ASC InSieme

Azienda Servizi per la Cittadinanza

Interventi Sociali Valli Reno, Lavino e Samoggia

Allegato 16

Piano per la sicurezza informatica

Piano della Sicurezza Informatica

Introduzione

Le Pubbliche Amministrazioni, ai sensi del paragrafo 3.9 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale – AgID, nell'ottica di ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017 predispongono il "Piano della sicurezza del sistema di gestione informatica dei documenti", prevedendo 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), anche in funzione delle tipologie di dati trattati.
Il suddetto Piano deve essere predisposto dal Responsabile della gestione documentale, d'intesa con il Responsabile della conservazione, il Responsabile per la transizione digitale.
La sicurezza di un sistema informativo è da intendersi come:

- la protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali.
- la limitazione degli effetti causati dall'eventuale occorrenza delle cause sopraindicate.

La sicurezza informatica è una caratteristica globale in grado di fornire il desiderato livello di disponibilità, integrità e riservatezza dei dati, informazioni, documenti e dei servizi erogati.
Gli aspetti principali che la compongono sono:

- l'analisi dei rischi, cioè la valutazione dello stato attuale della sicurezza del sistema informativo, al fine di individuare le vulnerabilità del sistema, stimare l'esposizione al rischio e individuare le possibili misure di protezione.
- le politiche di sicurezza, che specificano gli obiettivi, individuano le responsabilità e dichiarano l'impegno dell'Ente relativamente alla messa in sicurezza del sistema informativo.
- la gestione del rischio, cioè la ricerca dell'equilibrio tra i costi dei controlli individuati e il valore dei beni da proteggere (analisi costi/benefici), al fine di determinare il giusto livello di sicurezza da perseguire.
- 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.

Normativa di riferimento

La fonte normativa di riferimento sono le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale – AgID.

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 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)

- cambio delle password con cadenza trimestrale utilizzando apposite e rigide regole di sicurezza per la sua creazione
- l'accesso con autenticazione multi fattore oltre alla combinazione di user ID e password per accessi esterni alla rete intranet
- 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

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 18 del presente 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.

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/a, XML, EML.

Sottoscrizione

Prima della loro sottoscrizione con firma digitale, i documenti informatici sono convertiti in uno dei formati standard (PDF/a, XML). 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 dal sistema informatico di gestione dei documenti oppure dal sistema di posta elettronica certificata.

Datazione

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

I sistemi per la gestione dei documenti

Le disposizioni dettate dal Codice dell'amministrazione digitale – CAD richiedono alle amministrazioni di adeguare il proprio sistema informativo e l'insieme delle applicazioni preposte alla produzione ed alla gestione di documenti digitali; in particolare, l'introduzione della firma digitale necessita l'adeguamento dei processi documentali istituzionali per garantire la certezza giuridica dei documenti prodotti e archiviati e l'aderenza alla norma dei procedimenti, garantendo in particolare:

- conservazione a norma dei documenti;
- obbligo alla Trasparenza amministrativa,
- integrabilità informatica dei documenti nei flussi della organizzazione;
- rispetto della normativa della privacy.

Tutto ciò si rende possibile avviando un progetto di infrastruttura documentale centralizzata e definire una metodologia di integrazione graduale degli applicativi documentali che segua standard di interoperabilità.
ASC InSieme si è dotato dal 2023 un sistema di gestione "Protocollo e Atti" che permette una corretta gestione di documenti informatici, la cooperazione applicativa con i vari software verticali e la trasmissione verso il servizio di conservazione regionale (ParER).

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 ai sensi dell'art. 53, comma 5 DPR 445/2000.

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.

Il sistema inoltre:

a) consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
b) 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.

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.

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 46 del presente manuale di gestione.

L'architettura della sistema di gestione "Protocollo e Atti" La suite jEnte, utilizzata come sistema per la gestione documentale, possiede alcune applicazioni, tra le quali:

- "jEnte Atti" (per la gestione delle determinazioni dirigenziali, delibere Consiglio di Amministrazione)
- "jEnte Protocollo" (per la gestione del protocollo generale)
- "Albo Pretorio" (non in uso presso ASC InSieme)

jEnte è erogato ed usufruito come servizio cloud in modalità Software As A Service (SAAS). L'infrastruttura informatica erogante la suite è quindi demandata, gestita e garantita dal fornitore della suite Jente, Municipia, che agisce come cloud provider secondo i termini contrattuali di fornitura.
Questa scelta consente di avere un alto livello di disponibilità del servizio e di prevenire rischi che malfunzionamenti hardware o software impediscano al personale dell'Ente di utilizzare le applicazioni suddette.
L'applicativo di gestione del protocollo informatico sopra descritto è realizzato nel rispetto delle indicazioni fornite dalla normativa vigente, ed in particolare tenendo a riferimento quanto previsto dalle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

Sicurezza fisica dei documenti

La sicurezza fisica dei documenti ed i relativi backup sono demandati, gestiti e garantiti dal fornitore della suite Jente, Municipia che agisce come cloud provider secondo i termini contrattuali di fornitura della suite erogata in modalità Software As A Service (SAAS).

Conservazione dei documenti informatici

Le applicazioni "jEnte Atti" e "jEnte Protocollo" gestiscono l'invio in conservazione dei documenti informatici a PareER, (Polo archivistico regionale) in modalità "diretta" (connettore di jEnteProtocollo).

Accessibilità ai documenti informatici

Applicazioni che colloquiano sul sistema di gestione "Protocollo e Atti"

Le principali applicazioni verticali utilizzate per l'informatizzazione dei procedimenti amministrativi, che gestiscono o producono documenti informatici, sono state configurate per permettere la protocollazione in entrata ed in uscita dialogando con il sistema di protocollo utilizzando i relativi servizi web.

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.

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 (SIA) assicura la variazione sistematica delle password assegnate agli utenti per l'accesso alle funzioni del sistema di protocollo informatico con cadenza trimestrale.

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.

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, deve essere garantita 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
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.

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.

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

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.

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.