Allegato 4) al Manuale di gestione dei documenti della Provincia di Imperia

PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

Acronimi

Si riportano, di seguito, gli acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea;
- **RSP** - Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **SdP** – Sistema di Protocollo informatico - l'applicativo acquisito dall'Amministrazione/AOO per implementare il servizio di protocollo informatico.

Obiettivi

Il piano di sicurezza garantisce che le informazioni siano disponibili, integre, riservate e che per i documenti informatici sia assicurata l'autenticità, la non ripudiabilità, la validità temporale, l'estensione della validità temporale, la conservazione e leggibilità nel tempo. I dati, in relazione alle conoscenze acquisite in base al progresso tecnologico, alla loro natura e alle specifiche caratteristiche del trattamento, vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Generalità

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite nel manuale di gestione dei documenti della Provincia, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al decreto legislativo 30 giugno 2003, n. 196 e s.m.i. - Codice in materia di protezione dei dati personali, in caso di trattamento di dati personali e dal Regolamento UE 2016/679 "GDPR".

Il Servizio Sistema Informativo dell'Ente ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti:

- protezione della rete dell'Amministrazione/AOO;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione (username o nome utente), di una password e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno semestrale durante la fase di esercizio;
- con determinazione dirigenziale n. 2156 del 15/11/2024 è stato affidato alla società C&C Sistemi S.r.l. di Imperia il servizio di migrazione e conduzione della soluzione informatica di gestione documentale in uso, "Sicraweb" in cloud SaaS su Liguria Digitale S.p.A. di Genova come consigliato da AgID nel vigente Piano triennale per l'informatica nella Pubblica Amministrazione. Le due società indicate prestano nel servizio affidato, attività di backup delle copie giornaliere, mensili, semestrali e annuali a norma. Liguria Digitale è qualificata da AgID

come Polo Strategico Nazionale ed è dotata di sistema di disaster recovery per garantire la continuità del servizio in caso di eventi accidentali;
- continuità del servizio con particolare riferimento, sia all'esecuzione e alla gestione delle copie di backup dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informatico in caso di disastro;
- conservazione, a cura dell'Ufficio CED dell'Ente, delle copie di backup dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il SdP;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo;
- registrazione in apposito log della banca dati dell'AOO delle attività di protocollo effettuate da ciascun utente durante l'arco della giornata, comprese le modifiche autorizzate.

I dati registrati nei log dei sistemi operativi, e nella banca dati del sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità da soggetti autorizzati in virtù delle norme di legge.

Formazione dei documenti - aspetti di sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:
- l'identificabilità del soggetto che ha formato il documento e l'Amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Per il formato finale del documento si adottano preferibilmente i formati PDF, XML e TIFF, in accordo con le regole tecniche individuate dal CAD (Codice dell'Amministrazione Digitale di cui al D.Lgs. 82/2005 e s.m.i.).

I documenti informatici prodotti dall'AOO sono convertiti, prima della loro sottoscrizione con firma digitale, nel formato standard PDF o PDF/A come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento. Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui

alle linee guida AgID del 17 maggio 2021, sulla formazione, gestione e conservazione dei documenti informatici.
L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza.

Gestione dei documenti informatici
Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente.

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- l'accesso al server del protocollo informatico in modo che qualsiasi utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso;
- il sistema di gestione informatica dei documenti:
  - garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
  - assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata, in uscita e interni;
  - fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
  - consente il reperimento delle informazioni riguardanti i documenti registrati;
  - consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
  - garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Componente organizzativa della sicurezza
La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il Servizio Sistema Informativo dell'Amministrazione.

Componente fisica della sicurezza
L'accesso ai luoghi fisici in cui sono custodite le risorse del sistema informatico documentale è consentito solo:

- al personale del Servizio Sistemi Informativi dotato di opportune chiavi;
- al personale dei lavori pubblici in caso di urgenze e/o per la manutenzione dei locali e degli impianti annessi dotato di opportune chiavi.

Componente logica della sicurezza
La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Componente infrastrutturale della sicurezza
Il sistema informatico utilizza i seguenti impianti:

- Un server di rete su cui è installata la banca dati,
- Il sistema di protocollo, lato utente, funziona in modalità client-server,
- I server e tutte le postazioni di lavoro sono dotati di un prodotto software antivirus installato centralmente dal Servizio Sistema Informativo dell'Ente al fine di prevenire la diffusione di software malevolo (*virus* e *worms*) proteggendo sia la postazione di lavoro sia le reti alle quali l'utente è collegato. L'aggiornamento è automatico ad ogni connessione con il sistema informatico,
- Sistema periferico di protezione contro gli accessi indesiderati alla rete provinciale (firewall).

Gestione delle registrazioni di protocollo e di sicurezza
Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul SdP - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:
- dai log di sistema generati dal sistema operativo;
- dalle registrazioni delle attività del SdP.

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:
- l'accesso alle registrazioni è limitato, esclusivamente, ai sistemisti o agli operatori di sicurezza addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- i log di sistema sono accessibili ai sistemisti in sola lettura al fine di impedirne la modifica;
- l'operazione di scrittura delle registrazioni del SdP è effettuata direttamente dagli applicativi;
- le registrazioni sono soggette a copia giornaliera su dispositivi informatici e su supporto rimovibile;
- il periodo di conservazione del supporto rimovibile è conforme alla normativa vigente in materia.

Trasmissione e interscambio dei documenti informatici
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentito il trattamento e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Gli Uffici dell'Amministrazione si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica o mediante condivisione di file su cartelle condivise su elaboratore server opportunamente protette e riservate agli utenti fruitori.

Accesso ai documenti informatici
Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (username e password) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni delle attività che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale. Queste, in sintesi, sono:
- consultazione, per visualizzare in modo selettivo, le registrazioni di protocollo;
- inserimento, per inserire gli estremi di protocollo e effettuare una registrazione di protocollo ed associare i documenti;
- modifica, per modificare i dati opzionali di una registrazione di protocollo;
- annullamento, per annullare una registrazione di protocollo autorizzata dal RSP.

La username è attribuita ad un unico utente, trattandosi della chiave di identificazione dell'utente univoca nel database degli utenti. Le credenziali di accesso personali sono assegnate e gestite in modo da prevederne la disattivazione in caso di perdita della qualità che ne consentiva l'accesso alla procedura.
La password prevede un minimo di 8 caratteri ed ha durata semestrale sul SdP e trimestrale per l'accesso alla postazione di lavoro informatica.

Il SdP adottato dall'Amministrazione/AOO:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate, se autorizzata, e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Ciascun utente delle UOP può accedere solamente ai documenti che sono stati assegnati al suo gruppo.
Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'Amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

Utenti interni alla AOO
I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dai dirigenti responsabili per singolo settore e implementate dall'Ufficio CED.
Tali livelli si distinguono in: abilitazione alla consultazione, all'inserimento, alla cancellazione e alla modifica delle informazioni.

Politiche di sicurezza adottate dalla AOO

Postazioni di lavoro degli utenti del servizio
Per la corretta fruizione del servizio di protocollo informatico e di gestione documentale e al fine di tutelarne l'accesso è necessario che l'utente adotti almeno le seguenti buone norme di comportamento relative alla gestione del proprio posto di lavoro:

- la stazione di lavoro non deve essere lasciata incustodita, anche per brevi periodi, con la sessione attiva;
- prima di allontanarsi, anche momentaneamente, devono essere attivati i sistemi di protezione esistenti (ad esempio, blocco computer, screen saver con password).

In generale, deve essere adottata la politica della cosiddetta "scrivania pulita" che obbliga a non lasciare materiale riservato incustodito al di fuori dell'orario di lavoro e invita a riporre il materiale di lavoro (documenti, supporti) negli appositi armadi, secondo il livello di sicurezza, di disattivare o bloccare la stazione di lavoro, di tenere chiusi i locali.