Piano della sicurezza del sistema di gestione informatica dei documenti

Allegato A del Manuale di gestione documentale.

Prima versione

Sommario

1. INTRODUZIONE

1. Scopo e campo di applicazione del documento

Il presente *Piano per la Sicurezza Informatica del Sistema di Gestione e Conservazione* adottato dall'Ente (di seguito anche "**Piano**") ha l'obiettivo di garantire che:

- i documenti e le informazioni trattati dalla AOO siano sempre **disponibili**, **integri** e **riservati**;
- i dati personali, sia comuni che particolari, siano **tutelati** attraverso l'adozione di misure di sicurezza adeguate e preventive, atte a ridurre al minimo i rischi di:
    - distruzione o perdita, anche accidentale,
    - accessi non autorizzati,
    - trattamenti non consentiti o non conformi alle finalità per cui i dati sono stati raccolti, tenendo conto del progresso tecnico, della natura dei dati e delle specificità del trattamento.

Il documento è allegato al *Manuale di Gestione Documentale* (**MdGD**) e al *Manuale di Conservazione* (**MdC**) dell'Ente, approfondendo in particolare quanto previsto nella sezione "Misure di sicurezza" dei suddetti manuali.

Poiché il sistema di gestione documentale e il sistema di conservazione sono forniti in modalità **SaaS** (Software as a Service) dal fornitore dell'Ente, << NOME FORNITORE>>, come indicato nel paragrafo 2, il Piano illustra i criteri generali di sicurezza del sistema, ma si concentra principalmente sulle misure di sicurezza **di competenza dell'Ente**. Per gli aspetti affidati al fornitore, si rimanda alla relativa documentazione di sicurezza predisposta dallo stesso, in conformità con la normativa vigente per la Pubblica Amministrazione.

1.1 Riferimenti normativi

Codifica	Descrizione
TUDA	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
CAD	D.Lgs. 82/2005 - Codice dell'amministrazione digitale
GDPR	Regolamento UE 2016/679 tutela trattamento dati personali e dei diritti delle persone
CODICE DELLA PRIVACY	Decreto Legislativo 196/03 e ss.mm.ii.
LL.GG.	AgID - Linee guida sulla formazione, gestione e conservazione dei documenti informatici (determinazione AgID n. 407/2020)

1.2 Riferimenti documentali

Codifica	Descrizione

MdGD	Manuale di Gestione documentale dell'Ente
MdC	Manuale del Sistema di conservazione dell'Ente

POLICY DI SICUREZZA ICT	Documento interno inerente le Politiche e misure di sicurezza per il trattamento delle informazioni dell'Ente
MISURE MINIME DI SICUREZZA	Documento interno inerente l'attuazione della direttiva AgID sulle misure minime di sicurezza ICT per le pubbliche amministrazioni
SdC	Il Sistema di Conservazione è fornito in modalità SaaS da un soggetto esterno che provvede alla conservazione dei documenti informatici a norma del D.P.C.M. 3 dicembre 2013 – Regole tecniche in materia di sistema di conservazione, adottato in attuazione 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 (D.Lgs. 82/2005). Il sistema è conforme ai "Requisiti di qualità e sicurezza" definiti da AgID e viene descritto nel Manuale del Sistema di Conservazione dell'Ente, redatto ai sensi dell'articolo 8 del citato D.P.C.M. 3 dicembre 2013.

1.3 Termini e definizioni

Codifica	Descrizione
AOO	Area Organizzativa Omogenea ovvero l'Ente

Orario di servizio	Intervallo temporale entro il quale è garantita al cliente l'erogazione del "servizio" sulla base di quanto previsto da regolamento con le Camere o da contratti in essere con il Cliente. E' uno degli elementi che concorrono al calcolo dell'indicatore sulla disponibilità del servizio. Al di fuori di tale orario, il sistema è comunque disponibile ai clienti senza garanzia del livello di servizio.
DPIA	Data protection Impact Assessment

2. ORGANIZZAZIONE SICUREZZA DEL SISTEMA

2.1 Ambiti di responsabilità

L'ambiente del ciclo di vita dei documenti informatici dell'Ente comprende le fasi di produzione, gestione e conservazione, affidate a fornitori SaaS qualificati AgID. In particolare, le attività di conservazione sono in capo al fornitore specifico. La sicurezza complessiva del sistema di gestione e conservazione è garantita dall'insieme delle misure adottate dai soggetti coinvolti, ciascuno per il proprio ambito di responsabilità.

2.2 Coordinamento misure di sicurezza coordinate

Il presente documento descrive la policy di sicurezza del sistema di gestione e conservazione, che necessariamente focalizza maggiori dettagli sulla componente tecnologica e organizzativa dell'Ente mentre rimanda alla documentazione del fornitore per quanto di sua competenza.

3. POLITICHE PER LA SICUREZZA INFORMATICA DEI DOCUMENTI

3.1 Politica di gestione della sicurezza dei sistemi

Tenuto conto dei diversi ambiti di responsabilità (vedi punto 2.1), le politiche e le misure di sicurezza descritte nel presente paragrafo si riferiscono principalmente all'infrastruttura IT residua gestita direttamente dall'Ente. Va tuttavia precisato che l'attività di gestione documentale interna è marginale, poiché l'intero sistema è basato su soluzioni cloud in modalità SaaS qualificato. La maggior parte delle attività informatiche e dei relativi aspetti di sicurezza sono quindi condivisi con il fornitore del servizio, per le cui responsabilità specifiche si rimanda alle policy ufficiali dello stesso.

3.1.1 Inventario degli asset IT

Gli asset legati alle informazioni e alle relative infrastrutture di elaborazione sono identificati e registrati in un inventario ufficiale, che deve essere pubblicato e costantemente aggiornato.

Ogni asset viene censito, classificato in base alle sue caratteristiche specifiche e successivamente assegnato a un responsabile designato.

La valutazione degli asset avviene tenendo conto del loro valore per l'organizzazione, delle normative applicabili, dei requisiti di riservatezza, integrità e disponibilità, nonché della loro rilevanza e criticità per il funzionamento dell'Ente.

3.1.2 Installazione dei sistemi

L'integrità dei sistemi di produzione rappresenta un requisito di sicurezza fondamentale. Per questo motivo, sono attuate procedure specifiche per controllare e autorizzare l'installazione del software sulle postazioni di lavoro in ambiente di produzione.

I sistemi considerati critici — quali dispositivi di rete, sistemi e computer contenenti informazioni rilevanti per la sicurezza informatica — devono essere protetti da accessi non autorizzati, sia di tipo logico sia fisico.

Sono inoltre definite e implementate regole stringenti che limitano la possibilità per gli utenti di installare autonomamente software, al fine di prevenire rischi per la sicurezza e garantire la conformità alle policy interne.

Gestione dei cambiamenti.

Le modifiche a componenti hardware, software di sistema e software applicativo sono gestite attraverso processi strutturati di change management, che includono — a seconda della tipologia — attività di pianificazione, progettazione, sviluppo, test, rilascio e verifica. Ogni modifica deve essere sottoposta agli opportuni controlli e autorizzazioni prima dell'implementazione.

Documentazione.

Tutte le modifiche apportate all'infrastruttura IT vengono adeguatamente documentate e l'inventario aggiornato periodicamente, al fine di garantire la tracciabilità e il controllo del cambiamento.

3.1.3 Piano dei fabbisogni IT

Per garantire che l'infrastruttura tecnologica dell'Ente sia in grado di sostenere i livelli di servizio richiesti, tutte le componenti hardware e software vengono costantemente monitorate. Inoltre, vengono effettuate analisi previsionali sui requisiti di capacità futuri, al fine di assicurare prestazioni adeguate e continuità operativa.

Il processo di gestione della capacità si articola nelle seguenti fasi:

- analisi dei piani aziendali a breve e lungo termine, per allineare le esigenze tecnologiche con gli obiettivi strategici dell'Ente;
- monitoraggio delle prestazioni attuali delle componenti infrastrutturali, con individuazione di eventuali colli di bottiglia e verifica del carico di lavoro corrente e della sua possibile evoluzione;
- valutazione della crescita del carico nel tempo, anche in relazione all'adozione di nuovi servizi o cambiamenti organizzativi;
- pianificazione e, se necessario, attivazione delle attività di approvvigionamento delle risorse necessarie, in modo da garantire la capacità richiesta.

3.1.4 Configurazione dei sistemi

Nel tempo deve essere mantenuto un modello aggiornato dell'infrastruttura IT, attraverso l'identificazione, il controllo, la manutenzione e la gestione delle versioni delle informazioni di configurazione.

3.1.5 Backup

Il fornitore Saas qualificato si occupa di effettuare copie di backup delle informazioni, del software e delle immagini dei sistemi; le copie vengono sottoposte a test periodici di restore.

Il Processo che regola l'esecuzione del backup garantisce che la modalità di salvataggio sia selezionata in base ai parametri: tipologia del dato (dato di produzione / non produzione, dato strutturato / non strutturato), frequenza, ubicazione copie, periodo di *retention*, supporto fisico, ambiente tecnologico.

3.1.6 Amministratori di Sistema

Devono essere minimizzati i rischi di:

violazione alla compliance relativa agli Amministratori di Sistema

danneggiamento di dati e sistemi informatici derivanti da accessi non autorizzati o non adeguatamente controllati ai sistemi ed alle applicazioni da parte dei medesimi Amministratori.

In conformità a quanto previsto dal Garante per la protezione dei dati personali, la designazione degli Amministratori di Sistema all'interno dell'Ente viene effettuata previa valutazione puntuale delle caratteristiche soggettive del soggetto individuato. Tale valutazione deve tener conto dell'esperienza professionale, delle competenze tecniche e dell'affidabilità del candidato, il quale deve offrire adeguate garanzie di rispetto delle disposizioni vigenti in materia di protezione dei dati personali, incluse quelle relative alla sicurezza dei trattamenti.

La nomina deve essere formalizzata in modo individuale, riportando in maniera dettagliata gli ambiti di operatività autorizzati per ciascun Amministratore di Sistema, coerentemente con i privilegi di accesso necessari allo svolgimento delle proprie funzioni.

Gli estremi identificativi delle persone fisiche nominate, unitamente all'elenco delle attività e delle funzioni loro assegnate, sono registrati in un documento interno, mantenuto costantemente aggiornato e disponibile in caso di ispezioni o richieste da parte del Garante.

L'attività degli Amministratori di Sistema è sottoposta a verifica periodica al fine di accertare la conformità dell'operato alle misure organizzative, tecniche e di sicurezza adottate dall'Ente per la protezione dei dati personali, come previsto dalla normativa vigente.

3.2 Politica per le abilitazioni dell'utenza e per il controllo degli accessi logici

Anche nei servizi relativi alla gestione documentale e alla conservazione digitale, l'Ente adotta criteri rigorosi per il controllo degli accessi, ispirati al principio secondo cui l'accesso alle informazioni e ai sistemi deve essere concesso esclusivamente a chi ne ha effettiva necessità per svolgere le proprie mansioni. Questa impostazione rappresenta un pilastro della strategia di protezione delle informazioni.

Tutti i dipendenti e le parti esterne coinvolte nelle attività dell'Ente sono resi edotti dell'esistenza di regole specifiche in materia di accesso ai sistemi informatici e sono tenuti ad attenersi scrupolosamente alle indicazioni previste, in base al proprio ruolo e livello di autorizzazione.

Strumenti, meccanismi di controllo e istruzioni operative relativi alla gestione degli accessi sono soggetti a revisione e aggiornamento continuo, per rispondere sia all'evoluzione dei servizi offerti che ai mutamenti tecnologici e organizzativi che interessano l'Ente.

3.2.1 Gestione degli accessi nei servizi di gestione documentale e conservazione

L'accesso alle funzionalità applicative e ai dati trattati attraverso i sistemi informatici dedicati alla gestione e conservazione documentale deve essere limitato alle sole esigenze operative effettivamente motivate. L'assegnazione dei diritti di accesso viene effettuata sulla base del principio del minimo privilegio, in coerenza con il ruolo ricoperto dall'utente.

Alla cessazione del rapporto di lavoro o collaborazione, oppure in caso di modifica dell'incarico o trasferimento interno, tutti i diritti di accesso sono tempestivamente aggiornati o revocati. Gli account associati a personale non più operativo vengono disabilitati, e le relative credenziali rese inutilizzabili, pur mantenendone traccia ai fini di audit. Gli identificativi utente assegnati restano univoci e non possono essere riassegnati ad altri soggetti in futuro.

L'assegnazione di privilegi amministrativi è soggetta a un controllo rigoroso e limitata ai soli profili autorizzati. L'accesso straordinario da parte di personale non ancora abilitato può avvenire solo in situazioni di emergenza, previa autorizzazione e con rilascio di abilitazioni temporanee strettamente controllate.

In occasione della generazione o modifica delle credenziali, l'utente riceve una notifica prende visione delle informazioni assegnate e ne conferma l'accettazione.

La responsabilità dell'attuazione di tali processi ricade sulle figure interne formalmente designate. Le richieste operative vengono indirizzate al fornitore SaaS qualificato, il quale provvede alla loro esecuzione utilizzando strumenti tecnici appropriati, e garantisce riscontro documentato alle richieste ricevute.

3.2.2 Gestione delle credenziali

Nel contesto dei servizi di gestione e conservazione documentale, è fondamentale adottare misure efficaci per prevenire l'uso improprio delle credenziali di accesso, con particolare riferimento alle password e agli altri meccanismi di autenticazione.

Le regole per la creazione, l'utilizzo e la protezione delle password si applicano a tutto il personale dell'Ente e ai soggetti esterni autorizzati che accedono alle risorse informative. L'intero processo di gestione delle credenziali è, ove tecnicamente possibile, automatizzato, così da garantire il rispetto di criteri di sicurezza come la complessità, la scadenza periodica e la gestione dell'invecchiamento delle password.

Le credenziali devono essere personali, non trasferibili e assegnate esclusivamente in funzione delle effettive necessità operative, nel rispetto del principio del minimo privilegio. L'utilizzo delle stesse è sempre associato alle abilitazioni necessarie per l'accesso selettivo ai sistemi e ai dati.

Le password devono essere strutturate secondo criteri di robustezza, tali da renderne difficile la compromissione tramite tecniche di indovinamento o attacco automatizzato, e devono essere conservate con attenzione, evitando condivisioni o modalità di custodia insicure. È inoltre previsto un aggiornamento periodico delle stesse per ridurre il rischio derivante da esposizioni prolungate.

Le medesime disposizioni si applicano ai codici PIN associati a dispositivi di autenticazione dotati di certificati digitali, quali smart card, token USB o dispositivi wireless, che devono anch'essi essere gestiti in modo sicuro e riservato.

3.2.3 Responsabilità individuale nella gestione delle credenziali di accesso

Le credenziali di accesso e i dispositivi di autenticazione assegnati a ciascun utente sono strettamente personali e non possono essere condivisi con altri. Ogni utente è direttamente responsabile della protezione e dell'uso corretto della propria password, degli strumenti di identificazione elettronica e delle informazioni necessarie per accedere ai sistemi e ai dati gestiti dall'Ente.

È obbligo dell'utente custodire in modo sicuro le proprie credenziali e i dispositivi associati, evitando in ogni circostanza di lasciarli incustoditi o accessibili a terzi non autorizzati.

Tutte le attività svolte attraverso i servizi di gestione e conservazione documentale sono attribuite al titolare dell'utenza utilizzata. La responsabilità delle azioni eseguite tramite un'identità digitale rimane in capo all'utente assegnatario, anche nel caso in cui esse siano state compiute da altri in sua assenza o senza il suo consenso.

3.2.4 Servizi informatici forniti da fornitore Saas qualificato,

I processi organizzativi e le soluzioni tecniche adottate dal fornitore SaaS qualificato per la gestione delle richieste dell'Ente in materia di credenziali di accesso risultano pienamente allineati alle policy e alle procedure definite dall'Ente stesso.

In particolare, gli strumenti impiegati per l'amministrazione delle password garantiscono il rispetto dei requisiti di sicurezza previsti, in quanto:

prevedono modalità di gestione interattiva delle credenziali, tali da guidare l'utente nella creazione di password robuste;

applicano meccanismi di controllo automatico che impongono il rispetto della password policy adottata, inclusi i criteri di complessità, scadenza e lunghezza minima.

Tali misure assicurano che l'accesso ai servizi forniti dal sistema SaaS avvenga in modo conforme ai principi di sicurezza definiti dall'Ente.

3.2.5 Esecuzione degli accessi al Sistema

I sistemi di gestione e conservazione documentale utilizzati dall'Ente sono ospitati e amministrati su infrastruttura IT fornita da un fornitore SaaS qualificato. Tali sistemi sono progettati per garantire elevati standard di sicurezza, grazie all'adozione delle seguenti misure:

Procedure di autenticazione sicura: l'accesso ai sistemi e alle applicazioni è protetto da meccanismi di log-on sicuri, che riducono il rischio di accessi non autorizzati.

Controllo selettivo degli accessi: i diritti di accesso alle informazioni e alle funzionalità applicative sono configurati in base al principio del "least privilege", limitando l'operatività degli utenti e del personale di supporto alle sole attività strettamente necessarie.

Gestione delle password: le soluzioni tecniche impiegate dal fornitore garantiscono una

gestione coerente con la politica dell'Ente, imponendo requisiti di robustezza e complessità nella definizione delle credenziali, in linea con le buone pratiche di sicurezza.

3.3 Politica di sicurezza ai servizi di gestione e conservazione documentale

Le disposizioni contenute nel documento relativo alle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dei dati personali (ai sensi del Codice Privacy) si estendono anche all'ambito specifico dei servizi di gestione documentale e conservazione digitale. In tale contesto, devono essere rispettate le seguenti prescrizioni operative:

Aggiornamento dei sistemi

L'Ente assicura il mantenimento di un adeguato livello di aggiornamento del software installato sulle postazioni di lavoro, al fine di ridurre i rischi di vulnerabilità. Il personale è tenuto a non disattivare o ostacolare gli strumenti predisposti per l'aggiornamento automatico o centralizzato, qualora previsti.

Controllo sull'uso di supporti esterni

L'utilizzo non controllato di dispositivi rimovibili rappresenta un potenziale veicolo di compromissione dei dati riservati. Pertanto, il personale:

- non deve permettere a terzi il collegamento di dispositivi esterni alla propria postazione;
- non deve collegare dispositivi rimovibili e lasciarli incustoditi;
- deve evitare di lasciare tali dispositivi fuori dal controllo dell'Ente, in particolare al di fuori del perimetro aziendale.

Gestione delle configurazioni

Le configurazioni predefinite di sistema, sia hardware sia software, presenti su postazioni, dispositivi mobili o supporti assegnati in dotazione individuale, non devono essere modificate autonomamente. Ogni variazione deve essere autorizzata dalle funzioni preposte alla sicurezza IT.

Configurazione delle postazioni utente

L'accesso al sistema documentale avviene tramite interfaccia web, utilizzando browser aggiornati e compatibili. Le postazioni di lavoro e i browser devono essere configurati secondo le specifiche tecniche indicate e aggiornate dal fornitore SaaS qualificato, per garantire coerenza e sicurezza nell'accesso ai servizi.

Virtualizzazione delle postazioni

Per ottimizzare l'uso delle risorse tecnologiche, contenere i costi di esercizio e migliorare i livelli di sicurezza, l'Ente promuove l'adozione di tecnologie di virtualizzazione del desktop. Tali soluzioni possono essere utilizzate sia in modalità permanente (es. lavoro da remoto), sia in modalità occasionale (es. smart working).

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

Applicazione delle misure di sicurezza ai servizi di gestione e conservazione documentale

Le disposizioni previste nel documento sulle Misure minime di sicurezza e nelle lettere di

incarico per il trattamento dei dati personali (ai sensi del Codice Privacy) trovano piena applicazione anche nell'ambito dei servizi di gestione documentale e conservazione. Di seguito sono riportate le misure operative da osservare.

Gestione di dispositivi e supporti informatici

Tutti gli apparati e i supporti informatici, sia durante l'utilizzo che nelle fasi di inattività o trasporto, devono essere adeguatamente protetti per prevenire accessi non autorizzati, utilizzi impropri, alterazioni, danni fisici o furti.

Le postazioni mobili, generalmente assegnate in uso personale ai dipendenti, possono in casi specifici essere attribuite a un responsabile di struttura e condivise dal personale afferente.

Il personale autorizzato è tenuto ad adottare comportamenti cautelativi nel trasporto e nell'utilizzo degli apparati al di fuori delle sedi dell'Ente, in conformità alle indicazioni ricevute.

È vietato archiviare su dispositivi mobili dati personali non pertinenti alle attività istituzionali, salvo autorizzazione espressa da parte dell'Ente.

Dismissione di apparati e supporti informatici

Prima della dismissione o del riutilizzo, ogni apparato o supporto informatico deve essere sottoposto a verifica per garantire che eventuali dati sensibili o critici siano stati completamente rimossi o distrutti secondo modalità sicure e tracciabili.

Gestione dei supporti cartacei

Le informazioni contenute su supporto cartaceo, come documenti o appunti, devono essere sempre custodite con attenzione e non lasciate in aree non sorvegliate.

In particolare, materiali contenenti dati riservati non devono essere abbandonati su scrivanie, tavoli riunione o presso dispositivi di stampa, copia o scansione, né nelle loro immediate vicinanze.

Per le stampanti multifunzione condivise, l'Ente mette a disposizione modalità di stampa protetta, da utilizzarsi obbligatoriamente per documenti contenenti informazioni sensibili.

Fuori dalle sedi dell'Ente, la gestione della documentazione cartacea deve avvenire con ulteriore attenzione, evitando qualsiasi rischio di esposizione o smarrimento.

Dismissione dei supporti cartacei

I documenti cartacei contenenti informazioni riservate o rilevanti, non più necessari, devono essere distrutti in modo tale da renderli non leggibili o ricostruibili.

A tale scopo, il personale è tenuto a utilizzare gli appositi distruggidocumenti messi a disposizione dall'Ente per garantire la corretta eliminazione dei materiali.

3.5 Politica di protezione dal malware

Protezione da software malevolo (malware)

Le informazioni trattate dall'Ente e le infrastrutture informatiche utilizzate per la loro elaborazione devono essere adeguatamente protette da minacce informatiche, con particolare riferimento alla diffusione di malware.

Sono implementati strumenti e procedure per la rilevazione, la prevenzione e la rimozione di software dannoso, oltre a meccanismi di ripristino per garantire la continuità operativa

in caso di infezione.

In parallelo, l'Ente promuove attività di formazione e informazione rivolte al personale, al fine di aumentare la consapevolezza sui rischi associati al malware e sulle buone pratiche da adottare per prevenirli.

Contromisure tecniche per la protezione da malware

Tutti i dispositivi informatici utilizzati dall'Ente, inclusi server e postazioni di lavoro — sia fisici che virtuali — sono dotati di strumenti software per la protezione contro il malware (antivirus). Tali strumenti sono compatibili con i principali sistemi operativi adottati, quali Microsoft e/o Linux.

Nei cosiddetti "endpoint", l'antivirus è attivo in modo permanente e opera in tempo reale, eseguendo la scansione dei file in transito e un'analisi comportamentale per individuare eventuali attività sospette.

Le soluzioni adottate sono soggette ad aggiornamento periodico, per garantire la massima efficacia nella difesa contro nuove minacce.

Protezione della posta elettronica da spam e contenuti malevoli

I sistemi di gestione della posta elettronica dell'Ente sono dotati di strumenti di filtraggio per contrastare lo spam e i contenuti potenzialmente dannosi. Le funzionalità principali includono:

- analisi delle intestazioni e delle informazioni di provenienza dei messaggi;
- classificazione automatica dei messaggi: consegna, quarantena o eliminazione in base ai criteri di sicurezza;
- rilevamento ed eliminazione di eventuali allegati, codici o link considerati pericolosi;
- consultazione da parte dell'utente dell'elenco dei messaggi trattenuti in quarantena.

Inoltre, il personale può contribuire al miglioramento del sistema segnalando manualmente i messaggi indesiderati, alimentando così la base di conoscenza del filtro antispam.

Anche in questo caso, i componenti utilizzati vengono aggiornati con regolarità per assicurare un livello di protezione costantemente adeguato.

3.6 Misure organizzative: scrivania e schermo puliti

Le prescrizioni contenute nel documento sulle Misure minime di sicurezza e nelle lettere di incarico per il trattamento dei dati personali (ai sensi del Codice Privacy) si estendono anche al Servizio di Gestione Documentale. In tale ambito, è necessario adottare comportamenti che garantiscano la riservatezza delle informazioni, in particolare mediante l'applicazione rigorosa delle politiche di "scrivania pulita" e "schermo pulito".

Scrivania pulita

Per prevenire l'accesso non autorizzato a dati su supporto fisico, al termine delle attività lavorative o durante pause prolungate, non devono essere lasciati incustoditi documenti contenenti informazioni riservate, né supporti di memorizzazione rimovibili (es. chiavette USB, dischi esterni) su scrivanie o superfici esposte.

Schermo pulito

Durante l'assenza dalla propria postazione, l'utente deve assicurarsi che il terminale sia bloccato e che l'accesso sia protetto da password. Deve inoltre essere attivato un salvaschermo automatico con blocco, impostato per intervenire dopo un breve periodo di inattività.

Anche durante l'attività lavorativa, è importante evitare che informazioni sensibili non necessarie alla sessione corrente restino visibili sullo schermo, al fine di ridurre il rischio che vengano consultate involontariamente da terzi (es. documenti aperti inutilmente o finestre lasciate attive senza necessità).

Queste misure costituiscono un requisito fondamentale per la protezione degli asset informativi, sia su postazioni individuali che su postazioni condivise, come console di controllo, server o cartelle di rete.

Il rispetto di tali regole è obbligatorio per tutto il personale dell'Ente, così come per i fornitori e per le terze parti autorizzate ad accedere ai sistemi o alle informazioni.

4. CONTINUITÀ OPERATIVA

Continuità Operativa del Sistema di Gestione Documentale

Il Sistema di Gestione e Conservazione Documentale, essendo ospitato sull'infrastruttura IT di un fornitore SaaS qualificato, rientra nel perimetro del Sistema di Gestione della Continuità Operativa e del Disaster Recovery predisposto dal medesimo fornitore.

Tale soluzione si avvale di un'infrastruttura tecnologica dedicata, progettata con criteri di alta affidabilità e dotata delle necessarie caratteristiche di ridondanza geografica.

Il piano di Disaster Recovery garantisce un Recovery Point Objective (RPO) di massimo 24 ore, limitando il disallineamento dei dati in caso di incidente, e un Recovery Time Objective (RTO) di 72 ore per il ripristino completo della disponibilità dei servizi erogati in modalità outsourcing all'Ente.

Continuità Operativa del Servizio

Nel caso in cui eventi di natura ambientale colpiscano la sede operativa centrale dell'Ente, potrà essere valutato lo spostamento temporaneo del personale presso una sede alternativa. La scelta del luogo sarà effettuata sulla base di valutazioni condotte al momento dell'evento, tenendo conto delle criticità effettivamente rilevate e individuando la soluzione logistica più idonea a garantire la continuità operativa.

In ogni caso, l'infrastruttura di rete distribuita e la disponibilità di dispositivi mobili

permettono l'adozione di modalità operative flessibili, quali il lavoro da remoto o lo smart working, per assicurare la continuità delle attività essenziali.

In presenza di interruzioni prolungate dovute a cause diverse (es. guasti, interruzione prolungata dell'energia elettrica), sarà valutata la riallocazione del personale, sfruttando ove possibile la ridondanza degli impianti di rete e la disponibilità di postazioni già configurate.

5. MONITORAGGIO SERVIZIO

Ripristino del Servizio

Il referente incaricato della gestione del Sistema di Gestione e Conservazione Documentale è responsabile del coordinamento delle attività necessarie a ristabilire la piena operatività della piattaforma in caso di interruzioni, malfunzionamenti o anomalie tecniche. L'obiettivo è garantire il ripristino delle funzionalità entro 24 ore dall'interruzione, compatibilmente con le circostanze, e comunque nel minor tempo tecnicamente possibile, in conformità a quanto previsto dall'art. 61, comma 3 del Codice dell'Amministrazione Digitale (Testo Unico).

Livelli di Servizio Garantiti

In linea con quanto sopra, il fornitore SaaS qualificato si impegna a garantire una disponibilità dei servizi superiore al 99%, così come definito e previsto dalla qualificazione AgID.

Assistenza e Comunicazioni Operative

Il fornitore SaaS qualificato mette a disposizione dell'Ente un servizio di assistenza tecnica, accessibile tramite l'apertura di ticket da parte del personale autorizzato. Tale servizio consente di segnalare tempestivamente eventuali problematiche riscontrate nell'utilizzo della piattaforma.

In caso di anomalie significative o malfunzionamenti che incidano sulla continuità o integrità del servizio, il fornitore ha l'obbligo di informare il Responsabile del Servizio dell'Ente entro un massimo di due ore dal rilevamento del problema, purché all'interno dell'orario di servizio previsto nei giorni feriali.

6. MONITORAGGIO DELL'INFRASTRUTTURA IT

I Sistemi di Gestione e Conservazione Documentale sono ospitati presso l'infrastruttura IT del fornitore SaaS qualificato, il quale ne garantisce la supervisione continua attraverso specifici processi e strumenti di controllo, come descritto di seguito.

Procedure operative

Il fornitore adotta una procedura formalizzata di Operation & Event Management, che ha l'obiettivo di:

- assicurare il monitoraggio costante del corretto funzionamento dell'infrastruttura tecnologica su cui si basa il Sistema di Gestione Documentale;
- pianificare e gestire le attività necessarie affinché i sistemi e le applicazioni dispongano costantemente delle risorse operative indispensabili;

- garantire il supporto tecnico con una copertura completa, 24 ore su 24, 365 giorni all'anno.

Strumenti di monitoraggio

Il monitoraggio dell'infrastruttura IT è supportato da un insieme di strumenti e tecnologie che includono:

- sonde di rilevamento, per l'acquisizione in tempo reale di dati critici di funzionamento;
- sistemi di registrazione automatica degli eventi, finalizzati alla raccolta e tracciabilità delle anomalie;
- console di controllo, per la visualizzazione centralizzata dello stato dei sistemi;
- sistemi di alerting automatico, che generano segnalazioni tempestive in caso di malfunzionamenti o comportamenti anomali.

Gestione dei log

Il fornitore effettua un monitoraggio costante degli eventi significativi, in particolare quelli legati a malfunzionamenti o degrado delle performance, archiviando tali informazioni per scopi di analisi, revisione e audit.

I log raccolti sono distinti in due categorie principali:

- log infrastrutturali: riguardano sia i componenti hardware sia i software acquisiti da terze parti che costituiscono l'infrastruttura IT;
- log applicativi: riferiti alle applicazioni sviluppate internamente dal fornitore e rilevanti per il monitoraggio delle funzionalità operative.

Per ciascuna categoria di log vengono definite e applicate modalità specifiche di gestione, che regolano la registrazione, l'accesso, la conservazione e l'eventuale cancellazione, in base alla loro rilevanza e al livello di criticità.

7 ANALISI DEI RISCHI E VALUTAZIONE DI IMPATTO

E' stato esaminato il contesto generale in cui si colloca il sistema di gestione e conservazione documentale, con particolare attenzione ai trattamenti di dati personali, ai flussi documentali gestiti e alle modalità operative adottate dall'Ente, in un contesto ICT ormai ibrido e fortemente basato sull'infrastruttura del fornitore SaaS qualificato.

L'analisi dei rischi e la valutazione d'impatto si sono concentrate principalmente su tre macro-aree di minaccia:

- accessi non autorizzati a dati, documenti o informazioni gestite dal sistema;

- modifiche involontarie o dolose ai contenuti;
- perdita, danneggiamento o indisponibilità dei dati.

Tali scenari di rischio sono stati messi in relazione con le misure di sicurezza attualmente adottate – di natura fisica, organizzativa e tecnica – al fine di valutarne l'efficacia e il livello di copertura rispetto ai possibili impatti. L'intero asset ICT coinvolto nella gestione documentale è stato considerato nell'analisi, incluse sia le componenti infrastrutturali dell'Ente (come postazioni di lavoro, dispositivi di rete, supporti digitali, accessi logici), sia le piattaforme e i servizi erogati dal fornitore in modalità SaaS.

Modello organizzativo e valutazione dei rischi

Nel contesto del modello organizzativo della sicurezza del sistema di gestione documentale (cfr. punto 2.1), l'analisi di rischio sulle risorse direttamente gestite dall'Ente ha considerato che:

- l'infrastruttura locale dell'Ente è interconnessa con l'architettura tecnologica del fornitore SaaS qualificato, il quale gestisce i principali elementi infrastrutturali, inclusi collegamenti di rete geografica, firewall, antivirus, connettività Internet e manutenzione dei data center;
- i sistemi di gestione dei flussi documentali e di conservazione sono sviluppati e gestiti integralmente dal fornitore e utilizzati dall'Ente in modalità Software as a Service, attraverso connessioni Internet o Intranet sicure;
- il livello di rischio associato alla porzione infrastrutturale e applicativa in carico al fornitore è stato considerato basso o trascurabile, in ragione delle competenze organizzative e delle capacità operative del soggetto gestore, nonché delle certificazioni e qualificazioni da esso detenute.

Fonti e criteri di analisi

L'individuazione delle minacce e delle vulnerabilità potenziali è stata effettuata facendo riferimento a:

- standard internazionali e best practice in ambito di sicurezza ICT;
- caratteristiche tecniche e livello di maturità delle infrastrutture utilizzate;
- esperienze pregresse del personale, assetto organizzativo interno e scelte strategiche;
- riscontri derivanti da incidenti informatici reali o simulati, audit interni e valutazioni periodiche;
- suggerimenti emersi dal confronto con esperti del settore e organismi di settore.

Per ciascun rischio identificato, sono state associate le contromisure disponibili e valutato il livello di implementazione effettiva tramite un indicatore percentuale (es. 100% = pienamente attuata, 50% = attuata parzialmente, 0% = non attuata).

Mappatura dei rischi e impatto

La combinazione tra i fattori di rischio, la probabilità di accadimento e l'efficacia delle misure di sicurezza adottate ha consentito di elaborare una mappatura strutturata dei rischi, applicando la metodologia CNIL per la valutazione d'impatto.

Il risultato ha evidenziato un livello di rischio complessivamente contenuto o trascurabile, compatibile con il tipo di trattamento e con il livello di esposizione delle informazioni trattate.

Rischio residuo e formazione del personale

L'analisi ha evidenziato che il rischio residuo principale è legato alla componente umana, ovvero al grado di preparazione e consapevolezza degli operatori coinvolti nella gestione documentale. La misura di mitigazione più efficace è stata individuata nella formazione continua del personale.

A tal fine, l'Ente garantisce, in relazione ai servizi di gestione documentale, che:

- le iniziative di formazione e aggiornamento siano orientate al consolidamento e all'ampliamento delle competenze del personale, in un'ottica di formazione permanente capace di recepire le evoluzioni normative, istituzionali e tecnologiche;
- ogni percorso formativo sia costruito sulla base del ruolo ricoperto, delle attività svolte e delle potenzialità espresse, tenendo conto dei bisogni formativi individuali e di contesto.

La pianificazione e l'attuazione delle attività formative avviene in collaborazione tra il Responsabile della Gestione Documentale e il Responsabile per la Transizione digitale, articolandosi nelle seguenti fasi operative:

- Analisi dei fabbisogni formativi;
- Pianificazione degli interventi;
- Comunicazione interna e diffusione dei contenuti;
- Erogazione delle attività formative;
- Valutazione dell'efficacia degli interventi.

8 SICUREZZA INFORMATICA COME PROCESSO DINAMICO E CONTINUO

L'evoluzione costante delle tecnologie digitali e l'emergere di nuove minacce informatiche impongono un aggiornamento continuo delle misure di sicurezza adottate dall'Ente. L'implementazione di tali misure non è quindi un'attività statica, ma un processo ciclico e permanente, fondato sul monitoraggio periodico delle vulnerabilità, sull'analisi dei nuovi scenari di rischio e sulla valutazione delle soluzioni tecnologiche disponibili per la loro mitigazione.

In tale contesto, l'Ente, in sinergia con il proprio partner tecnologico – fornitore SaaS qualificato – mantiene un presidio costante sulla sicurezza ICT, adottando misure aggiornate e calibrate in base all'evoluzione delle minacce e ai risultati delle attività di analisi del rischio.

L'approccio adottato mira a garantire un elevato livello di protezione delle informazioni trattate e la resilienza dei servizi digitali offerti.