Piano per la sicurezza dei documenti informatici

Introduzione

1) Obiettivi del Piano di Sicurezza
Il piano di sicurezza garantisce che:
• i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
• i dati personali comuni, sensibili e/o giudiziari vengano 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 definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno dell'AOO
- le modalità di accesso al protocollo informatico
- gli interventi operativi sotto il profilo organizzativo, procedurale e tecnico
- l'aggiornamento del piano da effettuarsi con cadenza biennale fatte salve eventuali emergenze
- la protezione periferica della intranet comunale
- la protezione dei sistemi di accesso e conservazione delle informazioni
- l'assegnazione ad ogni utente che accede al sistema di protocollo informatico di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione
- cambio delle password con cadenza trimestrale utilizzando apposite e rigide regole di sicurezza per la sua creazione
- impiego di un efficace sistema antivirus
- gestione della continuità del servizio e della conservazione dei documenti
- applicazione di misure di sicurezza anche in caso di documenti cartacei
- archiviazione giornaliera delle singole operazioni svolte all'interno del protocollo informatico.

Le misure di sicurezza vengono individuate e gestite in stretta collaborazione con il SIA dell'Unione Comuni Valli del Reno, Lavino e Samoggia.

Formazione dei documenti informatici

3) I Contenuti
In ogni documento informatico deve essere obbligatoriamente riportata, in modo facilmente leggibile, l'indicazione del soggetto che lo produce e gli altri elementi di cui all'articolo 25 del manuale di gestione.
Per agevolare il processo di formazione dei documenti informatici e consentire la trattazione automatica dei dati in essi contenuti, l'amministrazione rende disponibili per via telematica, in modo centralizzato e sicuro, moduli e formulari elettronici validi ad ogni effetto di legge.
Al fine di tutelare la riservatezza dei dati personali, i certificati e i documenti trasmessi all'esterno contengono solo i dati utilizzati ai fini del procedimento amministrativo e nei termini previsti dalla legge.

4) Formati
Per la predisposizione dei documenti informatici si adottano formati che possiedono requisiti di leggibilità, interscambiabilità, non alterabilità durante le fasi di accesso e conservazione, immutabilità nel tempo del contenuto e della struttura. In via preferenziale si adottano i formati, PDF, XML, TIFF, JPG.

5) Sottoscrizione
Prima della loro sottoscrizione con firma digitale, i documenti informatici sono convertiti in uno dei formati standard (PDF, XML, TIFF, JPG). La firma digitale è basata su un certificato rilasciato da un certificatore accreditato e generata con un dispositivo sicuro. Per i documenti informatici che non necessitano di sottoscrizione, l'identificazione dei soggetti che li producono è assicurata della sistema informatico di gestione dei documenti oppure dal sistema di posta elettronica certificata.

6) Datazione
Per attribuire una data certa al documento informatico ci si avvale del servizio di marcatura temporale (time stamping) fornito dallo stesso certificatore accreditato.

Gestione dei documenti informatici

7) Registrazione
Tutti i documenti informatici ricevuti o prodotti dall'Amministrazione sono soggetti a registrazione obbligatoria ad esclusione di quelli soggetti a registrazione particolare da parte dell'ente il cui elenco è allegato al manuale di gestione (Allegato 4) ai sensi dell'art. 53, comma 5 DPR 445/2000 e quelli esclusi di cui all'Allegato 3.

8) Sistema di gestione informatica del protocollo e dei documenti
Il sistema operativo dell'elaboratore, su cui è realizzato il sistema di gestione informatica del protocollo e dei documenti, è conforme alle specifiche previste dalla normativa vigente. Esso assicura:
a) l'univoca identificazione ed autenticazione degli utenti;
b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
d) 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 da modifiche non autorizzate.
Il sistema inoltre:
1) consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
2) 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.
La conformità del sistema operativo alle specifiche di cui sopra sono garantite dal fornitore.

9) Registro informatico di protocollo
Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, al termine della giornata lavorativa, viene trasmesso presso il conservatore accreditato.

10) Modifica o annullamento delle registrazioni di protocollo
L'operazione di modifica o di annullamento di una registrazione di protocollo è eseguita con le modalità di cui all'articolo 8 del Dpcm 31/10/2000 e all'articolo 30 del manuale di gestione.

11) Sicurezza fisica dei documenti
L'accesso in lettura e scrittura alle directory di rete utilizzate come deposito dei documenti è effettuato dal processo server, mai dalle stazioni di lavoro. Il responsabile del SIA dell'Unione garantisce la puntuale esecuzione delle operazioni di backup dei dati e dei documenti registrati, su supporti informatici non riscrivibili, da parte di personale appositamente autorizzato. Ogni operazione di manutenzione o di backup effettuata sul sistema che ospita la base documentale e sul sistema di protocollo informatico è registrata su un file di log periodicamente controllato. Le copie di backup dei dati e dei documenti sono prodotte in una copia e sono conservate a cura del Responsabile del SIA.

Accessibilità ai documenti informatici

12) Gestione della riservatezza
A ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è associata una "Access Control List" (ACL) che consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso. Il sistema di autorizzazione all'accesso avviene sulla base di una profilazione degli utenti effettuata in via preventiva.
Per default il sistema segue la logica dell'organizzazione, nel senso che ciascun utente può accedere solamente ai documenti che sono stati assegnati alla sua struttura di appartenenza, o agli uffici ad esso subordinati.
L'Amministrazione adotta regole per l'accesso ai documenti sulla base della normativa vigente in materia di privacy.

13) Accesso da parte degli utenti interni all'Amministrazione
Il livello di autorizzazione all'utilizzo del sistema di gestione informatica dei documenti è attribuito dal Responsabile del Servizio Protocollo.
I livelli di autorizzazione si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.
Il controllo degli accessi ai dati di protocollo e alla base documentale da parte del personale dell'Amministrazione è assicurato utilizzando USER Id e PASSWORD assegnata ad ogni utente.
Il servizio informatico assicura la variazione sistematica delle password assegnate agli utenti per l'accesso alle funzioni del sistema di protocollo informatico con cadenza trimestrale.

14) Accesso da parte di altre pubbliche amministrazioni
L'accesso al sistema da parte di altre pubbliche amministrazioni, là dove previsto, avviene secondo gli standard e il modello architetturale della Rete nazionale della pubblica amministrazione e con le funzioni minime previste dall'articolo 60, comma 2, del DPR 445/2000.

15) Accesso da parte di utenti esterni
L'accesso per via telematica al sistema di protocollo informatico da parte di utenti esterni non è al momento previsto e consentito.
La consultazione allo sportello, che avviene presso l'Ufficio Relazioni Cittadino Amministrazione, deve essere garantito nel pieno rispetto della tutela della riservatezza delle registrazioni di protocollo. A tale proposito il dipendente incaricato posiziona il video in modo tale da evitare la diffusione di informazioni di carattere personale.

Trasmissione e interscambio dei documenti informatici

16) Sistema di posta elettronica
La trasmissione dei documenti informatici avviene attraverso un servizio di posta elettronica certificata conforme agli standard della rete nazionale delle pubbliche amministrazioni. L'Amministrazione si avvale di un servizio di "posta elettronica certificata" offerto da un soggetto in grado di assicurare la riservatezza e la sicurezza del canale di comunicazione; di dare certezza sulla data di spedizione e di consegna dei documenti, facendo ricorso al "time

stamping" e al rilascio di ricevute di ritorno elettroniche.
Il server di posta certificata di cui si avvale l'amministrazione, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:
a) accesso alla Certification Authority per la verifica dei Message Autentication Code (MAC) presenti sui messaggi ricevuti;
b) tracciamento delle attività nel file di log della posta;
c) gestione automatica delle ricevute di ritorno.

17) Interoperabilità e cooperazione applicativa
Lo scambio di documenti informatici soggetti a registrazione di protocollo avviene mediante messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni. I dati della segnatura informatica di protocollo di un documento informatico trasmesso ad un'altra pubblica amministrazione sono inseriti in un file conforme allo standard XML – XML 1.0. Le modalità di composizione dei messaggi protocollati, di scambio degli stessi e di notifica degli eventi sono conformi alle specifiche previste a livello normativo.
L'operazione di ricezione dei documenti informatici comprende i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi. I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica. L'operazione di spedizione include la verifica della validità amministrativa della firma.

18) Cifratura dei messaggi
Lo scambio di dati e documenti attraverso reti non sicure avviene con l'utilizzo dei sistemi di autenticazione e cifratura.
Lo scambio di dati e documenti attraverso reti sicure, come la Rete nazionale delle pubbliche amministrazioni o le reti interne, può avvenire anche senza adottare le misure di sicurezza di cui al precedente comma in quanto esse non sono ritenute necessarie.

Conservazione dei documenti informatici

19) Supporti di memorizzazione
Per l'archiviazione ottica dei documenti si utilizzano i supporti di memorizzazione digitale che consentono la registrazione mediante la tecnologia laser (CD-R, DVD-R).

20) Procedure di conservazione
La conservazione dei documenti digitali e dei documenti analogici (che comprendono quelli su supporto cartaceo) avviene nei modi e con le tecniche specificate nelle politiche di conservazione contenute nel manuale di gestione e nella deliberazioni CNIPA formulate in materia.
Il riferimento temporale, inteso come l'informazione, contenente la data e l'ora in cui viene ultimato il processo di conservazione digitale, associata ad uno o più documenti digitali, è generato secondo i canoni di sicurezza.

21) Tenuta dell'archivio informatico
Il Responsabile del procedimento di conservazione digitale (Conservatore) sulla base di quanto specificato nel manuale di gestione e nel piano di conservazione adottato dal Conservatore stesso:
a) adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza;
b) definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;
c) verifica periodicamente con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.