COMUNE DI DOVERA

Piazza XXV Aprile 1 26010 DOVERA (Cremona)
Part. IVA/Cod. fiscale 00330920190 pec: dovera@postemailcertificata.it

1

Allegato_10

Piano della Sicurezza del Sistema di Conservazione

Comune di DOVERA

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	22.07.2025		
Verifica			
Approvazione			

REGISTRO DELLE VERSIONI E RELATIVE DISTRIBUZIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni	Distribuito a
1	22.07.2025	Prima stesura		
2		Seconda stesura		

INDICE DEL DOCUMENTO

1. PREMESSA - RIFERIMENTI ED ALLEGATI

Il presente Piano della Sicurezza (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) dell'organizzazione del Comune di Dovera esclusivamente per quanto attiene le attività di conservazione documentale ex DPCM 3 dicembre 2013 e, quindi, inerenti quanto definito nell'ambito del Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni). Pertanto, ogni indicazione contenuta nel PdS è da intendersi riferita, ove altrimenti non indicato, esclusivamente alle predette attività di conservazione documentale.

Il PdS fa riferimento ad una serie di documenti e procedure che devono essere utilizzate all'interno della organizzazione stessa. Nel seguito, si fa riferimento agli aspetti della norma ISO/IEC 27001:2013, la cui certificazione è obbligatoria per l'accreditamento alla conservazione documentale e alle norme ISO/IEC 27002 e lo ETSI TS 101 533-01.Si considerano inoltre, a puro titolo di esempio, aspetti contemplati nella norma ISO 9001:2008, oltre che ad altre eventuali norme e/o dispositivi legislativi che devono essere in capo ad Gruppo Maggioli S.P.A.

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

In aggiunta ai termini indicati nell'allegato 1 del DPCM del 3 dicembre 2013 recante Regole tecniche in materia di sistema conservazione, all'interno del documento si fa riferimento alle definizioni riportate nella tabella che segue.

Glossario dei termini - definizioni	
Sistema	Applicazione/Servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell'informazione.
Disponibilità richiesta	Tempo in cui il sistema deve essere utilizzabile in conformità alle funzionalità previste, esclusi i tempi programmati per la manutenzione, rispetto alle ore concordate per l'esercizio.
Periodo criticità servizio	Data/periodo in cui il dato o il servizio deve essere tassativamente erogato per esigenze specifiche del business, quali scadenze o presentazione dei dati.
RBAC	Role Based Access Control - Sistema di controllo accessi basato sui ruoli in cui le entità del sistema che sono identificate e controllate rappresentano posizioni funzionali in una organizzazione o processi.
Tempo ripristino richiesto (Recovery Time Objective)	Tempo entro il quale un processo informatico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili.
Obiettivo temporale di recupero (Recovery Point	Indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a

Objective)	causa di un evento imprevisto.

Acronimi (suggerimento)	
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale; il testo vigente è costituito dal DLgs 82/2005, e successive modifiche.
DLgs	Decreto Legislativo
DM	Decreto Ministeriale
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento (*suggerimento*)

Quali esempi di normativa di riferimento, sono possibili i seguenti:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD) e in particolare art. 50 bis;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole

tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;

- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale ex al Decreto Legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

3.2 Standard di riferimento

Nella definizione del contesto normativo tramite il quale regolamentare l'operato dei conservatori, il legislatore ha provveduto ad identificare un set di standard tecnologici di valenza internazionale a cui riferirsi, sia al fine di recepire le ricerche e gli studi effettuati a livello internazionale sull'argomento, sia al fine di definire un percorso che permetta agli operatori Italiani di rispondere in maniera proattiva alla nascente normativa europea. Segue, quindi, l'attuale scenario tecnologico a cui qualsiasi soggetto accreditato come conservatore è tenuto ad attenersi:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V 1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems

Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- ETSI TR 101 533-2 V 1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The *Dublin Core* metadata element set, Sistema di metadata del *Dublin Core*.

4. ORGANIZZAZIONE DEL SISTEMA DI CONSERVAZIONE

4.1 Ruoli e responsabilità del sistema di conservazione

Lo svolgimento delle attività di conservatore richiede la presenza di più attori coinvolti nel progetto, ognuno dei quali ha la responsabilità di specifiche attività da svolgere.

Questi ruoli si inseriscono nell'organigramma generale dell'organizzazione del Comune di Dovera, arricchendo i ruoli e le procedure già previste per la gestione dei processi interni.

Per ogni figura prevista nel processo di gestione del sistema di conservazione sono richiesti specifici requisiti di onorabilità e di esperienza minima nel ruolo. Peraltro, così com'è previsto che alcune attività possano essere svolte dal medesimo soggetto è, altresì, previsto che alcune funzioni possano essere delegate ad altri soggetti, fermo restando i predetti vincoli di onorabilità e di requisiti di esperienza

del delegato.

Le attività relative al servizio di conservazione coinvolgono vari settori dell'organizzazione , che interagiscono tra loro al fine di garantire la gestione di tutte le esigenze del produttore dei documenti.

Specificamente le attività impattano sulle seguenti struttura organizzative:

- *Amministratore delegato o funzione omologa* richiede la formalizzazione delle procedure interne per la gestione dei rischi dell'organizzazione. A valle della fase di analisi dei rischi approva il piano di mitigazione e sicurezza presentato dal *Responsabile della Sicurezza*.
- *Commerciale/Amministrativo* nella fase di definizione dei parametri contrattuali relativi al servizio di conservazione;
- *Help desk*, coadiuvato dal *Responsabile del Servizio di Conservazione* e dal *Responsabile della Funzione Archivistica di Conservazione*, per le fasi di setup dell'integrazione tra i sistemi del produttore ed il sistema di conservazione;
- *IT Services*, coadiuvato dal *Responsabile dei Sistemi Informativi per la Conservazione* per il monitoraggio complessivo del sistema di conservazione.
- *Development*, coadiuvato dal *Responsabile per lo Sviluppo del Sistema di Conservazione* per la correzione di eventuali anomalie applicative che dovessero emergere nel processo di conservazione.
- *Responsabile del Servizio di Conservazione* per la definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione.
- *Responsabile della Funzione Archivistica di Conservazione*, per la definizione e gestione del processo di conservazione, incluse le modalità

di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato.

4.2 Ruoli e responsabilità della sicurezza informatica del sistema di conservazione

Nell'ambito del personale dell'organizzazione destinato alla gestione del sistema di conservazione è necessario definire quale di questo personale sia dedicato alla sicurezza informatica della conservazione, con le relative responsabilità.

Preminente è la figura del *Responsabile della Sicurezza*, ma l'attività di conservazione prevede obbligatoriamente che sia identificata la specifica figura del *Responsabile della sicurezza dei sistemi per la conservazione*, sebbene ulteriori altre figure possono essere previste dall'impianto organizzativo della Società Gruppo Maggioli S.P.A. realizzato conformemente alle ISO/IEC 27001:2013, ISO/IEC 27002 e ETSI TS 101 533-01.

4.3 Procedure di produzione, diffusione e gestione della documentazione di sicurezza

Le procedure di gestione della documentazione di sicurezza, riguardano le attività legate all'acquisizione, produzione, archiviazione e diffusione del materiale relativo alla Certificazione della Sicurezza delle Informazioni.

La Gestione Documentale della Sicurezza deve prevedere la produzione di documenti che debbono essere elaborati e pubblicati, in seguito alla fase di analisi dei rischi, dal Responsabile della Conservazione come strumento di condivisione delle procedure di sicurezza al personale.

4.4 Procedure per l'acquisto di prodotti e servizi

Il processo di acquisto dei prodotti e servizi all'interno del Comune di Dovera è regolamentato dalle procedure quali quelle, a esempio, derivanti dall'applicazione

della norma ISO 9001:2008 da parte della Società del Gruppo Maggioli S.P.A.

4.5 Procedure per l'alienazione degli asset dell'organizzazione

Il processo di dismissione o alienazione degli asset dell'organizzazione di conservazione viene regolamentato da procedure quali quelle, a esempio, previste dalla norma ISO 9001:2008, oltre che dalle norme ISO/IEC 27001:2013, ISO/IEC 27002 e ETSI TS 101 533-01. Devono comunque essere previste almeno le seguenti procedure (per tutte è necessario definire in dettaglio a quali oggetti si riferiscano, differenziando le eventuali diverse modalità a seconda della tipologia di oggetti):

- procedura di **cancellazione** delle informazioni;
- procedura di **distruzione** dei supporti non riscrivibili utilizzati per la memorizzazione delle informazioni;
- procedura di cancellazione sicura dai supporti riscrivibili utilizzati per la memorizzazione delle informazioni
- procedura di **triturazione** di supporti (quali quelli cartacei e analoghi).

4.6 Piano di formazione del personale

La formazione del personale di GolemNET S.r.l., dovrà essere eseguita come previsto nella norma ISO/IEC 9001:2008 e come specificato dalle ISO/IEC 27001:2013, ISO/IEC 27002 e ETSI TS 101 533-01.

4.7 Continuità operativa

Descrizione delle misure adottate a garantire la continuità operativa quali ad esempio il disaster recovery, il back up delle informazioni, gli apparati ridondati. Rappresentazione del grado di affidabilità mediante indicatori specifici (MTBF, MTTR). Programmazione della manutenzione delle apparecchiature e delle infrastrutture di supporto (idrico, elettrico, antintrusione, antifurto, antiallagamento, antincendio, continuità elettrica) al fine di assicurare la continua disponibilità e integrità.

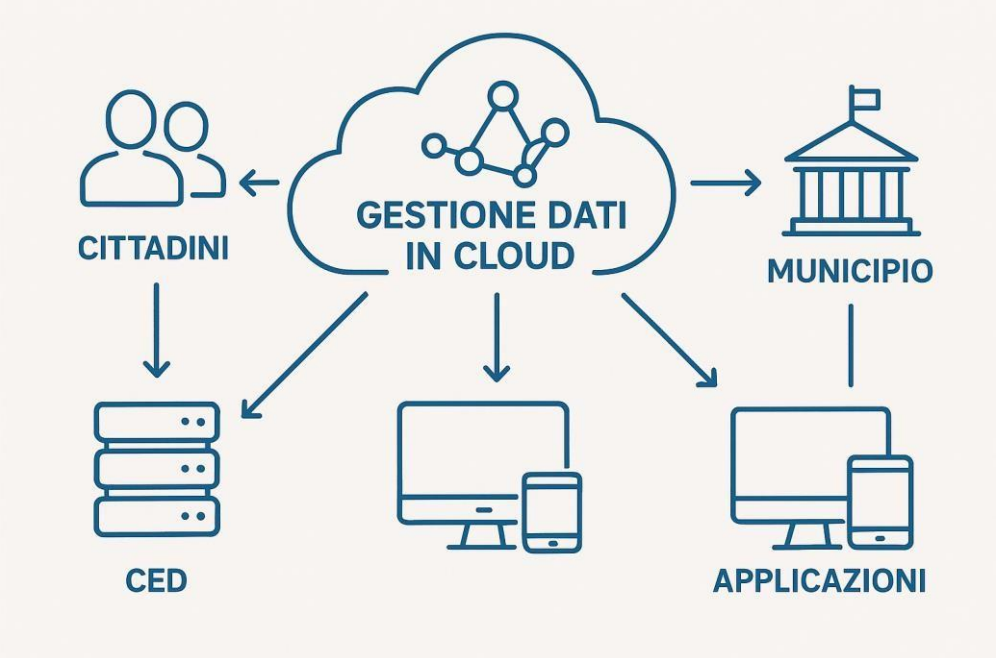
4.8 Piano degli audit interni del sistema

GolemNET S.r.l.,.dovrà dimostrare che è oggetto, con esito positivo, degli audit interni del sistema previsti dalle ISO/IEC 27007 e TR 101 533-02 per stabilire se i processi e le procedure siano efficacemente.

5. PERIMETRO DEL SISTEMA DI CONSERVAZIONE

Descrizione del Sistema di Conservazione. Analisi e implementazione di continuità operativa e disaster recovery a scopo di conservazione documentale.

5.1 Schema topologico



5.2 Componenti fisiche

Descrizione della infrastruttura hardware e di rete. Le procedure di riferimento per tale aspetto sono quelle previste dalle norme ISO/IEC 27001:2013, ISO/IEC 27007 e TR 101 533-02 messe in atto da GolemNET S.r.l.

5.3 Piani di manutenzione delle infrastrutture

I piani di manutenzione di tutti gli apparati fisici facenti parte del Sistema di Conservazione vengono effettuati secondo una periodicità stabilita dal fornitore del servizio.

5.4 Servizi tecnici ed impianti

L'infrastruttura di funzionamento dei servizi tecnici ed impianti si trova totalmente in Cloud pertanto gestita dal fornitore del servizio.

5.4.1 Impianto di anti intrusione e verifica accessi fisici

L'Ente è dotato di un sistema di controllo accessi sia attraverso sistema volumetri che perimetrale collegato con le Forze dell'Ordine.

5.4.2 Impianto di alimentazione elettrica e di emergenza (Sistemi UPS)

Tutti i sistemi elettronici di controllo accessi e antintrusione che i dispositivi di salvataggio dei dati sono collegati a sistema UPS sottoposti a regolare manutenzione e controllo della tenuta della carica.

5.4.3 Impianto di condizionamento

Nei locali CED dove sono allocati i dispositivi di ridistribuzione del segnale di Rete e di protezione della stessa sono allocati degli apparecchi di condizionamento che permettono di mantenere all'interno del locale una temperatura controllata onde evitare il surriscaldamento e rallentamento degli stessi.

5.4.4 Impianto antincendio

Tutti i locali dell'Ente sono dotati di dispositivi di rilevazione incendi e all'interno dei locali sono ubicati degli estintori portatili a polvere B/C con relativa segnalazione alle pareti e revisionati secondo apposito calendario di manutenzione.

Inoltre sono presenti attacchi Idrante UNI 45 in posizione fruibile e segnalato con relativa manutenzione secondo calendario dedicato.

5.4.5 Impianti di rete locale

All'interno dell'Ente tutta la struttura è cablata secondo la normativa e nel rispetto del DPIA stilato dal DPO secondo quanto previsto dalle linee guida AgID. Tutto il flusso dei dati e la conservazione viene effettuata su sistemi di recovery Full Cloud.

5.5 Sistemi di sicurezza logica

I controlli di accesso logico sono fondamentali per garantire che solo gli utenti autorizzati possano accedere ai sistemi e alle informazioni del Comune, in conformità con i principi di riservatezza, integrità e disponibilità dei dati.

Le misure implementate includono:

Identificazione e Autenticazione: Ogni utente è dotato di credenziali individuali e non condivisibili (nome utente e password), necessarie per l'accesso ai sistemi informativi. È obbligatorio l'utilizzo di password complesse, con scadenza periodica e vincoli sul riutilizzo.
Autenticazione a più fattori (MFA): Per i servizi critici o accessibili da remoto (es. VPN, PEC, gestionali), è previsto l'uso di un secondo fattore di autenticazione (es. token, OTP, smartcard o app mobile).
Gestione dei privilegi: L'accesso ai dati e alle risorse è concesso secondo il principio del minimo privilegio, tramite un modello di controllo basato su ruoli (RBAC). Le autorizzazioni vengono periodicamente riesaminate.
Timeout e blocco sessione: Le sessioni inattive vengono automaticamente bloccate dopo un tempo predefinito. È vietato lasciare postazioni incustodite con sessioni attive.

Revoca e disattivazione: Alla cessazione del rapporto di lavoro o cambio di mansioni, le credenziali vengono revocate o modificate entro 24 ore tramite procedura formalizzata.
Audit e Logging: Tutti gli accessi ai sistemi e ai dati sensibili sono registrati in log sicuri, protetti da alterazioni, e conservati per almeno 6 mesi, secondo la normativa vigente.

Sistemi di Protezione da Intrusioni (IDS/IPS)

Per garantire la sicurezza perimetrale e interna, il Comune adotta sistemi di rilevamento e prevenzione delle intrusioni:
Intrusion Detection System (IDS): Monitorano costantemente il traffico di rete e i sistemi, segnalando eventuali attività anomale o tentativi di accesso non autorizzati.
Intrusion Prevention System (IPS): Integrazione con firewall e antivirus per bloccare in tempo reale traffico sospetto, malware o exploit noti.
Analisi Comportamentale: L'infrastruttura può includere strumenti per l'analisi dei comportamenti degli utenti (UEBA), al fine di rilevare anomalie rispetto ai profili abituali.
Aggiornamento e manutenzione: I sistemi IDS/IPS sono regolarmente aggiornati con firme di minacce recenti e configurati per l'invio automatico di alert agli amministratori di sistema.

5.6 Disaster Recovery e Continuità Operativa

L'ente utilizza dei sistemi di gestione dati e conservazione degli stessi attraverso Microsoft 365 e APK i quali si trovano in Cloud e hanno dei sistemi di Disaster Recovery e Continuità Operativa.

5.6.1 Continuità operativa

L'Agenzia per l'Italia Digitale definisce la continuità operativa nel contesto ICT come la capacità di una organizzazione di adottare - per ciascun processo critico e per ciascun servizio istituzionale critico erogato in modalità ICT, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative - misure di reazione e contenimento ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale

funzionamento dei servizi e delle funzioni istituzionali.

5.6.2 Ridondanza geografica

L'infrastruttura informatica secondaria a supporto della continuità operativa è un insieme di risorse, sistemi e procedure progettate per garantire il mantenimento dell'erogazione dei servizi essenziali anche in caso di malfunzionamenti, guasti o eventi critici che compromettano l'infrastruttura primaria. Essa rappresenta un elemento chiave della strategia di **business continuity e disaster recovery.**

5.6.3 Infrastruttura di rete (geografica e locale)

L'infrastruttura di rete si compone di due livelli principali: la rete geografica (WAN – Wide Area Network) e la rete locale (LAN – Local Area Network). Questi livelli permettono la connessione tra le varie sedi comunali e garantiscono la comunicazione e l'accesso ai servizi digitali interni ed esterni.

5.6.4 Procedura per il disaster recovery

Lo scopo della procedura è quello di ripristinare il funzionamento dei servizi digitali in caso di problemi gravi (guasti, attacchi informatici, disastri naturali).

Cosa copre la procedura

- PC, server e dispositivi di rete (es. router, stampanti in rete)
- Connessione Internet
- Caselle email istituzionali
- Archivi digitali (file condivisi, documenti amministrativi, registro elettronico)

Quando si attiva

La procedura si attiva in caso di:

- Impossibilità ad accedere a email o software principali
- Perdita di documenti digitali
- Malfunzionamenti diffusi su più PC o server
- Virus o attacchi informatici

Cosa fare in caso di emergenza

Fase 1: Segnalazione
Chiunque noti un problema serio deve avvisare il responsabile IT.

Fase 2: Contenimento

- Spegnere o scollegare i PC infetti o malfunzionanti.
- Non tentare riparazioni senza autorizzazione.

Fase 3: Ripristino

- Il responsabile IT utilizza i **backup** (copie di sicurezza) per recuperare i dati.
- Si ripristinano prima i servizi più urgenti: email, accesso a documenti condivisi.

Fase 4: Comunicazione

- Informare il personale sullo stato del problema e sui tempi di ripristino.
- Se necessario, segnalare alle autorità eventuali violazioni dei dati personali (GDPR).

Prevenzione e preparazione

- Backup automatici giornalieri (in cloud)
- Aggiornamenti periodici dei programmi antivirus
- Formazione base del personale su sicurezza informatica
- Verifica dei backup almeno una volta ogni 6 mesi

6. VERIFICA DELLA CONFORMITÀ E MIGLIORAMENTO DELLA SICUREZZA DEI DATI

Per una corretta gestione del rischio è necessario identificare un insieme di attività critiche o operative dell'organizzazione, quali, a esempio, le seguenti :

6.1 Identificazione dei rischi

L'identificazione dei rischi ha l'obiettivo di individuare e analizzare potenziali situazioni che possono compromettere l'efficacia, l'integrità, la riservatezza e la disponibilità dei documenti durante tutto il ciclo di vita documentale, dai flussi interni alle procedure di conservazione.

6.2 Definizione dei rischi

I rischi intrinseci e potenziali che possono pregiudicare l'efficacia, la correttezza e la sicurezza del flusso documentale, al fine di identificare adeguate misure preventive, di correzione e mitigazione vengono così gestiti

Valida per tutti i processi documentali comunali, inclusi:

- la produzione, ricezione e protocollazione (cartacei e digitali);
- la conservazione, archiviazione e selezione;
- lo scambio, l'accesso e la riproduzione;

Stima della criticità dei rischi

La stima della criticità dei rischi può essere effettuata attraverso una metodologia di identificazione e valutazione del rischio.

6.3 Sviluppo di strategie

- Mappatura dei processi: analisi e interviste per capire flussi e attori;
- Raccolta dei rischi: brainstorming con responsabili di settore, archivisti, IT, audit, legali;
- Classificazione: assegnazione a categorie come sopra;
- Valutazione quantitativa/qualitativa: impatto (es. bassa, media, alta) × probabilità (es. raro, possibile, frequente);
- Prioritizzazione: concentrarsi sui rischi ad alto impatto × alta probabilità.

6.4 Elenco rischi

Rischi di integrità e completezza:

- Smarrimento o manomissione di documenti cartacei o digitali;
- Incompletezza dei metadati;
- Errori di indicizzazione o protocollazione;
- Versioni non coerenti o duplicati non autorizzati.

Rischi di riservatezza:

- Accessi non autorizzati a informazioni sensibili (anagrafe, atti deliberativi, dati sanitari, ecc.);
- Divulgazione accidentale tramite email, copia, stampa;
- Mancanza di controllo sugli accessi (ruoli, autorizzazioni, tracciamento).

Rischi di disponibilità e continuità operativa:

- Interruzioni hardware o software (server, linee di rete, servizio PEC, protocollo);
- Backup insufficienti o mal gestiti;

- Inadeguatezza della continuità operativa in caso di disaster recovery;
- Guasti ai sistemi di archiviazione cartacea (allagamento, incendio).

Rischi di conformità normativa

- Mancato rispetto della normativa (Codice Amministrazione Digitale, GDPR, disciplina archivistica);
- Procedure non aggiornate rispetto a leggi/regolamenti;
- Mancanza di tracciabilità (log, audit trail) nelle operazioni critiche.

Rischi operativi e umani

- Errori di digitazione o protocollazione;
- Inadeguata formazione del personale;
- Mancanza di istruzioni o manuali d'uso aggiornati;
- Sovraccarico di lavoro o turn-over elevato.

6.4 Gestione dei rischi

La gestione del rischio può essere effettuata attraverso una attenta analisi che si articola sulla verifica e il controllo di ciascun rischio identificato:

- Valutazione iniziale (priorità alto/media/basso);
- Contromisure esistenti (controlli organizzativi, tecnologici, fisici);
- Gap analysis (manca qualcosa?);
- Interventi consigliati (es. policy, formazione, miglioramento infrastrutture IT, backup, audit periodici);
- Responsabile (chi monitora e interviene);
- Tempistica (scadenze per realizzare contromisure);
- Rischio residuo (valutazione successiva alle contromisure).

6.5 Monitoring

Il rischio può essere mitigato attraverso una fase di analisi e controllo che si articoli

nelle seguenti modalità:

- Riesame almeno annuale o a seguito di modifiche normative, eventi (incidenti, cambiamenti organizzativi);
- Aggiornamento di mappatura, rischi e piano trattamento;
- Report alla Direzione per visibilità e monitoraggio.

6.6 Verifica e miglioramenti (auditing)

Misurazione dell'efficacia sul medio e lungo termine delle contromisure adoperate al fine di affinare, eliminare od inserire nuovi rischi e iniziare nuovamente il processo.

7. MONITORAGGIO E CONTROLLI

Descrizione delle procedure di monitoraggio e di controllo del funzionamento del sistema.

7.1 Procedure di monitoraggio

La procedura sarà costantemente tenuta controllata attraverso audit condotti dai responsabili degli uffici e con la supervisione dell'Amministrazione del presente comune.

7.2 Gestione dei log

La procedura di gestione dei Log ha lo scopo di garantire la tracciabilità, la sicurezza e la conformità dei dati relativi agli accessi, alle modifiche e alle operazioni effettuate sui sistemi informatici e documentali del comune.

7.3 Politiche di conservazione dei log

La conservazione dei Log consente di verificare le operazioni effettuate, prevenire accessi non autorizzati e assicurare la conformità alle normative vigenti. Questa politica si applica ai Log generati dai sistemi di gestione documentale, dalle piattaforme di protocollo informatico e dagli strumenti di archiviazione digitale utilizzati dal Comune.

Livello di severità	Periodo minimo di archiviazione	Periodo massimo di archiviazione
Log di accesso	5 anni	5 anni
Log di trasmissione	10 anni	10 anni
Log di back-up	3 anni	3 anni

8. POLITICHE DI SICUREZZA

Tutte le sezioni successive devono contenere la descrizione per ognuna delle politiche (eventualmente, come riferimento alla specifica documentazione di implementazione delle norme ISO/IEC 27001:2013, ISO/IEC 27007 e TR 101 533-02 dell'attività di conservazione documentale).

8.1 Politica di gestione della sicurezza dei sistemi

La gestione in sicurezza delle infrastrutture informatiche ha l'obiettivo di garantire che i sistemi, le postazioni di lavoro, le applicazioni, i servizi di rete, i servizi elaborativi forniscano le prestazioni elaborative ai livelli e con i requisiti di sicurezza definiti.

Vengono inoltre di seguito sintetizzati i principi generali in base ai quali porre in essere la gestione sicura dei sistemi:

- deve essere gestito ed aggiornato un inventario degli asset hardware e software;
- devono essere applicate regole standard per la installazione e la configurazione dei sistemi;
- le configurazioni dei sistemi devono essere disegnate tenendo in considerazione le esigenze attuali e future delle prestazioni;
- le configurazioni dei sistemi devono indirizzare nel modo più compiuto possibile la sicurezza built- in e devono facilitare l'installazione di ulteriori misure di sicurezza;
- devono essere adottate procedure standard di configurazione dei sistemi che indirizzino:
    - disabilitazione o restrizione nell'utilizzo di alcuni particolari servizi;
    - restrizioni nell'accesso ad utilities di sistema particolarmente critiche ed a funzioni di setting di sistema;
    - utilizzo di funzioni di time-out;
    - le principali esigenze di aggiornamenti in termini di patch e di fix di sicurezza;
- le configurazioni dei sistemi devono essere archiviate ed aggiornate

all'interno di un repository governato centralmente;

- devono essere condotte regolarmente attività di monitoraggio sulle prestazioni dei sistemi al fine di gestire adeguatamente eventi, problemi e incidenti.

E' inoltre fondamentale predisporre un'adeguata politica di backup, anche remoto, che naturalmente sia in accordo e coerenza con quanto previsto dal manuale della conservazione.

8.2 Politica per il controllo degli accessi fisici

Descrizione delle modalità di controllo degli accessi fisici, che prevedano, almeno le seguenti classi di accesso:

- personale dell'organizzazione;
- personale di fornitori esterni;
- personale della/delle amministrazione/amministrazioni servite dal sistema di conservazione;
- personale delegato dall'organizzazione (a esempio personale che esegue manutenzione/riparazione, ecc.).

La procedura deve anche regolare la gestione di badge/passi temporanei e le modalità di accompagnamento di personale esterno (clienti, manutenzione, ecc.) alle varie aree del sito da parte del personale dell'organizzazione.

8.3 Politica per l'inserimento dell'utenza e per il controllo degli accessi logici

Descrizione delle modalità di inserimento dell'utenza (preferibilmente basate su sistema RBAC) e attribuzione delle autorizzazioni per gli accessi a sistemi, applicazioni e applicativi dell'organizzazione; comprende anche le modalità di cancellazione o di cambio di autorizzazione, con specifico riferimento al sistema di conservazione documentale.

8.4 Politica di gestione delle postazioni di lavoro

Gli elementi essenziali di questa politica sono:

- provisioning delle postazioni di lavoro;
- regole per l'installazione del software sulle postazioni di lavoro;
- regole per gli aggiornamenti;
- regole per la limitazione della connettività a supporti esterni (CD/DVD, Pen Drive, ecc.);
- regole per la modifica delle impostazioni.

8.5 Politica di gestione dei contenuti applicativi

Descrizione delle attività riguardo la manutenzione dei sistemi, il controllo sul contenuto software dei client al fine di verificare l'assenza di codice malevolo e la conformità a quanto autorizzato e previsto dalle licenze d'uso.

8.6 Politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti

Particolare attenzione deve essere posta alla gestione degli apparati mobili (portatili, tablet, smartphone, cellulari, ecc.) e dei supporti esterni ai server e alle postazioni di lavoro quali, a esempio: HD esterni/CD/DVD/Pen Drive/DAT/LTO, ecc., ma anche carta stampata, che siano utilizzati e/o prodotti nell'ambito delle attività di conservazione documentale.

La politica regola, oltre che le modalità di utilizzo e conservazione dei dispositivi, anche quelle per la dismissione/distruzione degli apparati e dei supporti.

8.7 Politica di gestione dei canali di comunicazione

I canali di comunicazione, quali e-mail, sistemi di instant messaging, VoIP, internet, accessi wireless, fax, scanner, fotocopiatrici devono essere controllati al fine di preservare la confidenzialità, e l'integrità delle informazioni in transito, ed

allo stesso tempo ad impedire l'abuso che si potrebbe fare di tali strumenti di comunicazione. Di conseguenza la tipologia di controlli deve coprire le problematiche di utilizzo appropriato dello strumento, le problematiche di comportamento dell'utilizzatore dello strumento e le tecnologie coinvolte.

8.8 Manutenzione delle politiche di sicurezza

Deve essere previsto il perfezionamento, la divulgazione e il riesame delle politiche di sicurezza al verificarsi dei seguenti casi:

- incidenti di sicurezza;
- variazioni tecnologiche significative;
- modifiche all'architettura informatica;
- aggiornamenti delle prescrizioni normative;
- risultati delle eventuali attività di audit interni.

9. GESTIONE DEGLI INCIDENTI

Si definisce “incidente di sicurezza” qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell’organizzazione o l’integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore (con particolare riferimento al d.lgs. 196/2003, alla L. 547/1993 ed alla L. 38/2006).

Il processo di gestione degli incidenti è articolato nelle seguenti fasi:

- rilevazione/identificazione/classificazione - vengono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente ne viene assegnato un livello di gravità. Il rilevamento avviene a valle delle segnalazioni provenienti da strumenti automatici o ancora da segnalazioni del personale dell’amministrazione;
- contenimento - vengono attuate le prime contromisure, allo scopo di minimizzare i danni causati dall'incidente. In genere si tratta di azioni temporanee e veloci, di cui effettuare il roll-back dopo la successiva fase di eliminazione;
- eliminazione - vengono eliminate le cause che hanno portato al verificarsi dell'incidente;
- ripristino - vengono effettuate le operazioni necessarie per riparare i danni causati dall'incidente e si effettua il roll-back delle contromisure di contenimento;
- follow-up – viene verificata l'adeguatezza delle procedure di gestione degli incidenti e vengono identificati i possibili punti di miglioramento.

Per le procedure di gestione degli incidenti si rimanda alla specifica implementazione dell’organizzazione di GolemNET S.r.l. ISO/IEC 27001:2013,

30
ISO/IEC 27007 e TR 101 533-02.