Piano della sicurezza

Il presente "Piano della sicurezza" riporta, ai sensi dell'art. 3.9 delle linee guida Agid le misure adottate per la formazione, la gestione, la trasmissione, l'interscambio, dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali, nel rispetto delle misure minime di sicurezza previste.

Definizioni

- **strumenti elettronici**: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- **autenticazione informatica**: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- **credenziali di autenticazione**: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- **parola chiave**: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- **profilo di autorizzazione**: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- **sistema di autorizzazione**: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Quadro normativo di riferimento

- art. 3.9 linee guida Agid – Misure sicurezza per gestione informatica dei documenti
- art. 32 GDPR – Sicurezza del trattamento
- art. 33-34 GDPR – violazione dei dati personali
- circolare del 18 aprile 2017, n. 2/2017 Agid - misure minime di sicurezza ICT

Misure di sicurezza e sistema di gestione dei rischi

La sicurezza è *"la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"* e dunque l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco.

Sono tre gli aspetti fondamentali relativi alla sicurezza delle informazioni del sistema informativo aziendale:

- **riservatezza:** solo gli utenti autorizzati possono accedere alle informazioni necessarie;
- **integrità:** protezione contro alterazioni o danneggiamenti; tutela dell'accuratezza e completezza dei dati;
- **disponibilità**: le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

L'approccio alla sicurezza avviene in una logica di prevenzione (*risk management*) piuttosto che in una logica di gestione delle emergenze o di semplice controllo/vigilanza.

Misure di sicurezza dei sistemi e di protezione dei dati

Le azioni necessarie per l'adozione di idonee misure di sicurezza riguardano:

a) la prevenzione: attività che permette di impedire gli accadimenti negativi, agendo direttamente sulla diminuzione delle probabilità di manifestazione dei pericoli;

b) la protezione: attività che permette di diminuire la gravità degli effetti causati eventualmente dall'accadimento dell'evento di pericolo;

c) la garanzia della continuità operativa.

Con specifico riferimento alla protezione dei dati personali, l'articolo 32 del GDPR sulla privacy prevede l'obbligo di adottare **misure di sicurezza**, che hanno lo scopo di ridurre al minimo i rischi derivanti dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Misure generali di sicurezza per la gestione documentale

Le misure generali, tecniche e organizzative, adottate dal Comune di Belforte del Chienti inerenti la gestione documentale sono le seguenti :

Garanzia	Rischio	Misura di protezione	Check
Riservatezza	Accesso abusivo ai dati	Sistema anti intrusione (firewall)	La Task adotta due sistemi di sicurezza perimetrali un IPS (Antiintrusione) sulla rete Internet, ed un sistema di Firewall Iptable nella rete Intranet)

		Sistema di autenticazione	Tutti i sistemi prevedono l'autenticazione con rinnovo delle password trimestrale e con password complesse.
Integrità	Modifica dei dati	Sistema di autorizzazione	Non tutti gli utenti possono accedere a tutti dati, ma ognuno di loro accede esclusivamente a quella serie di dati che deve trattare per svolgere le sue mansioni. Allo scopo, per ciascun utente, al momento della registrazione nel sistema di protocollo informatico Paleo, viene individuato e configurato un 'profilo utente', con il quale effettuare le sole operazioni di trattamento dei dati che le competono. Tali profili di autorizzazioni riproducono la struttura dell'ente. Una o più volte l'anno, la Task insieme al referente per il protocollo informatico dell'ente, verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione di ciascun utente.
		Antivirus	Tutti i sistemi sono dotati di antivirus aggiornato quotidianamente.
Disponibilità dei dati	Perdita dei dati	Copie di back up con cadenza giornaliera	I server sono sottoposti a backup giornaliero relativamente ai Dati contenuti e settimanale relativamente alla macchina virtuale intera.
	Continuità delle registrazioni	Registro di protocollo giornaliero	La predisposizione del registro di protocollo giornaliero, per gli enti che utilizzano il sistema di protocollo Paleo, è completamente automatica. Paleo prevede la procedura di generazione del registro Giornaliero con la chiusura del protocollo automatica e generazione della stampa di registro,

			avvertendo l'utente, tramite mail, dell'esito della procedura. Il registro di protocollo è incluso nell'insieme dei dati sottoposto a back up giornaliero e settimanale.
	Mancanza di alimentazione	Gruppo di continuità	L'intera sala macchine è sotto Gruppo di continuità che ne garantisce il funzionamento anche in assenza di corrente per almeno 4 ore.
		Ridondanza	I gruppi di continuità sono ridondati, in caso di rottura di un Gruppo ne entra in funzione uno esattamente uguale.

Sicurezza nella formazione dei documenti

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici gestiscono:
· l'identificabilità del Comune di Belforte del Chienti, del Servizio/Ufficio che ha formato il documento;
· la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi della normativa vigente;
· 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 (adozione di formati aperti);
· l'interscambiabilità (interoperabilità) dei documenti con altre amministrazioni.
Per attribuire in modo certo la titolarità del documento, la sua integrità, la sua riservatezza e la validazione temporale, il documento è sottoscritto con firma digitale.

Sicurezza nella gestione dei documenti informatici

Il sistema che ospita i documenti informatici è configurato in modo tale da consentire:
· l'accesso esclusivo e tracciato (normativa relativa agli Amministratori di Sistema) al server del sistema informatico di protocollo e gestione documentale da parte del servizio Segreteria, in modo che qualsiasi altro utente non autorizzato non possa accedere ai documenti al di fuori del sistema di gestione documentale;
· accesso consentito, su specifica richiesta e tracciato, alla software house produttrice del programma, che gestisce l'assistenza applicativa in caso di interventi da remoto.
· la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso.

Sicurezza nella trasmissione dei documenti informatici

Come previsto dalla normativa vigente in materia di amministrazione digitale, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Il sistema informatico di protocollo e gestione documentale svolge anche le seguenti operazioni:
· accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
· tracciamento delle attività nel file di log della posta;
· gestione automatica delle ricevute di ritorno.
· verifica delle firme digitali;
Per garantire al soggetto ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata di norma la firma digitale con la posta elettronica certificata a disposizione dei soggetti coinvolti nello scambio dei messaggi.

Sicurezza nell'accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso nominali (utente e password) 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 sistema informatico di protocollo e gestione documentale.
Con specifico riferimento all'accesso e alle operazioni sui documenti, il sistema informatico di protocollo e gestione documentale:
· 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 e l'individuazione del suo autore (storia della scheda documentale).
Le password di accesso al sistema sono gestite all'interno di una struttura dati crittografata e accessibile soltanto da un processo di sistema.

Politiche di sicurezza adottate

Le politiche illustrate sono correlate alle responsabilità dirigenziali e dei dipendenti che sono adottate in caso di riscontrata violazione delle prescrizioni dettate in materia di gestione della visibilità e di accesso in sicurezza ai documenti informatici da parte di tutti gli utenti che, a qualunque titolo, interagiscono con il sistema informatico di protocollo e gestione documentale.
Il Responsabile della gestione documentale o suoi delegati, d'intesa con i responsabili della sicurezza e della tutela dei dati personali, procede al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.
Il riesame delle politiche di sicurezza è conseguente al verificarsi dei seguenti casi:
· incidenti di sicurezza;
· variazioni tecnologiche significative;
· modifiche all'architettura informatica che potrebbero incidere sugli obiettivi o sul livello di sicurezza complessiva;
· aggiornamenti delle prescrizioni normative;
· risultati delle attività di audit interni.
Di norma, tale attività è svolta con cadenza annuale.

Manutenzione ordinaria ed aggiornamenti

Allo scopo di garantire la continuità del servizio, si prevede un piano di manutenzione programmata del sistema utilizzato, che ne riduce al minimo le alterazioni e ne preserva la funzionalità.
In assenza di specifiche inefficienze, l'aggiornamento del software è rilasciato per rispondere ad esigenze frutto di modifiche o novità in ambito normativo.