISO/CD TR 26102	Requirements for long-term preservation of electronic records.
SIARD	Software Independent Archiving of Relational Databases 2.0 Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
METS	Metadata Encoding and Transmission Standard
PREMIS	PREservation Metadata: Implementation Strategies.
EAD 3	Encoded Archival Description
ISAD (G)	General International Standard Archival Description

EAC-CPF 2.0	Encoded Archival Context-Corporate Bodies, Persons and Families
ISAAR (CPF)	International Standard Archival Authority Records for Corporate Bodies, Persons and Families
ISDIAH	International Standard for Describing Institutions with Archival Holdings
NIERA (EPF)	Norme italiane per l'elaborazione dei record di autorità archivistici di enti, persone, famiglie

Torna al sommario

4. Ruoli e responsabilità

Conformemente al par. 4.4 delle Linee guida sulla Formazione, gestione e conservazione dei documenti informatici, si individuano i seguenti ruoli coinvolti nel processo di conservazione:

- **Titolare dell'oggetto di conservazione** (citato nel manuale come soggetto produttore), identificato come il soggetto produttore degli oggetti di conservazione.
- **Produttore dei PdV**, ovvero 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, identificato con il responsabile della gestione documentale nelle pubbliche amministrazioni
- **Utente abilitato**, ossia la persona, l'ente o il sistema che interagisce con i servizi di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
- **Responsabile della conservazione**, ovvero il soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
- **Conservatore**, è quella figura che si occupa dell'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, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti.

Il processo di conservazione vede direttamente coinvolti tutti i soggetti sopra elencati.

Unimatica ha individuato le seguenti figure di responsabilità per l'erogazione del servizio di conservazione, a garanzia di elevati standard di qualità e sicurezza:

Il **Responsabile del servizio di conservazione** espleta, a seguito di delega formale e in ogni caso rimanendo inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, le seguenti attività:

1. 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
2. gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
3. genera e sottoscrive il Rapporto di Versamento, secondo le modalità previste dal manuale di conservazione;
4. genera il pacchetto di archiviazione conforme allo Standard SInCRO UNI 11386 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali e lo sottoscrive con firma digitale;
5. genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione, ai fini dell'esibizione richiesta dall'utente;

6. effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
7. 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;
8. 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;
9. provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
10. adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
11. 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;
12. assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
13. 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

garantendo un particolare riguardo alla:

- 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 all'ente produttore;
- 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.

Il **Responsabile del servizio di conservazione** nominato da Unimatica è **Cecilia Canova**.

In assenza del Responsabile del servizio di conservazione, le sue funzioni operative vengono delegate a **Valentina Vetri.**

Il **Responsabile della funzione archivistica di conservazione**, in accordo con il Responsabile del servizio di conservazione, si occupa di

- definire e gestire il processo di conservazione, incluse le modalità di trasferimento da parte del produttore dei PDV, 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

- monitorare set di metadati di conservazione dei documenti, dei fascicoli informatici e delle aggregazioni documentali informatiche
- monitorare il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema
- collaborare con il Produttore dei PDV 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.

La **Responsabile della funzione archivistica di conservazione** nominata da Unimatica è **Eleonora Luzi.**

Responsabile sicurezza dei sistemi per la conservazione il quale si occupa di:

- monitorare e rispettare i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. In caso di eventuali difformità si occupa di segnalarle al Responsabile del servizio di conservazione e, quindi, individua e pianifica le necessarie azioni correttive.

Il **Responsabile sicurezza dei sistemi per la conservazione** nominato da Unimatica è **Massimo Ortensi**.

Responsabile dei sistemi informativi per la conservazione il quale si occupa di:

- gestire l'esercizio delle componenti hardware e software del sistema di conservazione e monitorare il mantenimento dei livelli di servizio (SLA) concordati con il Titolare e il Produttore
- segnalare le eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuare e pianificare le necessarie azioni correttive
- pianificare lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione e verifica i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.

Il **Responsabile dei sistemi informativi per la conservazione** nominato da Unimatica è **Massimo Ortensi.**

Responsabile sviluppo e manutenzione del sistema di conservazione il quale si occupa di:

- coordinare lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione
- pianificare e monitorare i progetti di sviluppo del sistema di conservazione
- monitora gli SLA relativi alla manutenzione del sistema di conservazione
- interfacciarsi con il Produttore dei PDV relativamente alle modalità di trasferimento dei documenti, fascicoli informatici e aggregazioni documentali informatiche in merito ai formati

elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche

- gestire lo sviluppo di siti web e portali connessi al servizio di conservazione.

Il **Responsabile dello sviluppo e manutenzione del sistema di conservazione** nominato da Unimatica è **Matteo Rossi**.

Nell'attribuire ruoli e responsabilità Unimatica presta importante attenzione alle competenze delle risorse valutate, vanta infatti personale altamente specializzato e formato sulle tematiche legate alla conservazione e all'archiviazione digitale.

Tale personale è costantemente aggiornato sull'evoluzione della normativa e sugli aspetti tecnologici, grazie alla documentazione interna messa a disposizione dall'azienda e garantisce, inoltre, l'opportunità ai dipendenti di partecipare ad appositi corsi qualificanti di approfondimento, interni ed esterni.

Torna al sommario

4.1. Ruoli di ausilio al processo di conservazione

In ottemperanza a quanto previsto dal Regolamento (UE) 2016/679 Unimatica, al fine di garantire una maggior tutela dei dati propri e di quelli dei clienti, ha nominato un **Data Protection Officer** il quale si occupa di

- offrire idonea consulenza per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, interagendo coi sistemi di gestione aziendali, compreso il sistema di conservazione, per curare l'adozione di misure di sicurezza finalizzate alla tutela dei dati trattati dall'azienda, che soddisfino i requisiti di legge e per evitare i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

La **DPO** nominato da Unimatica è **Anna Veltri.**

Torna al sommario

4.2. Precedenti responsabili

Ruolo	Nominativo	Periodo
Responsabile servizio di conservazione	SG	01/2004 – 06/2022
	PV	06/2022 – 06/2024
Delegato Responsabile del Servizio di Conservazione	AA	01/2009 – 09/2019
	PV	09/2019 – 06/2022
	RN	01/2010 – 12/2019
	CC	12/2019 – 06/2024
Responsabile Funzione Archivistica	SF	01/2012 – 06/2017
	RN	06/2017 – 12/2019
	RR *(ad interim)*	06/2018 – 04/2019
Responsabile Trattamento Dati Personali	SG	01/2004 – 09/2021
	AM	10/2021 – 05/2023
Responsabile Sistemi Informativi per la conservazione	AA	01/2008 – 09/2019
Responsabile Sviluppo e Manutenzione	SG	01/2008 – 09/2019
	PV	09/2019 – 12/2019
	AC	12/2019 – 03/2023
DPO	RR *(ad interim)*	04/2019 – 09/2019

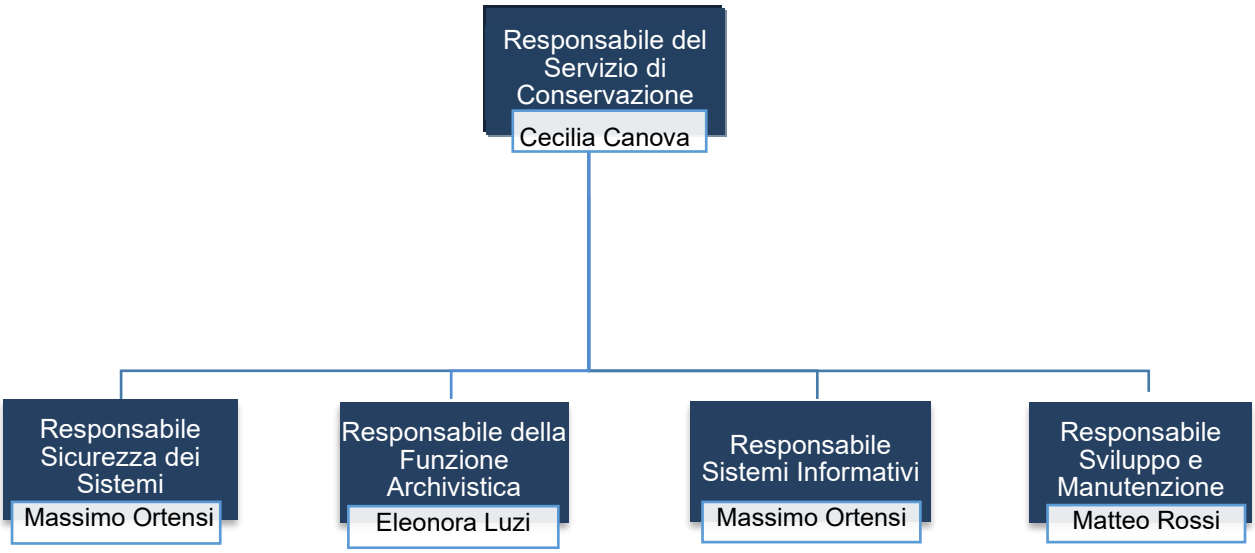
Torna al sommario

5. Struttura organizzativa per il servizio di conservazione

Il presente capitolo ha lo scopo di illustrare la struttura organizzativa del settore conservazione di Unimatica. L' espletamento di un processo di conservazione prevede una serie di complesse attività, pertanto la società si avvale di personale altamente qualificato e con esperienza decennale. Si riporta di seguito l'organigramma della struttura organizzativa e una sintetica descrizione[1] delle funzioni e delle responsabilità che intervengono nel processo di conservazione.

Torna al sommario

5.1. Organigramma



Torna al sommario

[1] La descrizione dettagliata del processo di conservazione è riportata nel capitolo 7 "Il processo di erogazione del servizio di conservazione".

5.2. Strutture organizzative

Nel presente paragrafo vengono descritte sinteticamente le fasi principali del processo di conservazione e le attività di gestione dei sistemi informativi, individuando per ciascuna di queste le figure che ne assumono le responsabilità.

Attività proprie di ciascun contratto di servizio			
Fase	Attività	Descrizione	Responsabilità
1	Attivazione del servizio di conservazione (a seguito della sottoscrizione del contratto).	Il Soggetto produttore invia una richiesta di attivazione del servizio che avviene in seguito alla compilazione del modulo "Scheda cliente" dove vengono dichiarati dettagli degli oggetti da conservare, come: dimensioni, frequenza invio, ecc.	RSC PM RFA RSM
2	Acquisizione, verifica e gestione dei Pacchetti di versamento e generazione del Rapporto di versamento.	Sui PdV vengono effettuate verifiche circa l'identificazione certa del Soggetto produttore, la firma digitale, formati e metadati sulla base di quanto concordato nella Fase 1. In caso di verifiche andate a buon fine viene generato il RdV, altrimenti viene generata la Comunicazione delle anomalie.	RSC RFA
3	Preparazione e gestione dei Pacchetti di archiviazione[2].	Gli oggetti versati vengono trasformati in PdA contenenti, oltre agli oggetti da conservare, l'IdPA[3] formato secondo le regole dello standard SInCRO. L'IdPA viene sottoscritto con firma digitale dal RSC e viene marcato temporalmente.	RSC RFA
4	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.	I PdD, vengono creati in base alle richieste dell'Utente. Possono essere visualizzati mediante interfaccia web, WS o, se richiesto, tramite memorizzazione su supporto.	RSC RFA PM
5	Scarto dei pacchetti di archiviazione	Entro tre mesi prima della scadenza del Periodo di conservazione per i documenti conservati da Unimatica, il Titolare dell'oggetto di conservazione dovrà prendere contatto con Unimatica ed indicare la volontà di continuare la conservazione digitale a norma, con opportuna estensione contrattuale ove necessario, oppure di procedere con l'attività dello scarto.	RSC RFA PM

[2] Traduzione di Archival Information Package dal Modello OAIS Open Archival Information Standard che individua nel sistema di archiviazione tre diversi tipi di Pacchetti: Submission Information Package (SIP), Archival Information Package (AIP) e Dissemination Information Package (DIP).
[3] Indice del pacchetto di archiviazione.

		Qualora ciò avvenga Unimatica attiverà la procedura di scarto e provvederà all'eliminazione delle UD selezionate. Per le UD provenienti da enti pubblici o da archivi privati per i quali è stato dichiarato l'interesse culturale si terrà conto dei piani di conservazione di questi e della decisione ultima della Soprintendenza archivistica. *(Per maggiori dettagli si rimanda al par. 7.9 del presente manuale).*	
6	Chiusura del servizio di conservazione (al termine di un contratto)	Il Titolare dell'oggetto della conservazione, in qualsivoglia momento, ha il diritto di rescindere dal contratto. Qualora ciò avvenga prima del termine previsto per il servizio di conservazione, il Soggetto Produttore potrà richiedere la restituzione dei documenti inviati in conservazione secondo le modalità operative concordate con il RSC. *(Per maggiori dettagli si rimanda al par. 7.11 del presente manuale).*	RSC PM

Attività proprie di gestione dei sistemi informativi			
Fase	Attività	Descrizione	Responsabilità
1	Conduzione e manutenzione del sistema di conservazione	Le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.	RSM RSSI
2	Monitoraggio del sistema di conservazione	Viene effettuato il monitoraggio del sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Tra le attività di monitoraggio rientrano anche la verifica dell'integrità degli archivi e la gestione delle anomalie.	RSC RFA RSSI
3	Change management	Vengono definite politiche, priorità e tempistiche dell'adeguamento all'evoluzione tecnologica affinché il sistema di conservazione possa garantire nel tempo integrità, disponibilità e sicurezza.	RFA RSI

4	Verifica periodica di conformità a normativa e standard di riferimento	La conformità a normativa e standard è costantemente monitorata ed eventualmente aggiornata.	RSC RSSI

Legenda	
RSC	Responsabile del Servizio di Conservazione
RSSI	Responsabile Sicurezza dei Sistemi Informativi per la Conservazione
PM	Privacy Manager
RFA	Responsabile Funzione Archivistica per la Conservazione
RSI	Responsabile Sistemi Informativi per la Conservazione
RSM	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione

Torna al sommario

6. Oggetti sottoposti a conservazione

Unimatica mediante il proprio sistema di conservazione Unistorage, sviluppato integralmente dalla società, è in grado di accettare e gestire, come richiesto ai sensi dell'art. 44, comma 1-bis, del CAD[4],

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 e il Conservatore garantiscono specifico monitoraggio al fine di evitare rischi di obsolescenza tecnologica che possono sopravvenire prima della chiusura.

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

In accordo con il soggetto produttore, Unimatica 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.

Unimatica 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.

Torna al sommario

6.1. Metadati

Come previsto dal par. 4.1 delle Linee guida, il sistema di conservazione assicura dalla presa in carico fino all'eventuale scarto, la conservazione di oggetti digitali tramite l'adozione di regole, procedure e tecnologie, necessarie al mantenimento delle caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Al fine di rendere agevole ed efficiente la ricerca di un documento, di un fascicolo, o di un'aggregazione documentale informatica conservati, è necessario corredare tali oggetti da un set di metadati che ne descrivono il contenuto e lo identificano all'interno del sistema. Unimatica, in piena conformità alle Linee guida e all'Allegato 5, garantisce l'acquisizione, la gestione e la conservazione di:

- Metadati del documento informatico
- Metadati del documento amministrativo informatico
- Metadati delle aggregazioni documentali informatiche
- Metadati del documento informatico di natura fiscale e contabile

Nei paragrafi successivi si elencano per ogni tipologia, a titolo esemplificativo e non esaustivo, i metadati obbligatori individuati dalle Linee guida. Per tutti i dettagli specifici sul lessico, campi e schemi si rimanda alle schede di dettaglio presenti all'interno dell'*Allegato 5* alle Linee guida e

[4] L'art. 44, comma 1-bis, del CAD prevede che: "[…] Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi"

all'Elenco AgID "*L'utilizzo dei metadati del documento informatico - I metadati del documento informatico di natura fiscale e contabile*"

Torna al sommario

6.1.1 Metadati del documento informatico

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi *obbligatori* del documento informatico:

IdDoc: Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione

Il metadato è costituito dai seguenti:

- Impronta: sottocampo in cui viene memorizzato l'hash del documento
- Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"
- Identificativo: come da sistema di identificazione formalmente definito

Modalità di formazione: modalità di generazione del documento informatico

Sono previste le seguenti modalità:

- creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- 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;
- memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Tipologia documentale: metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività

Metadato testuale libero per indicare le tipologie documentali trattate (ad esempio, fatture, delibere, determine, etc)

Dati di registrazione: Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato. Si intende per registrazione l'operazione che, in senso lato, associa ad un documento una data e un numero. In tale ottica, quindi potrebbe non essere identificabile uno specifico registro, ma sono sempre identificabili una data di registrazione e un numero di registrazione del documento.

Sono previsti i seguenti campi:

- Tipologia di flusso: indica se si tratta di un documento in uscita, in entrata o interno.
- Tipo registro: indica il sistema di registrazione adottato: protocollo ordinario/protocollo emergenza, o Repertorio/Registro.
- Data: è la data associata al documento all'atto della registrazione
- Numero documento: Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato.
- Codice Registro: Identificativo del registro nel caso in cui il tipo registro sia protocollo ordinario/ protocollo emergenza, o Repertorio/Registro.

Soggetti: indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo.

Sono definiti i seguenti attributi:

- Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di rendere i dati di registrazione univoci deve essere sempre indicato il Soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla). Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento

Chiave descrittiva: metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura.

È costituito da seguenti campi:

- Oggetto: testo libero

Allegati: Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- IdDoc: Identificativo del documento relativo all'allegato
- Descrizione: Titolo dell'Allegato

Classificazione: classificazione del documento secondo il Piano di classificazione utilizzato da indicare sia nel caso di documento protocollato che nel caso di documento non protocollato (*facoltativo*, per le specifiche si rimanda all'Allegato 5)
Riservato: rappresenta il livello di sicurezza di accesso al documento:

- vero: se il documento è considerato riservato
- falso: se il documento non è considerato riservato

Consente di gestire gli accessi al documento al solo personale autorizzato.

Identificativo del formato: indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso.

É costituito da:

- formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida.
- prodotto software: prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:
  - nome prodotto
  - versione prodotto
  - produttore

Verifica: check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.

Identificativo dell'Aggregazione documentale: identificativo univoco dell'Aggregazione come definito nel paragrafo dei Metadati delle aggregazioni documentali informatiche. Metadato ricorsivo (*facoltativo*, per le specifiche si rimanda all'Allegato 5).

Identificativo del Documento Primario: identificativo univoco e persistente del Documento primario (*obbligatorio nel caso in cui sia presente un documento primario*).

Nome del documento\file: nome del documento\file così come riconosciuto all'esterno.

Versione del documento: versione del documento.

Tracciature modifiche documento: metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore" (*obbligatorio nel caso di versione > 1 o in caso di annullamento*).

Tempo di conservazione: tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente" (*facoltativo*).

Note: eventuali indicazioni aggiuntive utili ad indicare situazioni particolari (*facoltativo*).

Nella scheda cliente è possibile personalizzare ed indicare i set di metadati in base alle esigenze del soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

Torna al sommario

6.1.2 Metadati del documento amministrativo informatico

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi obbligatori del documento informatico:

IdDoc: Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione

Il metadato è costituito dai seguenti:

- Impronta crittografica del documento: a sua volta suddiviso in:
  - Impronta: sottocampo in cui viene memorizzato l'hash del documento
  - Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"
- Identificativo: come da sistema di identificazione formalmente definito
- Segnatura: segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida.

Modalità di formazione: modalità di generazione del documento informatico

Sono previste le seguenti modalità:

- creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- 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;
- memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Soggetti: indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo.

Sono definiti i seguenti attributi:

- Ruolo: consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Al fine di rendere i dati di registrazione univoci deve essere sempre indicato il Soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla). Obbligatorio inoltre indicare almeno l'autore o il mittente. Nel caso di documento protocollato deve essere obbligatoriamente indicato il mittente.
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere). Il Tipo Soggetto = SW è indicabile solo se si è indicato il ruolo = "Produttore". Per ogni Tipo Soggetto sono indicati i metadati di riferimento

Chiave descrittiva: metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura.

È costituito da seguenti campi:

- Oggetto: testo libero

Allegati: Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- IdDoc: Identificativo del documento relativo all'allegato
- Descrizione: Titolo dell'Allegato

Classificazione: classificazione del documento secondo il Piano di classificazione utilizzato da indicare sia nel caso di documento protocollato che nel caso di documento non protocollato

- Indice di classificazione: codifica del documento secondo il Piano di classificazione utilizzato
- Descrizione: descrizione per esteso dell'Indice di classificazione indicato.

Riservato: rappresenta il livello di sicurezza di accesso al documento:

- vero: se il documento è considerato riservato
- falso: se il documento non è considerato riservato

Consente di gestire gli accessi al documento al solo personale autorizzato.

Identificativo del formato: indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso.
É costituito da:

- formato: secondo quanto previsto dall'Allegato 2 delle Linee Guida.
- prodotto software: prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi:

- nome prodotto
- versione prodotto
- produttore

Verifica: check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.

Identificativo dell'Aggregazione documentale: identificativo univoco dell'Aggregazione come definito nel paragrafo dei Metadati delle aggregazioni documentali informatiche. Metadato ricorsivo.

Identificativo del Documento Primario: identificativo univoco e persistente del Documento primario (*obbligatorio nel caso in cui sia presente un documento primario*).

Nome del documento\file: nome del documento\file così come riconosciuto all'esterno.

Versione del documento: versione del documento.

Tracciature modifiche documento: metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore" (*obbligatorio nel caso di versione > 1 o in caso di annullamento*).

Tempo di conservazione: tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente" (*facoltativo*).

Note: eventuali indicazioni aggiuntive utili ad indicare situazioni particolari (*facoltativo*).

Nella Scheda Cliente predisposta da Unimatica, è possibile personalizzare ed indicare i set di metadati in base alle esigenze del soggetto produttore e alle diverse tipologie documentali conservate. In un'apposita tabella il cliente specificherà i metadati di proprio interesse.

6.1.3 Metadati delle aggregazioni documentali informatiche

Di seguito vengono elencati i metadati, ed i principali campi e sottocampi obbligatori delle aggregazioni documentali informatiche:

Identificativo dell'Aggregazione documentale: si tratta di 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 di 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.

Sono definiti i seguenti attributi:

- TipoAggregazione
  - Fascicolo
  - Serie Documentale
  - Serie Di Fascicoli
- IdAggregazione: come da sistema di identificazione formalmente definito

Tipologia fascicolo: I fascicoli sono organizzati 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.
- 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.
- persona fisica: comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.
- persona giuridica: comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte
- procedimento amministrativo: conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

Soggetti: indica il metadato che consente di individuare le informazioni relative a tutti i Soggetti che, a vario titolo, sono coinvolti nella costituzione dell'aggregazione.

Sono definiti quindi i seguenti attributi:

- Ruolo:
  - Amministrazione titolare
  - Amministrazioni partecipanti
  - Assegnatario
  - Soggetto intestatario persona fisica
  - Soggetto intestatario persona giuridica
  - RUP: da indicare solo in caso di TipoAggregazione = 'Fascicolo'
- Tipo soggetto: consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche (italiane ed estere) in funzione del Ruolo. Per ogni tipo soggetto sono indicati i metadati di riferimento. Nel caso in cui sia stato definito un Ruolo=RUP è obbligatorio indicare anche l'UOR corrispondente.

Assegnazione: indica il metadato che consente di individuare le informazioni relative all'assegnazione per conoscenza o per competenza. I Soggetti indicati in questo metadato devono essere stati dichiarati nel metadato Soggetti. Sono definiti quindi i seguenti attributi:

- Tipo assegnazione (obbligatorio in caso di fascicolo)
- Soggetto assegnatario (obbligatorio in caso di fascicolo)
- Data inizio assegnazione (obbligatorio in caso di fascicolo)
- Data fine assegnazione (facoltativo)

Il metadato ha una struttura ricorsiva.

Data Apertura: data di apertura dell'aggregazione documentale.

Classificazione: classificazione dell'aggregazione:

- Indice di classificazione: Codifica del documento secondo il Piano di classificazione utilizzato
- Descrizione: Descrizione per esteso dell'Indice di classificazione indicato.
- Piano di classificazione: se presente, riportare eventualmente l'URI di pubblicazione del Piano di classificazione (facoltativo)

Progressivo: progressivo numerico calcolato nell'ambito della chiave della classificazione o in ordine cronologico nell'ambito dell'anno.

Chiave descrittiva: metadato funzionale volto a chiarire la natura del fascicolo o della serie.

È costituito da seguenti campi:
- Oggetto: testo libero

Data Chiusura: data di chiusura dell'aggregazione documentale.

Procedimento Amministrativo: metadato funzionale volto ad indicare il procedimento a cui il fascicolo afferisce, nonché lo stato di avanzamento e le relative fasi.

È costituito da seguenti campi:

- Materia\ Argomento\ Struttura: indicare la materia o l'argomento o la struttura per la quale sono stati catalogati i procedimenti amministrativi
- Procedimento: denominazione del Procedimento
- Catalogo procedimenti: URI di pubblicazione del catalogo
- Fasi: a sua volta suddiviso, in una struttura ricorsiva:
    - Tipo Fase
        - Preparatoria
        - Istruttoria
        - Consultiva
        - decisoria o deliberativa
        - integrazione dell'efficacia
    - Data inizio fase
    - Data fine fase (facoltativo)

    da "Data inizio fase" e "Data fine fase" deve considerarsi dinamico, destinato ad essere aggiornato con lo stato di avanzamento dell'iter del procedimento\processo.

Indice documenti: elenco degli identificativi dei documenti contenuti nell'aggregazione, definiti secondo le regole indicate per i documenti informatici o i documenti amministrativi informatici. Metadato ricorsivo.

È costituito da seguenti campi:
- Tipo documento
    - documento amministrativo informatico
    - documento informatico
- IdDoc
    - se documento amministrativo informatico
      IdDoc come definito nel precedente paragrafo dei Metadati del documento amministrativo informatico
    - se documento informatico

IdDoc come definito nel precedente paragrafo dei Metadati del documento informatico

Posizione fisica Aggregazione Documentale: posizione fisica dell'aggregazione. Nel caso di fascicoli ibridi indica la posizione della componente cartacea del fascicolo.

6.1.4 Metadati del documento informatico di natura fiscale e contabile

In relazione alla valorizzazione dei metadati specifici del documento informatico di natura fiscale e contabile si rimanda alle specifiche descritte nelle istruzioni dal titolo *I metadati del documento informatico di natura fiscale e contabile* pubblicato nella sezione Linee guida del sito di AgID.

Torna al sommario

6.2 Formati

Unistorage, in conformità all'*Allegato 2 "Formati di file e riversamento"* alle Linee guida AgID, accetta e gestisce formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo e che garantiscano i principi dell'interoperabilità.
Tuttavia, in accordo con il soggetto produttore, Unimatica permette anche l'accettazione di formati non esplicitati nell'Allegato 2. Infatti qualora l'ordinamento giuridico preveda degli obblighi relativamente all'uso di formati specifici per alcuni Titolari, questi assolvendo tali obblighi, sono chiamati ad effettuare una valutazione di interoperabilità utile anche per garantire la conservazione e la fruibilità degli stessi nel tempo. L'indicazione di tali formati, compresa la gestione di questi, verrà indicata nella scheda cliente.

Torna al sommario

6.2.1 Riversamento

Unistorage, in relazione all'obsolescenza dei formati, tiene un censimento dei formati di file ricevuti in conservazione a seguito di un'attività di ingestion (compreso il recupero da precedente conservatore). Il responsabile del servizio di conservazione, assieme al responsabile della funzione archivistica, al responsabile sviluppo e manutenzione del sistema di conservazione e al responsabile sicurezza dei sistemi per la conservazione, con cadenza non superiore ai 5 anni, fatta una fotografia dei formati di file censiti al momento sul sistema, ne valuta il grado di obsolescenza.
In fase di analisi dei formati, come da procedura stabilita, per ogni formato si attribuisce un grado di obsolescenza, basandosi sulle caratteristiche di apertura, sicurezza, portabilità, funzionalità, supporto allo sviluppo e diffusione. Al termine della verbalizzazione di questo processo di verifica, a fronte di evidenze di formati di file per cui è impossibile individuare soluzioni in grado di rappresentare fedelmente il contenuto di questi file, il responsabile del servizio di conservazione attiva il processo di riversamento dei file appartenenti ai formati risultati a rischio di obsolescenza, previa certificazione di processo.
Per tutti i dettagli inerenti all'intero processo di gestione del riversamento si rimanda al documento di sistema "PRO_CONS01 - Procedure di Conservazione".

Torna al sommario

6.3 Struttura dati del Pacchetto di versamento

Unimatica mediante il prodotto applicativo UniStorage, con la supervisione del Responsabile del servizio di conservazione permette un duplice iter per la ricezione dei Pacchetti di Versamento: ricezione dei file tramite canale SSH File Transfert Protocol e ricezione tramite sistema Web service.

- La ricezione mediante SSH File Transfert Protocol prevede l'upload del Pacchetto di versamento composto da un file indice e da un insieme di file, in formato .zip. Per maggiori dettagli circa la struttura dei Pacchetti di versamento, fare riferimento al documento Flusso per la conservazione dei Documenti in Unistorage.

- La ricezione tramite Sistema Web Service è possibile da qualsiasi piattaforma che permetta di eseguire e ricevere chiamate Web Service conformi allo standard WS-I Basic Profile 1.0. Con questo servizio il sistema di conservazione riceve singoli documenti ed eventuali allegati, ne verifica la firma digitale se presente e ne gestisce la conservazione autentica. Per maggiori dettagli circa la ricezione degli oggetti digitali tramite Sistema Web Service si rimanda al documento "Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione".

Torna al sommario

6.4 Struttura dati del Pacchetto di archiviazione

Terminato il processo di acquisizione dei Pacchetti di versamento, il prodotto applicativo UniStorage sotto la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica provvede alla creazione dei Pacchetti di archiviazione e dell'Indice del pacchetto di archiviazione previsto dallo standard UNI 11386 SInCRO – Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali.
I Pacchetti di archiviazione contengono[5]:

- l'oggetto o gli oggetti da conservare;
- l'Indice del Pacchetto di archiviazione, formato secondo le regole dettate dallo Standard UNI 11386 SInCRO – Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Tutti i pacchetti di archiviazione prodotti fino al 31 dicembre 2021 implementano lo standard UNI 11386:2010 SInCRO. A partire dal 1° gennaio 2022 viene applicata la versione 2020 dello standard.

Torna al sommario

6.5 Struttura dati del Pacchetto di distribuzione

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'Utente.

[5] Sono elencate le caratteristiche indicate nell'allegato 4 al DPCM 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione.

L'esibizione del materiale di interesse avviene via interfaccia web o, su esplicita richiesta al team di delivery conservazione, mediante deposito su canale sicuro SFTP o memorizzazione su supporto rimovibile fornito dal titolare dell'oggetto di conservazione. La descrizione dettagliata delle procedure è indicata nel capitolo 7 "Il processo di erogazione del servizio di conservazione", Fase 6.

I Pacchetti di distribuzione generati contengono sia gli oggetti che l'insieme delle evidenze di conservazione.

Torna al sommario

7. Il processo di erogazione del servizio di conservazione

Il processo di conservazione eseguito da Unimatica adotta il modello standard OAIS - Open Archival Information System[6] che definisce concetti e funzionalità degli archivi digitali. Lo schema seguente illustra brevemente gli aspetti principali di un generico processo di conservazione: il Soggetto produttore invia il Pacchetto di versamento, di cui ha piena responsabilità, al Soggetto conservatore il quale provvede a trasformarlo in Pacchetto di archiviazione. Ai fini dell'esibizione e della distribuzione richiesti dalla comunità di riferimento[7], il Soggetto conservatore provvederà a creare i Pacchetti di distribuzione in una forma tale che venga garantita la corretta visualizzazione di questi.

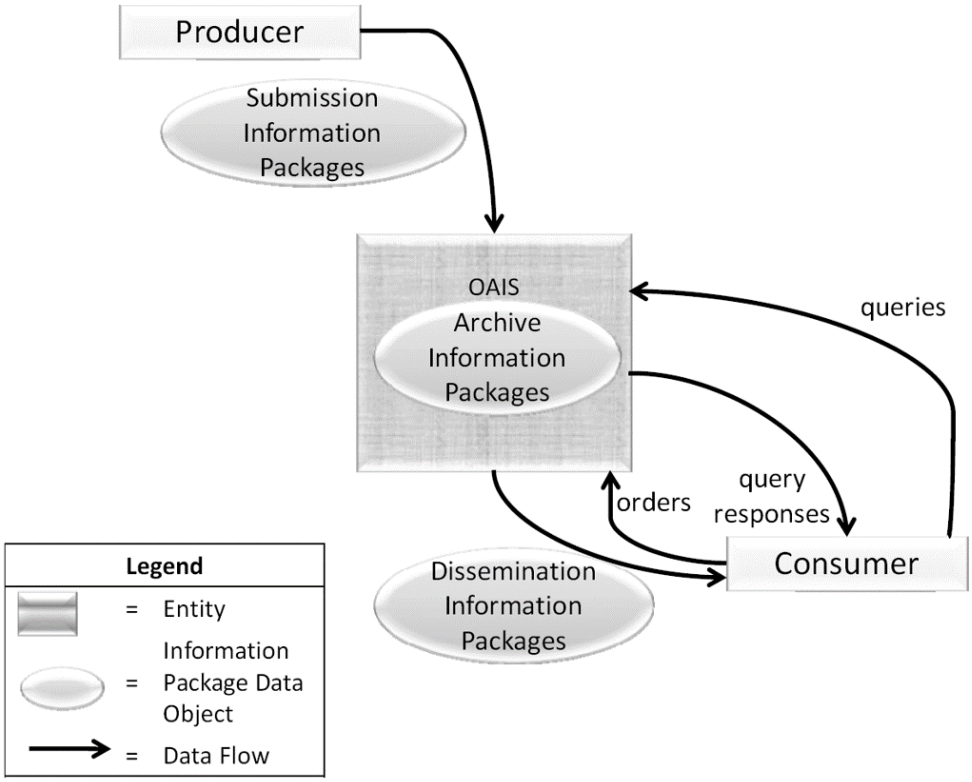


Figura 1 - Modello OAIS

Torna al sommario

7.1. Il processo di conservazione

Il servizio offerto da Unimatica ad ogni Soggetto produttore viene avviato al termine di un processo di attivazione che segue queste fasi fondamentali:

[6] L'Open Archival Information System è lo standard ISO per la conservazione a lungo termine di archivi digitali.
[7] Comunità di riferimento: il sottoinsieme degli utenti in grado di comprendere autonomamente l'informazione archiviata nella forma in cui è conservata e resa disponibile dall'OAIS

- 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.

Di seguito vengono dettagliate le fasi del processo.

Torna al sommario

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

In questa fase il 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 Unimatica

L'attivazione del servizio avviene attraverso la compilazione del Modulo 'Scheda cliente'. 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;

Il Responsabile del servizio di conservazione, valuterà in accordo con il Privacy manager, con il Responsabile della funzione archivistica e con il Responsabile dello sviluppo e della manutenzione

la domanda di acquisizione del servizio collaborando con il Soggetto produttore guidandolo nella compilazione della domanda per l'attivazione del servizio.

Il Responsabile del servizio di conservazione e il Responsabile della funzione archivistica una volta ricevuta la richiesta, si impegnano a valutarne l'impatto stimando la data di evasione e fornendo al Soggetto produttore una pianificazione delle fasi successive. Se la richiesta di configurazione implica un aggravio di costi, verrà fornita parallelamente al Soggetto produttore la quotazione economica dell'attività redatta dal Referente Commerciale di Unimatica

L'acquisizione dei Pacchetti di versamento avviene mediante due canali: tramite SSH File Transfert Protocol e tramite canale Web service descritti dettagliatamente nel capitolo "Oggetti sottoposti in conservazione", paragrafo 6.3.

Ad ogni attivazione verranno consegnate le credenziali per accedere all'applicativo web reso disponibile da Unimatica, in base ai dati presenti nella Scheda cliente. Tale accesso garantirà la piena esibizione dei Pacchetti di distribuzione.

Torna al sommario

7.3. Verifiche effettuate sui Pacchetti di versamento e sugli oggetti in esso contenuti

I parametri gestionali del Pacchetto di versamento vengono verificati e messi a punto dal Responsabile del servizio di conservazione e dal Responsabile della funzione archivistica in accordo con il Soggetto produttore. Le verifiche effettuate sui Pacchetti di versamento sono le seguenti:

- **identificazione certa del Soggetto produttore**;

- verifica delle **firme digitali** se presenti mediante un controllo crittografico dell'integrità del documento e della validità formale delle firme stesse. In un secondo momento viene verificata l'identità del sottoscrittore. Se una chiave privata sia stata usata in una firma è verificabile, mediante processo crittografico, con la corrispondente chiave "pubblica". Le chiavi pubbliche sono riportate nei "certificati di firma digitale", documenti informatici anch'essi, che definiscono anche i dati d'identità del sottoscrittore. I certificati sono a loro volta firmati da una autorità di certificazione emittente (C.A. - Certification Authority). In generale si risalirà la catena di certificazione fino a raggiungere un "certificato fidato", ovvero pubblicamente noto. Tra le evidenze informatiche che Unimatica conserva ci sono, per ogni Pacchetto, tutti i certificati a vario modo coinvolti nelle catene di certificazione necessarie alle verifiche di firma digitale. Questo consente di costituire un insieme "auto-contenuto" di evidenze che possono essere verificate anche a posteriori. Si può anche verificare il caso che l'autorità emittente non sia direttamente un'autorità pubblicamente nota, ma che esista una "catena di certificazione" (trust chain) per cui l'autorità di un certificato vada a sua volta identificata risalendo ad un'autorità terza.

- verifica che i **formati** degli oggetti da conservare siano conformi con quanto dichiarato nella scheda cliente e nell'Allegato 2 alle Linee guida per la Formazione, gestione e conservazione dei documenti informatici. Alla ricezione del documento il sistema, attraverso l'uso di una libreria WAZFORMAT, la cui procedura utilizzerà un metodo di indagine diretta con tecniche euristiche, riconosce il formato controllando il valore descritto nel magic number. Questo passaggio permette di associare il formato al documento per garantirne la corretta visualizzazione e quindi leggibilità utilizzando gli opportuni i visualizzatori.

- relativamente alle verifiche dei **metadati** sono previste tre livelli di controllo:
    - *strict:* l'assenza di anche solo un metadato obbligatorio (Allegato 5 alle Linee guida) comporta la restituzione di un errore alla richiesta di versamento ed il documento non viene conservato
    - *permissive*: l'assenza di metadati obbligatori (Allegato 5 alle Linee guida) viene segnalata con un warning, ma il processo di conservazione prosegue generando i metadati assenti con un valore nullo.
    - *skip*: applicato a tutti i soggetti produttori non vincolati alla normativa italiana (Allegato 5 alle Linee guida). In questo caso i metadati obbligatori sono concordati con il soggetto produttore in base alle buone prassi o ai vincoli normativi del paese di origine.

Torna al sommario

7.4. Accettazione dei Pacchetti di versamento e generazione del Rapporto di versamento di presa in carico

L'esito positivo delle verifiche effettuate sui Pacchetti di versamento viene registrato in un Rapporto di versamento di presa in carico. Il Rapporto conterrà un'impronta del file originale comprensivo di algoritmo con la quale tale impronta viene calcolata (hash) e un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del Rapporto collegato all'istante indicato (Tcons).
Apponendo un timestamp al Rapporto di versamento, lo si "sigilla" e contemporaneamente si fissa il riferimento temporale. Tale procedimento costituisce un riferimento temporale certificato per il Rapporto di versamento.
Il Rapporto di versamento attesta la corretta esecuzione del processo di immissione dei Pacchetti, ha la funzione di raccogliere evidenze indirette di tutti i documenti del Pacchetto e garantisce due principali funzioni:

- la possibilità di provare l'integrità dei dati di ogni file contenuto nel pacchetto,
- di permettere il controllo dell'integrità per ogni file in modo separato, senza creare un'interdipendenza tra i file ai fini dell'esibizione e del controllo.

Il Rapporto di versamento è un file in formato XML che riporta, per ognuno dei file inclusi nel Pacchetto, alcune informazioni tra cui un "URN" (unified resource name) e un "hash". L'URN è una stringa univoca che identifica l'oggetto digitale, mentre l'hash è un'impronta del documento, ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che garantisce una corrispondenza esatta col contenuto originale (in modo pratico possiamo dire di avere la garanzia che a due file differenti corrispondono sempre due impronte distinte).

La modalità di conservazione mediante Rapporto di versamento permette di verificare l'integrità di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso pacchetto. Infatti sarà sufficiente essere in possesso di un file "candidato" e conoscere il suo URN identificativo per poter eseguire la funzione di hash e confrontare l'impronta ricalcolata con la stringa riportata nel Rapporto.
In questa fase vengono associate all'indice tutte le evidenze di autenticità delle firme digitali che verranno verificate all'istante del riferimento temporale:

- i certificati di firma di tutte le firme presenti nel Pacchetto di versamento,
- tutti i certificati appartenenti alle catene di certificazione (trusting chain),

- le liste di revoca dei singoli certificati (CRL).

Il Rapporto di versamento viene conservato all'interno del sistema garantendone l'ininterrotta custodia e la non modificabilità.

Torna al sommario

7.5. Rifiuto dei Pacchetti di versamento e modalità di comunicazione delle anomalie

Le verifiche effettuate sui Pacchetti di versamento possono risultare negative. Nei casi in cui anche solo su uno dei controlli indicati nella fase 2 si dovesse riscontrare una mancanza o non corrispondenza di informazioni viene generato un file di Comunicazione delle anomalie che verrà comunicato mediante un file di esito al Soggetto produttore. Tale Comunicazione comprenderà i dettagli delle verifiche eseguite sui Pacchetti di versamento comprensive delle precisazioni sulle anomalie.
Le anomalie, in relazione a quanto descritto nella fase 2, possono essere identificate nell'assenza dei metadati obbligatori ovvero nella mancata corrispondenza di ciò che viene versato a quanto dichiarato dal soggetto produttore nella scheda cliente in termini di firma digitale, formati e metadati.
Qualora l'anomalia venisse riscontrata soltanto su una parte di documenti inclusi nel Pacchetto di versamento, è facoltà del soggetto produttore decidere se bloccare l'intero pacchetto o soltanto i documenti segnalati. In questo ultimo caso i file conformi vengono inviati in conservazione e gli altri spediti successivamente mediante nuovo Pacchetto di versamento.

Torna al sommario

7.6. Preparazione e gestione dei Pacchetti di archiviazione

I Pacchetti versati in UniStorage, con la supervisione del Responsabile del servizio di conservazione e del Responsabile della funzione archivistica vengono raggruppati in Pacchetti di archiviazione. Questi pacchetti vengono assemblati dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati con il Soggetto produttore, indicati nella Scheda Cliente (ad es. Pacchetti di archiviazione per tipologie documentali o in base alla cadenza temporale di consegna).
Il processo di costruzione dei Pacchetti di archiviazione, così come previsto dallo standard SInCRO UNI 11386– Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali, avviene con le seguenti modalità:

- individuazione dei documenti destinati a far parte del pacchetto di archiviazione sulla base dei criteri scelti. Tali criteri vengono concordati con il cliente e sono definiti nella scheda cliente e si possono basare sia su caratteristiche legate allo stato del documento, sia sui metadati.
- i Pacchetti di archiviazione vengono chiusi in seguito a due tipi di regole:
  - automatiche: collocano nel pacchetto i documenti per i quali ci sia almeno un certificato di firma prossimo alla scadenza. Questa tipologia di regole ha la precedenza su quelle descritte nel punto successivo, le quali riguardano la dimensione massima del Pacchetto di archiviazione e il tempo limite oltre il quale un Pacchetto di archiviazione deve essere forzatamente chiuso,
  - attuate dal Responsabile del servizio di conservazione in accordo con il soggetto produttore: definite nella scheda cliente.

Nei casi in cui i Pacchetti di archiviazione contengano referti sanitari, questi vengono crittografati mediante funzione crittografica della suite standard del linguaggio Java. In particolare è definita nel package crypto di JCE e impiega l'algoritmo AES a 128 bit ECB.

I Pacchetti di archiviazione vengono sottoscritti con firma digitale dal Responsabile del servizio di conservazione e marcati temporalmente.
La sottoscrizione dei Pacchetti di archiviazione effettuata da Unimatica attesta esclusivamente la corretta esecuzione del processo di conservazione secondo la normativa vigente in materia di conservazione. Unimatica non è responsabile dell'errato contenuto informativo degli oggetti versati.

Torna al sommario

7.7. Preparazione e gestione dei Pacchetti di distribuzione ai fini dell'esibizione

La gestione dei Pacchetti di distribuzione fa capo al Responsabile del Servizio di Conservazione, al Responsabile della Funzione archivistica e al Privacy manager.

La produzione di Pacchetti di distribuzione avviene in seguito alla richiesta da parte dell'utente.

UniStorage, 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.
Unimatica permette l'accesso ai Pacchetti di distribuzione esclusivamente agli utenti autorizzati. 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.

È possibile visualizzare i documenti tramite triplice canale:

- via web: i Soggetti produttori titolari dei documenti potranno ricercare e visualizzare tutti i documenti conservati direttamente sul portale di Unimatica 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. La descrizione di dettaglio dell'interfaccia web per le richieste di esibizione dei documenti è contenuta nell'allegato 'Funzionalità_portale'. 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.
- 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 architetturale di UniStorage 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.
Torna al sommario

7.8. Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento di un pubblico ufficiale

Con la richiesta da parte dell'utente di esibizione dei Pacchetti di distribuzione mediante supporto removibile, viene generata una copia autentica del documento, conforme all'originale. Per i dettagli sulla modalità di richiesta di esibizione dei Pacchetti di distribuzione, fare riferimento al capitolo 6 "Oggetti sottoposti a conservazione" paragrafo 6.5 e al capitolo 7 "Il processo di erogazione del servizio di conservazione", fase 6.

Nei casi in cui, come previsto dall'art. 23-bis, c. 2 del Codice dell'Amministrazione Digitale[8] il Soggetto produttore richieda la presenza di un pubblico ufficiale, Unimatica garantirà tale presenza mettendo a disposizione tutte le necessarie risorse che serviranno all'espletamento delle attività, rimandando in ogni caso la scelta al Soggetto produttore al quale saranno addebitate le spese.

Inoltre, in caso di adeguamento del formato dovuto all'evoluzione tecnologica verranno rispettate tutte le procedure elencate nell'Allegato 'Infrastrutture' al presente Manuale. Anche in questo caso, l'eventuale presenza del pubblico ufficiale per l'attestazione di conformità, sarà garantita in seguito alla richiesta del Soggetto produttore a cui vengono attribuiti i costi di gestione.

Torna al sommario

7.9. Scarto dei Pacchetti di archiviazione

Il Periodo di conservazione dei documenti è, per ciascuna tipologia documentale, la durata temporale, espressa in anni, per la quale il Soggetto produttore prevede il servizio di conservazione. Tale durata temporale sarà riportata all'interno del piano di conservazione, qualora redatto dal Soggetto produttore, e sarà condivisa dal Soggetto produttore con Unimatica per mezzo di una comunicazione certa, relativamente a tutte le tipologie documentali per le quali Unimatica eroga servizi di conservazione al Soggetto produttore. Il Soggetto produttore si impegna altresì a comunicare tempestivamente ad Unimatica eventuali modifiche apportate ai Periodi di conservazione per le tipologie documentali conservate da Unimatica.

Entro tre mesi prima della scadenza del Periodo di conservazione per i documenti conservati da Unimatica, il Titolare dell'oggetto di conservazione dovrà prendere contatto con Unimatica ed indicare la volontà di continuare la conservazione digitale a norma, con opportuna estensione contrattuale ove necessario, oppure di procedere con l'attività dello scarto.
Qualora il Titolare non prenda contatti si intenderà prorogato, a parità di condizioni contrattuali, il periodo di conservazione per un ulteriore anno rispetto all'avvenuta scadenza.

[8] "Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico."

Qualora il Titolare prenda contatto con Unimatica e decida di avviare la procedura di scarto, saranno concordate con il Responsabile del servizio di conservazione di Unimatica le modalità operative per procedere allo scarto.

Su indicazione del Titolare, il responsabile del servizio di Unimatica genera l'elenco delle Unità Documentarie da destinare allo scarto e lo invia al Titolare dell'oggetto di conservazione che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale, ove previsto.

In caso di archivi pubblici o privati dichiarati di interesse storico particolarmente importante l'autorizzazione finale è rilasciata ai sensi della normativa vigente in materia di beni culturali[9].

Il Titolare, una volta effettuate le verifiche e/o ricevuta l'autorizzazione da eventuali parti coinvolte, provvede a firmare digitalmente ed a trasmettere i seguenti documenti:

a) Provvedimento di autorizzazione allo scarto, del Titolare, che indichi gli allegati di cui ai due punti seguenti;
b) Elenco definitivo dei documenti per i quali si autorizza lo scarto;
c) Nulla osta da parte dell'autorità competente in materia di beni culturali, ove previsto dalla normativa vigente;

Il Responsabile del servizio di conservazione di Unimatica analizza la richiesta ricevuta ed in caso di congruità avvia la procedura di scarto con conseguente cancellazione dei documenti e successiva conservazione della documentazione formale di scarto.

Al termine della procedura di scarto viene generato un verbale di scarto sottoscritto digitalmente dal Responsabile del servizio di conservazione e marcato temporalmente, che verrà conservato insieme ai documenti di cui ai precedenti punti a), b), c) , e di cui verrà data opportuna comunicazione al Titolare.

Torna al sommario

7.10. Predisposizione di misure per l'interoperabilità e la trasferibilità ad altri conservatori

Unimatica, come descritto al par. 6.4 Struttura dati del Pacchetto di archiviazione, genera i PDA applicando le specifiche tecniche dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali. Accoglie, inoltre, formati conformi all'Allegato 2 delle Linee guida o concordati a seguito di opportuna valutazione di interoperabilità, pertanto Unistorage supporta sia l'acquisizione di PDD provenienti da altri conservatori, sia il riversamento verso altro sistema di conservazione.

Torna al sommario

[9] L'intervento della Soprintendenza archivistica è previsto anche nel caso di archivi privati per i quali è stato dichiarato l'interesse culturale, secondo quanto disposto dall'art. 21, comma 1, lettera d del Codice dei beni culturali (D. Lgs. 22 gennaio 2004, n. 42).

7.11. Chiusura del contratto

Il Titolare dell'oggetto di conservazione, in qualsivoglia momento, ha il diritto di rescindere dal contratto. La procedura prevede la compilazione di un apposito modulo, debitamente firmato e timbrato, da inviare ad Unimatica utilizzando una delle modalità di seguito indicate:

1. invio dell'originale cartaceo con firma autografa tramite posta all'indirizzo corrispondente alla sede legale di Unimatica S.p.A.;

2. invio dell'originale firmato digitalmente dal rappresentante legale, all'indirizzo di posta elettronica certificata (PEC): pec@pec.unimaticaspa.it

Qualora il Titolare intenda disdire il servizio di conservazione a norma dei documenti informatici affidato alla società Unimatica prima del termine contrattualmente previsto per il servizio di conservazione, potrà richiedere la restituzione degli stessi secondo modalità operative che saranno concordate con il Responsabile del servizio di conservazione di Unimatica. A seguito della restituzione le credenziali di accesso al sistema saranno disattivate.

Qualora, per un sottoinsieme di documenti informatici versati in conservazione, si raggiunga il termine contrattualmente previsto per il servizio di conservazione ma non sia stata raggiunta la scadenza del Periodo di conservazione, il Titolare potrà decidere di:

a) mantenere il servizio di conservazione a norma per una durata che sarà concordata tra il Titolare ed Unimatica, che terrà conto del periodo di conservazione previsto per le tipologie documentali trattate e che sarà formalizzata con un apposito contratto;

b) non mantenere la conservazione a norma dei documenti informatici presso Unimatica e procedere alla restituzione degli stessi secondo modalità operative che saranno concordate con il Responsabile del servizio di conservazione di Unimatica. A seguito della restituzione le credenziali di accesso al sistema saranno disattivate.

Qualora, per un sottoinsieme di documenti informatici versati in conservazione, si raggiunga il termine contrattualmente previsto per il servizio di conservazione e questo coincida con la scadenza del Periodo di conservazione, varrà quanto previsto al paragrafo Scarto dei Pacchetti di archiviazione

I documenti informatici che sono stati oggetto di conservazione a norma possono essere restituiti, a richiesta, all'utente nel formato standard previsto dalla normativa in vigore (SInCRO – standard UNI 11386 – Supporto all'Interoperabilità nella Conservazione e nel recupero degli Oggetti digitali).

Torna al sommario

8. Procedure di gestione e di evoluzione

A coordinare la gestione del sistema, l'aggiornamento di questo e le procedure di adeguamento all'evoluzione tecnologica è la figura del Responsabile sviluppo e manutenzione che esegue una costante attività di controllo dell'attività di conservazione in conformità agli standard di qualità e sicurezza ISO 9001 e ISO 27001.
Affinché venga garantito un controllo totale sul sistema e un buon funzionamento di questo, le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software e viene condotta una quotidiana verifica delle attività sulle infrastrutture parallelamente ad una pianificazione delle eventuali procedure straordinarie da condurre in caso di anomalie.

Torna al sommario

8.1. Misure di sicurezza logica

Il presente paragrafo ha l'obiettivo di descrivere le misure di sicurezza adottate per l'erogazione del Servizio e per la protezione dei dati che fanno riferimento al Piano per la sicurezza del sistema di conservazione di Unimatica In particolare, verranno descritte, a titolo esemplificativo ma non esaustivo, le misure di sicurezza tecniche e organizzative adeguate adottate da Unimatica per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR:

- la gestione utenze,
- la gestione sistemi di protezione,
- la gestione degli incidenti di sicurezza,
- la gestione dei backup,
- la gestione dei supporti di memorizzazione.

Torna al sommario

8.1.1 Gestione utenze

La policy di riferimento per la gestione delle utenze applicative e di sistema adottata da Unimatica prevede che le utenze siano rilasciate da un ente (o persona) differente dall'ente o persona che le utilizzerà.
Nell'ambito del servizio di conservazione, le utenze applicative e di sistema sono gestite secondo criteri idonei a garantire il rispetto dell'applicazione di misure di sicurezza tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR. Si riportano di seguito alcune delle misure di sicurezza adottate:

- Utilizzo di password complesse definite secondo i seguenti criteri:
  - la password non deve essere visibile in fase di inserimento nelle sessioni di login e sia criptata all'interno del Data Base;
  - la password:
    - deve avere una lunghezza compresa fra 8 e 25 caratteri,
    - deve contenere almeno un carattere speciale, un carattere maiuscolo, un carattere minuscolo ed un numero
    - non può contenere il nome dell'utente,
    - non può contenere il cognome dell'utente,
    - non può contenere l'username dell'utente,

- non può essere una delle ultime 4 utilizzate;

- la scadenza della password è configurabile attraverso un parametro;
- il sistema deve forzare l'utente a cambiare la password al primo utilizzo;
- il sistema deve avvertire l'utente della necessità di rinnovare la password;

- Applicazione del principio 'segregation of duty' nel rilascio delle credenziali (utente, password e profilo), vale a dire separazione tra chi rilascia e chi utilizza le credenziali di accesso ai dati;
- Applicazione del principio 'need to know' nel rilascio dei profili, vale a dire rilascio dei soli diritti per eseguire le attività di competenza;
- Assegnazione ad ogni utente di credenziali (user e password) personali, uniche e non assegnabili ad altri utenti;
- Revisione periodica degli utenti e dei relativi profili.

Torna al sommario

8.1.2 Gestione sistemi di protezione

Net Security
La realizzazione logica della rete è fatta secondo i seguenti criteri:

- controllo degli accessi e dei flussi realizzato tramite firewall in cross-mode (doppio Cisco Pix-535) ed utilizzo di software IP Tables per il port e IP filtering;
- filtro sui flussi di traffico da/per Internet costituito da sistemi McAfee Sidewinder ridondati, che effettuano deep packet inspection e forniscono funzionalità di firewall applicativo (livello 7 OSI);
- segregazione della rete e suddivisione della medesima in differenti porzioni dedicate alla rete di Back End dati per i server contenenti i data base, alla rete di Front End per la parte di presentazione, alla rete di gestione per l'amministrazione (funzione di supporto tecnico) della piattaforma;

Gli accessi alla rete sono segregati a livello di porte ed indirizzi IP. Gli accessi agli apparati di rete sono sottoposti a misure rigide di controllo e sono consentiti solamente agli amministratori della medesima.

IDS e IPS
Allo scopo di evitare che eventuali malintenzionati possano forzare le protezioni presenti per accedere in maniera illecita a dati riservati, la barriera di firewall applicativi fornisce anche un costante monitoraggio contro accessi non autorizzati tramite funzionalità IPS (Intrusion Prevention System).

Torna al sommario

8.1.3 Gestione degli incidenti di sicurezza

Si definisce incident uno stato, in un sistema, un servizio od una rete, che implichi il mancato funzionamento, il possibile mancato rispetto di uno SLA o il mancato funzionamento di contromisure.

Se l'incident coinvolge le proprietà di sicurezza dell'informazione (RID), si configura come incident di sicurezza.

La segnalazione di anomalie può scaturire
- dalle attività di monitoraggio
- da specifica segnalazione da parte di un utente o di personale interno

In entrambi i casi, qualora la segnalazione implichi un problema di sicurezza inficiando quindi l'integrità, riservatezza o disponibilità del dato, la prassi per la gestione degli incident può prevedere l'apertura di un ticket sulla specifica coda OTRS (strumento elettronico di ticketing Open-source Ticket Request System) del servizio di conservazione oppure dell'area sistemi.

Una volta preso in carico il ticket dal Responsabile del settore Conservazione o da un operatore designato egli diventa Incident Owner, cui sono delegate le azioni di: Contenimento[10], Eliminazione delle cause[11], Ripristino[12].

La gestione degli incidenti di sicurezza è regolamentata da specifiche procedure dettagliatamente descritte secondo requisiti conformi allo standard ISO 27001:2013. Maggiori dettagli sono descritti nel capitolo 3 del Piano della Sicurezza.

Torna al sommario

8.1.4 Gestione dei backup e Disaster Recovery

8.1.4.1 Siti Settimo Torinese (TO) e Firenze

L'architettura del sistema backup è composta da un master server per ogni sito e da differenti media server che hanno il compito di archiviare i dati ed inserirli in una rete dedicata, parallela a quella di erogazione dei singoli servizi, per non impattare sulle prestazioni e sulla disponibilità di questi ultimi, durante la normale esecuzione delle attività di backup.
I singoli agent installati sull'infrastruttura di virtualizzazione e sui server non virtualizzati comunicano con il backup server che esegue il salvataggio dei dati su un appliance Data Domain. Il salvataggio dei dati su un appliance Data Domain viene replicato sul sito secondario. Questo sistema consente:

- Semplicità di integrazione anche con future evoluzioni del software di backup
- De-duplicazione del dato ad alta velocità
- Replica efficiente in rete
- Scalabilità dell'infrastruttura

L'architettura di backup utilizza le seguenti tecnologie:

---

[10] **Contenimento**: processo che rappresenta la fase di esecuzione delle attività di contrasto, atte a mitigare le compromissioni della sicurezza derivanti da un incidente. Una delle attività principali del processo di contenimento è quella di determinare il patrimonio informativo che viene messo a rischio a seguito di un incidente.
[11] **Eliminazione delle cause**: processo che elenca le azioni indirizzate alla rimozione delle cause che scatenano un incidente informatico. E' opportuno sottolineare l'importanza che rappresenta la comprensione del problema che è all'origine dell'incidente; a tale scopo appare determinante descrivere con il maggior dettaglio possibile il modo con cui l'evento di sicurezza si è verificato.
[12] **Ripristino**: processo tramite il quale viene attuato il ritorno alle normali condizioni di operatività aziendale e di chiusura formale dell'incidente. Un obiettivo determinante che emerge dalla corretta applicazione delle misure qui contemplate, è garantire che per i dati e per i sistemi/applicazioni siano ristabilite le funzionalità e performance in essere prima dell'incidente.

- Data Domain DD4200
- Data Domain DD4100
- Data Domain DD2500
- Software di backup NetBackup di Symantec
- Software di backup vRanger di DELL
- Software di backup con modulo di cifratura dei dati
- Rete di backup con throughput a 10 Gbit/s
- Replica dei dati di backup tramite link a 400 Mbit/s fra sito primario e secondario

La funzionalità di backup sulla base dati è implementata utilizzando Oracle RMAN o BARMAN, con cadenza giornaliera e settimanale a seconda delle necessità.

Torna al sommario

8.1.4.2 Siti di Cornaredo (MI) e Roma

L'architettura di backup si basa sul software open-source bacula, costituito da un modulo director che sovrintende le operazioni di backup, su due unità dischi SATA (una con dischi fissi e una con dischi rimuovibili) collegate a server di backup su cui gira il modulo storage di bacula, e su una serie di moduli client (agenti) di bacula disposti sulle macchine contenenti i dati di cui effettuare il backup.

Le categorie di dati oggetto del backup sono:
- Directory di sistema dei sistemi Unimatica
- DB Postgres[nella modalità export DB]

Nell'ambito del backup dei dati appartenti alla categoria Directory di sistema, è eseguito anche il backup delle cartelle di rete utilizzate dal personale Unimatica.
Il backup avviene in due modalità:
- diretto: i dati vengono backuppati direttamente sul server che li contiene tramite un agente bacula
- indiretto: i dati vengono backuppati su NAS da uno script di backup che gira sul server da backuppare, e dal NAS vengono poi prelevati da un agente bacula che li inserisce nel flusso dei backup diretti

Le modalità di backup sono riassumibili in estrema sintesi nei seguenti punti:
- i dati di backup sono conservati per 7 giorni su Dischi, i backup full eseguiti ogni fine settimana sono conservati per 1 mese su dischi;
- vengono eseguiti backup mensili su dischi rimuovibili, in singola copia, conservati in cassaforte ignifuga, con retention di un anno;
- l'ultimo backup mensile su disco di ogni anno viene conservato con ritenzione infinita;
- backup su disco di dati con esigenze di retention specifiche (superiori all'anno), sono eseguiti in doppia copia, in base a specifiche degli "owner" dei dati;
- il salvataggio dei documenti su CD-ROM con consegna al Soggetto produttore, può essere eseguito su richiesta;
- il salvataggio dell'applicazione sia server che client è realizzato su supporto fisico esterno (Data tape o CD-ROM) per eseguire una rapida reinstallazione in caso di necessità;
- i supporti di backup hanno rotazione con frequenza settimanale.

Per le attività di salvataggio si eseguono i seguenti controlli:

- monitoraggio e controllo dei log-files dei risultati dei salvataggi (con frequenza quotidiana);
- ripristino periodico a campione dei dati;
- controllo della validità e della funzionalità (leggibilità) dei supporti.

Torna al sommario

8.1.4.3 Disaster Recovery

I servizi di conservazione di Unimatica sono erogati tramite due Data Center Primari due Data Center Secondari che svolgono il compito di Backup Remoto e di Disaster Recovery (D/R), al fine di garantire gli opportuni livelli di continuità del servizio.
I Data Center hanno una distanza fra loro superiore 200 e 300 Km e la disponibilità di servizio è H24 per tutti e 4.
I Data Center secondari permettono di usufruire dei servizi in Produzione anche in caso di indisponibilità dei Data Center Primari.
Per questo servizio Unimatica definisce con il Cliente il livello dei parametri che caratterizzano il servizio di D/R e di continuità operativa.

- Recovery Point Objective (RPO)
  Rappresenta il massimo tempo che intercorre tra la produzione di un dato sui siti primari e la sua messa in sicurezza (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di disastro e che devono essere successivamente ripresi.
- Recovery Time Objective (RTO)
  È il tempo necessario per il pieno recupero dell'operatività di un sistema e del relativo processo organizzativo.

Torna al sommario

8.1.5 Gestione dei supporti di memorizzazione

La gestione dei supporti di memorizzazione, ove richiesti, segue i seguenti criteri:

- i media di memorizzazione elettronica sono correttamente etichettati in modo da fornire le seguenti informazioni: tipologia del media, tecnica della scrittura, data della scrittura, contenuto. Per tecnica della scrittura si intende il formato in cui il media è stato preparato, nel nostro caso formato ISO, dipendentemente dal tipo supporto (CD o DVD);
- in caso di media che vengano riutilizzati per altri dati, essi vengono preventivamente riformattati tramite le tecniche di formattazione a basso livello, allo scopo di evitare che le informazioni ed i dati in essi contenuti possano essere presi e divulgati a soggetti non autorizzati;
- nel caso in cui i dati registrati sui media non più utilizzati non possano essere definitivamente cancellati si procede alla distruzione del media stesso, impedendone quindi il riutilizzo;
- i media sui quali sono eseguiti i salvataggi aziendali sono conservati in una sede differente rispetto a quella dove sono le strumentazioni cui i salvataggi si riferiscono ed in un luogo non accessibile se non al personale autorizzato,
- periodicamente è eseguita una verifica dei media e della disponibilità degli strumenti di accesso ai medesimi. In caso che per qualche media sia verificata la non disponibilità (anche prevista nel breve futuro) degli strumenti di accesso, si procede allo svecchiamento dei media tramite riversamento del loro contenuto in altro media.

Torna al sommario

8.2. Procedure di evoluzione e Change management

I cambiamenti che vengono apportati al sistema di conservazione di Unimatica risultano essere il prodotto di un'adeguata corrispondenza alle procedure di evoluzione tecnologica sia sulle strutture hardware sia su quelle software. Il Responsabile della funzione archivistica e il Responsabile dei sistemi informativi definiscono politiche, priorità e tempistiche affinché vengano garantite nel tempo integrità, disponibilità e sicurezza.

In caso di disservizi causati da problematiche riscontrate durante il processo di aggiornamento, è possibile effettuare il ripristino delle versioni precedenti così da assicurare il corretto e continuo svolgimento delle attività.

Il Responsabile del servizio di conservazione e il Responsabile della sicurezza dei sistemi informativi periodicamente si occuperanno di aggiornare la normativa e gli standard di riferimento in base all'evoluzione di questi.
La descrizione delle procedure di evoluzione e gestione dei cambiamenti è riportata nel paragrafo 3.2.2 del documento "Piano della sicurezza del sistema di conservazione".

Torna al sommario

8.3. Cessazione del Servizio di conservazione

Il servizio di Conservazione digitale a norma è, dal 2005, uno dei principali asset di Unimatica e gli obiettivi della Direzione per gli anni futuri sono di continuare ad evolvere il sistema ed il servizio di conservazione per mantenerlo adeguato alla tecnologia ed alla normativa e di espandere sempre più nel mercato target, non solo italiano, la penetrazione dell'azienda.
A fronte dei suddetti obiettivi, è stata comunque stabilita una procedura per definire le modalità secondo le quali dovrà essere gestito l'evento, ad oggi non prevedibile, di cessazione del servizio di Conservazione da parte di Unimatica
La gestione della cessazione del Servizio di Conservazione, in fase iniziale, è in carico alla Direzione la quale stabilisce un tempo di almeno 10 mesi prima della data di attuazione prevista.

Dal momento della comunicazione, la Direzione, supportata in questo dal Responsabile del servizio di conservazione, provvede a far sì che non vengano stipulati nuovi contratti, in vista della cessazione del servizio.

Alla ricezione della comunicazione suddetta il Responsabile del servizio di conservazione coinvolge i Responsabili delle diverse aree inerenti alla Conservazione (Sicurezza, Servizio, Archivistica, Sviluppo) con i quali deve collaborare strettamente per la gestione della cessazione e la relativa pianificazione delle attività.
La procedura e le attività che verranno eventualmente eseguite sono descritte nel dettaglio all'interno del documento PRO_CONS - Piano di Cessazione, qualora venga richiesto, tale procedura viene resa disponibile fornendola al soggetto produttore interessato.

Torna al sommario

9. Monitoraggio e controlli

L'attività di monitoraggio e controllo viene portata avanti dal Responsabile della sicurezza dei sistemi e dal Responsabile della funzione archivistica, in accordo con il Responsabile del sistema di conservazione. Tale attività è finalizzata alla rilevazione di eventi di sicurezza, identificabili come stati che indicano il mancato rispetto delle politiche di sicurezza, che possano costituire una possibile fonte di rischio per il sistema di conservazione. Nello specifico gli obiettivi delle attività di monitoraggio sono la valutazione del livello del rischio associato agli eventi di sicurezza e la gestione di tali eventi, mediante strumenti come i Report dei controlli, agendo per il contenimento e/o eliminazione delle cause.

Gli eventi di sicurezza sono monitorati tramite il sistema di Log che consente la registrazione degli accessi e degli eventi (operazioni). Il sistema di Log è organizzato per registrare eventi ai vari livelli di astrazione della piattaforma:

- log del sistema operativo (incluso file system) atto ad identificare ingressi, anomalie ed errori;
- log del Data Base atti ad identificare ingressi, anomalie ed errori;
- log dei sistemi di rete (firewall e router) atti ad identificare ingressi, anomalie ed errori;
- log delle applicazioni software utilizzate (realizzati con vista a livello di singolo utente) atti ad identificare ingressi, principali attività svolte dagli utenti, sequenze del processo, accessi ai dati.

I log file degli applicativi contengono almeno le seguenti informazioni:

- utente che ha eseguito l'operazione;
- data e ora dell'operazione;
- operazione eseguita.

I file di log non sono modificabili o eliminabili da parte degli Utenti che usano il sistema (che non dispongono dei diritti di accesso).
I log di sistema sono analizzati da parte dei sistemisti qualora si rendesse necessaria un'indagine a seguito di un malfunzionamento del sistema.
La dettagliata descrizione dei processi relativi alle attività di monitoraggio e controlli è riportata nel documento "Piano della sicurezza del sistema di conservazione", capitolo 3 e nella PRO_CONS - Procedure di conservazione.
I log vengono successivamente inviati in conservazione per mantenere traccia delle comunicazioni tra Soggetto produttore e sistema di conservazione.

Torna al sommario

9.1 Audit interni e Verifica dell'integrità degli archivi

Le verifiche ispettive interne vengono pianificate dal Responsabile del sistema di gestione per la sicurezza delle informazioni e dal Responsabile della qualità in accordo con il Responsabile sviluppo e manutenzione del sistema di conservazione, dal Responsabile sicurezza dei sistemi per la conservazione e dal Responsabile del servizio di conservazione tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposte le verifiche ispettive interne è almeno annuale. Unimatica si rende disponibile qualora un soggetto produttore volesse richiedere audit di terza parte. La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.

Unimatica prevede in allegato al Manuale "Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti" tenente traccia delle seguenti informazioni:

- registro delle modifiche al Manuale del sistema di conservazione
- registro dei documenti distrutti

Torna al sommario

9.2 Reportistica di servizio

Il sistema di conservazione UniStorage gestisce un sistema di tracciatura nel quale vengono registrati tutti i singoli eventi che riguardano sia la gestione dei Pacchetti, dalla fase di versamento a quella di distribuzione, sia i singoli documenti. Questa tracciatura, costruita per implementare un "forensic log", è in un formato rigido e non disabilitabile. La tracciatura è prerequisito indispensabile per l'esecuzione delle operazioni.
Nel dettaglio, il sistema di log prevede la registrazione di informazioni relative alle diverse funzioni del processo di conservazione per tutte le fasi descritte nel capitolo 7 "Il processo di erogazione del servizio di conservazione".

La reportistica di servizio che Unimatica gestisce è di due Tipologie:

1. Reportistica relativa al processo di Conservazione,
2. Reportistica del servizio di Supporto Utente (Service Desk e AM Settore conservazione e Settore sistemi).

Tipologia 1:
vengono prodotti periodicamente i seguenti report:

- Report Consuntivo Pacchetti di archiviazione,
- Report Excel che fornisce la lista dei Pacchetti di archiviazione e che comprende questo set Minimo di informazioni:
    1. Ragione Sociale Cliente;
    2. Numero documenti conservati e spazio occupato nel periodo totali e per tipologia di documento;
    3. Numero documenti conservati e spazio occupato totali e per tipologia di documento.

Tipologia 2:
viene prodotto un report di Servizio che fornirà le seguenti evidenze:

- Numero Incident Segnalati
- Media Tempo di presa in carico Incident
- Media Tempo di chiusura Incident
- Numero Service Request
- Media Tempo di presa in Carico Service Request
- Media Tempo di Chiusura Service Request

Torna al sommario

10. La server farm di Unimatica

Per la descrizione della server farm di Unimatica si rimanda al documento allegato ‘Unimatica_DataCenter_2025’.

Appendice A

Allegati al Manuale del sistema di conservazione:

- Allegato ‘Unimatica_DataCenter_2025’
- Allegato ‘Infrastrutture’
- PRO_CONS - Piano di Cessazione

Specificità del contratto e documenti di riferimento:

- Scheda Cliente.
- Flusso per la conservazione dei Documenti in Unistorage
- Specifiche del servizio web per la consegna anticipata di documenti nel Sistema di conservazione.
- ‘Funzionalita_portale'.
- Elenco delle modifiche apportate al Manuale della conservazione e dei documenti obsoleti.

Torna al sommario