COMUNE DI POGLIANO MILANESE

Allegato n. 4

PIANO DI SICUREZZA

II presente documento riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

1. Obiettivi del piano di sicurezza

II piano di sicurezza garantisce che:

● i documenti e le informazioni trattate dall'AOO sono disponibili, integre e riservate;

● i dati personali comuni, sensibili e/o giudiziari 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, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2. Generalità

Considerata la particolare modalità di fruizione del servizio di gestione del protocollo, gran parte delle funzioni/responsabilità di sicurezza sono demandate all'operatore dell'Ufficio Protocollo. All'AOO, in quanto fruitrice del servizio, è demandata la componente "locale" della sicurezza, poiché attraverso la propria organizzazione, nonché le sue misure e le politiche di sicurezza, essa contribuisce a stabilire adeguati livelli di sicurezza proporzionati alla tipologia di dati/documenti trattati.

Il piano di sicurezza:

● si articola, di conseguenza, in due componenti: una di competenza dell'Ufficio Protocollo, una di competenza della AOO;

● si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e i documenti trattati, rispettivamente, nei locali dove risiedono le apparecchiature utilizzate dall'Ufficio di Protocollo e nei locali della AOO;

● si fonda sulle direttive strategiche di sicurezza stabilite;

● definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- definisce le modalità di accesso all'Ufficio Protocollo;
- gli aspetti operativi della sicurezza, con particolare riferimento alle misure minime di sicurezza, *di cui al Disciplinare tecnico richiamato nell'allegato B) del D.lgs. 196/2003 - Codice in materia di protezione dei dati personali;*
- i piani specifici di formazione degli addetti;
- le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione formale con cadenza almeno biennale. Esso può essere modificato a seguito di eventi gravi. I dati personali registrati nel *log* del sistema operativo, del Manuale di sistema di controllo degli accessi e delle operazioni svolte con il Servizio di Protocollo, saranno conservati secondo le vigenti norme e saranno consultati solo in caso di necessità.

3. Formazione dei documenti - Aspetti attinenti alla 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'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 e con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, XML e TIFF.

I documenti informatici redatti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, XML e TIFF), 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 della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici".

4. Gestione dei documenti informatici

II sistema operativo del software gestionale destinato 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 maniera da consentire:

● l'accesso al *server* del protocollo informatico in modo che qualsiasi altro 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. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

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 ed in uscita;

● 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.
Per la gestione dei documenti informatici all'interno dell'AOO, il Responsabile della Sicurezza fa riferimento alle norme stabilite dal responsabile del sistema informativo dell'AgID.

4.1. Componente organizzativa della sicurezza
La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte per l'erogazione del Servizio di Protocollo.

4.2. Componente fisica della sicurezza
II controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:
● l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;
● i dipendenti di aziende esterne non possono entrare e trattenersi nelle aree riservate se non accompagnati da personale comunale autorizzato;
● il personale della sede ha l'obbligo di utilizzare il *badge* sia in ingresso che in uscita dalla sede stessa.

4.3. Componente logica della sicurezza
La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente, nell'ambito del Servizio di Protocollo, è stata realizzata attraverso:
● l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico:
- identificazione, autenticazione ed autorizzazione degli addetti delle AOO e degli operatori dell'erogatore del Servizio di Protocollo;
- riservatezza dei dati;
- integrità dei dati;
- integrità del flusso dei messaggi;
- non ripudio dell'origine (da parte del mittente);
- non ripudio della ricezione (da parte del destinatario);
- *audit* di sicurezza;

● la ridondanza dei sistemi di esercizio.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura "a strati multipli di sicurezza" conforme alle *best practices* correnti.
L'architettura realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione degli addetti delle AOO e degli operatori dell'erogatore del SdP, con le seguenti caratteristiche:
● unico *login server* per la gestione dei diritti di accesso ai servizi applicativi;
● unico sistema di *repository* delle credenziali di accesso degli utenti;
● unico database delle anagrafiche contenente tutti i profili di utenza.

La componente della sicurezza logica dell'AOO viene descritta nelle politiche di sicurezza dall'Area "Funzionamento" Ufficio sistema informativo del AgID.

4.4. Componente infrastrutturale della sicurezza

Presso la sede comunale sono disponibili i seguenti impianti:

● antincendio;

● luci di emergenza;

● continuità elettrica;

● i server e tutte le postazioni di lavoro sono dotate di un prodotto antivirus installato centralmente al fine di prevenire la diffusione di *virus* e *worms*, proteggendo sia la stazione di lavoro sia le reti alle quali l'utente è collegato. L'aggiornamento è automatico ad ogni connessione con il sistema informativo centrale:

● sistema di protezione contro gli accessi indesiderati alla rete comunale tramite *firewall* e *proxy*.

4.5. Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad esempio: dati, transazioni), presenti o transitate sul gestionale, che occorre 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* dei dispositivi di protezione periferica del sistema informatico *(intrusion detection system-IDS,* sensori di rete *e firewall),*

● dalle registrazioni delle attività sull'applicativo.

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:

● il *backup* dei dati è giornaliero e viene effettuato con software Nod32 Vers. 5.0 per server e client. Avviene sia su nastri, che sono conservati in cassaforte, che su nas (Network Area Storage). Il controllo dell'esito dei *backup* viene fatto giornalmente dal Responsabile della gestione documentale, che in caso di errore provvede ad attivare le procedure di diagnosi dei problemi riscontrati. In caso di guasti e/o malfunzionamenti, è possibile il recupero dei dati al giorno precedente fino al recupero totale al massimo al mese precedente.