PIANO DI SICUREZZA INFORMATICA

Premessa
Le Linee Guida al paragrafo 3.5 descrivono i contenuti del manuale di gestione del protocollo, al punto 8, relativamente alle misure di sicurezza e protezione dei dati personali adottate, dispongono "*che siano riportate le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali*".

Al paragrafo 3.9 delle Linee Guida si ribadisce che "*le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017"* descrivendo puntualmente il percorso per la predisposizione del *piano della sicurezza del sistema di gestione informatica dei documenti:*

Il responsabile della gestione documentale predispone il piano della sicurezza:
- in accordo con il responsabile della conservazione e con il responsabile per la transizione al digitale
- acquisito il parere del responsabile della protezione dei dati personali.

Il piano di sicurezza
- deve prevedere *"opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)39, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso".*
- deve contenere "la descrizione della proceduta da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/201640".

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art. 28 "Responsabile del trattamento" del Regolamento UE 679/201640.

1 Obbiettivi del piano di sicurezza

Il 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 e delle aggregazioni informatiche, anche in relazione alle norme sulla protezione dei dati personali.

Il piano di sicurezza garantisce che:
- i documenti e le informazioni trattate dal sistema per la gestione informatica dei documenti sono disponibili, integre e riservate;
- i dati personali comuni, particolari 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

Il piano di sicurezza:
- si fonda sulle direttive strategiche di sicurezza stabilite dall'Amministrazione nelle Politiche di sicurezza, Allegato 2 al Manuale di gestione;
- si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e i documenti trattati,
- definisce:
  - ✓ le modalità di accesso al sistema per la gestione informatica dei documenti e al Programma Informatico di protocollo
  - ✓ gli aspetti operativi della sicurezza, con particolare riferimento alle "Misure minime di sicurezza ICT per le pubbliche amministrazioni"circolare AgID n° 2/2017 e alle misure di sicurezza, di cui al del Regolamento UE 679/201640
  - ✓ i piani di formazione degli addetti;
  - ✓ le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano è soggetto a revisione formale con cadenza periodica e può essere modificato a seguito di eventi gravi.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema per la gestione informatica dei documenti, saranno conservati dal responsabile del sistema informativo secondo le vigenti norme e saranno consultati solo in caso di necessità

3 Formazione dei documenti informatici: aspetti attinenti la 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 il servizio 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 dell'Amministrazione e con le altre PA.

I documenti informatici sono formati dall'Amministrazione secondo quanto previsto dal capitolo 3 del Manuale di gestione del protocollo.
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 previste dalla normativa vigente.

4 Gestione dei documenti informatici

Il sistema operativo delle risorse elaborative del sistema per la gestione informatica dei documenti 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 esclusivamente al server del programma di protocollo 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 per la gestione informatica dei documenti

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti, del registro di protocollo e degli altri registri particolari;
- 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 protezione dei dati personali, 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.

5 Componente organizzativa della sicurezza

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

- ✓ sicurezza informatica: si occupa principalmente della definizione dei piani di sicurezza e della progettazione dei sistemi di sicurezza;
- ✓ sicurezza operativa: ha il compito di realizzare, gestire e mantenere in efficienza le misure di sicurezza così da soddisfare le linee strategiche di indirizzo definite dalla funzione sicurezza informatica;

- ✓ revisione: ha il compito di controllare le misure di sicurezza adottate, verificandone l'efficacia e la coerenza con le politiche di sicurezza.

Nell'Amministrazione le tre funzioni sono affidate al responsabile dei sistemi informativi che si coordina, per gli aspetti di loro competenza con il responsabile della gestione documentale, il responsabile per la transizione al digitale, il responsabile della conservazione dei documenti informatici ed il responsabile della protezione dei dati personali.
Il responsabile del sistema informativo nella definizione del piano di sicurezza e nella progettazione dei sistemi di sicurezza potrà avvalersi , ove necessario, di soggetti dotati delle necessarie competenze tecniche interni o esterni all'Amministrazione.
Il responsabile del sistema informativo per la realizzazione di quanto attiene alla sicurezza operativa potrà avvalersi dei responsabili dei servizi specialistici dei fornitori di hardware e software dell'Amministrazione o di altri soggetti interni o esterni qualificati.

6 Componente fisica della sicurezza

La componente fisica della sicurezza riguarda, data la struttura del sistema informatico del Comune, l'accesso alla sala macchine nella quale sono collocate le risorse elaborative.
Il controllo degli accessi fisici alla sala macchine è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale, interno ed esterno, autorizzato per motivi di servizio;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti devono esplicare la procedura di registrazione; essi non possono entrare e trattenersi se non accompagnati da personale del Comune autorizzato;
- ogni persona che accede alle risorse informatiche nella sala macchine è identificata in modo certo.
- gli accessi alla sede sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;

Il controllo degli accessi fisici alle risorse della sala macchine è regolato secondo i principi stabiliti dal responsabile del sistema informativo.

7 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 sistema per la gestione informatica dei documenti, 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 utenti;
- 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;

8 Componente infrastrutturale della sicurezza

Il locale che ospita la parte centrale del sistema informatico, residente nei locali dell'Amministrazione, (sala macchine) deve essere dotata delle necessarie infrastrutture di sicurezza:

- protezione degli accessi (porte e finestre accessibili) con adeguate strutture,
- impianto antincendio;
- impianto di condizionamento;
- luci di emergenza;
- apparato per la continuità elettrica.

9 Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo, presenti o transitate sul programma gestionale di protocollo che occorre mantenere, sia dal punto di vista regolamentare, sia in caso di controversie legali che abbiano ad

oggetto le operazioni effettuate sul programma gestionale di protocollo, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono formate:

- dai log di sistema, generati dal sistema operativo,
- dai log dei dispositivi di protezione periferica del sistema informatico (intrusion detection system-IDS, sensori di rete e firewall),
- dalle registrazioni del programma gestionale di protocollo

Le registrazioni di sicurezza devono essere effettuate tramite una specifica procedura.

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

- l'accesso alle registrazioni è limitato, esclusivamente, agli amministratori di sistema agli operatori addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- le registrazioni del programma di protocollo sono elaborate tramite procedure automatiche da parte degli operatori di sicurezza;
- l'accesso dall'esterno da parte di persone non autorizzate non è consentito essendo controllato dal sistema di autenticazione e di autorizzazione e dal firewall.

I supporti con le registrazioni di sicurezza sono conservati all'interno di un idoneo contenitore (esempio armadio blindato ignifugo) in un locale diverso dalla sala macchine.

10 Trasmissione e interscambio di documenti informatici

Gli addetti dell'Comune alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

11 Accesso ai documenti informatici

Il controllo degli accessi al sistema per la gestione informatica dei documenti è assicurato utilizzando le credenziali di autenticazione ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale. Queste, in sintesi, sono le abilitazioni/autorizzazioni:

- consultazione visualizzare in modo selettivo registrazioni già presenti;
- inserimento effettuare una nuova registrazione di protocollo e associare i documenti;
- modifica modificare i dati opzionali di una registrazione
- annullamento annullare una registrazione di protocollo, può essere autorizzata solo dal responsabile della . gestione documentale

Il sistema per la gestione informatica dei documenti di cui dispone il Comune deve consentire 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 e l'individuazione del suo autore.
Tali registrazioni sono protette da modifiche non autorizzate.
Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una Access Control List (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).
Ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo servizio.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca full text.

UTENTI INTERNI
I livelli di abilitazione/autorizzazione alle funzioni del sistema per la gestione informatica dei documenti sono disposti dai responsabili di servizio per il proprio ambito di competenza.
I livelli di abilitazione/autorizzazione alle funzioni del programma di protocollo sono disposti dal responsabile della gestione documentale.

La gestione delle abilitazioni/autorizzazioni è realizzata dal sistema in modo che gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati.

12 Conservazione di documenti informatici

Gli aspetti di sicurezza relativi al sistema di conservazione dei documenti informatici saranno trattati nel "Manuale di conservazione di cui al paragrafo 4.6 delle Linee Guida.

13 Politiche di sicurezza

Le Politiche di sicurezza, riportate nell'Allegato 2, stabiliscono, sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure correttive per la gestione degli incidenti informatici.
È compito del responsabile della transizione al digitale e del responsabile della protezione dei dati personali procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.
Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti attinenti alla sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza o a seguito dei risultati delle attività di audit.

14 Misure minime di sicurezza AgID

Alla data di approvazione del presente documento il Comune ha provveduto, da tempo, ad avviare la definizione e l'attuazione delle misure minime per la sicurezza ICT come previsto dalla circolare AgID n° 2 del 18 aprile 2017. Le misure di sicurezza di cui si tratta sono attualmente oggetto di perfezionamento considerato che è in corso il passaggio alla modalità cloud per la quasi totalità delle procedure in uso.
I documenti che espliciterannono le citate misure minime di sicurezza, di prossima approvazione sono:

- il "Modulo di implementazione delle misure minime di sicurezza per le pubbliche amministrazioni"
- il "Regolamento sui soggetti cui sono affidati i privilegi di amministratori del sistema informatico"

15 Formazione degli addetti

Il responsabile del sistema informativo definisce in accordo con il responsabile della transizione al digitale, con il responsabile della gestione documentale e conservazione e con il responsabile della protezione dei dati un piano di formazione sui temi della sicurezza informatica rivolto a tutto il personale.
Nel caso di introduzione di novità rilevanti nel sistema informatico, ad esempio sostituzione o introduzione di nuove procedure, il responsabile del sistema informativo dispone la realizzazione di specifiche attività informative rivolte al personale interessato.
Il responsabile del sistema informativo provvede alla formazione iniziale del personale di nuova assunzione.

16 Revisione e controllo

Il responsabile del sistema informativo dispone la tenuta e l'aggiornamento del registro dei guasti e del malfunzionamenti del sistema informatico; nel quale vengono annotati gli eventi riguardanti la sicurezza informatica.
Nel registro vengono riportate:

- la data e l'ora della segnalazione di guasto o malfunzionamento e la sintetica descrizione dell'evento di sicurezza;
- la descrizione dell'intervento effettuato per contenere e/o risolvere l'evento di sicurezza;
- la data e l'ora della soluzione dell'evento di sicurezza.

Il responsabile del sistema informativo almeno una volta all'anno pianifica e realizza una attività di controllo delle misure di sicurezza oggetto del presente Piano, attraverso:

a) l'esame del registro dei guasti e malfunzionamenti;
b) l'individuazione di specifiche misure di sicurezza che devono essere verificate e le modalità di verifica delle stesse;
c) la verifica delle misure di sicurezza di cui al punto precedente.

L'esito dell'attività di verifica deve essere verbalizzato e sottoscritto dal responsabile del sistema informativo.
A seguito dell'esito delle attività di controllo o del verificarsi di rilevanti eventi di sicurezza il responsabile del sistema informativo può proporre la revisione del Piano,