Consorzio Culturale del Monfalconese

Provincia di Gorizia

MANUALE DI GESTIONE DOCUMENTALE

Schema di Manuale di Gestione Documentale - Approvato con delibera del Consiglio di Amministrazione n. 21 del 24/06/2025

Sommario

1. INTRODUZIONE E PRINCIPI GENERALI7

1.1 Ambito di applicazione**7**

1.2 Terminologia e definizioni chiave**7**

1.3 Definizione dell'Area Organizzativa Omogenea (AOO)**7**

1.4 Struttura responsabile della gestione del protocollo informatico**8**

1.5 Responsabile della gestione documentale (RGD)**8**

1.6 Cessazione dei protocolli non informatici, gestione dei documenti esclusi dalla registrazione di Protocollo e Registri particolari**8**

1.7 Principio di unicità del protocollo informatico**9**

1.8 Norme sull'accesso agli atti e protezione dei dati personali**10**

1.9 Piano di sicurezza informatica**11**

2. SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI (SGID)12

2.1 Requisiti e capacità tecnologiche**12**

2.2 Requisiti funzionali**13**

3. FORMAZIONE DEI DOCUMENTI14

3.1 I documenti del Consorzio Culturale del Monfalconese**14**

3.2 Classificazione delle diverse tipologie di documenti**14**

3.3 Forma dei documenti**16**

3.4 Documentazione particolare**16**

3.4.1 Firma digitale con certificato di firma scaduto o revocato16

3.4.2 Lettera anonima16

3.4.3 Lettere prive di firma16

3.4.4 Firma illeggibile17

3.4.5 Allegati17

3.5 Requisiti per la Formazione e Gestione dei Documenti Informatici**17**

3.6 Formato dei documenti informatici**18**

3.7 Sottoscrizione dei documenti informatici**19**

3.8 Metadati dei documenti informatici**19**

4. REGISTRAZIONE DEI DOCUMENTI20

4.1 Registro giornaliero di protocollo**20**

4.2 Documenti soggetti a registrazione di protocollo**20**

4.3 Documenti non soggetti a registrazione di protocollo**20**

4.4 Registrazione di protocollo dei documenti ricevuti e spediti**20**

4.5. Registrazione dei documenti interni**21**

4.6 Protocollazione dei documenti informatici e cartacei**21**

4.7 Segnatura di protocollo documenti cartacei (analogici)**22**

4.8 Segnatura di protocollo documenti digitali**22**

4.9 Annullamento delle registrazioni di protocollo**23**

4.10 Immodificabilità del Registro Protocollo**23**

4.11 Differimento dei termini di registrazione**24**

4.12 Registro di emergenza**24**

4.13 Acquisizione dei Documenti informatici**24**

4.14 Scansione dei Documenti cartacei**25**

5. GESTIONE DEI FLUSSI DOCUMENTALI26

5.1 Schema di metadati per i documenti informatici, i documenti amministrativi informatici e le aggregazioni documentali informatiche**26**

5.2 Piano di classificazione**26**

5.3 Classificazione dei documenti**26**

5.4 Piano di organizzazione delle aggregazioni documentali**27**

5.5 Formazione dei fascicoli e delle ADI**28**

5.6 Gestione dei flussi documentali e dei flussi di lavoro**30**

5.7 Ricezione**30**

5.7.1 Ricezione dei documenti cartacei30

5.7.2 Ricezione dei documenti informatici31

5.7.3 Ricezione di documenti informatici su supporti rimovibili32

5.7.4 Ricezione dei documenti su casella istituzionale (PEC)32

5.7.5 Utilizzo della posta elettronica ordinaria33

5.7.6 Procedura di apertura e gestione della corrispondenza in entrata33

5.7.7 Rilascio di ricevute34

5.7.8 Assegnazioni e modifiche dei documenti34

5.7.9 Correzione di una assegnazione34

5.7.10 Orari di apertura per il ricevimento della documentazione cartacea35

5.8 Spedizione**35**

5.8.1 Spedizione dei documenti cartacei35

5.8.2 Spedizione dei documenti informatici36

5.8.3 Spedizioni massive37

5.8.4 Documenti interni e giuridici37

5.9 Gestione documentale nell'ambito del lavoro agile**38**

5.9.1 Accesso remoto ai sistemi documentali38

5.9.2 Formazione e gestione dei documenti in modalità agile38

5.9.3 Misure di sicurezza specifiche38

5.9.4 Monitoraggio e controllo39

6. TENUTA E CONSERVAZIONE DELL'ARCHIVIO40

6.1 Piano di conservazione dell'archivio**40**

6.2 Tenuta e conservazione della componente analogica**40**

6.3 Conservazione della componente digitale**41**

6.4 Procedure di selezione e scarto in ambiente digitale e analogico**42**

6.5 Ricerca, accesso e fruizione delle unità conservate**43**

7. TRASPARENZA AMMINISTRATIVA.45

7.1 Amministrazione Trasparente**45**

7.2 Albo Pretorio**45**

7.3 Modalità della pubblicazione**46**

7.4 Completezza, integrità e qualità degli atti pubblicati**46**

7.5 Atti soggetti a pubblicazione e durata**46**

8. DISPOSIZIONI FINALI47

8.1 Redazione del Manuale**47**

8.2 Esame tecnico-organizzativo interno**47**

8.3 Nulla osta della Soprintendenza archivistica**47**

8.4 Adozione formale del Manuale**47**

8.5 Pubblicazione e decorrenza**47**

8.6 Aggiornamenti successivi**47**

Allegato 1 – Glossario48

Allegato 2 – Struttura Uffici e Servizi60

Allegato 3 – Registrazioni particolari61

Allegato 4 - Piano di classificazione del Consorzio Culturale del Monfalconese62

Allegato 5 – Manuale della Conservazione63

Allegato 6 – Formato dei documenti informatici e riversamento72

Allegato 7 - Tipologie di documenti di originali informatici74

Allegato 8 - Manuale operativo del software di gestione del protocollo75

Allegato 9 - Piano di sicurezza informatica76

Allegato 10 - Dichiarazione di Adozione del Piano di Sicurezza Informatica*Errore. Il segnalibro non è definito.*

1. INTRODUZIONE E PRINCIPI GENERALI

1.1 Ambito di applicazione

Le Linee guida sulla formazione, gestione e conservazione dei documenti informatici, emanate dall'Agenzia per l'Italia Digitale (AgID) ai sensi dell'articolo 71 del Codice dell'Amministrazione Digitale (CAD), sono entrate in vigore il 1° gennaio 2022 e impongono a tutte le Pubbliche Amministrazioni, compresi gli Enti locali, l'obbligo di adottare un Manuale di gestione documentale.

Questo Manuale deve fornire una descrizione dettagliata delle modalità operative utilizzate per la gestione dei documenti informatici, con particolare attenzione ai processi di creazione, classificazione, protocollazione, fascicolazione, accesso e conservazione degli stessi. Il documento costituisce uno strumento fondamentale per assicurare la conformità alle normative vigenti, promuovere la trasparenza amministrativa, migliorare l'efficienza operativa e garantire la sicurezza nella gestione dei dati e dei documenti.

Inoltre, il Manuale di gestione documentale deve contenere informazioni specifiche su diversi aspetti critici, tra cui:

- **le modalità di gestione del protocollo informatico**, che disciplinano l'attribuzione di univoci numeri di protocollo per ogni documento in entrata e in uscita;
- **le regole per l'accesso agli atti**, che definiscono i criteri e le procedure per garantire il diritto di accesso ai documenti amministrativi;
- **le norme per la tutela dei dati personali**, che assicurano la protezione dei dati particolari (ex dati sensibili) e personali in conformità con le leggi sulla privacy;
- **le procedure per la conservazione a lungo termine dei documenti digitali**, necessarie per garantire la validità e l'integrità dei documenti nel tempo, preservandone l'accessibilità e la leggibilità.

Ogni Pubblica Amministrazione ha l'obbligo di redigere e adottare formalmente il Manuale di gestione documentale attraverso un provvedimento ufficiale. Successivamente, deve pubblicarlo sul proprio sito web istituzionale, in una sezione chiaramente identificabile dell'area "Amministrazione trasparente", come richiesto dall'articolo 9 del Decreto Legislativo n. 33 del 2013. Questo assicura che le informazioni siano facilmente accessibili al pubblico e rispettino i requisiti di trasparenza amministrativa.

1.2 Terminologia e definizioni chiave

***Allegato 1*.**

1.3 Definizione dell'Area Organizzativa Omogenea (AOO)

Ai fini della gestione dei documenti, l'Amministrazione individua un'unica area organizzativa omogenea, denominata **CONSORZIO CULTURALE DEL MONFALCONESE**, composta dall'insieme di tutte le sue unità organizzative (UO) come da elenco in ***Allegato 2.***

Il codice identificativo del Consorzio Culturale del Monfalconese nell'Indice delle Pubbliche Amministrazioni (IPA) è **ccm_**.

1.4 Struttura responsabile della gestione del protocollo informatico

Nell'ambito dell'Area Organizzativa Omogenea, e in conformità con l'articolo 61, comma 1 del D.P.R. 28 dicembre 2000, n. 445 (Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - TUDA), è stato istituito il Servizio di gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi.

Questo servizio, ai sensi dell'articolo 61, comma 3 del TUDA, è incaricato della gestione complessiva di tutta la documentazione archivistica dell'Amministrazione, indipendentemente dal luogo in cui viene trattata, distribuita o conservata. Le sue responsabilità comprendono la corretta registrazione, classificazione, conservazione, selezione e ordinamento dei documenti.

1.5 Responsabile della gestione documentale (RGD)

Il comma 2 dell'art. 61 del TUDA istituisce la figura del Responsabile della gestione documentale. In questo Consorzio la nomina del Responsabile della gestione documentale è stata effettuata mediante la Determinazione n. 78 del 09/03/2021 individuando come persona predisposta a ricoprire questo ruolo la dott.ssa Tanja Tuta. Al Responsabile della gestione documentale spetta il compito di redigere e mantenere costantemente aggiornato il Manuale di gestione documentale e tutti i suoi allegati, assicurando che le procedure e le norme siano sempre in linea con le disposizioni vigenti e le esigenze dell'Amministrazione. Oltre a questo, al RGD spetta il compito, in ambito archivistico, di assicurare la predisposizione e il continuo aggiornamento del Piano di classificazione, di fascicolazione e conservazione. Inoltre, il Responsabile è tenuto a garantire la corretta formazione, gestione e conservazione dell'archivio ibrido, nel rispetto della normativa di riferimento.

Il RGD possiede competenze informatiche consolidate tali da permettere la scelta di un buon sistema di gestione documentale in grado di operare in una infrastruttura tecnologica sicura e affidabile. Al Responsabile della gestione documentale spetterà il compito di predisporre il Piano per la sicurezza informatica volto a garantire la protezione, l'integrità e la riservatezza dei documenti digitali e le procedure messe in campo dall'Amministrazione in caso di possibili violazioni.

Il Responsabile della gestione documentale definisce le modalità di firma e validazione temporale dei documenti informatici, oltre che stabilire le regole e le procedure in materia di accesso documentale. In questa Amministrazione

Il Responsabile della Conservazione è individuato nella figura del dott. Roberto del Grande con Determinazione n. 174 del 10/06/2025. Verranno esplicitate le responsabilità in carico a questa figura nell'***Allegato 5***, dedicata alla conservazione dell'Ente in questione

1.6 Cessazione dei protocolli non informatici, gestione dei documenti esclusi dalla registrazione di Protocollo e Registri particolari

Tutti i documenti inviati e ricevuti dall'Amministrazione devono essere registrati esclusivamente nel Registro di protocollo informatico. Con l'adozione del sistema di gestione informatica del protocollo, tutti i registri di settore preesistenti verranno aboliti e rimossi, garantendo così una centralizzazione e una standardizzazione della registrazione documentale.

Sono esclusi dalla registrazione di Protocollo tutti i documenti di cui all'art. 53, comma 5, del TUDA:

- Gazzette ufficiali;
- bollettini ufficiali della Pubblica Amministrazione;
- notiziari della Pubblica Amministrazione;
- note di ricezione circolari ed altre disposizioni;
- materiali statistici;
- atti preparatori interni;
- giornali, riviste, libri;
- materiali pubblicitari;
- inviti a manifestazioni che non attivino procedimenti amministrativi;
- tutti i documenti già soggetti a registrazione particolare dell'Amministrazione.

Le categorie di documenti che spesso richiedono una registrazione in Registri particolari per motivi di gestione, tracciabilità e conformità normativa, sono dettagliate nell'***Allegato 3***.

Questi Registri particolari aiutano a mantenere un sistema di gestione documentale ordinato e conforme alla normativa, garantendo che ogni tipo di documento sia trattato in modo adeguato secondo le sue specificità e requisiti.
Non sono previste altre forme di registrazioni particolari.

1.7 Principio di unicità del protocollo informatico

Il Consorzio Culturale del Monfalconese gestisce un sistema di protocollo centralizzato con un'unica Area Organizzativa Omogenea (AOO), in cui tutta la corrispondenza in entrata e in uscita è registrata in un unico registro di protocollo progressivo e univoco. Il Servizio di Protocollo dell'Ente è l'unico responsabile della gestione del registro di protocollo informatico, assicurando la corretta protocollazione, classificazione, conservazione e integrità dei documenti, nel rispetto delle disposizioni normative vigenti. La protocollazione è centralizzata e coordinata da questo servizio, che garantisce l'unicità della numerazione e la gestione integrata dei flussi documentali dell'intera amministrazione.

Questo Registro riveste un'importanza cruciale in quanto certifica, con valore di atto pubblico, tutte le informazioni relative ai documenti protocollati nel corso della stessa giornata.

La numerazione del protocollo informatico deve avvenire secondo criteri specifici stabiliti dalla normativa vigente e dalle Linee Guida per la gestione documentale, le quali regolano la gestione del Registro e garantiscono la pubblicità e la tutela delle informazioni, assicurandone così la validità giuridica e la protezione. I principali requisiti e modalità da seguire, secondo il TUDA e le Linee Guida dell'Agenzia per l'Italia Digitale (AgID) per la formazione, gestione e conservazione dei documenti informatici, sono:

- **Unicità e Progressività**:

  La numerazione deve essere unica e progressiva. Ogni documento registrato deve ricevere un numero di protocollo che non può essere duplicato o riutilizzato, anche se il documento è correlato ad altri già protocollati.

- **Ciclo Annuale**:

  La numerazione dei protocolli è ciclica e si conclude il 31 dicembre di ogni anno. Il nuovo ciclo numerico riprende il 1° gennaio dell'anno successivo, iniziando da un numero predefinito.

- **Composizione del Numero**:

  In conformità con l'articolo 57 del TUDA il numero di protocollo deve essere composto da almeno sette cifre numeriche. Questo formato assicura una numerazione sufficientemente estesa per coprire un ampio numero di documenti nel corso dell'anno.

- **Automazione**:

  La numerazione deve essere gestita automaticamente dal sistema informatico di protocollo. Questo aiuta a garantire l'unicità e la progressività dei numeri e minimizza il rischio di errori manuali nella registrazione.

- **Data di Protocollazione**:

  Oltre al numero di protocollo, ogni documento deve essere accompagnato da una data di protocollazione, e talvolta anche dall'ora, per garantire una tempistica precisa del trattamento dei documenti.

- **Registro Unico**:

  Il Registro di Protocollo deve essere unico e centralizzato, gestito da un Servizio di Protocollo dedicato all'interno dell'Ente. Questo Registro tiene traccia di tutti i documenti in entrata e in uscita, assicurandone la tracciabilità e la gestione corretta.

Per assicurare una classificazione e un'organizzazione uniforme dei documenti, viene adottato un Piano di classificazione unificato. Il protocollo conferisce valore giuridico ai documenti, attestando il loro effettivo ricevimento e spedizione. Di conseguenza, qualsiasi documentazione non registrata, sia nel Registro di Protocollo che negli eventuali Registri particolari previsti dal Manuale, sarà considerata giuridicamente inesistente presso l'Ente.

1.8 Norme sull'accesso agli atti e protezione dei dati personali

I procedimenti amministrativi e il sistema di protocollo informatico dell'Ente sono progettati per garantire il rispetto delle normative relative al diritto di accesso e alla protezione dei dati personali e particolari, conformemente al Codice in materia di protezione dei dati personali e al GDPR. In particolare, si pone attenzione al principio di accountability, ovvero alla responsabilità nella gestione dei dati e alla capacità di adottare processi efficaci per minimizzare i rischi di violazione.

1. **Gestione del diritto di accesso**: l'Ente regolamenta l'accesso e la consultazione dei documenti amministrativi e dei fascicoli da parte di terzi, assicurando la conformità alle normative vigenti.
2. **Accesso civico**: l'Ente stabilisce le modalità per l'accesso civico e l'accesso civico generalizzato ai dati e ai documenti detenuti, in linea con le disposizioni legali.
3. **Protezione dei dati**: l'Ente, responsabile dei dati di protocollo e dei dati personali contenuti nella documentazione amministrativa, applica le disposizioni del Codice in materia di protezione dei dati personali e del GDPR attraverso atti sia interni che esterni.

Per quanto riguarda il personale incaricato dell'apertura e della registrazione della corrispondenza, è essenziale che sia regolarmente autorizzato al trattamento dei dati personali. Tutti i dipendenti devono osservare il segreto d'ufficio e rispettare le normative vigenti, evitando di trarre benefici personali o di danneggiare terzi e l'immagine dell'Ente attraverso la conoscenza di informazioni sensibili.

Nel caso in cui la corrispondenza riservata venga recapitata erroneamente a un altro ufficio, è fondamentale restituire il materiale integro, senza aprire buste o plichi, nella stessa giornata al personale del Servizio di Protocollo, per garantire la protezione dei dati personali e particolari contenuti.

1.9 Piano di sicurezza informatica

Il Piano di Sicurezza Informatica è parte integrante del sistema di gestione documentale dell'Ente e ha l'obiettivo di descrivere le misure organizzative, tecniche e procedurali adottate per garantire la sicurezza, l'integrità, la disponibilità, la riservatezza e la tracciabilità dei documenti informatici e dei sistemi che li gestiscono. Il Piano è redatto in conformità alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, al Codice dell'Amministrazione Digitale (D.lgs. 82/2005 e s.m.i.), nonché alle normative in materia di protezione dei dati personali. Esso definisce ruoli, responsabilità, misure di prevenzione e gestione dei rischi, nonché le modalità di controllo e verifica dell'efficacia dei sistemi di sicurezza, al fine di assicurare la continuità operativa e la tutela del patrimonio documentale digitale dell'Ente, ***Allegato 9.***

2. SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI (SGID)

La scelta di uno SGID è una delle fasi più critiche del processo di transizione alla modalità digitale. In assenza di una soluzione tecnologicamente avanzata è molto difficile formare e gestire un archivio ibrido/digitale. Il Piano triennale per l'informatica nella Pubblica Amministrazione spinge verso una architettura informatica orientata al Cloud Computing. Il modello Cloud adottato deve rispettare il Cloud First, principio che impone di privilegiare soluzioni cloud favorendo l'uso di servizi SaaS, PaaS e IaaS.

I principali vantaggi del Cloud sono:

- Virtualizzazione
- Interoperabilità
- Utilizzo di sistemi distribuiti e interconnessi su reti ad alta velocità
- L'impiego di Browser Web
- La capacità di autogestione dei sistemi.

In un'ottica di digitalizzazione, Il Consorzio Culturale del Monfalconese ha opportunamente attivato il suo Sistema di gestione informatica dei documenti in un ambiente sicuro, così come specificato nell'allegato B della circolare 5/2017 dell'AgID.

2.1 Requisiti e capacità tecnologiche

Il Consorzio Culturale del Monfalconese ha deciso di utilizzare come Sistema di Gestione Informatica dei Documenti, il sistema prodotto e commercializzato dalla Software House Insiel S.p.A. Nell'implementazione dello SGID Il Consorzio ha tenuto in considerazione le misure minime di sicurezza ICT emanate dall'AgID con la circolare n. 2 del 2017. L'Amministrazione in questione ha considerato anche le esigenze per la protezione dei dati personali, così come indicato dal GDPR in materia di requisiti per i Sistemi di Gestione Informatica dei Documenti (Privacy Design e by Default). Nella scelta dello SGID, Il Consorzio ha tenuto in considerazione l'importanza di implementare modelli di interoperabilità, tali da permettere lo scambio automatico di dati e documenti tra sistemi in utilizzo nelle Pubbliche Amministrazioni.

Il Sistema di Gestione Documentale permette di leggere e produrre documenti in formato XML, oltre che permettere l'integrazione con la PEC o altro servizio di recapito qualificato conforme al regolamento Eidas. Il Sistema di Gestione Informatica dei Documenti, in uso in questo Consorzio, possiede tutti i requisiti tecnologici delineati da AgID nelle sue Linee Guida sulla formazione, gestione e conservazione dei documenti informatici:

- **Formati di File** - Il SGID supporta formati standardizzati e aperti per garantire l'accessibilità e la conservazione a lungo termine
- **Metadati** - Il Sistema permette l'associazione delle informazioni necessarie per assicurare la tracciabilità e le operazioni di ricerca e gestione dei documenti
- **Registrazione e Classificazione** - Il Sistema permette la registrazione univoca dei documenti e la loro classificazione secondo un piano di fascicolazione o di aggregazione documentale predefiniti, garantendo l'organizzazione efficiente dell'archivio digitale
- **Segnatura di Protocollo** - Il Sistema garantisce l'apposizione automatica della segnatura di

protocollo sui documenti in entrata ed in uscita, assicurando l'integrità e l'autenticità delle informazioni

- **Registrazione e Gestione degli accessi** - Ogni utente che ha accesso al Sistema viene identificato e autentificato in maniera univoca. L'accesso alle risorse verrà tracciato permanentemente attraverso dei log di sistema e consentito solo agli utenti in possesso di una abilitazione.

2.2 Requisiti funzionali

Il Sistema di Gestione Documentale garantisce funzionalmente la rappresentazione dell'organizzazione di riferimento, andando a valorizzare i metadati identificati del Soggetto Produttore, l'AOO di riferimento, le varie UOR e l'articolazione gerarchica. All'interno del Sistema verranno identificati gli utenti, specificandone le responsabilità, i ruoli, le operazioni abilitate e le UOR di riferimento. Per garantire il corretto tracciamento delle attività giornaliere.

3. FORMAZIONE DEI DOCUMENTI

3.1 I documenti del Consorzio Culturale del Monfalconese

Il documento amministrativo è definito come qualsiasi rappresentazione, in qualsiasi forma e su qualsiasi supporto, del contenuto di atti conservati, che viene utilizzata per le finalità dell'attività amministrativa. In questo contesto, i documenti del Consorzio Culturale del Monfalconese comprendono tutti i materiali prodotti, inviati, ricevuti o comunque acquisiti dagli organi e dagli uffici dell'Ente, secondo le modalità stabilite dalla normativa vigente, durante l'espletamento delle proprie funzioni istituzionali.

Questi documenti sono legati da un vincolo originario, necessario e specifico, noto come vincolo archivistico, che ne determina l'interconnessione e l'indivisibilità come parte del sistema documentale dell'Ente. Tale vincolo garantisce la conservazione e l'organizzazione dei documenti come parte integrante dell'Archivio, assicurando che tutti gli atti siano gestiti in modo coerente, trasparente e conforme ai requisiti di legge.

3.2 Classificazione delle diverse tipologie di documenti

I documenti di questa Amministrazione si distinguono in:

- Documento Analogico

  Un documento analogico, tipicamente cartaceo, rappresenta una forma non digitale di atti, fatti o dati che hanno rilevanza giuridica. I documenti cartacei devono essere creati in un numero predefinito di copie originali, pari al numero dei destinatari più una copia aggiuntiva da archiviare nel fascicolo relativo al procedimento. Le delibere e le determine, di norma, devono essere redatte in almeno due copie originali: una da conservare nella serie archivistica del repertorio di riferimento e l'altra da archiviare nel fascicolo concernente il procedimento in questione.

  L'originale di un documento analogico si presenta su supporto cartaceo e deve essere munito di firma autografa per avere validità legale.

  Il Consorzio in questione acquisisce e produce le seguenti fattispecie documentali:

  1. documenti cartacei aventi carattere e contenuto ufficiale;
  2. documenti cartacei aventi contenuto effimero;
  3. moduli cartacei;

- Documento informatico

  Un documento informatico è un documento in formato elettronico che contiene una rappresentazione digitale di atti, fatti o dati giuridicamente rilevanti. I documenti informatici rispettano gli elementi formali e sostanziali indicati per quelli analogici.

  L'Ente redige i propri documenti originali utilizzando strumenti informatici, in conformità alle disposizioni del Codice dell'Amministrazione Digitale (CAD) e alle regole tecniche previste dall'articolo 71 dello stesso.

  Ogni documento deve riportare un unico numero di protocollo e può essere associato a più fascicoli. Tutte le firme necessarie per la validità giuridica di un documento in uscita devono essere apposte prima della sua protocollazione. Inoltre, l'Ente ha aggiornato il proprio sistema di gestione dei

documenti informatici in linea con le Linee Guida per la formazione, l'archiviazione e la trasmissione di documenti mediante strumenti informatici e telematici.

Gli operatori del Consorzio Culturale del Monfalconese possono trasmettere i documenti informatici anche tramite una casella di posta istituzionale certificata dopo aver eseguito le operazioni di registrazione di protocollo.

Il Consorzio in questione acquisisce e produce le seguenti fattispecie documentali:

1. e-mail trasmesse a mezzo posta elettronica certificata (PEC);
2. comunicazioni interne;
3. e-mail trasmesse tramite PEO;
4. tutta la documentazione prodotta e gestita attraverso specifiche applicazioni informatiche.

- Documento in entrata

I documenti in entrata comprendono tutti gli atti, con valore giuridico-probatorio, che sono prodotti da soggetti esterni e acquisiti dall'Ente nell'ambito delle proprie funzioni.

I documenti informatici ricevuti possono essere trasmessi tramite posta elettronica certificata (PEC) o posta elettronica ordinaria, su supporto digitale rimovibile (ad esempio, CD-ROM, DVD, pen drive) consegnato direttamente al personale del Servizio di Protocollo.

I documenti analogici ricevuti da soggetti esterni possono essere consegnati a mezzo posta ordinaria o corriere, tramite posta raccomandata, con consegna diretta da parte dell'interessato o di una persona da lui delegata.

- Documento in uscita

I documenti in uscita sono tutti gli atti con valore giuridico-probatorio prodotti dal personale dell'Ente nell'esercizio delle proprie funzioni, destinati a soggetti esterni.

I documenti informatici vengono inviati ai destinatari tramite posta elettronica certificata (PEC) o e-mail istituzionali. In alcuni casi, i documenti informatici possono essere salvati su supporto rimovibile non modificabile e inviati al destinatario.

I documenti analogici, invece, possono essere spediti tramite posta ordinaria, raccomandata, raccomandata online, corriere, consegna diretta.

- Documento interno

I documenti interni sono tutti gli atti generati all'interno dell'Ente, generalmente utilizzando strumenti informatici. Questi documenti possono essere classificati in due categorie principali: quelli di carattere prevalentemente informativo, tra cui rientrano i documenti preparatori, accompagnatori o propedeutici, prodotti o acquisiti nel corso delle attività interlocutorie e conoscitive; e quelli di carattere prevalentemente giuridico-probatorio, con rilevanza procedimentale, redatti dalle Unità Organizzative Responsabili (UOR) nell'esercizio delle loro funzioni. Questi ultimi hanno lo scopo di attestare fatti, stati o qualità relativi all'attività svolta, garantendo la regolarità delle azioni amministrative, o rappresentano qualsiasi altro documento da cui possano derivare diritti, obblighi o legittime aspettative

per terzi.

3.3 Forma dei documenti

I documenti interni di natura istruttoria, procedimentale, certificatoria, valutativa, vincolante o giuridica possono essere redatti in formato analogico con firma autografa oppure in formato digitale con firma digitale.

I documenti in uscita possono essere redatti anch'essi in formato analogico o digitale, in conformità con la normativa riguardante i documenti informatici e le scelte dell'Ente.

3.4 Documentazione particolare

3.4.1 Firma digitale con certificato di firma scaduto o revocato

I documenti informatici sottoscritti con firma elettronica o firma digitale, il cui certificato di firma risulti scaduto o revocato prima del momento della sottoscrizione, e che siano ricevuti tramite posta elettronica, vengono acquisiti nel sistema informatico dell'Ente e, pertanto, sono soggetti a protocollazione.

Tuttavia, sarà cura del Responsabile del procedimento prendere contatto con il mittente per informarlo della criticità riscontrata e, ove necessario, richiedere la trasmissione di una nuova copia del documento correttamente sottoscritto con un certificato valido e vigente.

Tutte le comunicazioni inviate ai mittenti devono essere archiviate a corredo del procedimento amministrativo di riferimento, al fine di garantire la tracciabilità delle azioni intraprese.

Il rispetto rigoroso di tali procedure è essenziale per:

- Assicurare la conformità normativa in materia di gestione documentale.
- Garantire la validità giuridica dei documenti amministrativi trattati.
- Prevenire eventuali contenziosi derivanti dalla gestione impropria di documenti con sottoscrizione non conforme.

3.4.2 Lettera anonima

Le lettere anonime ricevute tramite il servizio postale, una volta aperte e constatata l'assenza di ogni indicazione del mittente, devono essere sottoposte alla valutazione del Responsabile della gestione documentale, che stabilirà come procedere.

Se il contenuto della comunicazione presenta elementi di rilevanza giuridica o risulta comunque pertinente alle funzioni e alle attività istituzionali dell'Ente, la lettera sarà registrata a protocollo, indicando "Anonimo" nel campo relativo al mittente.

La successiva conservazione del documento avverrà sotto la responsabilità del Responsabile della conservazione, nel rispetto delle regole tecniche e organizzative previste.

3.4.3 Lettere prive di firma

I documenti cartacei ricevuti dall'Ente, che risultano privi di sottoscrizione ma con il mittente chiaramente identificabile, sono comunque registrati nel sistema di protocollo e assegnati all'Unità organizzativa competente.

Il Responsabile del procedimento, preso in carico il documento, è tenuto a valutarne il contenuto e a

determinare se, ai fini della validità e dell'efficacia del procedimento, sia necessaria l'acquisizione di una versione debitamente sottoscritta.

In caso affermativo, il Responsabile provvederà a richiedere formalmente al mittente l'invio del documento in originale cartaceo recante firma autografa.

Il procedimento potrà essere istruito e proseguire regolarmente solo successivamente all'acquisizione della documentazione sottoscritta, fatta salva l'applicabilità di specifiche disposizioni normative che consentano la trattazione anche di comunicazioni prive di firma.

3.4.4 Firma illeggibile

I documenti cartacei ricevuti, privi di firma leggibile o senza sottoscrizione, e nei quali non sia possibile identificare il mittente, vengono comunque protocollati, indicando nel campo "mittente" le diciture "mittente non identificabile" o "firma illeggibile".

Tali documenti sono successivamente inoltrati alle Unità organizzative competenti. Il Responsabile del procedimento, ricevuto il documento, avrà il compito di valutare se sia necessario acquisire le informazioni mancanti o procedere alla regolarizzazione del documento per consentirne il perfezionamento.

3.4.5 Allegati

Tutti gli allegati devono essere registrati insieme ai documenti di riferimento.

Nel caso in cui gli allegati vengano inviati tramite posta elettronica, il sistema informatico li registra automaticamente come parte integrante del documento elettronico. Se una comunicazione via email contiene allegati illeggibili, sarà necessario richiedere chiarimenti al mittente riguardo ai documenti allegati.

3.5 Requisiti per la Formazione e Gestione dei Documenti Informatici

L'Ente forma gli originali dei propri documenti con mezzi informatici nel rispetto delle disposizioni contenute nel Codice dell'Amministrazione digitale e delle regole tecniche ad esso collegato.

Secondo le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, come specificato al paragrafo 2.1.1, lettera a), l'Amministrazione è tenuta a redigere gli originali dei documenti utilizzando strumenti informatici e software gestionali appropriati. Tra questi software si annoverano sia applicativi di produttività individuale, come Microsoft Word ed Excel, sia applicativi specifici per la gestione di documenti amministrativi, quali quelli per la gestione di tributi, delibere e determinazioni.

Per l'inoltro di un documento, sia all'interno che all'esterno dell'Amministrazione, devono essere rispettati i seguenti requisiti:

- **Argomento Unico**: ogni documento deve trattare un unico argomento, che deve essere descritto in modo chiaro e sintetico dall'autore del documento.
- **Protocollo Unico**: il documento deve essere associato a un solo numero di protocollo.
- **Riferimento a Fascicoli:** sebbene possa riferirsi a più fascicoli, ogni documento deve essere identificabile attraverso un singolo protocollo.

Prima della protocollazione, il documento deve essere completo di tutte le firme necessarie per garantire la sua validità giuridica. Questo passaggio deve essere verificato dal Responsabile del Servizio incaricato della protocollazione oppure dal Responsabile della gestione documentale.

Inoltre, il documento deve consentire l'identificazione dell'Amministrazione mittente attraverso le seguenti informazioni:

- **Denominazione e Logo**: deve riportare il nome e il logo dell'Amministrazione.
- **Indirizzo Completo**: deve includere l'indirizzo completo dell'Amministrazione.
- **Codice Fiscale e/o Partita IVA**: deve essere indicato il codice fiscale e/o la partita IVA dell'Amministrazione.
- **Ufficio di Provenienza**: deve essere specificato l'ufficio che ha prodotto il documento, corredato dai numeri di telefono e dagli eventuali orari di apertura al pubblico.

Il documento deve contenere anche le seguenti informazioni:

- **Luogo e Data**: deve indicare il luogo e la data (giorno, mese, anno) di redazione.
- **Destinatario**: deve riportare il destinatario, per i documenti in partenza.
- **Oggetto**: deve essere specificato un oggetto chiaro e completo del documento (ogni documento deve trattare un solo argomento).
- **Classificazione**: deve includere la classificazione, ovvero categoria, classe e fascicolo.
- **Numero degli Allegati**: deve indicare il numero degli allegati, se presenti.
- **Numero di Protocollo**: deve riportare il numero di protocollo assegnato.
- **Testo**: deve contenere il testo completo del documento.
- **Autore**: deve indicare il nome e cognome (anche abbreviato) dello scrittore del documento.
- **Responsabile del Procedimento**: deve riportare gli estremi identificativi del Responsabile del Procedimento, come previsto dalla L. 241/90.
- **Sottoscrizione**: deve essere firmato con firma autografa o, in alternativa, tramite firma elettronica/digitale.

3.6 Formato dei documenti informatici

L'Ente è organizzato per la creazione di documenti informatici, i quali devono essere firmati digitalmente, conformemente all'articolo 40 del Codice dell'Amministrazione Digitale (CAD). La garanzia di immodificabilità e integrità di tali documenti, redatti utilizzando software specializzati, è assicurata tramite una o più delle seguenti operazioni:

- Firma digitale o firma elettronica qualificata sul documento informatico.
- Apposizione di una validazione temporale.
- Trasmissione a soggetti terzi tramite posta elettronica certificata.
- Memorizzazione nei sistemi di gestione documentale.

- Versamento in un sistema di conservazione.

Per dettagli sui software utilizzati e sui formati previsti, si rimanda all'***Allegato 6***.

Per quanto riguarda i documenti acquisiti telematicamente o su supporto informatico, inclusi quelli ottenuti tramite copia per immagine di documenti analogici o mediante copia informatica di documenti analogici, l'immodificabilità e l'integrità sono garantite tramite:

- Memorizzazione nei sistemi di gestione documentale.
- Versamento in un sistema di conservazione.
- Registrazione informatica delle informazioni derivanti da transazioni o processi informatici, oppure dalla presentazione telematica di dati tramite moduli o formulari.
- Produzione di un'estrazione statica dei dati e trasferimento nel sistema di conservazione.

Come stabilito dall'articolo 47 del CAD, le comunicazioni tra pubbliche amministrazioni devono avvenire tramite posta elettronica certificata o cooperazione applicativa.

I documenti informatici prodotti dall'Ente, che richiedono una firma elettronica o digitale, devono essere convertiti in uno dei formati standard previsti dalle Linee Guida per la gestione, formazione e conservazione, prima di apporre la firma.

3.7 Sottoscrizione dei documenti informatici

Le tipologie di documenti elencate nell'***Allegato 7*** possono essere sottoscritte tramite un processo di firma digitale. La firma può essere apposta dall'interessato utilizzando la propria postazione di lavoro, a condizione che sia adeguatamente configurata, oppure presso un'altra postazione. In ogni caso, la firma digitale deve essere apposta prima che il documento venga protocollato.

Per il servizio di certificazione delle firme digitali, l'Amministrazione utilizza i servizi forniti da società fornitrici accreditate.

3.8 Metadati dei documenti informatici

Al documento informatico è associato l'insieme minimo dei metadati, come specificato nell'Allegato 5 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di AgID. Questo insieme di metadati è essenziale per garantire la corretta gestione, conservazione e consultazione del documento informatico, assicurando che tutte le informazioni necessarie siano adeguatamente registrate e facilmente accessibili.

4. REGISTRAZIONE DEI DOCUMENTI

L'attività di registrazione è essenziale per identificare i documenti all'interno dell'archivio. Il processo consiste nell'individuazione e memorizzazione delle informazioni essenziali del documento, in maniera tale da identificarlo univocamente. La registrazione serve per attestare l'esistenza di un documento all'interno del sistema e certifica in modo inoppugnabile la data archivistica, dalla quale partono gli effetti giuridici del documento (L. 241/1990). Ai sensi del DPR 445/200, art. 56 le operazioni di registrazione e di segnatura di protocollo costituiscono operazioni necessarie e sufficienti per la tenuta dell'intero Sistema di gestione informatica dei documenti.

4.1 Registro giornaliero di protocollo

Quotidianamente viene prodotto il registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno solare. Il registro è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

4.2 Documenti soggetti a registrazione di protocollo

I documenti ricevuti o spediti sono soggetti a registrazione obbligatoria di protocollo, fatti salvi quelli di cui al successivo paragrafo.

4.3 Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo tutti i documenti indicati nell'art. 53, comma 5, del TUDA, tra cui:

- Gazzette ufficiali;
- bollettini ufficiali della Pubblica Amministrazione;
- notiziari della Pubblica Amministrazione;
- note di ricezione di circolari e altre disposizioni;
- materiali statistici;
- atti preparatori interni;
- giornali, riviste, libri;
- materiali pubblicitari;
- inviti a manifestazioni che non attivano procedimenti amministrativi;
- documenti già soggetti a registrazione particolare dell'Amministrazione, ***Allegato 3***.

Sono inoltre esclusi dalla registrazione di protocollo i documenti destinati ad un altro Ente o ad una persona fisica o giuridica (da trasmettere a chi di competenza o restituire al mittente), così come tutta la corrispondenza interna, salvo gli atti interni per i quali il mittente richieda esplicitamente la protocollazione.

4.4 Registrazione di protocollo dei documenti ricevuti e spediti

Per ogni documento che l'Amministrazione riceve o invia, viene effettuata una registrazione di protocollo tramite il sistema informatizzato di gestione documentale. Questa registrazione deve avvenire in un'unica

operazione, senza possibilità per l'operatore di inserire o modificare le informazioni obbligatorie in più momenti.

Ogni registrazione di protocollo prevede l'inclusione di dati obbligatori e dati facoltativi.

Le informazioni obbligatore sono:

- Numero di protocollo, generato automaticamente dal sistema e non modificabile.
- Data di registrazione, assegnata automaticamente dal sistema e non modificabile.
- Tipo di corrispondenza (in arrivo, in partenza, interna).
- Mittente o destinatario dei documenti ricevuti o inviati, registrato in forma non modificabile.
- Oggetto del documento, registrato in forma non modificabile.
- Data e numero di protocollo del documento ricevuto, se presenti.
- Impronta digitale del documento informatico, se trasmesso per via telematica, registrata in forma non modificabile.
- Numero e descrizione degli allegati associati al documento principale
- Classificazione del documento: categoria, classe, fascicolo.

I dati facoltativi includono:

- Data di ricezione.
- Allegati (quantità e descrizione).
- Estremi del provvedimento per il differimento dei termini di registrazione.
- Modalità di ricezione/spedizione (es. posta ordinaria, prioritaria, raccomandata, corriere, ecc.).
- Tipo di documento.
- Specifica di riservatezza, se applicabile.
- Elementi identificativi del procedimento amministrativo, se necessario.
- Ufficio responsabile o di assegnazione.

4.5. Registrazione dei documenti interni

Quando l'Ufficio utente ha un interesse oggettivo e motivato, può procedere con una protocollazione interna per inviare la propria documentazione a un'altra Unità Organizzativa (UO) all'interno dello stesso Ente (soggetti interni alla medesima Area Organizzativa Omogenea - AOO di appartenenza).

Tale procedura è ammessa esclusivamente per atti che non rientrano nelle categorie di documenti esclusi dalla registrazione di protocollo; non è comunque consentita la protocollazione di documenti preparatori e/o bozze.

4.6 Protocollazione dei documenti informatici e cartacei

Tutti i documenti informatici dotati di firma digitale devono essere registrati obbligatoriamente. Prima di procedere con la registrazione, è necessario verificare la validità della firma. Ogni documento informatico deve essere accompagnato da un file di segnatura, che, insieme al documento stesso, deve essere sottoposto al

processo di archiviazione. Anche i documenti informatici rilevanti per i procedimenti amministrativi devono essere registrati nel sistema di protocollo.

Il Consorzio adotta un sistema di protocollo centralizzato, con una unica Area Organizzativa Omogenea (AOO) e un unico sistema di gestione del protocollo. La protocollazione dei documenti è svolta da più uffici operativi, dotati di personale autorizzato, che agiscono all'interno della medesima AOO secondo criteri e regole comuni. L'unicità del numero di protocollo, la tracciabilità e la coerenza dei dati sono garantite dal sistema documentale integrato.

I documenti, sia cartacei che informatici, ricevuti dall'Ente vengono protocollati e inviati all'ufficio competente. Se un documento non è di competenza dell'ufficio che lo riceve, gli operatori ne valutano il contenuto e lo inoltrano al Responsabile del servizio competente, il quale verifica la propria competenza, effettua l'eventuale protocollazione e gestisce il documento.

I documenti ricevuti dall'Ente da altri soggetti giuridici vengono registrati una sola volta come documenti in entrata. I documenti inviati dall'Ente ad altri soggetti giuridici sono registrati una sola volta come documenti in uscita.

I documenti interni di rilevante valore giuridico e probatorio sono registrati una sola volta, sia dal servizio Archivio e Protocollo sia da ciascuna Unità Organizzativa di Riferimento (UOR).

4.7 Segnatura di protocollo documenti cartacei (analogici)

L'operazione di segnatura di protocollo viene eseguita contemporaneamente alla registrazione di protocollo (TUDA, artt. 55 e 57).

La segnatura di protocollo di un documento cartaceo viene effettuata applicando, sulla prima pagina, un'etichetta adesiva prodotta da una stampante dedicata, sulla quale sono riportate le seguenti informazioni minime:

- Nome dell'Amministrazione;
- Codice identificativo dell'Area Organizzativa Omogenea;
- Data e numero di protocollo del documento;

Alla copia digitale dell'originale cartaceo, se prodotta e qualora in formato PDF (non firmato) o TIFF, può essere automaticamente apposta dal sistema di protocollo una segnatura elettronica, a protocollazione avvenuta.

4.8 Segnatura di protocollo documenti digitali

La segnatura deve essere associata in maniera permanente al documento principale. A tal fine lo SGID dell'AOO mittente deve riportare nella segnatura l'impronta del documento principale e applicare un sigillo elettronico qualificato in grado di assicurare l'autenticità e integrità della segnatura. Le informazioni della segnatura di protocollo devono essere memorizzate nei sistemi informatici delle AOO comunicanti. Il Consorzio Culturale del Monfalconese, nei rispetti di quanto stabilito dall'allegato 6 delle linee guida AgID, definisce la struttura della segnatura di protocollo in:

- Intestazione: contiene i dati identificativi dell'AOO mittente, estremi del registro, numero e data di protocollo, oggetto, classificazione, riferimenti al fascicolo;

- Descrizione: contiene le informazioni di mittente e destinatario e i riferimenti al documento principale e agli eventuali allegati. In particolare contiene le impronte digitali del documento;
- Signature: contiene le informazioni necessarie per assicurare la firma della segnatura di protocollo da parte dell'AOO mittente, assicurandone di fatto l'autenticità e l'integrità.

Per i documenti informatici inviati o ricevuti da altre pubbliche amministrazioni, i dati relativi alla segnatura di protocollo sono inclusi, una sola volta, all'interno dello stesso messaggio in un file conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD), come stabilito dall'Allegato 6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

Tutti i documenti elettronici, indipendentemente dal canale di ricezione, possono essere sottoposti a segnatura elettronica dal sistema di protocollo informatico, se sono in formati modificabili come PDF e TIFF (esclusi i documenti firmati digitalmente).

4.9 Annullamento delle registrazioni di protocollo

Le registrazioni di protocollo possono essere annullate tramite una funzione specifica del sistema di gestione del protocollo, riservata esclusivamente al Responsabile della gestione documentale.

Solo il Responsabile della gestione documentale è autorizzato ad annullare o a disporre l'annullamento delle registrazioni di protocollo, mediante un atto formale (determinazione) di annullamento.

Per richiedere l'annullamento di una registrazione, il Responsabile dell'Ufficio interessato deve inviare una richiesta scritta e motivata al Responsabile della gestione documentale.

Durante il processo di annullamento, il sistema registra i dettagli del provvedimento di autorizzazione redatto dal Responsabile della gestione documentale, inclusi ora, data e nome dell'Operatore che effettua l'operazione (TUDA, artt. 54 e 61).

Le registrazioni annullate rimangono memorizzate nel registro di Protocollo e sono evidenziate chiaramente dal sistema. Sui documenti cartacei annullati viene applicato un timbro che riporta gli estremi del verbale di annullamento; il documento è conservato, anche mediante foto-riproduzione, a cura del Responsabile del servizio.

In caso di protocollazione di messaggi che coinvolgono interoperabilità tra le Pubbliche Amministrazioni, l'annullamento sarà notificato automaticamente all'interlocutore nel formato previsto dall'Allegato 6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

Per ulteriori dettagli sull'annullamento, si rimanda all'art. 3.1.5 delle Linee Guida di AgID.

4.10 Immodificabilità del Registro Protocollo

Per una registrazione di protocollo, le informazioni non modificabili sono (TUDA art. 54):

- Numero di protocollo;
- Data di registrazione;
- Oggetto;
- Mittente per i documenti ricevuti o, in alternativa, destinatario per i documenti spediti;

- Data e numero di protocollo del documento ricevuto, se disponibili;
- Impronta del documento informatico principale e degli eventuali allegati;
- Documento principale e eventuali allegati.

Qualora si renda necessaria una modifica ad una di queste informazioni, è obbligatorio annullare l'intera registrazione di protocollo e creare una nuova registrazione (con un nuovo numero di protocollo) contenente le informazioni corrette.

Le uniche informazioni modificabili in una registrazione di protocollo, non comprese in quelle sopra elencate, devono essere tracciate e storicizzate, registrando le operazioni di modifica o annullamento eseguite, insieme all'identificativo dell'operatore che ha effettuato l'operazione.

Le informazioni originali rimangono visibili e confrontabili con quelle modificate (TUDA art. 54, c.2).

4.11 Differimento dei termini di registrazione

Sebbene il principio generale sia quello della tempestività della registrazione, un eventuale differimento può essere consentito esclusivamente in presenza di specifiche circostanze e condizioni ben definite dai regolamenti interni al Consorzio e che riguardano:

- Motivi organizzativi e logistici (es. emergenze, calamità naturali, crisi sanitarie che impediscono il corretto espletamento degli obblighi di registrazione)
- Specifiche condizioni normative straordinarie (es. norme emergenziali statali che dispongono una sospensione temporanea degli adempimenti di registrazione)

Il differimento deve essere limitato nel tempo, adeguatamente motivato e circoscritto a situazioni eccezionali.

4.12 Registro di emergenza

L'art. 63 del TUDA stabilisce la possibilità per Il Consorzio di utilizzare uno o più registri di emergenza ogni volta che per cause tecniche non sia possibile utilizzare la procedura informatica ordinaria. Nel registro dovranno essere riportate le cause, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino delle funzionalità ordinarie del sistema. Il registro di emergenza permette l'identificazione univoca di tutta la documentazione del Consorzio anche in momenti di interruzione. A seguito del ripristino funzionale del sistema informatico ordinario, le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati; a ciascun documento viene quindi attribuito un numero di protocollo del sistema ordinario così da mantenere la correlazione con il numero utilizzato in emergenza.

4.13 Acquisizione dei Documenti informatici

L'art. 20 del CAD stabilisce l'efficacia giuridica del documento informatico quando vi è apposta una firma digitale o comunque è formato attraverso un processo che consente l'immodificabilità, l'integrità e la sicurezza del documento, permettendo allo stesso tempo la sua riconducibilità all'autore. I documenti informatici possono essere acquisiti in vari modi, tra cui:

- Tramite posta elettronica certificata;
- Tramite posta elettronica ordinaria;

- In cooperazione applicativa;
- Attraverso l'acquisizione di una copia conforme di un documento analogico
- Attraverso memorizzazione in formato digitale di transazioni o processi informatici;
- Generazione o raggruppamento di dati o registrazioni provenienti da una o più banche dati

4.14 Scansione dei Documenti cartacei

In caso di corrispondenza in arrivo su carta, l'AOO provvede alla scansione immediata dopo la registrazione, così che il documento digitalizzato possa essere utilizzato. Eventuali flussi interni cartacei sono fortemente limitati. Qualora si producano documenti cartacei interni che abbiano rilevanza amministrativa, il personale è tenuto a digitalizzarli e inserirli nel sistema documentale. Il Consorzio Culturale del Monfalconese persegue come obiettivo primario la migrazione progressiva dei flussi cartacei verso quelli digitali, così come stabilito dall'approccio "digital first", in linea con il CAD e gli obiettivi di dematerializzazione. Gli atti redatti dalle Pubbliche Amministrazioni mediante strumenti informatici, nonché i dati e i documenti informatici da esse detenuti, costituiscono informazione primaria e originale. Da tali documenti è possibile effettuare duplicazioni e copie, su supporti identici o differenti, per gli usi consentiti dalla legge.

Ai sensi dell'articolo 23-ter, comma 1-bis, la copia informatica di documentazione originariamente cartacea è prodotta tramite processi e strumenti idonei a garantire che il documento informatico riproduca fedelmente il contenuto dell'originale analogico, previa verifica diretta dei documenti oppure mediante certificazione del processo nei casi in cui siano utilizzate tecnologie in grado di assicurare tale corrispondenza.

In base al comma 3 del medesimo articolo, le copie informatiche di documenti formati originariamente su supporto analogico da parte della Pubblica Amministrazione hanno lo stesso valore giuridico degli originali, a tutti gli effetti di legge, purché la loro conformità all'originale sia attestata da un funzionario incaricato, mediante l'apposizione della firma digitale o di altra firma elettronica qualificata, nel rispetto delle linee guida vigenti.

5. GESTIONE DEI FLUSSI DOCUMENTALI

5.1 Schema di metadati per i documenti informatici, i documenti amministrativi informatici e le aggregazioni documentali informatiche

Nel contesto di una gestione informatica dei documenti, i metadati sono informazioni essenziali che descrivono e caratterizzano i documenti digitali, facilitando la loro organizzazione, ricerca, accessibilità e conservazione. La gestione corretta dei metadati è essenziale per garantire che ogni documento prodotto o ricevuto dal Consorzio possa essere recuperato, utilizzato e conservato in conformità alle linee guida AgID e al Codice dell'Amministrazione Digitale (CAD).

Ogni documento amministrativo, prodotto o ricevuto dal Consorzio, deve essere corredato da metadati adeguati che ne descrivano le caratteristiche, la provenienza e il ciclo di vita. Le principali categorie di metadati sono:

- Metadati descrittivi: riguardano informazioni che identificano il contenuto del documento, andando a valorizzare l'oggetto, la descrizione, il titolo, l'autore e la data di creazione del contenuto;
- Metadati strutturali: indicano come il documento è strutturato e organizzato (es. formato del file, versione del documento principale e dei relativi allegati). Queste informazioni sono essenziali per la corretta visualizzazione e fruizione del documento;
- Metadati amministrativi: relativi alla gestione e al trattamento del documento all'interno dell'ente. Questi comprendono informazioni come numero di protocollo, data di registrazione, scadenza, tipo di documento (delibera, determina) e stato del documento (es. assegnazioni e fasi di lavorazione);
- Metadati di sicurezza: sono relativi alla protezione dei documenti e includono le informazioni necessarie per valorizzare la firma digitale, i livelli di autorizzazione per l'accesso e la privacy dei dati.

L'allegato 5 delle linee guida in materia di "Formazione, gestione e conservazione dei documenti informatici" individua una serie di informazioni obbligatorie e da valorizzare per i documenti informatici, i documenti amministrativi e le aggregazioni documenti informatiche.

5.2 Piano di classificazione

Per piano di classificazione si intende un sistema precostituito di partizioni astratte, gerarchicamente ordinate (dal generale al particolare), fissate sulla base delle analisi delle funzioni dell'ente, ai quali deve ricondursi la molteplicità dei documenti prodotti per organizzare la sedimentazione ordinata dell'archivio. Il piano di classificazione è stabilito dall' AOO col supporto del Responsabile della Gestione Documentale.

Il Piano di classificazione non è retroattivo ed è stato ricavato da un'analisi funzionale interna al Consorzio. L'AOO di riferimento ha il potere di modificarne i contenuti ogni volta che viene ritenuto necessario, in virtù di ogni modifica funzionale alle attività documentali dell'Amministrazione

Si rimanda all'***Allegato 4*** per quanto riguarda lo schema di classificazione in uso in questa Amministrazione.

5.3 Classificazione dei documenti

L'art. 56 del D.P.R 445/2000 stabilisce come la classificazione sia una operazione necessaria e sufficiente per la tenuta del Sistema di Gestione Documentale. Ogni documento registrato a protocollo deve essere

immediatamente classificato in base al Piano adottato dal Consorzio. La classificazione è un'operazione obbligatoria e necessaria e consiste nell'assegnare a ciascun documento un titolo, una classe ed eventualmente una sottoclasse di appartenenza per oggetto e funzioni del Consorzio. Il Piano indica la posizione logica ed intellettuale dei documenti all'interno dell'archivio corrente. La classificazione è un'operazione obbligatoria per tutta la documentazione non protocollata e in uscita.

Nel classificare il documento, l'operatore deve verificare la coerenza tra l'oggetto e il contenuto del documento e la classe di titolario scelta. La classificazione verrà effettuata tenendo conto della natura dell'atto e della materia trattata: il riferimento al titolo e alla classe rifletterà fedelmente l'argomento del documento. Il Piano di classificazione fornisce definizioni e ambiti per ciascuna voce classificatoria; è buona pratica consultare tali definizioni e, se necessario, l'istruzione del Responsabile della Gestione Documentale per assicurarsi di selezionare la categoria adeguata. In caso di documenti dal contenuto multidisciplinare o potenzialmente riferibili a più voci di titolario, si sceglie la classificazione prevalente in base all'oggetto principale del documento.

La classificazione coinvolge diverse figure all'interno dell'Amministrazione:

- l'AOO di riferimento gestisce la protocollazione della documentazione in entrata ed in uscita dell'Amministrazione ed assegna titolo e classe al documento secondo il Piano di classificazione.
- il RUP prende in carico il documento dopo la classificazione: Il suo compito è quello di verificare che il titolo e la classe assegnate al documento corrispondano al contenuto dell'atto nell'ambito del procedimento di competenza, segnalando eventuali incongruenze da correggere.
- Il Responsabile della Gestione Documentale sovrintende all'intero sistema, incluse le attività di classificazione. È compito del RGD assicurare che il Piano di Classificazione sia adottato correttamente e aggiornato quando intervengono cambiamenti normativi o organizzativi. Il RGD cura la formazione del personale abilitato alla classificazione, fornendo istruzioni sull'uso corretto del titolario e comunicando tempestivamente eventuali modifiche dello stesso.

La tempistica dell'assegnazione è immediata: l'assegnazione dell'indice di classificazione avviene contestualmente o immediatamente alla protocollazione del documento. In altre parole, appena un documento viene registrato a protocollo, gli si attribuisce subito la relativa classe archivistica, prima che il documento prosegua nel suo iter. È possibile effettuare modifiche o aggiornamenti nel caso in cui la classificazione presenti degli errori. Eventuali azioni di modifica devono avvenire con modalità tracciabili e in tempi rapidi.

Tutte le operazioni di classificazione devono essere tracciate nel Sistema di Gestione Documentale. Il sistema registra in un log ogni azione significativa, dall'assegnazione iniziale della classe all'eventuale modifica successiva. In particolare, per ogni documento il sistema memorizza i metadati della classificazione insieme all'identificativo dell'operatore che ha effettuato l'operazione.

5.4 Piano di organizzazione delle aggregazioni documentali

L'esigenza di evidenziare il vincolo archivistico spinge a completare le attività di registrazione con la fascicolazione dei documenti, che consiste nel riunire in un'unità archivistica tutta la documentazione relativa ad uno stesso procedimento amministrativo, processo o comunque riferiti a una stesa attività, affare, persona fisica o giuridica. È stato compito del Consorzio Culturale del Monfalconese, in collaborazione con il

Responsabile della Gestione Documentale, effettuare un censimento dei procedimenti amministrativi, tale da garantire un Piano di Organizzazione il più conforme possibile alle reali esigenze operative dell'Amministrazione.

L'art 64, comma 4 del TUDA esplicita come sia competenza del Consorzio attribuire, all'interno dell'AOO di riferimento le competenze e le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti.

Le principali tipologie di aggregazione documentali sono le seguenti:

- Fascicolo per procedimento amministrativo: raccoglie tutti i documenti relativi allo svolgimento di un procedimento amministrativo;
- Fascicolo per affare: aggrega documenti relativi a un'attività o tema specifico non configurabile come procedimento formale;
- Fascicolo per attività: documenta e raggruppa un'attività continuativa e ricorrente dell'UOR;
- Fascicolo per soggetto o persona giuridica: raccoglie e gestisce la documentazione riferita a un soggetto specifico.

5.5 Formazione dei fascicoli e delle ADI

Ad ogni documento protocollato e successivamente classificato deve essere obbligatoriamente associato un fascicolo. La fascicolazione continuativa di tutti i documenti rientra negli obblighi di gestione documentale previsti dalla normativa vigente.

La creazione di un nuovo fascicolo o di una nuova Aggregazione Documentale Informatica è effettuata dalla UOR competente per materia, facendo ricadere l'unità archivistica nel corretto titolo e classe del Piano di Classificazione. Ad ogni fascicolo viene assegnato una serie di informazioni tali da garantire la corretta fruizione all'interno del servizio Essi sono:

- anno di apertura;
- indice di classificazione;
- un numero progressivo univoco nell'ambito di quella classifica/anno;
- un oggetto descrittivo che identifichi in modo chiaro il tema trattato.

Ogni Aggregazione Documentale Informatica deve riportare tutti i metadati archivistici obbligatori, cosi come stabilito dall'allegato 5 delle linee guida AgID. Queste informazioni sono:

- tipo di aggregazione (indicando se l'oggetto è un fascicolo oppure una serie);
- identificativo univoco dell'aggregazione (definito automaticamente dal sistema);
- titolo e classe di riferimento;
- l'oggetto del fascicolo informatico o la denominazione della serie;
- tipologia di fascicolo;
- assegnazioni;

- la data di apertura e quando applicabile la data di chiusura dell'aggregazione.

Le UOR sono responsabili dell'aggiornamento costante dei fascicoli con i nuovi documenti ricevuti o prodotti e inerenti allo stesso affare/procedimento. Quando l'attività o il procedimento si conclude, la UOR competente procede a chiudere il fascicolo, registrando nel sistema la data di chiusura e lo stato concluso. La chiusura avviene al termine dell'anno solare per i fascicoli ancora aperti di affari non conclusi oppure immediatamente al completamento dell'affare se questo si esaurisce prima. Dopo la chiusura, il fascicolo diventa inattivo per ulteriori aggiunte; eventuali documenti successivi sullo stesso tema dovranno essere inseriti in un nuovo fascicolo.

Tutta la documentazione che necessita di registrazione particolare è aggregata all'interno di serie documentali. Quest'ultimi sono chiamati repertori e raggruppano atti con forma omogenea ma con contenuto diverso; prodotti con continuità nel tempo. Essi possono essere: registri di determinazioni dirigenziali, deliberazioni di Giunta o Consiglio, contratti, verbali e ordinanze. Per ciascuna serie documentale, il servizio informatico indica l'UOR responsabile e la numerazione progressiva per ogni anno. Alla fine di ogni periodo la serie viene chiusa e riaperta con nuova numerazione all'inizio di ogni anno di riferimento.

Ogni fascicolo informatico e ogni serie documentale riporta tutti i metadati obbligatori stabiliti dalle Linee Guida AgID con l'allegato 5. Tali metadati comprendono:

- tipo di aggregazione;
- identificativo univoco dell'aggregazione;
- classificazione di riferimento;
- chiave descrittiva, ossia l'oggetto;
- la data di apertura;
- e quando applicabile la data di chiusura.

Il Responsabile della Gestione Documentale svolge un ruolo di supervisione sull'intero piano di organizzazione delle aggregazioni documentali. Inoltre effettua controlli periodici e monitoraggi per assicurare la corretta applicazione delle regole. Il RGD assicura la chiusura regolare dei fascicoli e coordina il trasferimento di quest'ultimi verso l'archivio di deposito o il sistema di conservazione digitale.

Lo SGID in uso in questa Amministrazione permette la corretta organizzazione delle informazioni che descrivono i collegamenti tra i documenti di uno stesso fascicolo. Il Sistema Informatico permette inoltre di reperire con facilità le informazioni riguardanti le Aggregazioni Documentarie, il procedimento e il relativo Responsabile. Un fascicolo può essere articolato in sotto fascicoli e questi in inserti per facilitare la gestione dei flussi documentari e di lavoro. Ad ogni livello si può assegnare un livello di riservatezza o di accessibilità. Un documento può essere associato a uno o più fascicoli senza necessità di duplicazione del file, ma valorizzando semplicemente una serie di metadati che permetteranno al documento di appartenere a più di un fascicolo.

I fascicoli che si creano all'interno dell'Amministrazione vengono annotati all'interno del repertorio dei fascicoli. Questo è uno strumento dinamico e concreto che registra in maniera univoca e progressiva tutti i fascicoli o le Aggregazioni Documentarie gestite dal Consorzio.

5.6 Gestione dei flussi documentali e dei flussi di lavoro

L'Amministrazione gestisce la documentazione assicurando che ogni fase del ciclo di vita del documento, dalla ricezione o creazione fino alla conservazione, avvenga secondo procedure uniformi e nel rispetto della normativa vigente. Eventuali flussi cartacei residui vengono integrati nel sistema digitale tramite protocollazione e successiva scansione dei documenti analogici.

Tutta la corrispondenza in entrata viene presa in carico dall'AOO e registrata tempestivamente nel registro di protocollo informatico. Al documento viene assegnato un numero progressivo di sette cifre, la data (giorno e ora) di registrazione, le informazioni sul mittente/destinatario, l'oggetto e altre informazioni di classificazione preliminare, assicurandone la tracciabilità legale della ricezione come richiesto dal D.P.R. del 445/200. La protocollazione avviene tramite il Sistema Informatico dedicato che genera anche la segnatura di protocollo sul documento registrato. Successivamente ogni documento viene assegnato alla UOR competente per materia, avviando di fatto il relativo flusso di lavoro interno. L'assegnazione è effettuata dall'AOO, utilizzando le funzionalità del Sistema Documentale. Quest'ultimo notifica l'assegnazione al Responsabile creando di fatto un'attività nel workflow documentale. Ogni documento interno creato dall'Amministrazione segue un processo analogo di smistamento tramite il sistema di workflow documentale. In tutti i casi, l'assegnazione formalizza quale ufficio e quale RUP sono responsabili della trattazione di quel documento. Contestualmente all'assegnazione, possono essere indicati anche uno o piò destinatari interni in copia conoscenza se il documento richiede coinvolgimento di altri uffici. All'assegnazione segue la presa in carico del documento: il responsabile accede al Sistema di Gestione Documentale e conferma la presa in carico. Il sistema registra la data/ora della presa in carico e l'identità dell'operatore, tracciando il passaggio di consegne. In questa fase, il documento viene anche classificato secondo il Piano di Classificazione ed inserito nel fascicolo informatico pertinente. Se il documento si riferisce a una pratica già esistente, sarà agganciato al fascicolo già aperto; viceversa sarà compito del personale dell'UOR di aprire un nuovo fascicolo. Quando la gestione di un documento giunge ad una fase conclusiva, l'atto viene sottoscritto con firma digitale conforme ai requisiti del CAD e in grado di garantire l'autenticità, l'integrità e la validità legale del documento informatico. A conclusione del procedimento, la UOR responsabile procede alla chiusura del fascicolo. La chiusura avviene mediante apposita funzione sul sistema documentale: il fascicolo informatico viene chiuso con decorrenza di una data certa, impedendo di fatto l'aggiunta di ulteriori documenti.

5.7 Ricezione

5.7.1 Ricezione dei documenti cartacei

I documenti cartacei possono pervenire agli uffici di protocollazione attraverso diverse modalità, ciascuna delle quali deve essere gestita con attenzione per garantire una corretta registrazione e trattamento. Le principali modalità di ricezione dei documenti sono le seguenti:

1. **Servizio Postale**: I documenti possono essere inviati tramite il servizio postale, sia ordinario che raccomandato. In questo caso, la posta viene recapitata direttamente all'ufficio competente per la protocollazione.
2. **Consegna Diretta**: I documenti possono essere consegnati fisicamente agli uffici, ai funzionari responsabili o agli uffici specificamente abilitati all'amministrazione per ricevere la documentazione. Questo può avvenire in presenza o tramite corrieri autorizzati.

Quando i documenti giungono ad altri uffici, che non sono direttamente incaricati della protocollazione, siano essi consegnati di persona, tramite posta, il personale che li riceve è tenuto a provvedere alla loro trasmissione all'Ufficio Protocollo Generale. Questo passaggio è cruciale per assicurare che tutti i documenti siano correttamente registrati e trattati secondo le normative vigenti.

Nel caso in cui sia richiesta una conferma della consegna di un documento cartaceo, gli uffici abilitati alla ricezione forniscono una fotocopia del primo foglio del documento stesso. Questa fotocopia è timbrata con il nome dell'Amministrazione, la data e l'ora di arrivo, e la sigla dell'operatore che ha gestito la ricezione.

In alternativa, se l'ufficio ricevente è dotato dei necessari strumenti e procedure, effettua la registrazione del documento nel sistema di protocollo informatico e fornisce una ricevuta cartacea generata dalla procedura informatica. Questa ricevuta contiene tutti i dettagli principali della registrazione, inclusi il numero, la data, l'oggetto e il mittente del documento.

Inoltre, i documenti cartacei vengono acquisiti in formato elettronico mediante l'uso di uno scanner ottico o di un dispositivo multifunzione. I documenti elettronici risultanti dalla scansione sono poi registrati nel protocollo come documento principale, con la possibilità di includere eventuali allegati che accompagnano il documento originale. Questo processo di digitalizzazione è essenziale per garantire una gestione efficace e una facile consultazione dei documenti.

5.7.2 Ricezione dei documenti informatici

La ricezione dei documenti informatici presso l'Ente avviene principalmente attraverso le caselle di posta elettronica certificata (PEC), che sono specificamente predisposte per tale scopo. Queste caselle sono accessibili esclusivamente al personale autorizzato, incaricato della gestione e della protocollazione dei documenti. Nel caso in cui un documento informatico, corredato di firma digitale, venga erroneamente inviato a una casella di posta personale anziché alla casella istituzionale, è necessario che venga prontamente reindirizzato alla casella ufficiale dell'Ente. Inoltre, il mittente deve essere tempestivamente informato dell'indirizzo corretto a cui inviare futuri documenti.

Il personale addetto al Servizio di Protocollo svolge un controllo quotidiano dei messaggi ricevuti nella casella di posta istituzionale. Questo processo di monitoraggio include l'esclusione dei messaggi che sono sottoposti a protocollazione automatica. Dopo aver effettuato una verifica approfondita dell'integrità e della validità del messaggio, il personale procede alla registrazione di protocollo del documento, rispettando, in linea di massima, l'ordine cronologico di ricezione, salvo particolari eccezioni che verranno trattate separatamente.

Secondo l'articolo 20, comma 1-bis, del Codice dell'Amministrazione Digitale (CAD), un documento informatico è considerato valido e conforme ai requisiti della forma scritta se è firmato digitalmente, con una firma elettronica qualificata, avanzata, o se è prodotto tramite un processo che garantisca sicurezza, integrità e immodificabilità, e che permetta l'identificazione chiara dell'autore. Per i documenti privi di tali firme, la loro idoneità a soddisfare il requisito della forma scritta e il loro valore probatorio devono essere valutati individualmente, in base alle specifiche caratteristiche di sicurezza e integrità.

La firma elettronica utilizzata per l'invio e la ricezione di documenti, nonché per la loro sottoscrizione, rappresenta lo strumento essenziale che assicura l'identificabilità del sottoscrittore e l'integrità del documento stesso. Come stabilito dall'articolo 24, comma 2, del CAD, la firma digitale sostituisce tutti i sigilli, punzoni, timbri e contrassegni previsti dalla normativa vigente. Per la generazione della firma digitale è indispensabile

utilizzare un certificato qualificato che sia attualmente valido, non scaduto, e non revocato o sospeso. Tale certificato deve consentire la verifica della sua validità, degli elementi identificativi del titolare e del certificatore, nonché degli eventuali limiti d'uso. Le Linee Guida definiscono anche le modalità e i tempi per l'apposizione della firma.

Se un documento informatico è firmato con un certificato elettronico che risulta revocato, scaduto o sospeso, la firma viene considerata nulla, a meno che lo stato di sospensione non sia stato precedentemente annullato. Il certificato di firma viene verificato dalle postazioni apposite per la registrazione dei documenti in ingresso.

Nel caso in cui il messaggio o il documento ricevuto risulti illeggibile, incompleto o infetto da virus, gli operatori autorizzati alla gestione delle caselle di posta certificata del Consorzio Culturale del Monfalconese devono informare il mittente, comunicando che il documento non sarà sottoposto a protocollazione. Inoltre, i documenti elettronici ricevuti in formati non conformi a quelli stabiliti dalle Linee Guida e dal Manuale dell'Ente saranno restituiti al mittente con una spiegazione, senza procedere alla protocollazione.

I dipendenti autorizzati sono responsabili delle operazioni di ricezione dei documenti informatici, che comprendono la verifica della loro autenticità, provenienza, integrità, leggibilità, e la conferma dell'ammissibilità alla registrazione di protocollo. La notifica al mittente dell'avvenuta ricezione del messaggio è garantita dagli standard specifici del servizio di posta elettronica certificata.

5.7.3 Ricezione di documenti informatici su supporti rimovibili

L'Amministrazione si prepara ad acquisire e trattare tutti i documenti informatici ricevuti su supporti rimovibili che è in grado di decodificare e interpretare con le tecnologie disponibili. Una volta decodificato, il documento viene acquisito, integrato nel flusso di lavorazione e sottoposto agli adempimenti previsti dalle modalità stabilite nel presente Manuale.

5.7.4 Ricezione dei documenti su casella istituzionale (PEC)

La ricezione dei documenti digitali è garantita tramite l'utilizzo di una casella di Posta Elettronica Certificata (PEC). L'indirizzo di tale casella PEC è il seguente: consorzio-culturale-monfalconese@certgov.fvg.it.

La casella di PEC è accessibile per la ricezione e l'invio della documentazione esclusivamente all'ufficio protocollo. La manutenzione e la gestione tecnica della casella PEC sono affidati al Servizio informatico, in modo analogo a quanto avviene per le altre caselle di posta elettronica ordinaria.

I documenti pervenuti tramite la posta elettronica certificata, che sono strutturati in conformità con le normative per garantire l'interoperabilità dei sistemi di protocollo informatico tra le Pubbliche Amministrazioni, verranno protocollati nel momento in cui l'operatore provvede a tale operazione utilizzando le informazioni contenute nella segnalazione informatica del mittente.

Il software di protocollo crea e invia automaticamente le seguenti notifiche per garantire l'interoperabilità:

- Messaggio di conferma ricezione;
- Messaggio di notifica eccezione;
- Messaggio di aggiornamento conferma;
- Messaggio di annullamento protocollazione.

I documenti ricevuti via PEC che non riguardano l'interoperabilità saranno valutati per verificarne il contenuto e l'autenticità e, se necessario, registrati immediatamente.

I documenti informatici ricevuti su altri indirizzi e-mail devono essere respinti al mittente, indicando chiaramente l'indirizzo PEC istituzionale. Questo permetterà al mittente di rinviare correttamente la documentazione attraverso il canale appropriato.

Per quanto riguarda la ricezione dei documenti tramite posta elettronica, la notifica dell'avvenuta ricezione è assicurata dal sistema di posta elettronica certificata utilizzato dal mittente. Come previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (All. 6), qualora il mittente ne faccia richiesta, il sistema informatico in uso genererà un messaggio di posta elettronica che notifica al mittente l'avvenuta protocollazione dell'atto, includendo numero e data di protocollazione.

Infine, è consentito l'utilizzo di caselle di posta elettronica non certificata, seguendo le modalità e le procedure dettagliate nel presente Manuale.

5.7.5 Utilizzo della posta elettronica ordinaria

Ogni ufficio dispone di una casella di posta elettronica istituzionale non certificata, i cui indirizzi sono pubblicati nella sezione "Trasparenza" del sito web dell'Ente, in conformità con quanto previsto dal D.lgs. 33/2013. Inoltre, ogni dipendente è assegnato a una casella di posta elettronica nominativa non certificata.

La posta elettronica è utilizzata per l'invio di comunicazioni, informazioni e documenti sia all'interno dell'Ente che nei rapporti con cittadini, soggetti privati e altre Pubbliche Amministrazioni. Tuttavia, le comunicazioni formali e la trasmissione di documenti informatici che comportano impegni ufficiali dell'Ente verso terzi devono avvenire tramite le caselle di posta elettronica istituzionale.

I documenti informatici ricevuti presso uffici non designati per la ricezione devono essere inoltrati all'indirizzo di posta elettronica istituzionale.

Invece, le comunicazioni informali ricevute o trasmesse per posta elettronica, che non comportano impegni ufficiali dell'Ente, possono non essere protocollate. Tuttavia, deve sempre essere confermato l'avvenuto ricevimento a chi ne fa richiesta.

È vietato inviare messaggi dalla casella di posta elettronica nominativa quando il contenuto di questi messaggi implica impegni dell'Amministrazione verso terzi. Nei messaggi di posta elettronica non certificata è automaticamente inserito il seguente avviso di riservatezza:

Le informazioni del presente documento e allegati sono riservate esclusivamente al destinatario indicato. La diffusione del messaggio da parte di terzi non è consentita salvo autorizzazione espressa. Non potendo assicurare l'integrità dei messaggi trasmessi via internet, il CCM declina ogni responsabilità in merito.

Se avete ricevuto questa documentazione per errore vi preghiamo di eliminarla dai vostri archivi e darne comunicazione a: info@ccm.it. Grazie!

. Infine, la posta elettronica nominativa non può essere utilizzata per la ricezione o l'invio di documenti firmati digitalmente, per i quali è prevista l'uso di una casella ufficiale apposita.

5.7.6 Procedura di apertura e gestione della corrispondenza in entrata

Il personale incaricato della protocollazione in entrata è responsabile dell'apertura di tutta la corrispondenza

ricevuta dall'Ente, sia essa cartacea che elettronica pervenuta tramite PEC istituzionale. Questo include anche le buste indirizzate direttamente al personale, che devono essere aperte dal servizio protocollo. Tuttavia, non vengono aperte le buste contrassegnate con le diciture: "riservato", "personale", "confidenziale", o quelle che, per la loro confezione, indicano chiaramente un carattere di corrispondenza privata. Inoltre, non vengono aperte le buste contrassegnate con "offerta", "gara d'appalto", "preventivo-offerta" o altre diciture simili come "non aprire".

Qualora un dipendente riceva documenti tramite corrispondenza privata riguardanti affari o procedimenti amministrativi dell'Ente, è obbligato a consegnarli al Servizio di Protocollo per la tempestiva protocollazione.

Le buste pervenute tramite posta registrata, quelle specificamente indicate dalle UOR, e quelle contenenti documenti senza destinatario specificato, devono essere trasmesse insieme ai documenti. Le buste delle raccomandate e tutte quelle contenenti elementi utili per le operazioni di protocollazione devono essere conservate insieme ai documenti a cui si riferiscono.

Di norma le buste dei documenti analogici pervenuti non s'inoltrano agli uffici destinatari, ad eccezione delle buste dei corrieri espressi, raccomandate ecc. che sono consegnate insieme ai documenti stessi.

5.7.7 Rilascio di ricevute

Se si dovesse richiedere il rilascio di una ricevuta che attesti la consegna diretta di un documento cartaceo, gli uffici incaricati della ricezione dei documenti possono emettere una fotocopia della prima pagina del documento stesso. Questa fotocopia deve essere opportunamente timbrata con la data di ricezione e la sigla dell'operatore responsabile.

In alternativa, se l'ufficio in questione dovesse disporre delle abilitazioni necessarie, potrebbe effettuare la registrazione formale del documento attraverso la procedura di protocollo in uso e, successivamente, rilasciare una ricevuta ufficiale. Nel caso in cui il documento sia pervenuto tramite posta elettronica certificata (PEC), la conferma di avvenuta ricezione sarà garantita dal sistema di posta elettronica certificata adottato dal Consorzio, che provvederà a notificare automaticamente l'avvenuta ricezione del documento.

5.7.8 Assegnazioni e modifiche dei documenti

Per "assegnazione" si intende il processo di identificazione dell'ufficio, o degli uffici, responsabili della trattazione di un documento, ossia l'ufficio di competenza. Dopo aver elaborato la posta secondo le modalità descritte nelle sezioni precedenti, il Dirigente dell'ufficio che riceve il documento in carico, valutato il contenuto dello stesso, dispone la sua registrazione a protocollo.

In caso di smistamento errato, l'ufficio che riceve il documento lo trasmette, nel minor tempo possibile, all'ufficio competente, che provvederà a protocollarlo nel sistema informatico. Il sistema di gestione informatica dei documenti registra e traccia questi passaggi, memorizzando le modifiche con la relativa data e ora di esecuzione.

5.7.9 Correzione di una assegnazione

Nel caso in cui un documento venga assegnato o inoltrato erroneamente e debba essere inviato a un altro utente o UOR sotto lo stesso Responsabile, il processo di correzione deve essere gestito direttamente dall'ufficio che ha effettuato l'assegnazione iniziale. Questo ufficio è responsabile della modifica dell'assegnazione nel sistema di protocollo, assicurandosi che il documento venga reindirizzato correttamente.

Il destinatario del documento può decidere di rifiutare l'inoltro se ritiene che non sia corretto. In tal caso, il destinatario deve annotare le motivazioni del rifiuto. Gli inoltri rifiutati vengono restituiti all'ufficio mittente insieme alla spiegazione del rifiuto, in modo che quest'ultimo possa correggere l'errore e procedere con un inoltro corretto.

Il sistema di gestione documentale tiene un registro dettagliato di tutte queste operazioni. Ogni passaggio viene tracciato, memorizzando l'identificativo dell'operatore che ha effettuato la modifica, nonché la data e l'ora precise dell'intervento, garantendo così una completa trasparenza e tracciabilità delle modifiche effettuate.

5.7.10 Orari di apertura per il ricevimento della documentazione cartacea

L'ufficio predisposto a ricevere la documentazione cartacea è aperto con i seguenti orari:

- Lunedì dalle ore 9:00 alle ore 13:00, con apertura pomeridiana dalle ore 14:00 alle ore 18:00;
- Martedì dalle ore 9:00 alle ore 13:00;
- Mercoledì dalle ore 9:00 alle ore 13:00, con apertura pomeridiana dalle ore 14:00 alle ore 18:00;
- Giovedì dalle ore 9:00 alle ore 13:00;
- Venerdì dalle ore 9:00 alle ore 13:00.

Tutti i settori e servizi seguono questi orari per le richieste di registrazione dei documenti e per la comunicazione riguardante la ricezione di buste, domande di concorso o altra documentazione.

I documenti inviati tramite servizio postale vengono consegnati all'U.O. Protocollo direttamente dal servizio postale.

5.8 Spedizione

5.8.1 Spedizione dei documenti cartacei

Quando il destinatario non dispone di un domicilio digitale, sarà inviata una copia cartacea dell'originale informatico firmato digitalmente, come previsto dall'art. 3-bis, comma 4-bis del Codice dell'Amministrazione Digitale (CAD).

Procedura per la spedizione dei documenti cartacei:

1. **Registrazione e Preparazione dei Documenti:**
    - I documenti destinati alla spedizione su supporto cartaceo devono essere prima protocollati, segnati, classificati e fascicolati secondo le normative vigenti e le procedure interne.
    - Dopo aver completato queste operazioni, i documenti sono preparati per la spedizione.
2. **Imballaggio e Spedizione:**
    - I documenti devono essere inviati all'ufficio Protocollo/Spedizione all'interno di buste aperte, che devono essere già intestate e indirizzate dagli uffici utente.
    - Sono escluse da questa regola le comunicazioni riservate ai sensi del D.lgs. 196/2003 e successive modifiche. Per tali documenti, il Responsabile del servizio può autorizzare la spedizione direttamente dagli uffici utente competenti, evitando così la trasmissione tramite l'ufficio Protocollo/Spedizione.

3. **Spedizioni Speciali:**
    - Per spedizioni tramite raccomandata con ricevuta di ritorno, posta celere, corriere o altri mezzi che richiedano documentazione aggiuntiva, gli uffici utente sono responsabili della preparazione della modulistica necessaria. Questo include la compilazione di moduli specifici e l'inclusione di eventuali documenti di supporto.
4. **Operazioni dell'Ufficio Centrale di Spedizione:**
    - L'ufficio centrale di spedizione si occupa della pesatura dei documenti, del calcolo delle spese postali e della gestione della relativa contabilità.
    - Gli uffici utente devono consegnare la posta in partenza all'ufficio centrale di spedizione..
    - In caso di situazioni di urgenza, il Responsabile del servizio potrà autorizzare procedure alternative a quelle standard, se necessario.
5. **Gestione degli Indirizzi:**
    - I destinatari dell'Amministrazione sono registrati in elenchi specifici che formano l'anagrafica unica dell'Ente.
    - Le modalità di registrazione e modifica degli indirizzi già registrati sono regolamentate dalle norme di scrittura stabilite per la gestione delle anagrafiche del sistema.

Queste procedure assicurano una gestione efficiente e conforme dei documenti amministrativi e delle spedizioni.

5.8.2 Spedizione dei documenti informatici

Per assicurare una gestione e trasmissione adeguata dei documenti informatici tra le Pubbliche Amministrazioni e per rispettare le normative vigenti, è cruciale seguire queste regole e linee guida:

1. **Trasmissione tramite PEC**:
    - I documenti informatici devono essere inviati tramite Posta Elettronica Certificata (PEC), a meno che non sia possibile ottenere l'indirizzo PEC del destinatario. La trasmissione dalla casella PEC istituzionale a quella del destinatario fornisce evidenza giuridico-probatoria dell'invio e della consegna (art. 47 del CAD).
2. **Riservatezza dei Dati Particolari e Giudiziari**:
    - In conformità con l'art. 46 del CAD, i documenti trasmessi ad altre Pubbliche Amministrazioni devono contenere solo i dati sensibili e giudiziari autorizzati da legge o regolamento e strettamente necessari per le finalità per le quali i dati sono stati acquisiti.
3. **Segretezza della Corrispondenza**:
    - Gli addetti alla spedizione devono rispettare le disposizioni dell'Art. 49, comma 1 del CAD, che garantisce la segretezza della corrispondenza trasmessa telematicamente.
4. **Ricevute Digitali**:
    - Le ricevute digitali di accettazione e consegna dei messaggi PEC devono essere automaticamente collegate ai messaggi stessi per fornire prova della trasmissione.

5. **Gestione dei Documenti**:
    - La spedizione dei documenti deve avvenire all'interno del sistema informatico di gestione documentale, garantendo l'interoperabilità tra i sistemi di protocollo. L'inoltro tramite PEC deve essere effettuato solo dopo che i documenti sono stati protocollati, segnati, classificati e fascicolati correttamente.
6. **Regole di Processamento**:
    - Le Amministrazioni Organizzatrici (AOO) devono seguire regole specifiche per la formazione del messaggio di protocollo destinato ad altra pubblica amministrazione, assicurando che i metadati siano compilati correttamente e che i documenti rispettino gli standard di interoperabilità.

In sintesi, è essenziale garantire che i documenti informatici siano gestiti e trasmessi in conformità con le normative vigenti sul trattamento dei dati e sulla segretezza, assicurando che siano correttamente protocollati e registrati per garantirne l'integrità e la tracciabilità.

Per dettagli specifici sulle modalità operative relative al software utilizzato, consultare il manuale operativo del software (***Allegato 8***)**,** che fornisce le procedure e i requisiti tecnici necessari per la corretta gestione dei documenti e delle comunicazioni via PEC.

5.8.3 Spedizioni massive

Nel caso di produzione massiva di documenti con intestazione nominale, come avvisi bonari, avvisi di pagamento o bollettini, è possibile adottare un'unica protocollazione per tutti i documenti emessi, assegnando un solo numero di protocollo al "ruolo" o gruppo di documenti.

Tuttavia, è fondamentale che ogni documento emesso sia riconducibile in modo univoco alla sua posizione nel Registro o nella banca dati dell'Unità Operativa (U.O.) che lo ha prodotto. Questo significa che, anche se viene utilizzato un solo numero di protocollo per un'intera serie di documenti, ogni documento deve avere un identificatore specifico che permetta di tracciarne la posizione e il relativo stato all'interno del sistema di gestione documentale.

In pratica, potresti avere un numero di protocollo principale per il gruppo di documenti, ma ogni singolo documento potrebbe avere un identificativo interno aggiuntivo che consente di risalire a tutti i dettagli necessari nel registro o nella banca dati. Questo approccio garantisce sia la semplificazione del processo di protocollazione che la tracciabilità e l'unicità di ciascun documento nel sistema.

5.8.4 Documenti interni e giuridici

La comunicazione interna informale tra uffici (o documento interno informale) si riferisce allo scambio di messaggi, con o senza documenti allegati, che non richiede una registrazione ufficiale in archivio. Questo tipo di comunicazioni è solitamente gestito via posta elettronica e non viene acquisito nel sistema di protocollo informatico.

Al contrario, un documento interno avente rilevanza giuridica procedimentale (o comunicazione interna formale) è una comunicazione, con o senza documenti allegati, che ha importanza per l'azione amministrativa e per la quale è necessario mantenere traccia nel fascicolo relativo al procedimento a cui si riferisce. Tali

comunicazioni sono gestite attraverso il sistema di protocollo informatico e devono essere registrate a protocollo.

La registrazione dei documenti interni formali è responsabilità dell'ufficio mittente, che si occupa della creazione e della gestione del fascicolo relativo all'affare o al procedimento amministrativo. I documenti interni di rilevanza giuridica procedimentale devono essere registrati, classificati e fascicolati nel sistema di protocollo informatico dal Responsabile del Procedimento Amministrativo (RPA). Il destinatario del documento non è tenuto a fare una nuova registrazione, ma deve limitarsi a "prendere in carico" il documento ricevuto. Se la UOR ricevente deve fornire un parere, redatto in formato analogico o informatico, deve registrare questo parere nel protocollo informatico unico e collegarlo al documento di richiesta. La UOR che riceve il documento di risposta lo inserisce nel fascicolo pertinente.

Anche i documenti interni che, pur non avendo un valore giuridico-probatorio, sono importanti come testimonianza dei processi decisionali e dell'attività complessiva dell'Ente, devono generalmente essere classificati e fascicolati. Questo garantisce che rimanga traccia dell'attività interlocutoria e conoscitiva dell'Ente in tutte le sue fasi. La classificazione e la fascicolazione sono compiti del Responsabile della gestione documentale.

5.9 Gestione documentale nell'ambito del lavoro agile

L’Ente riconosce il lavoro agile come modalità di esecuzione del rapporto di lavoro che può interessare anche personale coinvolto nella gestione documentale. Per garantire la continuità dei servizi e la corretta gestione dei documenti anche in tale contesto, vengono adottate le seguenti misure operative:

5.9.1 Accesso remoto ai sistemi documentali

Il personale autorizzato al lavoro agile accede al Sistema di Gestione Informatica dei Documenti attraverso una connessione VPN sicura, utilizzando dispositivi forniti dall'Amministrazione o, se espressamente autorizzati, dispositivi personali conformi alle policy di sicurezza dell'Ente. L'autenticazione avviene esclusivamente mediante sistemi di identificazione forte (strong authentication) basati su più fattori (credenziali di accesso personali e sistemi OTP - One Time Password).

5.9.2 Formazione e gestione dei documenti in modalità agile

La formazione, gestione e trasmissione dei documenti in contesto di lavoro agile segue le stesse regole e procedure stabilite per il lavoro in presenza. In particolare:

- È vietata la stampa di documenti contenenti dati riservati o personali sui dispositivi domestici privati;
- Qualsiasi documento prodotto durante l'attività in lavoro agile deve essere tempestivamente inserito nel Sistema di Gestione Documentale dell'Ente;
- La protocollazione dei documenti in entrata è centralizzata e resta di competenza del personale in presenza, salvo situazioni eccezionali espressamente autorizzate dal Responsabile della Gestione Documentale;
- La protocollazione in uscita può essere effettuata anche in modalità agile, nel rispetto delle procedure di sicurezza.

5.9.3 Misure di sicurezza specifiche

Durante lo svolgimento del lavoro in modalità agile, il dipendente:

- Deve operare in un ambiente che garantisca adeguata riservatezza per le attività di gestione documentale;
- È tenuto a bloccare la sessione di lavoro in caso di allontanamento dalla postazione;
- Non deve archiviare documenti dell'Ente su sistemi di storage personali o cloud non autorizzati;
- Deve segnalare immediatamente al Responsabile per la transizione digitale qualsiasi anomalia o possibile violazione di sicurezza.

5.9.4 Monitoraggio e controllo

Il Responsabile della Gestione Documentale, in collaborazione con il Responsabile della transizione digitale, monitora periodicamente l'efficacia delle procedure di gestione documentale in contesto di lavoro agile, attraverso:

- Verifiche a campione sulle attività di protocollazione e fascicolazione eseguite in modalità remota;
- Analisi dei log di sistema per rilevare eventuali anomalie o criticità;
- Raccolta di feedback dai dipendenti per identificare possibili miglioramenti operativi.

I risultati di tale monitoraggio sono utilizzati per aggiornare, se necessario, le procedure operative e le misure di sicurezza.

6. TENUTA E CONSERVAZIONE DELL'ARCHIVIO

6.1 Piano di conservazione dell'archivio

Il Piano di Conservazione è lo strumento che definisce per quanto tempo i documenti dell'Ente devono essere conservati e la loro destinazione finale (scarto o conservazione permanente). Il Piano di conservazione dell'archivio dell'Ente è adottato in conformità alla normativa vigente in materia di archivi pubblici, in particolare al Codice dei beni culturali (D.lgs. 42/2004) e al Testo Unico sulla documentazione amministrativa (D.P.R. 445/2000). Esso viene predisposto dal Responsabile della Gestione Documentale (RGD), con il coinvolgimento dei responsabili delle aree organizzative, e sottoposto all'approvazione degli organi competenti. Nel caso di enti pubblici, il massimario di conservazione è normalmente approvato dalla Soprintendenza archivistica competente, che esercita la vigilanza sulla corretta applicazione delle norme di tutela. Il Piano viene aggiornato periodicamente (o in occasione di modifiche normative/organizzative) per garantire che i tempi di conservazione restino adeguati alle esigenze amministrative e ai requisiti di legge. Dal punto di vista operativo, il Piano di conservazione funge da guida per tutte le operazioni di gestione archivistica. In fase di archiviazione, il personale addetto associa a ciascun fascicolo la categoria di classificazione e il corrispondente tempo di conservazione previsto. Tali informazioni sono registrate nel sistema di protocollo informatico così da permettere il calcolo automatico delle scadenze di conservazione. In questo modo Il Consorzio assicura l'osservanza degli obblighi di conservazione e può individuare facilmente i documenti la cui custodia ha superato i termini previsti.

6.2 Tenuta e conservazione della componente analogica

La componente analogica dell'archivio consiste nei documenti su supporto cartaceo prodotti o acquisiti dal Consorzio. La gestione di questi documenti avviene secondo i principi archivistici tradizionali, distinguendo tre fasi di vita dell'archivio:

- Archivio corrente: insieme dei fascicoli e documenti relativi ad affari in corso di trattazione presso le unità organizzative competenti. Tali documenti sono conservati presso gli uffici produttori fino alla conclusione dell'affare o procedimento;
- Archivio di deposito: insieme dei fascicoli relativi ad affari conclusi (pratiche chiuse) che non sono più necessari all'attività corrente degli uffici, ma che devono essere conservati fino al raggiungimento dei termini temporali. L'archivio di deposito è gestito dal Consorzio che ne cura l'ordinamento e la custodia;
- Archivio storico: costituito dai documenti relativi ad affari conclusi e destinati alla conservazione permanente per il loro valore storico-culturale. Il Consorzio Culturale del Monfalconese versa regolarmente ogni anno tutta la documentazione che ha raggiunto il limite di conservazione all'Archivio Storico. Quest'ultimo garantisce la pubblica fruizione dei documenti storici ed è soggetto alla vigilanza del Ministero della Cultura, attraverso le azioni che svolge la Soprintendenza archivistica.

Per la tenuta dell'archivio analogico, Il Consorzio adotta misure organizzative e fisiche adeguate. I fascicoli conclusi vengono versati dalle UOR all'Archivio di deposito con cadenza annuale, accompagnati da elenchi di trasferimento che ne descrivono il contenuto. Il personale dell'Archivio di deposito provvede a collocare i fascicoli in appositi locali dedicati, mantenendo l'ordinamento originario secondo il titolario di classificazione e assicurando che ogni scatola o contenitore sia etichettato con le informazioni necessarie (classe, anno,

estremi degli atti). I locali adibiti ad archivio sono dotati di misure di sicurezza e di condizioni ambientali idonee (es. controllo di umidità, temperatura, protezione da luce diretta e agenti infestanti) per garantire la conservazione a lungo termine dei materiali cartacei, in linea con gli standard archivistici e le indicazioni delle Linee guida AgID e delle norme tecniche vigenti. Sono definite chiaramente le responsabilità per la custodia della componente analogica. Durante la fase di archivio corrente, ogni ufficio è responsabile della tenuta dei propri documenti fino a quando sono attivi. Una volta trasferiti in archivio di deposito, la responsabilità passa al Responsabile della Conservazione il quale assicura che i documenti siano protetti da alterazioni, accessi non autorizzati o dispersione. Eventuali consultazioni dei documenti depositati da parte degli uffici o di terzi devono avvenire sotto la supervisione del personale archivistico, senza alterare l'ordine dei documenti. L'archivio di deposito mantiene aggiornati gli strumenti di corredo (registri di trasferimento, inventari, elenchi di consistenza e guide) che permettono di individuare rapidamente la documentazione conservata. Si rimanda al manuale di Conservazione dell'Ente per conoscere nel dettaglio le procedure in questione.

6.3 Conservazione della componente digitale

Il Sistema Conservativo è normato dal CAD e dalle Linee Guida AgID; questo assicura la conservazione dei seguenti oggetti digitali:

- i documenti informatici e amministrativi;
- le aggregazioni documentali informatiche (fascicoli e serie documentali).

Il processo di conservazione può essere svolto all'interno o all'esterno della struttura organizzativa dell'Ente. Il Consorzio Culturale del Monfalconese ha deciso di affidare il Servizio ad Insiel S.p.A., una società esterna alla propria struttura. Il Conservatore qualificato, incaricato di svolgere il servizio, risulta conforme allo standard ISO/IEC 27001 in materia di "Gestione della sicurezza delle informazioni", allo standard OAIS (ISO 14721:2012) che delinea le funzioni, le responsabilità e l'organizzazione di un sistema che vorrebbe preservare le informazioni nel lungo periodo per garantirne l'accesso ad una comunità di riferimento e allo standard UNI SInCRO (UNI 11386:2020) in materia di "Interoperabilità e recupero degli oggetti digitali". In tal caso è stata nominata quale Responsabile del Servizio di Conservazione la dott.ssa Elisabetta Bombardieri. Il Sistema di Conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione degli oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità. Il sistema garantisce l'accesso all'oggetto di conservazione dell'Amministrazione in questione.

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

- pacchetti di versamento;
- pacchetti archiviazione;
- pacchetti di distribuzione.

Spetta al Responsabile della Gestione Documentale predisporre i Pacchetti di versamento da inviare in conservazione. Il sistema effettuerà tutte le verifiche formali e alimenterà il Pacchetto di archiviazione con quello di versamento. Il processo conservativo prevede, ai soli fini della interoperabilità tra sistemi, la produzione di pacchetti di distribuzione coincidenti con i pacchetti di archiviazione. Si rimanda al manuale di Conservazione dell'Ente per le descrizioni dei processi di conservazione e distribuzione degli oggetti digitali.

6.4 Procedure di selezione e scarto in ambiente digitale e analogico

Le procedure di selezione e scarto documentale rappresentano il momento in cui l'Ente decide quali documenti eliminare al termine del periodo di conservazione obbligatorio e quali mantenere permanentemente, procedendo di fatto con il versamento all'Archivio Storico. Tali procedure sono condotte in modo coordinato per l'ambiente analogico e quello digitale, nel rispetto della normativa archivistica (D.lgs. 42/2004, art. 21 e art. 30 e ss.) e delle Linee guida AgID (par. 4.11 e 4.12). L'obiettivo è assicurare che nessun documento di rilevanza storica venga distrutto e che l'eliminazione dei documenti non più necessari avvenga in modo sicuro e tracciato. Per la componente analogica, la selezione e lo scarto avvengono periodicamente. Il personale individua i fascicoli o le serie documentali custodite nell'archivio di deposito che hanno superato i termini di conservazione previsti. Viene quindi compilato un elenco di scarto dettagliato, che descrive i documenti proposti per l'eliminazione, indicando estremi, anni, titolario, e motiva la mancanza di interesse storico degli stessi in base al massimario. Questo elenco viene sottoposto all'autorizzazione della Soprintendenza Archivistica competente, organo del Ministero della Cultura deputato a vigilare sugli archivi pubblici. Solo dopo aver ottenuto la prescritta autorizzazione scritta la fase di scarto può essere eseguita. Una volta autorizzato, lo scarto dei documenti cartacei avviene tramite distruzione fisica controllata (ad esempio triturazione o conferimento al macero) in modo da tutelare la riservatezza di eventuali dati sensibili. Della distruzione viene redatto un verbale di avvenuto scarto, conservato agli atti, che riepiloga i documenti eliminati e gli estremi dell'autorizzazione ottenuta. Le unità archivistiche destinate invece alla conservazione permanente vengono trasferite all'Archivio Storico, dove saranno ordinate e descritte in inventari per la consultazione pubblica futura.

Per la componente digitale, il processo di selezione e scarto è impostato in modo analogo, tenendo conto delle peculiarità informatiche. I documenti (o meglio i pacchetti di archiviazione) sono associati a una data di fine conservazione. Il Responsabile della Conservazione, coadiuvato dal Responsabile dell'ente conservatore accreditato, effettua periodiche verifiche sulle aggregazioni documentali che hanno raggiunto la fine del periodo di conservazione. Per ciascun insieme di documenti scaduti, si procede a valutare se siano privi di interesse storico e dunque eliminabili, oppure se presentino elementi di valore tale da giustificarne la conservazione oltre i termini. Anche in ambiente digitale, prima di procedere allo scarto effettivo, è richiesta l'autorizzazione dell'autorità archivistica per gli archivi pubblici di interesse storico: le Linee guida AgID ribadiscono che, nel caso di archivi soggetti a tutela, lo scarto dei pacchetti di archiviazione avviene previa autorizzazione del MiBAC (Ministero della Cultura), in conformità alla normativa vigente. Ottenuta l'eventuale autorizzazione, il Responsabile della Conservazione attiva la procedura di scarto informatico nel Sistema: il conservatore accreditato provvede quindi a eliminare dai propri sistemi i pacchetti di archiviazione indicati. Tale operazione è svolta con modalità sicure, assicurando che i documenti eliminati non siano più recuperabili. Il sistema di conservazione genera un log di eliminazione che viene conservato dall'Ente, contenente l'elenco dei pacchetti/documenti eliminati, la data e l'ora dello scarto e il riferimento all'autorizzazione ricevuta. In tal modo l'Ente mantiene evidenza documentale delle eliminazioni effettuate, a futura memoria e a garanzia di trasparenza. Nel caso in cui alcuni documenti informatici, giunti a fine periodo di conservazione, vengano ritenuti meritevoli di conservazione permanente, il Responsabile della conservazione dispone la loro esclusione dallo scarto. Tali documenti rimarranno nel sistema di conservazione oltre i termini iniziali. È importante notare che la conservazione illimitata di documenti digitali comporta l'onere continuo di migrazione tecnologica e monitoraggio dell'integrità: l'Ente, insieme al conservatore, pianificherà quindi eventuali

riversamenti periodici e verifiche per assicurare la leggibilità futura di questi documenti storici, così come avviene per i documenti analogici nella fase storica.

Le procedure di selezione e scarto dell'Ente prevedono sempre:

- l'identificazione dei documenti scaduti;
- la verifica del loro valore storico;
- l'ottenimento delle necessarie autorizzazioni normative per lo scarto;
- l'eliminazione sicura dei supporti o dei file;
- la redazione e conservazione di adeguata documentazione attestante le operazioni svolte.

Queste attività sono sotto la responsabilità del Responsabile della Gestione Documentale e del Responsabile della Conservazione, che collaborano per garantire il pieno rispetto delle linee guida nazionali e delle regole di tutela del patrimonio archivistico pubblico.

6.5 Ricerca, accesso e fruizione delle unità conservate

La ricerca e accesso ai documenti conservati è garantita mediante strumenti e procedure che assicurano sia l'efficienza interna sia il rispetto delle norme sulla trasparenza amministrativa e sulla tutela dei dati personali. L'Ente mette a disposizione del personale autorizzato strumenti di ricerca sui propri archivi, sia analogici che digitali, per facilitare il reperimento di pratiche concluse, atti e fascicoli conservati. Per la componente analogica, gli strumenti di corredo archivistici (inventari, elenchi di versamento e guide) consentono di individuare con precisione le unità archivistiche conservate. In particolare, l'inventario dell'archivio di deposito descrive i fascicoli e le serie documentali, permettendo di effettuare ricerche per intestazione, anno, materia. o al modulo di consultazione integrato nel sistema documentale dell'Ente.

È possibile effettuare ricerche per metadati (protocollo, data, mittente/destinatario, oggetto, classificazione, etc.) e individuare i documenti o fascicoli conservati di interesse. Quando un documento informatico conservato deve essere esibito per esigenze interne o per richieste esterne, l'utente abilitato richiede al sistema di conservazione la generazione di un Pacchetto di Distribuzione, ossia una copia del documento completa dei metadati e delle evidenze di conservazione (ad esempio impronte hash, riferimenti alle marche temporali e firme digitali.

Dal punto di vista della fruizione pubblica dell'archivio, l'Ente assicura il rispetto delle norme in materia di consultabilità degli Archivi Storici. Ai sensi del Codice dei beni culturali (D.lgs. 42/2004, Parte II, Capo III), i documenti conservati negli archivi storici degli enti pubblici sono liberamente consultabili da chiunque, fatte salve le limitazioni necessarie a tutela di interessi riservati. In particolare, per proteggere la riservatezza di dati personali sensibili eventualmente contenuti nei documenti, la legge prevede alcune restrizioni temporali alla consultazione: ad esempio, gli atti contenenti informazioni riservate su persone (dati sensibili, orientamento politico o religioso, appartenenza a partiti o sindacati, etc.) diventano liberamente consultabili dopo 40 anni dalla loro formazione, mentre quelli contenenti dati ancora più delicati (dati su salute, vita sessuale, casellari giudiziari, etc.) sono consultabili dopo 70 anni. Trascorsi tali termini, i documenti sono considerati di libero accesso storico. Prima dello scadere di questi limiti, eventuali richieste di consultazione per fini storici devono essere valutate caso per caso e possono richiedere un'autorizzazione speciale da parte del Ministero competente (ad esempio, per atti riservati relativi alla sicurezza dello Stato, tramite il Ministero dell'Interno).

L’Ente, attraverso il Responsabile dell’Archivio storico, disciplina le modalità di accesso pubblico: di norma la consultazione avviene su appuntamento nei locali dell’archivio, sotto la vigilanza del personale archivistico, e previa registrazione dell’utente e sottoscrizione di un registro di consultazione in cui si impegna al rispetto delle regole (uso dei documenti, divieto di riproduzione non autorizzata, ecc.). Laddove possibile, l’Ente favorisce anche la fruizione digitale dei documenti storici: ad esempio pubblicando online gli inventari e digitalizzando i documenti di maggior interesse, in modo da permetterne la consultazione da remoto nel rispetto delle liberatorie e delle norme sul diritto d’autore e privacy.

7. TRASPARENZA AMMINISTRATIVA.

Per Trasparenza Amministrativa si intende la comprensibilità e la conoscibilità dall'esterno dell'attività amministrativa, finalizzate a realizzare imparzialità e buon andamento dell'azione amministrativa per rendere maggiormente chiare le scelte rivolte alla cura dell'interesse generale. È compito di questa Amministrazione garantire il rispetto e l'applicabilità dei principi cardine della Trasparenza Amministrativa, incoraggiando la corretta formazione e gestione di tutta la documentazione che necessita di pubblicazione e che rimane accessibile attraverso gli strumenti di accesso a disposizione dal legislatore.

In un'ottica di fruibilità e accessibilità dei documenti, l'Amministrazione si preoccupa di utilizzare uno stile di redazione degli atti amministrativi il più conforme possibile con quanto disposto dal Dipartimento per la Funzione Pubblica, per garantire il massimo della comprensione delle informazioni e dei dati contenuti in ogni documento amministrativo a disposizione del fruitore.

7.1 Amministrazione Trasparente

Il d.lgs. 33 del 2013 e le successive semplificazioni del d.lgs. 97 del 2017 hanno introdotto l'obbligo per le Amministrazioni Pubbliche di alimentare una sezione specifica del proprio sito web denominata Amministrazione Trasparente, con l'obiettivo esplicito di aumentare la trasparenza delle Amministrazioni. Il Consorzio Culturale del Monfalconese è tenuto a popolare la sezione in questione con tutta la documentazione, le informazioni e i dati necessari a garantire il massimo livello di conoscibilità in materia di:

- Struttura organizzativa e composizione del personale;
- Atti generali di programmazione;
- Dati finanziari;
- Procedimenti amministrativi.

Ogni singolo Ufficio competente, coadiuvato dal proprio Responsabile, gestisce in completa autonomia le pubblicazioni attraverso la gestione degli accessi al sistema di gestione dell'area Amministrazione Trasparente. Ad avvenuta pubblicazione sarà compito del Responsabile attestare il corretto adempimento.

7.2 Albo Pretorio

L'albo pretorio è la sezione del sito web istituzionale del Consorzio Culturale del Monfalconese dove vengono pubblicati gli atti e i provvedimenti che sono soggetti a obblighi di pubblicazione con effetto di pubblicità legale. In altre parole è il luogo virtuale in cui l'Ente assolve all'obbligo di affissione pubblica degli atti. L'Albo Pretorio deve essere strettamente integrato con il Sistema Informatico Documentale. L'integrazione garantisce coerenza tra la gestione interna dei documenti e la loro pubblicazione esterna. Attraverso funzionalità dedicate, il documento viene inviato al modulo che gestisce la fase di trasparenza e pubblicità, insieme ai metadati in questione:

- Tipologia atto;
- Ufficio competente;
- Oggetto;

- Periodo di pubblicazione;
- Numero atto;
- Link alla copia conforme del documento.

Ad avvenuta pubblicazione sarà compito del Responsabile attestare il corretto adempimento.

7.3 Modalità della pubblicazione

Le pubblicazioni sono gestite autonomamente dai vari Responsabili delle UOR. Una volta che il documento è stato registrato e classificato all'interno del Sistema Informatico di Gestione Documentale, l'Ufficio responsabile del suo trattamento avrà il compito di pubblicare l'atto. Sarà compito del Responsabile assicurare che la documentazione sia tempestivamente pubblicata e aggiornata all'interno della corretta sottosezione. In caso di errori nell'espletamento degli obblighi sarà possibile per le varie UOR modificare le varie destinazioni di pubblicazione. Il Responsabile della Gestione Documentale, in stretta collaborazione con i vari responsabili degli uffici, avrà il compito di supervisionare la qualità e il rispetto degli standard informatici così come stabilito dalle linee guida AgID.

7.4 Completezza, integrità e qualità degli atti pubblicati

L'art. 6 del d.lgs. 33/20213 ribadisce l'importanza di osservare criteri di qualità per quanto riguarda la documentazione amministrativa sottoposta ad obbligo di pubblicazione. Tra le caratteristiche ricordiamo: l'integrità del documento, il suo costante aggiornamento, la sua completezza nelle informazioni, la sua semplicità di consultazione, la sua comprensibilità, l'omogeneità nei contenuti e la facile accessibilità. A ribadire l'importanza della qualità degli atti pubblicati ci ha pensato ANAC con la delibera 495 del 25 settembre 2024 che ha sottolineato l'importanza di effettuare delle operazioni preliminari volte a garantire che la documentazione rispetti degli standard qualitativi. Per garantire la massima aderenza a quanto predisposto dall'art. 6 del d.lgs. 33/2013 e dalla delibera 495 del 25 settembre 2024 dell'ANAC, Il Consorzio Culturale del Monfalconese nel momento di formazione della sua documentazione e rispettando le indicazioni contenute nell'allegato 2 delle Linee Guida AgID, opta per formati generici come PDF/A per gli atti, il CSV per quanto riguarda informazioni o dati in formato tabellare e il RTF per quanto riguarda documentazione di testo.

7.5 Atti soggetti a pubblicazione e durata

Per garantire la pubblicità legale e la trasparenza amministrativa, la normativa vigente prevede disposizioni relative alla pubblicazione degli atti sull'Albo Pretorio online (pubblicazione avente effetto legale) e disposizioni relative alla pubblicazione in Amministrazione Trasparente del sito istituzionale. È compito dell'Amministrazione garantire la costante pubblicazione di tutti i documenti, i dati e le informazioni negli appositi spazi, così come stabilito dalla normativa in materia di trasparenza amministrativa.

8. DISPOSIZIONI FINALI

8.1 Redazione del Manuale

Il Responsabile della gestione documentale (RGD) redige o aggiorna il Manuale secondo quanto previsto dalle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici, nel rispetto del DPCM 9 dicembre 2021 e della normativa archivistica.

8.2 Esame tecnico-organizzativo interno

Il Manuale viene esaminato in collaborazione con:

- il Responsabile della transizione digitale (RTD),
- il Responsabile della conservazione,
- e le strutture coinvolte nella gestione dei documenti (protocollo, archivio, sistemi informativi).

8.3 Nulla osta della Soprintendenza archivistica

Prima dell'adozione, Il Consorzio trasmette il Manuale alla Soprintendenza archivistica e bibliografica competente per territorio per ottenere il nulla osta in base al D.Lgs. 42/2004 (Codice dei Beni culturali).

8.4 Adozione formale del Manuale

Ottenuto il nulla osta, il Manuale è adottato con atto formale:

Decreto del Presidente/Deliberazione del Consiglio di Amministrazione, n. ___ e data ___/___/_____.

8.5 Pubblicazione e decorrenza

Il Manuale, unitamente agli atti di nomina e di approvazione, deve essere pubblicato sul sito istituzionale del Consorzio, nella sezione **"Amministrazione trasparente - Disposizioni generali - Atti generali - Documenti di programmazione strategico-gestionale"**, ed entra in vigore dalla data stabilita nel provvedimento di adozione.

8.6 Aggiornamenti successivi

Il Manuale deve essere aggiornato ogni volta che intervengono:

- modifiche normative rilevanti,
- cambiamenti organizzativi interni,
- variazioni nei sistemi informativi o nella gestione documentale.

Gli aggiornamenti seguono lo stesso iter: revisione a cura del RGD, nulla osta della Soprintendenza, adozione con atto formale.

Allegato 1 – Glossario

Lo scopo del presente allegato è il seguente:

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

a) Glossario dei termini

TERMINE	DEFINIZIONE
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche
Area Organizzativa Omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
ATTESTAZIONE DI CONFORMITÀ DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITÀ	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel

	contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
CLASSIFICAZIONE	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
CLOUD DELLA PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
CODEC	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un *wrapper* (codifica), così come di estrarli da esso (decodifica).
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato
Digest	Vedi Impronta crittografica

Documento amministrativo informatico	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
eSeal	Vedi sigillo elettronico.
Esibizione	Operazione che consente di visualizzare un documento conservato
eSignature	Vedi firma elettronica
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
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.

File container	Vedi Formato contenitore.
File wrapper	Vedi Formato contenitore.
File-manifesto	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Vedi articolo 3 del Regolamento eIDAS
Firma elettronica avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS.
Firma elettronica qualificata	Vedi articolo 3 del Regolamento eIDAS
Flusso (binario)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
Formato contenitore	Formato di file progettato per consentire l'inclusione ("imbustamento" o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; Consorziomente è identificato attraverso l'estensione del file.
Formato "deprecato"	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.

Funzione di 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.
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.
Naming convention	Vedi Convenzioni di denominazione
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di file (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	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.
Path	Percorso (vedi).
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.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano della sicurezza del sistema di gestione Informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata
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.
qSeal	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
qSignature	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
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 perle transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.

Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile del servizio di conservazione	Soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della funzione archivistica di conservazione	Soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.
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 storicoculturale.
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
Sidecar (file)	File-manifesto (vedi).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di 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.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, alfine 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.

b) Glossario degli acronimi

ACRONIMO	DEFINIZIONE
AGID	Agenzia per l'Italia digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
eIDAS	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
FEA	Vedi firma elettronica avanzata
FEQ	Vedi firma elettronica qualifica.
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
PdA (AiP)	Pacchetto di Archiviazione.
PdD (DiP)	Pacchetto di Distribuzione.
PdV (SiP)	Pacchetto di Versamento.
TUDA	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.

UOR	Unità Organizzativa Responsabile

Allegato 2 – Struttura Uffici e Servizi

- **AOO**

CODICE UNIVOCO AOO	DENOMINAZIONE AOO	DOMICILIO DIGITALE	INDIRIZZO	RESPONSABILE: NOME E CONTATTI
AB4D0F6	CONSORZIO CULTURALE DEL MONFALCONESE	consorzio-culturale-monfalconese@certgov.fvg.it	Piazza dell'Unità 24 - Ronchi dei Legionari (GO)	Roberto Del Grande, info@ccm.it; 0481474298

- **Unità Organizzative**

CODICE UNIVOCO	DENOMINAZIONE UO	INDIRIZZO	RESPONSABILE: NOME E CONTATTI
UFTZL3	Uff_eFatturaPA	Piazza dell'Unità 24 - Ronchi dei Legionari (GO)	Davide Iannis, consorzio-culturale-monfalconese@certgov.fvg.it
OYULCQ	Ufficio per la transizione al Digitale	Piazza dell'Unità 24 - Ronchi dei Legionari (GO)	Monica Rossi, consorzio-culturale-monfalconese@certgov.fvg.it

Figure chiave della digitalizzazione:

Responsabile della Transizione Digitale	***Monica Rossi***
Responsabile della Conservazione	***Roberto del Grande***
Responsabile della gestione documentale	***Tanja Tuta***
Responsabile del servizio di conservazione	***Elisabetta Bombardieri***
Responsabile della Protezione dei Dati Personali	***Fabio Romano Balducci***
Responsabile della prevenzione della corruzione e trasparenza (RPCT)	***Monica Rossi***

Allegato 3 – Registrazioni particolari

Elenco degli atti soggetti a Registrazione Particolare:

TIPOLOGIA ATTO	FORMATO DIGITALE E/O CARTACEO
Contratti	***Digitale***
Convenzioni	***Digitale***
Determinazioni	***Digitale***
Delibere	***Digitale***
Documenti di Spesa	***Digitale***
Fatture	***Digitale***

L'Ente avvierà un processo graduale di dematerializzazione dei documenti per facilitare la transizione verso il formato digitale.

Allegato 4 - Piano di classificazione del Consorzio Culturale del Monfalconese

Il Consorzio Culturale del Monfalconese adotta come proprio Piano di classificazione la versione aggiornata del Titolario contenuto nella circolare ANCI del 2005.

Il Piano di classificazione è articolato gerarchicamente in: **titoli** definiti a partire dall'analisi delle funzioni istituzionali dell'Ente.

L'aggiornamento del Piano di classificazione è di competenza del Responsabile della gestione documentale, e avviene nel rispetto della normativa vigente e secondo le modalità indicate nel manuale di gestione.

TITOLO I	*AMMINISTRAZIONE*
TITOLO II	*FINANZE*
TITOLO III	*EDITORIA*
TITOLO IV	*BIBLIOTECA*
TITOLO V	*FOTOTECA E ARCHIVIO DELLA MEMORIA*
TITOLO VI	*SISTEMA BIBLIOTECARIO E SERVIZIO CIVILE*
TITOLO VII	*LOCALI*
TITOLO VIII	*ORGANI ISTITUZIONALI*
TITOLO IX	*ATTIVITA' CULTURALI DIVERSE*
TITOLO X	*SERVIZI ESTERNI*
TITOLO XI	*ALTRO*

Allegato 5 – Manuale della Conservazione

1. RIFERIMENTI NORMATIVI

Questo Manuale della conservazione è redatto tenendo conto della normativa vigente in materia di formazione, gestione, conservazione, scarto e accessibilità del documento informatico amministrativo e dei relativi fascicoli digitali:

- **Decreto legislativo 7 marzo 2005, n. 82** – *Codice dell'Amministrazione Digitale (CAD) (norme generali su documenti informatici, firme digitali, conservazione, sistemi informativi pubblici)*
- **Decreto legislativo 22 gennaio 2004, n. 42** – *Codice dei beni culturali e del paesaggio (rilevante per la tutela degli archivi storici pubblici e per i procedimenti di scarto)*
- **Regolamento (UE) n. 910/2014 del 23 luglio 2014** – *Regolamento eIDAS (sull'identificazione elettronica e i servizi fiduciari, comprese le firme digitali e i sigilli)*
- **Regolamento (UE) 2016/679 (GDPR) e D.lgs. 30 giugno 2003, n. 196**, come modificato dal *D.lgs. 101/2018 – (normativa europea e nazionale in materia di protezione dei dati personali, rilevante per accesso, consultazione e sicurezza dei documenti digitali)*
- **D.P.R. 28 dicembre 2000, n. 445** – *Testo unico sulla documentazione amministrativa (regola la formazione, validità e gestione dei documenti amministrativi, anche in formato elettronico)*
- **Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014** – *(disciplinante le modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro conservazione)*
- **Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici** – *(adottate ai sensi dell'art. 71 del CAD; costituiscono l'attuale riferimento tecnico e normativo primario)*
- **Determina AgID n. 455/2021 del 25 giugno 2021** – "*Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici" (definisce i requisiti per la qualificazione dei Conservatori accreditati)*

1.1 Standard tecnici e best pratiche (nazionali e UE)

Per garantire l'interoperabilità, la conservazione a lungo termine, la tracciabilità e l'accessibilità dei documenti informatici, il sistema di conservazione si conforma ai seguenti standard tecnici:

- **UNI 11386:2020** *(Standard SInCRO – Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali*)
- **Standard OAIS – ISO 14721:2012** (*Open Archival Information System*)
- **UNI ISO 15489-1:2016** (*Records Management*) -
- **ISO/IEC 27001:2013** – *Sistemi di gestione della sicurezza delle informazioni*

- **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)*
- **SIARD** - *Software Independent Archiving of Relational Databases 2.0*
- **ISO/CD TR 26102** - *Requirements for long-term preservation of electronic records*
- **METS** - *Metadata Encoding and Transmission Standard*
- **PREMIS** – *PREservation Metadata: Implementation Strategies*
- **EAD (3) /ISAD (G**)
- **EAC (CPF)/ISAAR (CPF)/NIERA (CPF)**
- **SCONS2/EAG/ISDIAH**

Nell'ambito delle best practice, per l'Amministrazione in questione assume un rilievo importo l'utilizzo di formati di file idonei alla conservazione a lungo termine. Tra questi troviamo il PDF/A, XML, formati ODF, TXT e TIFF per le immagini. Inoltre per i documenti firmati digitalmente si fa riferimento agli standard europei ETSI sulle firme elettroniche o digitali: ad esempio PAdES, CAdES e XAdEs.

2. SOGGETTI COINVOLTI

Le Linee Guida AgID, al paragrafo 4.4, individuano una serie di figure operative utili a garantire il corretto svolgimento del processo di conservazione. I ruoli individuati sono:

- **titolare dell'oggetto della conservazione;**
- **produttore dei PdV;**
- **utente abilitato;**
- **responsabile della conservazione;**
- **conservatore**.

2.1 Titolare dell'oggetto della conservazione

Il titolare dell'oggetto della conservazione è l'Amministrazione che detiene la titolarità giuridica dei documenti informatici e ne assicura la conservazione a norma di legge. È responsabile della corretta classificazione, conservazione e accessibilità dei documenti prodotti, secondo quanto previsto dal Piano di Classificazione.

2.2 Soggetto produttore

Il soggetto produttore è la figura incaricata di predisporre e trasferire al sistema di conservazione i documenti da conservare, insieme ai relativi metadati e secondo le modalità stabilite dall'Accordo di servizio.

2.3 Utente abilitato

L'utente abilitato è la figura che usufruisce dei servizi del sistema di conservazione, ovvero chi può richiedere ed ottenere l'accesso ai documenti conservati nei limiti consentiti dalla legge e nel rispetto della normativa in materia di privacy. L'utente abilitato può assumere diverse entità a seconda dei casi:

Personale interno autorizzato: in un Ente saranno utenti abilitati i dipendenti o funzionari che, per motivi di servizio, hanno titolo a consultare i documenti conservati

Soggetti esterni aventi diritto: possono essere utenti abilitati anche soggetti esterni all'ente, nei casi previsti dalla normativa. Ad esempio, cittadini o altre amministrazioni che esercitano il diritto di accesso ai documenti.

Tutti gli accessi sono tracciati e regolati secondo le politiche di sicurezza previste dal sistema di conservazione e dalla normativa in materia di protezione dei dati personali.

2.4 Responsabile della conservazione

Il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD.

Nella Pubblica Amministrazione, il responsabile della conservazione:

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

Per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di 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.

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.

In particolare, il responsabile della conservazione:

- 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 documentale adottato;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

- genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- 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;
- 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;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;
- 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;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- 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;
- 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.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore accreditato, le attività suddette o alcune di esse), potranno essere affidate al responsabile del servizio di conservazione.

Si precisa che il nominativo ed i riferimenti del responsabile della conservazione devono essere indicati nelle specifiche del contratto o della convenzione di servizio con il Conservatore accreditato nel quale sono anche riportate le attività affidate al responsabile del servizio di conservazione.

2.5 Conservatore

Il Conservatore è il soggetto, pubblico o privato, che esegue il processo di conservazione per conto del Titolare dell'oggetto. Deve essere in possesso dei requisiti organizzativi, tecnologici e professionali previsti dalle Linee guida AgID e deve adottare un sistema di conservazione conforme allo standard UNI 11386:2020 – SInCRO.

L'Amministrazione ha affidato il servizio di conservazione a Insiel S.p.A, in qualità di Conservatore esterno, mediante apposito accordo di servizio, che disciplina in dettaglio le responsabilità, le modalità operative, la sicurezza, il tracciamento delle attività e il livello di servizio.

3. IL PROCESSO CONSERVATIVO E GLI OGGETTI DELLA CONSERVAZIONE

La conservazione è un momento chiave nella vita di un documento. Affrontare la conservazione porta a confrontarsi con produzione, validazione e gestione del documento informatico, garantendo la sua totale fruibilità anche in presenza di cambiamenti tecnologici. Infatti, conservare significa porre l'accento su quale formato usare e su come valorizzare il contenuto e i relativi metadati. Il sistema di conservazione, e i relativi Pacchetti di Archiviazione, sono totalmente indipendenti dagli applicativi che li hanno prodotti. Indipendenza è la parola chiave quando parliamo di conservazione.

Le linee guida AgID e l'art. 41 del CAD stabiliscono che un sistema di conservazione deve possedere delle caratteristiche tecnologiche in grado di assicurare l'autenticità, integrità, affidabilità, leggibilità e reperibilità degli oggetti digitali. Il sistema, inoltre, garantisce l'accesso all'oggetto conservato per il periodo di conservazione previsto dal medesimo piano, indipendentemente dall'evoluzione del contesto tecnologico.

L'accordo di servizio stipulato da questa Amministrazione e il conservatore esterno, individuato nella società Insiel S.p.A, ha permesso di definire un processo ben definito, in grado di assicurare le caratteristiche di:

- **autenticità**: caratteristica di un documento che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico;
- **integrità**: insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato;
- **affidabilità**: caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico;
- **leggibilità**: insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti sono fruibili durante l'intero ciclo di gestione dei documenti;
- **reperibilità**: caratteristica di un documento informatico di poter essere trovato.

Ai sensi dell'art. 41 del CAD, il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione:

- i fascicoli informatici chiusi e le serie informatiche chiuse;
- i fascicoli informatici chiusi e le serie che non sono ancora chiuse, trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'ente.

Il sistema di conservazione è disciplinato dal Codice dell'Amministrazione Digitale (CAD) e dalle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici. Il Sistema assicura la conservazione dei seguenti oggetti digitali:

- i documenti informatici e i documenti amministrativi;
- le aggregazioni documentali (fascicoli e serie).

Il Consorzio Culturale del Monfalconese realizza il processo conservativo ai sensi dell'art. 34, comma 1-bis del CAD. Questa Amministrazione ha deciso di esternalizzare il processo di conservazione, mantenendo tuttavia stretti rapporti con l'ente per garantire l'efficienza della conservazione. Il sistema assicura, dalla presa in carico fino all'eventuale scarto, la conservazione degli oggetti digitali tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il sistema di conservazione garantisce l'accesso all'oggetto di conservazione. Si rimanda al Manuale di Gestione Documentale del Consorzio Culturale del Monfalconese e al relativo allegato per ulteriori dettagli.

3.1 Creazione e versamento dei pacchetti di versamento (PdV)

I pacchetti di versamento (PdV) rappresentano l'insieme strutturato delle informazioni e dei documenti informatici destinati alla conservazione, secondo quanto previsto dallo standard UNI 11386:2020 – SInCRO.

Ciascun PdV è composto da:

- un contenitore, dipendente dal canale trasmissivo, che racchiude i contenuti del pacchetto informativo;
- un file indice XML, con i metadati identificativi dell'ente produttore, dei documenti informatici e delle aggregazioni informatiche;
- l'insieme dei file elencati nell'indice XML.

In conformità a quanto stabilito dall'Allegato 5 delle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici, il PdV deve garantire l'acquisizione, la gestione e la conservazione dei metadati obbligatori relativi a:

- documento informatico;
- documento amministrativo informatico;
- aggregazioni documentali.

L'acquisizione del PdV nel sistema di conservazione può avvenire secondo una delle seguenti modalità:

- **Versamento massivo**: i pacchetti vengono posizionati in un'area di accesso remoto dedicata all'ente produttore, configurata nel rispetto delle specifiche tecniche del sistema di conservazione;
- **Versamento tramite interfaccia web**: l'utente, previa autenticazione e autorizzazione, inserisce i dati necessari tramite un'apposita interfaccia, completando il versamento attraverso la compilazione di un form;
- **Versamento tramite interoperabilità tra sistemi**: l'applicazione versante, autenticata e autorizzata, trasmette i PdV al sistema di conservazione mediante Web Services, secondo le modalità previste dalle regole tecniche vigenti.

Il processo di acquisizione si avvia con l'autenticazione dell'utente incaricato del versamento. Il sistema di conservazione procede quindi alla verifica tecnica del PdV, con analisi dei metadati e dei formati degli oggetti digitali. In caso di esito positivo, il sistema genera un rapporto di versamento, che:

- è univocamente identificato dal sistema;

- contiene un riferimento temporale opponibile a terzi;
- è sottoscritto con firma digitale dal Responsabile della conservazione.

Il rapporto di versamento viene conservato all'interno del Sistema di Conservazione, garantendone l'ininterrotta custodia e la non modificabilità.

3.2 Pacchetto di archiviazione (PdA)

Una volta acquisito il pacchetto di versamento (PdV) da parte del sistema di conservazione, i relativi contenuti alimentano il pacchetto di archiviazione (di seguito, PdA).

Il PdA è costituito da un aggregato logico che comprende:

- il documento principale, oggetto del processo di conservazione;
- eventuali allegati e documenti correlati, funzionalmente connessi al documento principale.

La gestione, la preparazione e la sottoscrizione con firma digitale del PdA avvengono nel rispetto delle disposizioni contenute nello standard UNI 11386:2020 – SInCRO, nonché secondo le modalità operative dettagliate nel Manuale della conservazione del conservatore esterno, al quale si rinvia per ogni ulteriore approfondimento.

3.3 Pacchetto di distribuzione (PdD)

Ai fini dell'esibizione dei documenti su richiesta dell'utente esterno, il pacchetto di distribuzione (di seguito, PdD) viene costituito a partire da uno o più pacchetti di archiviazione (PdA) e sottoscritto con firma digitale dal Responsabile del servizio di conservazione, in conformità alle modalità operative previste nel Manuale della conservazione del conservatore esterno, cui si rinvia per ulteriori dettagli.

Il processo di conservazione prevede, ai soli fini dell'interoperabilità tra sistemi, la produzione di PdD coincidenti con i corrispondenti PdA, generati secondo le specifiche di struttura dati previste dallo standard UNI 11386:2020 – SInCRO.

3.4 Scarto dei pacchetti di archiviazione

L'eventuale scarto di un pacchetto di archiviazione (PdA) dal sistema di conservazione avviene alla scadenza dei termini di conservazione. Il Responsabile della conservazione procede alla generazione dell'elenco dei PdA contenenti documenti destinati allo scarto e lo comunica all'Amministrazione, che provvede alla verifica del rispetto dei termini temporali indicati nel Piano stesso.

A seguito dell'ottenimento delle necessarie autorizzazioni allo scarto, l'Amministrazione trasmette al soggetto conservatore l'elenco dei PdA da eliminare.

L'intera operazione di scarto è oggetto di tracciamento all'interno del sistema di conservazione, mediante la produzione e conservazione delle informazioni essenziali, tra cui:

- gli estremi delle richieste di nulla osta;
- il relativo provvedimento autorizzativo

Il processo di scarto si considera concluso esclusivamente al termine dell'aggiornamento delle copie di sicurezza del sistema, che deve riflettere la definitiva eliminazione degli oggetti digitali e dei relativi metadati, in conformità alle disposizioni normative e regolamentari vigenti.

4. PRODUZIONE DI DUPLICATI INFORMATICI O DI COPIE INFORMATICHE

La produzione di duplicati informatici e di copie informatiche di documenti deve avvenire nel rispetto della normativa vigente (Codice dell'Amministrazione Digitale – CAD, D.lgs. 82/2005 e s.m.i.) e delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate da AgID. Un duplicato o una copia informatica realizzati secondo queste disposizioni hanno la stessa validità giuridica del documento originario.

4.1 La certificazione di processo

La validità delle copie e/o di estratti di documenti informatici è consentita mediante uno dei metodi indicati dall'Allegato 3 delle "**Linee Guida sulla formazione, gestione e conservazione dei documenti informatici**":

- **raffronto dei documenti;**
- **certificazione di processo.**

L'attestazione di conformità, opportunamente firmata dal Responsabile incaricato della conservazione, può essere inserita nel documento informatico contenente la copia o l'estratto. Alternativamente, l'attestazione potrà essere prodotta come documento informatico separato contenente un riferimento temporale opponibile a terzi e l'impronta digitale di ogni copia o estratto informatico. Anche in questa casistica, rimane l'obbligo di firma da parte del Responsabile della Conservazione.

Nel modello di certificazione di processo concorrono tre elementi:

- la descrizione e certificazione della procedura in cui verranno specificati i requisiti tecnici a cui il processo, le fasi e i controlli a cui il processo dovrà attenersi;
- la presenza di una procedura tecnologica in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia;
- la validazione della conformità della copia informatica rispetto ad un documento informatico, a cui seguirà l'attestazione di conformità della copia con successiva.

Ai sensi dell'art. 23-bis, comma 1, CAD, il duplicato informatico così formato ha il medesimo valore giuridico dell'originale da cui è tratto, purché la produzione avvenga alle disposizioni sopra richiamate. La società incaricata della gestione del processo di conservazione per questa Amministrazione si avvale di una infrastruttura tecnologica idonea a garantire l'estrazione di duplicati dotati delle medesime caratteristiche dell'originale, assicurandone integrità e immodificabilità. Per ulteriori dettagli, si rinvia al Manuale della Conservazione redatto dalla società Insiel S.p.A.

4.2 Riversamento

Il sistema di conservazione adottato consente la produzione di copie informatiche mediante attività di riversamento, finalizzata ad adeguare i formati alle esigenze conservative di leggibilità nel tempo, secondo quanto stabilito dall'Allegato 2 delle Linee Guida ("Formati di file e riversamento").

Per riversamento si intende la migrazione di un documento informatico da un formato a un altro, che può comportare anche il trasferimento tra diversi sistemi di storage. In tal caso, è necessario conservare anche la versione originale del file. Il documento risultante costituisce una copia informatica, la cui conformità all'originale deve essere attestata ai sensi dell'art. 23-bis del CAD e delle relative Linee Guida.

Nel caso di riversamento massivo, devono essere seguite le seguenti fasi:

- documentazione dell'esito della verifica dell'indice di interoperabilità;
- esecuzione del riversamento mediante un processo certificato, in grado di garantire integrità e riproducibilità del contenuto;
- produzione di una attestazione di riversamento specifica per ogni file riversato. Le attestazioni dei documenti riversati sono collezionate in un registro di riversamento.

Qualora sussistano obblighi normativi, e il documento in formato originario venga conservato congiuntamente alla versione riversata, tale associazione logica deve essere registrata nel suddetto registro.

Per ulteriori informazioni si rinvia al Manuale della Conservazione della società Insiel S.p.A, che dettaglia:

- i software applicativi e le procedure tecniche adottate per garantire la riproducibilità del riversamento;
- le modalità di rappresentazione dell'associazione logica tra documento originale e documento riversato ai fini del rispetto degli obblighi normativi;
- le analisi relative alle eventuali informazioni perse durante il riversamento;
- la gestione dei nuovi metadati generati e la modalità di registrazione delle informazioni perse all'interno del registro.

Allegato 6 – Formato dei documenti informatici e riversamento

Un qualsiasi contenuto digitale viene memorizzato come file su un supporto di memorizzazione digitale. Un file è un insieme di bit (0 e 1), considerati come un'entità unica dal punto di vista logico e fissati con una certa organizzazione fisica su una memoria. Il formato è quell'informazione che ci permette di rendere leggibile un testo. Il Consorzio in questione, per favorire la creazione dei documenti informatici, utilizza formati che garantiscono i requisiti di leggibilità, interoperabilità, integrità durante le fasi di accesso e conservazione, e immutabilità del contenuto e della struttura nel tempo.

Il Consorzio Culturale del Monfalconese, nella scelta dei formati da utilizzare, fa riferimento alle indicazioni contenute nell'Allegato 2 delle Linee Guida AgID in materia di "Formazione, Gestione e Conservazione dei Documenti Informatici". In particolare, questa Amministrazione utilizza quello che l'allegato 2 definisce come categoria generale di formati, rispetto ai quali tutte le Pubbliche Amministrazioni sono in grado di riprodurre i documenti. È tuttavia concessa una deroga a questa limitazione nel caso in cui Il Consorzio, per necessità funzionali, dovesse utilizzare un formato di tipo specifico. È il caso del documento informatico contenente informazioni fiscali relative ad una prestazione, cessazione di beni o servizi; Il Consorzio dovrà utilizzare il formato "**Fattura PA**", individuato dal legislatore come il dialetto XML per quell'utilizzo specifico.

Per facilitare la consultazione, i formati "generici" elencati nell'Allegato sono i seguenti:

- PDF
- DOCX, DOTX
- ODT
- RTF
- XML
- HTML, HTM
- JSON
- EML
- XLSX, XLTX
- PPTX, PPSX, POTX
- ODS
- ODP
- PNG
- JPG, JPEG
- TIFF, TIF
- GIF
- SVG, SGVZ
- OTF

- TTF
- WAV, BWF, RF64
- MP3
- MJPG, MJPA, MJPB
- MP4, M4A, M4V
- AVI
- TAR
- ZIP, ZIPX
- GZIP

Allegato 7 - Tipologie di documenti di originali informatici

I seguenti documenti possono essere gestiti come originali informatici e possono essere firmati digitalmente:

- **Deliberazioni:** atti ufficiali adottati dagli organi decisionali dell'Ente Locale che riportano decisioni e risoluzioni formali.
- **Determinazioni:** documenti amministrativi che stabiliscono disposizioni specifiche o misure operative all'interno dell'Ente.
- **Atti di Liquidazione:** documenti che certificano la verifica e la conclusione di transazioni finanziarie, relative a spese o pagamenti.
- **Decreti:** atti ufficiali emessi e firmati dal Presidente dell'Ente Locale, che comprendono decisioni, nomine o altre disposizioni di rilevanza.
- **Fatture Elettroniche**: documenti fiscali che devono essere emessi e conservati in formato elettronico, registrando transazioni commerciali.
- **Mandati e Reversali:** documenti contabili che autorizzano pagamenti e registrano le operazioni finanziarie effettuate dall'Ente.
- **Contratti:** documenti di accordo che hanno lo scopo di regolare creare, modificare o estinguere un rapporto giuridico.
- **Convenzioni:** documenti di accordo tra due o più soggetti con il quale gli stessi regolano questioni di interesse comune.

Tutti questi documenti possono essere trattati come originali informatici e possono essere firmati digitalmente per garantire la loro autenticità e integrità.

Allegato 8 - Manuale operativo del software di gestione del protocollo

Ogni dipendente, mediante accesso con credenziali personali, può consultare liberamente il manuale operativo del software di gestione del protocollo, disponibile tramite apposito link. La società fornitrice del software provvede inoltre all'organizzazione periodica di corsi di formazione finalizzati a garantire un corretto e aggiornato utilizzo dello stesso.

Allegato 9 - Piano di sicurezza informatica

Premessa

Il Piano di sicurezza dell'Ente è stato redatto nel rispetto delle Linee Guida AgID e del Regolamento UE 2016/679 (GDPR), con l'obiettivo di garantire una protezione adeguata dei dati trattati e la salvaguardia del patrimonio documentale digitale. Questo Piano definisce le misure necessarie per la sicurezza e la gestione dei documenti informatici, ponendo particolare attenzione alla tutela della privacy e al rispetto delle normative in materia di protezione dei dati.

Scopo del Piano

Il Piano di sicurezza informatica ha l'obiettivo di proteggere le informazioni personali e i sistemi informatici da attacchi, incidenti e perdite di dati. Questo Piano è essenziale per garantire la sicurezza dei servizi digitali offerti ai cittadini e proteggere l'integrità, la riservatezza e la disponibilità dei dati.

Obiettivi

Il Piano di sicurezza si prefigge di:

- proteggere i sistemi informatici da attacchi interni ed esterni;
- garantire la protezione dei dati personali dei cittadini;
- assicurare la continuità operativa dei servizi digitali;
- rispondere adeguatamente agli incidenti informatici.

In particolare, si impegna a:

- garantire che i documenti e le informazioni gestite dall'Ente siano sempre accessibili, integre e protette da ogni forma di divulgazione non autorizzata;
- tutelare i dati personali, adottando misure preventive per evitare rischi legati alla perdita, al danneggiamento accidentale, all'accesso illecito o al trattamento non conforme agli scopi per cui sono stati raccolti.

A tal fine, il Piano si basa sull'analisi dei rischi associati ai dati e ai documenti trattati, e stabilisce una serie di linee guida e azioni specifiche, tra cui:

- le politiche di sicurezza generali e specialistiche da adottare all'interno dell'Ente per garantire una protezione costante e adeguata;
- le modalità per l'accesso sicuro e la gestione del Sistema di Gestione Informatica dei Documenti, in modo da preservare l'integrità e la confidenzialità dei dati;
- le misure operative, organizzative, procedurali e tecniche da adottare per garantire il rispetto delle disposizioni del GDPR e le misure minime di sicurezza, come indicato nell'art. 32 del Regolamento UE 2016/679;
- la formazione continua del personale coinvolto nella gestione dei documenti e nella protezione dei dati;
- il monitoraggio periodico e l'analisi dell'efficacia delle misure di sicurezza implementate.

Revisione periodica e aggiornamenti

Il Piano di Sicurezza segue i criteri previsti dalle Linee Guida AgID per i sistemi di protocollo informatico e rappresenta uno strumento fondamentale per garantire che l'Ente operi nel pieno rispetto delle normative sulla protezione dei dati e della sicurezza dei documenti.

Questo Piano è soggetto a una revisione periodica almeno ogni due anni, ma può essere aggiornato anticipatamente qualora si verifichino le seguenti circostanze:

- evoluzioni normative: modifiche legislative, regolamentari o giuridiche, comprese quelle derivanti da disposizioni europee;
- innovazioni tecnologiche: l'introduzione di nuove soluzioni tecnologiche che possano incidere sulla gestione della sicurezza dei dati e dei documenti;
- cambiamenti organizzativi: modifiche strutturali o procedurali all'interno dell'Ente che possano influire sulle modalità di trattamento o accesso ai dati.

Il Piano verrà aggiornato prontamente nel caso si renda necessario introdurre misure di sicurezza più appropriate per rispondere a nuovi rischi o per conformarsi alle modifiche normative, garantendo in ogni momento la protezione dei dati e dei documenti trattati.

MISURE OPERATIVE DI SICUREZZA

Analisi dei rischi e minacce principali

L'Ente deve identificare e documentare i principali rischi associati ai documenti e ai dati trattati nel Sistema di Gestione Informatica dei Documenti (SGID). Tra i rischi da considerare, devono essere inclusi almeno:

- Accessi non autorizzati ai dati e ai documenti;
- Cancellazioni o manomissioni non autorizzate;
- Perdite accidentali di documenti o dati;
- Trattamenti non conformi alla normativa vigente, in particolare al GDPR.

L'Ente è tenuto a svolgere regolarmente una valutazione dei rischi aggiornata, al fine di individuare eventuali nuove minacce e vulnerabilità.

Per mitigare tali rischi, l'Ente deve adottare e mantenere politiche di prevenzione e protezione adeguate, che dovranno essere descritte e implementate secondo le indicazioni fornite nei paragrafi successivi del presente documento.

Accesso degli utenti interni

L'accesso al SGID è consentito esclusivamente tramite credenziali personali, con l'assegnazione di autorizzazioni basate sui profili utente. Le regole per la gestione delle credenziali sono le seguenti:

- le password devono essere composte da almeno 8 caratteri, includendo numeri e caratteri speciali;
- le password vanno cambiate al primo accesso e successivamente con frequenza mensile;
- le credenziali non devono essere condivise né facilmente riconducibili all'utente;
- le credenziali inattive per oltre 6 mesi vengono disattivate automaticamente;
- tutti gli accessi al sistema sono registrati tramite log delle attività per garantire la tracciabilità.

Trattamento dei dati particolari e giudiziari

L'accesso a dati particolari e giudiziari, ex artt. 9 e 10 GDPR, è consentito esclusivamente previa autorizzazione specifica e configurazione di profili ad hoc.

- Le postazioni utilizzate per il trattamento di tali dati non devono mai essere lasciate incustodite durante l'operatività;
- le autorizzazioni vengono verificate con cadenza almeno annuale per garantire la conformità e la necessità di accesso.

Sicurezza del protocollo informatico

L'accesso al registro di protocollo informatico è riservato al personale autorizzato.

Sicurezza logica del Sistema di Gestione Informatica dei Documenti (SGID)

Per garantire un livello adeguato di sicurezza logica del Sistema di Gestione Informatica dei Documenti (SGID), si raccomanda di:

- abilitare l’accesso ai documenti solo previa autenticazione basata su credenziali personali e autorizzazioni definite dai profili utente;
- implementare un sistema di tracciatura di tutte le operazioni (creazione, modifica, eliminazione) sui documenti, assicurandone la protezione da alterazioni non autorizzate;
- adottare protocolli di comunicazione sicuri (ad esempio HTTPS) per la trasmissione dei dati;
- garantire l’aggiornamento regolare del sistema operativo e del software applicativo, così da mantenere elevati standard di sicurezza.

Backup e ripristino

Si raccomanda, in linea con le best practice di settore, di implementare un sistema di backup e ripristino dei dati del SGID con le seguenti caratteristiche:

- effettuare backup con frequenza almeno giornaliera, preferibilmente tramite processi automatizzati e gestiti da personale qualificato;
- includere nei backup sia i dati contenuti nel SGID sia i sistemi operativi correlati;
- conservare le copie di backup sia in locale sia in remoto;
- cifrare i dati di backup remoto prima della trasmissione per garantire la riservatezza delle informazioni;
- prevedere la conservazione di almeno una copia offline dei backup in repository immodificabili (ad esempio supporti WORM o sistemi equivalenti) per prevenire modifiche o cancellazioni non autorizzate;
- eseguire test di ripristino almeno ogni sei mesi, secondo le best practice, per verificare l’affidabilità delle procedure di recupero;
- applicare un controllo rigoroso sugli accessi ai backup, adottando il principio di minimizzazione e assegnando profili di accesso esclusivamente al personale autorizzato;
- conservare i log relativi alle operazioni di backup per un periodo di almeno 180 giorni (o altro periodo conforme alle policy interne), così da consentire il monitoraggio delle eventuali anomalie;
- garantire tempi di ripristino dei dati conformi alle best practice di settore: ad esempio entro 24 ore per malfunzionamenti ordinari e entro 72 ore in caso di disastro, con la possibilità di adeguarli alle esigenze specifiche dell’Ente.

L’Ente potrà definire autonomamente, in base alle proprie esigenze operative e risorse, i tempi e le modalità effettive di backup e ripristino, purché siano garantiti livelli adeguati di sicurezza e disponibilità dei dati.

Sicurezza fisica e infrastrutturale

L’Ente adotta le misure minime di sicurezza ICT definite da AgID per garantire la protezione delle infrastrutture fisiche e logiche.

Formazione del personale

Si raccomanda che l'Ente organizzi attività formative dedicate per il personale, con l'obiettivo di garantire un adeguato aggiornamento in materia di sicurezza informatica, in linea con quanto previsto dal Piano Triennale per l'informatica nella Pubblica Amministrazione 2024-2026, elaborato da AGID.

Qualora non siano attualmente attivi corsi formativi specifici in sicurezza informatica, si raccomanda di pianificare iniziative dedicate per assicurare l'adeguato aggiornamento continuo del personale, in modo da mantenere elevati standard di competenza e conformità.

Monitoraggio delle misure di sicurezza

Il Responsabile della gestione documentale effettua verifiche periodiche sull'efficacia delle misure di sicurezza implementate, anche tramite controlli a campione.

DISPOSIZIONI PER IL PERSONALE

Premessa e finalità

La sicurezza delle informazioni e dei dati personali trattati all'interno del Consorzio rappresenta un valore imprescindibile e un obbligo normativo fondamentale. Il presente insieme di disposizioni operative è stato elaborato con l'obiettivo di definire chiaramente le responsabilità e i comportamenti che ogni dipendente deve adottare **prima** e **dopo** il verificarsi di un incidente informatico, per garantire la protezione dei dati, prevenire danni, e contribuire alla continuità operativa degli uffici.

Un incidente di sicurezza informatica è un evento che comporta la violazione della riservatezza, integrità o disponibilità di dati e sistemi. Può variare da un malware che rallenta i processi aziendali fino a una violazione dei dati che coinvolge informazioni sensibili.

La prevenzione è fondamentale per ridurre il rischio di incidenti informatici. Tuttavia, anche in presenza di misure preventive adeguate, possono verificarsi eventi di sicurezza imprevisti (ad esempio un data breach, un accesso non autorizzato ad atti riservati, etc). In questi casi, è essenziale sapere come comportarsi, collaborare con il DPO (Data Protection Officer/Responsabile della Protezione dei Dati) e rispettare le procedure previste.

Per questo motivo, si invita tutto il personale a rispettare le disposizioni operative ivi riportate, ad applicarle con rigore e a segnalare tempestivamente qualsiasi anomalia o evento che possa costituire una minaccia alla sicurezza.

Disposizioni operative

1) Prevenzione degli incidenti informatici e sicurezza dei dati (PRIMA DI UN INCIDENTE INFORMATICO)

a) PRINCIPI GENERALI

Ogni dipendente è tenuto a:

- Trattare esclusivamente i dati necessari all'attività lavorativa
- Applicare il principio di necessità, pertinenza e non eccedenza
- Mantenere la massima cautela nel trattamento dei dati personali
- Segnalare immediatamente situazioni anomale o richieste eccedenti il proprio incarico

b) SICUREZZA FISICA

Accessi e Locali:

- Custodire in sicurezza tutte le chiavi di accesso agli uffici
- Segnalare immediatamente furto o smarrimento di chiavi
- Garantire il presidio degli uffici o chiuderli a chiave in caso di assenza
- Mantenere scrivanie e tavoli di lavoro liberi da documenti contenenti dati personali visibili
- Custodire i documenti in luoghi non accessibili a soggetti non autorizzati

Gestione Documenti:

- Archiviare immediatamente supporti cartacei ed elettronici dopo l'utilizzo
- Rimuovere prontamente documenti da scanner, stampanti e fotocopiatrici
- Distruggere correttamente i documenti non più utilizzati con macchine distruggi-documenti

c) SICUREZZA INFORMATICA

Posta Elettronica - DIVIETI ASSOLUTI:

- NON aprire messaggi contenenti link sospetti, file .zip, eseguibili o macro
- NON rispondere a messaggi che propongono disattivazione invii email
- NON aprire comunicazioni di sanzioni, cartelle esattoriali, denunce
- NON aprire comunicazioni di consegna pacchi con file "rischiosi"
- NON inoltrare dati personali a indirizzi email personali
- NON inviare dati "particolari" via email

Posta Elettronica - PRECAUZIONI:

- Verificare i link prima di aprirli (passare il mouse sopra)
- Prestare attenzione ai messaggi anche di utenti conosciuti (possibili malware)
- Attenzione all'uso di CC multipli (condivisione indirizzi)
- Verificare l'autocompletamento dei destinatari
- Utilizzare piattaforme cloud solo se autorizzate dal Titolare

Postazioni di Lavoro:

- Spegnere la postazione in caso di assenza prolungata
- Bloccare sempre il computer con CTRL + ALT + CANC durante assenze brevi
- NON lasciare mai incustodita la postazione durante sessioni di lavoro attive
- Mantenere aggiornati i sistemi di sicurezza
- Conoscere quali dati sono sottoposti a backup

Dispositivi Portatili:

- Proteggere notebook con sistemi di cifratura se contengono dati personali
- Proteggere smartphone con sistemi di blocco se usati per email aziendali
- Prestare attenzione alle fotografie salvate in memoria
- Utilizzare dispositivi personali (BYOD) solo se espressamente autorizzati

d) CONTROLLO REMOTO

Prima di autorizzare accessi remoti verificare sempre:

- Identità dell'operatore remoto (conoscenza diretta o comunicazione preventiva)
- Autorizzazione all'intervento (ticket, autorizzazione scritta)
- Presidiare la postazione durante l'intervento salvo diversi accordi

e) GESTIONE CREDENZIALI

Password - OBBLIGHI:

- Utilizzare password lunghe e complesse
- NON utilizzare dati personali (date di nascita, nomi familiari)
- Cambiare le password secondo gli standard di sicurezza
- Utilizzare credenziali diverse per contesti diversi
- NON condividere mai le credenziali personali
- NON lasciare credenziali scritte vicino alla postazione

f) RAPPORTI CON TERZI

Prima di rilasciare qualsiasi informazione:

- Verificare sempre l'identità del richiedente
- Accertare la presenza di autorizzazioni al rilascio
- Comunicare solo dati preventivamente autorizzati dal Titolare
- NON fornire mai dati, credenziali o accessi senza identificazione e autorizzazione
- Confrontarsi sempre con il referente del Titolare per richieste dubbie

g) NAVIGAZIONE INTERNET

- Verificare l'affidabilità dei siti visitati
- Tenere aggiornati i sistemi di protezione
- Utilizzare le credenziali solo sui siti ufficiali dedicati
- Prestare attenzione a tentativi di phishing

h) SEGNALAZIONE INCIDENTI

In caso di incidente di sicurezza:

- Comunicare IMMEDIATAMENTE al referente del Titolare
- Non tentare soluzioni autonome
- Documentare l'accaduto
- Collaborare per l'implementazione di misure di mitigazione

i) RESPONSABILITÀ

- Gli obblighi di riservatezza permangono anche dopo cessazione del rapporto di lavoro

- Osservare scrupolosamente tutte le misure di sicurezza in atto
- Seguire ogni ulteriore istruzione impartita per trattamenti specifici
- Rispettare tutte le future disposizioni normative

Queste disposizioni sono tassative e devono essere scrupolosamente osservate da tutto il personale per garantire la sicurezza dei dati personali e prevenire incidenti informatici.

2) <u>Procedura per affrontare l'eventualità di violazione di dati personali (data breach) (DOPO UN INCIDENTE INFORMATICO)</u>

La definizione di "data breach"

Ai sensi dell'art. 4 del GDPR, punto 12, il termine "data breach" indica una violazione di sicurezza che può verificarsi sia accidentalmente che in modo illecito e che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali che vengono trasmessi, conservati o comunque trattati. Questa violazione può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali stessi.

È importante comprendere che una violazione dei dati personali non riguarda solamente un'azione dolosa, ma anche eventi accidentali che possono mettere a rischio la sicurezza delle informazioni. Per esempio, alcune situazioni che possono configurare un data breach includono:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici, come computer portatili, smartphone o chiavette USB, che contengono dati personali;
- la modifica non autorizzata o deliberata dei dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o a seguito di attacchi informatici quali virus, malware o altri software malevoli;
- la perdita o la distruzione dei dati a causa di incidenti, eventi avversi, incendi o altre calamità naturali;
- la divulgazione non autorizzata di dati personali, ad esempio attraverso la pubblicazione su canali non protetti o la trasmissione a soggetti non autorizzati.

Per prevenire e gestire tali rischi, l'Ente, in accordo con il DPO, adotta il presente modello organizzativo, che rappresenta un documento fondamentale sia come misura di prevenzione sia come risposta tempestiva a possibili violazioni della sicurezza dei dati personali.

Questo documento costituisce inoltre un elemento avanzato di conformità (compliance) rispetto al principio di responsabilizzazione (accountability) del Titolare del trattamento, come previsto dal Regolamento UE n. 679/2016 (GDPR). Esso si affianca e integra le altre misure di sicurezza che il Titolare è tenuto ad adottare nell'ambito delle attività di trattamento dei dati personali.

Come l'Ente gestisce una violazione dei dati personali

Nel caso in cui si verifichi una violazione dei dati personali, l'Ente si attiva senza alcun ritardo per procedere alla segnalazione al Garante per la Protezione dei Dati Personali, secondo quanto previsto dagli articoli 33 e 34 del GDPR.

La procedura di gestione della violazione prevede una serie di azioni fondamentali, che includono:

- l'attivazione di procedure di contenimento e notifica della violazione, al fine di limitare l'impatto e di informare tempestivamente le autorità competenti e, se necessario, gli interessati;
- l'analisi approfondita dell'evento per comprenderne le cause e le modalità di accadimento;
- l'adozione di misure correttive efficaci volte a prevenire il ripetersi di analoghe violazioni in futuro.

Queste fasi sono fondamentali per garantire una gestione responsabile e trasparente dell'evento, in linea con i principi di sicurezza e tutela previsti dalla normativa europea.

Workflow autovalutativo del data breach

Ogni volta che si sospetta una perdita di sicurezza che possa coinvolgere dati personali, oltre ad attivare tutte le altre misure di tutela previste dall'ordinamento, è necessario procedere a un'attenta autovalutazione interna. In particolare, nell'ambito della privacy, occorre porsi una serie di domande fondamentali che guidano verso comportamenti e decisioni conformi ai principi stabiliti dal GDPR.

Questa fase autovalutativa aiuta a identificare con precisione la natura e l'entità della violazione, a valutare i rischi per i diritti e le libertà delle persone interessate, e a stabilire le azioni più appropriate da intraprendere.

a) Verifica dell'incidente di sicurezza

Domanda: Si è verificato un incidente di sicurezza che ha comportato la perdita di riservatezza, integrità o disponibilità dei dati?

Definizione: Un incidente di sicurezza è un evento (o una serie di eventi) di origine dolosa o accidentale, esterno o interno all'organizzazione, che può compromettere uno o più dei tre principi della sicurezza delle informazioni: riservatezza, integrità e disponibilità.

Un incidente può interessare contemporaneamente una o più di queste dimensioni.

Esempi:

- Attacchi informatici;
- Comportamenti umani illeciti o accidentali;
- Catastrofi naturali;
- Malfunzionamenti hardware o software.

Si verifica:

- Una violazione della riservatezza in caso di divulgazione o accesso non autorizzato ai dati;
- Una violazione dell'integrità in caso di modifica non autorizzata o accidentale;
- Una violazione della disponibilità in caso di perdita o distruzione non autorizzata o accidentale dei dati.

Azione:

- **Se NO**: Non si è verificato un incidente di sicurezza che comporti perdita di riservatezza, integrità o disponibilità dei dati, pertanto non c'è stata una violazione dei dati personali. Nessuna ulteriore azione specifica è necessaria.
- **Se SÌ**: Procedere con la domanda successiva.

b) Verifica coinvolgimento di dati personali

Domanda: L'incidente di sicurezza ha coinvolto dati personali?

Definizione: Per dati personali si intendono tutte le informazioni riguardanti una persona fisica identificata o identificabile, direttamente o indirettamente, come previsto dall'art. 4, punto 1 del GDPR e dall'art. 2, comma 1, lett. a) del D.Lgs. 51/2018. Questi dati possono includere nome, codice fiscale, dati di localizzazione, identificativi online, dati biometrici, dati sanitari, informazioni su opinioni politiche, orientamento sessuale e altro.

Esempi:

- Dati anagrafici (nome, cognome, data di nascita);
- Dati di contatto (indirizzo, email, telefono);
- Dati di accesso e identificazione (username, password);
- Dati di geolocalizzazione;
- Dati di pagamento;
- Dati sensibili come quelli relativi alla salute, origine razziale, opinioni politiche, ecc.

Azione:

- **Se NO:** L'incidente non ha coinvolto dati personali, pertanto non si configura una violazione dei dati personali. Procedere con le normali attività.
- **Se SÌ:** L'incidente costituisce una violazione dei dati personali (data breach). Procedere con la domanda successiva.

c) Valutazione del rischio per i diritti e le libertà degli interessati

Domanda: È probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche coinvolte?

Definizione: Il rischio sussiste quando la violazione può causare danni materiali o immateriali, come discriminazione, furto di identità, perdite finanziarie, danni reputazionali, perdita di riservatezza o altri effetti negativi.

Normativa: Il titolare del trattamento deve notificare la violazione all'Autorità di controllo (Garante) a meno che non sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati (art. 33 GDPR).

Fattori da considerare:

- Tipo di violazione;
- Natura, carattere sensibile e volume dei dati;
- Facilità di identificazione delle persone coinvolte;
- Gravità delle conseguenze;
- Caratteristiche particolari degli interessati e del titolare;
- Numero di persone coinvolte.

Azione:

- **Se NO (rischio improbabile):** Non è obbligatoria la notifica al Garante, ma è necessario documentare la valutazione e adottare misure correttive per evitare futuri incidenti.
- **Se SÌ (rischio significativo):** Procedere immediatamente alla notifica della violazione all'Autorità di controllo e, se richiesto, alla comunicazione agli interessati. Procedere con la domanda successiva.

d) Valutazione del rischio elevato per gli interessati

Domanda: La violazione comporta un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte?

Definizione: Il rischio elevato si riferisce a situazioni in cui la violazione può causare danni significativi agli interessati, come discriminazione, furto di identità, perdite finanziarie, danni alla reputazione o altri effetti gravi sulla privacy e i diritti fondamentali.

Normativa di riferimento:

- Art. 33 e 34 del Regolamento (UE) 2016/679
- Art. 26 e 27 del D.Lgs 51/2018

Esempi di rischio elevato:

- Furto di dati sanitari o biometrici;
- Compromissione di dati finanziari sensibili (es. numeri di carte di credito, conti correnti);
- Dati che potrebbero essere usati per furto di identità o phishing;
- Violazioni che possono provocare gravi danni reputazionali o psicologici agli interessati.

Azione:

- **Se NO**: non è obbligatorio comunicare la violazione agli interessati. Si deve comunque notificare la violazione al Garante, salvo che sia improbabile che presenti rischio per i diritti e le libertà delle persone (art. 33 GDPR). Documentare la violazione, le valutazioni effettuate e le misure adottate.
- **Se SÌ**: notificare la violazione al Garante entro 72 ore dal momento in cui se ne è venuti a conoscenza, fornendo tutte le informazioni previste dalla normativa. Comunicare la violazione agli interessati coinvolti con modalità dedicate, a meno che ciò richieda uno sforzo sproporzionato (in tal caso si ricorre a comunicazioni pubbliche). Fornire indicazioni agli interessati su come

proteggersi dagli effetti della violazione (es. cambiare password, monitorare movimenti bancari). Documentare accuratamente tutta la gestione della violazione e le azioni correttive adottate.

Come notificare la violazione al Garante

Quando notificare:

In caso di violazione dei dati personali, il titolare del trattamento deve notificare la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che sia improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche. Se la notifica è tardiva, devono essere indicati i motivi del ritardo (art. 33 GDPR, art. 26 D.Lgs 51/2018).

Contenuto della notifica:

- Descrizione della natura della violazione, categorie e numero approssimativo di interessati e dati coinvolti;
- Nome e contatti del Responsabile della Protezione dei Dati (RPD) o punto di contatto;
- Probabili conseguenze della violazione;
- Misure adottate o previste per mitigare gli effetti negativi.

Notifica in più fasi:

Se non tutte le informazioni sono disponibili subito, possono essere inviate in fasi successive senza ulteriore ritardo, specificando che si tratta di una notifica preliminare (art. 33, par. 4, GDPR).

Procedura:

Dal 1° luglio 2021 la notifica va effettuata tramite procedura telematica sul portale del Garante: https://servizi.gpdp.it/databreach/s/

È disponibile un modello facsimile per la verifica preliminare dei contenuti, ma NON va utilizzato per la notifica ufficiale.

Prima di procedere:

Effettua la valutazione del rischio e contatta sempre il Responsabile della Protezione dei Dati personali.

Come comunicare la violazione agli interessati

Quando comunicare:

Se la violazione comporta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve comunicare la violazione direttamente agli interessati senza ingiustificato ritardo (art. 34 GDPR).

Modalità di comunicazione:

- Comunicazione diretta tramite email, SMS o posta;
- Se lo sforzo è sproporzionato, comunicazione pubblica efficace (banner, sito web, stampa).

Contenuto della comunicazione:

La comunicazione deve essere chiara, trasparente e inviata separatamente da altre informazioni (no newsletter o messaggi standard).

Consigli pratici da fornire:

- Cambiare password e non usare più quelle compromesse;
- Monitorare transazioni bancarie o attività sospette;
- Contattare gli istituti bancari in caso di compromissione di dati di pagamento.

Obbligo di documentazione

Il titolare deve documentare tutte le violazioni, con relative circostanze, conseguenze e misure adottate, anche se non vi è obbligo di notifica. Questa documentazione serve per dimostrare il rispetto della normativa (art. 33, par. 5, GDPR; art. 26 D.Lgs 51/2018).

Si raccomanda di predisporre un registro interno delle violazioni per eventuale consultazione da parte del Garante.

VALUTAZIONE DI IMPATTO

La valutazione di impatto rappresenta un'attività fondamentale che può essere svolta in due momenti distinti:

- **prima dell'avvio di un trattamento (DPIA)**:

  la Valutazione di Impatto sulla Privacy (DPIA) è un processo che aiuta gli enti locali a identificare e gestire i rischi per i diritti e le libertà delle persone coinvolte nel trattamento dei loro dati personali. La DPIA si effettua prima di avviare il trattamento ed è obbligatoria per alcuni trattamenti, come quelli che comportano un rischio elevato o che utilizzano nuove tecnologie. Questa valutazione permette agli enti di individuare il livello di gravità di un trattamento, al fine di adottare misure adeguate per ridurre i rischi e garantire la conformità alle normative sulla protezione dei dati;

- **dopo il verificarsi di un incidente informatico:**
  quando si verifica un incidente informatico, è necessario effettuare una prima valutazione di impatto per indirizzare le risorse necessarie alla sua gestione. Questa valutazione aiuta a comprendere la gravità dell'evento, a determinare eventuali obblighi di notifica alle autorità competenti e a pianificare interventi di mitigazione adeguati.

<u>La valutazione d'impatto prima dell'avvio di un trattamento (DPIA)</u>

La DPIA, come previsto dall'art. 35 del GDPR, si articola in diversi passaggi che gli Enti locali devono seguire:

1. **Descrizione sistematica del trattamento:**

   è necessario descrivere in modo chiaro e dettagliato le finalità del trattamento, le modalità operative, le categorie di dati trattati, i soggetti coinvolti e gli eventuali destinatari, specificando anche la base giuridica del trattamento.

2. **Valutazione della necessità e proporzionalità del trattamento:**

   occorre valutare se il trattamento sia strettamente necessario e proporzionato rispetto alle finalità dichiarate, verificando il rispetto dei principi di minimizzazione dei dati e limitazione delle finalità.

3. **Analisi dei rischi per i diritti e le libertà degli interessati:**

   vanno identificati e valutati i potenziali rischi derivanti dal trattamento, tenendo conto della probabilità e della gravità degli impatti sulle persone fisiche, come la perdita di riservatezza, discriminazioni o danni reputazionali.

4. **Individuazione delle misure di mitigazione dei rischi:**

   è necessario definire le misure tecniche e organizzative per ridurre i rischi individuati, come la cifratura dei dati, il controllo degli accessi, la formazione del personale e i meccanismi di audit.

5. **Consultazione del Responsabile della protezione dei dati (DPO):**

   il DPO, figura obbligatoria per gli Enti locali, deve essere coinvolto per fornire un parere sulla DPIA e assistere nella verifica della correttezza e completezza dell'analisi effettuata.

6. **Eventuale consultazione preventiva dell'Autorità di controllo:**

il titolare del trattamento, prima di procedere, consulta l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che, in assenza di misure adottate per attenuare il rischio, il trattamento comporterebbe un rischio elevato, ex art. 36 del GDPR.

7. **Riesame periodico:**

   è importante riesaminare periodicamente la DPIA, specialmente quando emergono nuove circostanze o cambiamenti che possono incidere sui rischi del trattamento.

La valutazione di impatto dopo il verificarsi di un incidente informatico

Gli incidenti di sicurezza informatica possono essere classificati in diverse categorie:

Tipo di incidente	Descrizione
Accesso non autorizzato	Accesso (sia logico che fisico) a reti, sistemi, applicazioni, dati o altre risorse tecnologiche di proprietà dell'Ente da parte di personale non autorizzato
Denial of Service	Attacco informatico alla disponibilità di una rete o sistema. Qualora abbia successo, comporta la difficoltà all'accesso o la totale indisponibilità di determinati sistemi e/o servizi
Codice malevolo	Un virus, worm, trojan, spyware, o qualsiasi altro codice malevolo che infetti un sistema
Uso Inappropriato	Violazione delle politiche di sicurezza e delle disposizioni su corretto utilizzo
Data leakage	Diffusione di informazioni riservate a seguito di un attacco informatico riuscito
Alterazione delle informazioni	Modifica del contenuto di dati riservati a seguito di un attacco informatico riuscito
Phishing	Truffa effettuata su Internet, che sfrutta tecniche di ingegneria sociale, attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso
Furto/smarrimento totale o parziale di apparecchiature che contengono dati particolari	Il furto o smarrimento di singoli dispositivi di memorizzazione (hard disk, memorie di massa rimovibili, etc.) oppure dei computer/server che li

	ospitano. Una violazione dei dati personali sensibili contenuti configura una condizione di data breach che richiede, ai sensi del GDPR, l'attivazione delle specifiche procedure di notifica verso l'autorità Garante e gli utenti coinvolti
Multiplo	Incidente di sicurezza che comprende due o più di quelli sopra elencati
Malfunzionamento grave	Danneggiamento di un componente hardware o software, oppure degrado delle performance per cause esterne che possa arrecare impatti gravi alla disponibilità di servizio
Data breach	Una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati
Disastro	Qualsiasi evento distruttivo, non provocato direttamente da azione di operatori informatici (es.: black out, incendio, allagamento, terremoto) in grado di condizionare direttamente l'operatività dei sistemi informatici

Valutazione del rischio per i diritti e le libertà

Al fine di valutare il potenziale rischio per le persone fisiche, le "Linee guida" suggeriscono di considerare diversi fattori, tra cui:

- tipo di violazione;
- natura, carattere sensibile e volume dei dati personali;
- facilità di identificazione delle persone fisiche;
- gravità delle conseguenze per le persone fisiche;
- caratteristiche particolari dell'interessato;
- caratteristiche particolari del titolare del trattamento;
- numero di persone fisiche interessate.

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha elaborato «Raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione dei dati personali», che possono essere utili ai fini della valutazione del rischio.

Calcolo della gravità

Sulla base dei criteri sopra esposti, l'approccio di questa metodologia è il seguente:

- Il DPC è il fulcro della metodologia e valuta la criticità di un determinato set di dati in uno specifico contesto di elaborazione.
- L'EI è un fattore correttivo del DPC. La criticità complessiva di un trattamento dati può essere ridotta in base al valore di EI. In altre parole, più bassa è la facilità di identificazione, più basso sarà il punteggio complessivo. Pertanto, la combinazione di EI e DPC (moltiplicazione) fornisce il punteggio iniziale della gravità (SE) della violazione dei dati.
- Il CB quantifica le circostanze specifiche della violazione che possono essere presenti o meno in una particolare situazione. Quando è presente, il CB può soltanto aumentare la gravità della violazione specifica. Per questo motivo, il punteggio iniziale può essere ulteriormente modificato dal CB.

Pertanto, il punteggio finale della valutazione della gravità può essere calcolato utilizzando la seguente formula:

SE = DPC * EI + CB

I livelli di gravità

Gravità di una violazione dei dati		
SE < 2	**Bassa**	Gli individui non saranno colpiti o potrebbero incontrare pochi inconvenienti, che supereranno senza alcun problema (tempo speso a reinserire informazioni, fastidi, irritazioni, ecc.)
2 ≤ SE < 3	**Media**	Gli individui potrebbero incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, negazione di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, piccoli disturbi fisici, ecc.)
3 ≤ SE< 4	**Alta**	Gli individui potrebbero incontrare conseguenze significative, che dovrebbero essere in grado di superare sebbene con serie difficoltà (appropriazione indebita di fondi, inserimento in liste nere

		da parte delle banche, danni alla proprietà, perdita del lavoro, convocazione in tribunale, peggioramento della salute, ecc.)
4 ≤ SE	**Molto Alta**	Gli individui potrebbero incontrare conseguenze significative o addirittura irreversibili, che potrebbero non superare (difficoltà finanziarie come debiti sostanziali o incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)

Contesto di Elaborazione dei Dati (DPC)

Contesto di Elaborazione dei Dati (DPC)		**Punteggio**
Dati semplici	Es. dati biografici, dettagli di contatto, nome completo, dati sull'istruzione, vita familiare, esperienza professionale, ecc.	
	Punteggio base preliminare: quando la violazione riguarda "dati semplici" e il titolare non è a conoscenza di alcun fattore aggravante.	
Dati comportamentali	Es. posizione, dati sul traffico, dati sulle preferenze e abitudini personali, ecc.	
	Punteggio base preliminare: quando la violazione riguarda "dati comportamentali" e il titolare non è a conoscenza di alcun fattore aggravante o attenuante.	
	Il punteggio DPC potrebbe essere ridotto di 1, ad esempio quando la natura del set di dati non fornisce alcuna informazione sostanziale sul comportamento dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) tramite fonti pubblicamente disponibili (ad es. combinazione di informazioni da ricerche sul web	
Dati finanziari	Qualsiasi tipo di dato finanziario (ad esempio reddito, transazioni finanziarie, estratti conto bancari, investimenti, carte di credito, fatture, ecc.). Include dati di assistenza sociale relativi alle informazioni finanziarie.	
	Qualsiasi tipo di dato finanziario (ad esempio reddito, transazioni finanziarie, estratti conto bancari, investimenti, carte di credito,	

	fatture, ecc.). Include dati di assistenza sociale relativi alle informazioni finanziarie.	
	Il punteggio DPC potrebbe essere ridotto di 2, ad esempio quando la natura del set di dati non fornisce alcuna informazione sostanziale sulle informazioni finanziarie dell'individuo (ad esempio, il fatto che una persona sia cliente di una certa banca senza ulteriori dettagli)	
DPC=		

Facilità di Identificazione

Numero di carta d'identità/passaporto/numero di previdenza sociale

Sono tutti considerati identificatori unici e possono essere utilizzati per identificare l'individuo, purché sia possibile collegarli a un database di riferimento (ad esempio, collegando una carta d'identità a una persona particolare). Ad esempio, quando l'identificazione viene effettuata utilizzando solo uno di questi numeri:

- **EI = 0,25 (Trascurabile)**: quando non vengono fornite altre informazioni sull'individuo o non è possibile trovare informazioni aggiuntive a meno che non si ottenga l'accesso al database di riferimento.
- **EI = 0,75 (Significativo)**: quando l'identificatore rivela informazioni identificative aggiuntive sull'individuo (ad esempio, il numero di previdenza sociale che rivela la data di nascita) ed è collegato ad altri dati (ad esempio, indirizzo postale o email).
- **EI = 1 (Massimo)**: quando sono disponibili anche informazioni dal database di riferimento (ad esempio, carta d'identità e nome completo e/o foto).

EI=

Circostanze della violazione (CB)

A1 Perdita di riservatezza

- **+0,5** –Dati inviati a un numero sconosciuto di destinatari:
    - I dati vengono pubblicati online.

A2 Perdita di integrità

- **0** – i dati non sono stati alterati

A3 Perdita di disponibilità

- **0** – Dati recuperabili senza alcuna difficoltà:

A4 Intenzionalità malevola

- **+0,5** – La violazione è dovuta a un'azione intenzionale, per causare problemi al titolare del trattamento.

CB=

4 Valutazione del Rischio

DPC	
EI	
CB	
SE = DPC * EI + CB=	

4.1 Ulteriori fattori di correzione

Fattore	Dato	Valore correttivo
Numero di interessati		
Intelligibilità (accessibilità) dei dati		

Livello di gravità	
Rischio	

Gli interessati potrebbero incontrare inconvenienti significativi, che dovrebbero essere in grado di superare a dispetto di alcuni problemi.