Piano di sicurezza

Allegato 8 al Manuale di gestione flusso documentale

Sommario

Premessa

Il presente piano di sicurezza, adottato ai sensi dell'art. 4, comma 1, lettera c), del DPCM 3/12/2013 "Regole tecniche per il protocollo informatico", descrive le politiche adottate da questo Comune affinché:

- i documenti e le informazioni trattati dall'Ente siano sempre disponibili, integri e rimangano 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.

A tali fini, l'art. 7 del suddetto DPCM, individua i **requisiti minimi di sicurezza** dei sistemi di protocollo informatico a cui il presente piano si conforma.

Il piano di sicurezza, in base ai rischi cui sono esposti i dati (personali e non) e/o i documenti trattati, definisce:

- le **politiche generali** e particolari di sicurezza da adottare all'interno del Comune;
- le **modalità di accesso** al Sistema di Gestione Informatica dei Documenti (Sistema Halley);
- gli **interventi operativi** adottati sotto il profilo **organizzativo, procedurale e tecnico**, con particolare riferimento alle *misure minime di sicurezza*, di cui alla normativa cogente in materia di protezione dei dati personali, in caso di trattamento di dati personali, sensibili o giudiziari;
- la formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia delle misure di sicurezza.

Il piano di sicurezza è soggetto a revisione con cadenza almeno biennale; a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche, potrà essere modificato anticipatamente.

Elementi di rischio cui sono soggetti documenti e dati contenuti nel Sistema

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'ausilio delle tecnologie informatiche sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato, sia esso inteso come accesso al Sistema o come accesso ai documenti, dati e unità archivistiche in esso contenuti;
- cancellazione o manomissione dei documenti e dei dati, includendo a tale proposito tutti i dati archiviati all'interno del Sistema;
- perdita dei documenti e dei dati contenuti nel Sistema;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, questo Comune adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Accesso al Sistema e ai documenti e dati in esso contenuti da parte di utenti interni all'ente

L'accesso al Sistema di Gestione Informatica dei Documenti da parte degli utenti interni all'ente avviene attraverso l'utilizzo di credenziali di autenticazione; i profili di abilitazione alle funzionalità del Sistema stesso sono attribuiti a ciascun utente sulla base di quanto stabilito dal Manuale di Gestione Flusso Documentale. L'accesso ai documenti e ai dati presenti sul Sistema è definito in base al ruolo che ricopre l'utente.

- Nel file server sono presenti diverse *condivisioni* accessibili solo ad utenti appartenenti a gruppi autorizzati. Generalmente condivisioni e gruppi coincidono con i settori del comune o d ambiti trasversali ad utenti appartenenti a settori diversi.
- Nei gestionali (Halley, ecc.) gli utenti sono profilati in base a ruoli e uffici di appartenenza.

Le credenziali di autenticazione consistono in un codice (User-Id), per l'identificazione dell'incaricato, associato ad una password, conosciuta solamente dal medesimo.

Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della Password; quest'ultima è composta di almeno 8 caratteri (di cui almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale). La Password è modificata dall'incaricato al suo primo utilizzo e, successivamente, ogni 3 mesi.

Qualora il titolare delle credenziali di autenticazione dimenticasse la propria password si procederà all'assegnazione di una nuova chiave di accesso provvisoria che dovrà essere cambiata al primo accesso.

Accesso al trattamento di dati personali sensibili o giudiziari e politiche di sicurezza espressamente previste

L'accesso ai documenti contenenti dati personali, sensibili o giudiziari e ai dati medesimi avviene per mezzo dell'individuazione di specifici profili di autorizzazione, stabiliti sulla base al ruolo dell'incaricato; tali profili, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento.

Trattamento dei dati personali, sensibili o giudiziari senza l'ausilio di strumenti elettronici

I documenti sono controllati e custoditi dagli incaricati del trattamento per tutto il tempo di

svolgimento dei relativi compiti; nell'arco di tale periodo gli incaricati si assicureranno che a tali documenti non accedano persone prive di autorizzazione.
Gli archivi contenenti dati sensibili o giudiziari sono conservati sotto chiave e l'accesso è consentito solo previa autorizzazione.

Formazione dei documenti

I documenti informatici del Comune di Sant'Angelo in Vado sono prodotti utilizzando i formati previsti dal DPCM 3/12/2013 (*Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*) .

L'apposizione della firma digitale, volta a garantire l'attribuzione certa della titolarità del documento e la sua integrità, avviene previa conversione in un formato, tra quelli previsti dal suddetto DPCM, che garantisca la leggibilità, l'interscambiabilità, la non alterabilità, l'immutabilità nel tempo del contenuto e della struttura del documento medesimo (ad esempio il PDF-A); l'eventuale acquisizione mediante scansione dei documenti analogici avverrà in uno dei formati avente le medesime caratteristiche.
L'apposizione della firma digitale o di altre eventuali sottoscrizioni elettroniche, nonché la validazione temporale del documento sottoscritto digitalmente avvengono in conformità di quanto sancito dalle regole tecniche contenute nel DPCM 22/02/2013 (*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*), emanate ai sensi dell'art. 71 del D. Lgs. 82/05.
La sottoscrizione del documento con firma digitale avviene prima dell'effettuazione della registrazione di protocollo.

Sicurezza delle registrazioni di protocollo

L'accesso al registro di protocollo al fine di effettuare le registrazioni o di apportare modifiche è consentito soltanto al personale abilitato.
Di norma i dipendenti che operano nell'ambito dei vari uffici sono abilitati ad accedere esclusivamente ai dati di protocollo dei documenti da essi prodotti, ad essi assegnati o di competenza del proprio ufficio di riferimento.
Ogni registrazione di protocollo viene memorizzata dal Sistema di Gestione Informatica dei Documenti, unitamente all'identificativo univoco dell'autore che l'ha eseguita e alla data e all'ora della stessa.
Eventuali modifiche, vengono registrate per mezzo di log di sistema che mantengono traccia dell'autore, della modifica effettuata, nonché della data e dell'ora; il Sistema mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione.
Il Sistema non consente la modifica del numero e della data di protocollo; in tal caso l'unica possibile modifica è l'annullamento della registrazione stessa di cui, analogamente al caso precedente, il Sistema manterrà traccia. L'annullamento di una registrazione di protocollo deve sempre essere accompagnata da autorizzazione scritta del Responsabile della gestione documentale e il Sistema

deve recare, in corrispondenza della registrazione annullata, gli estremi del provvedimento di autorizzazione.
Al fine di garantire l'immodificabilità delle registrazioni di protocollo, il Sistema permette, al termine della giornata lavorativa, la produzione del registro giornaliero delle registrazioni di protocollo, in formato digitale; tale registro, formato nel rispetto di quanto previsto nel manuale di conservazione, sarà trasferito nell'arco della giornata lavorativa successiva, alla struttura di conservazione accreditata di cui il Comune si serve.

Gestione dei documenti e sicurezza logica del Sistema

Il Sistema consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il Sistema effettua, inoltre, il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.
Il Sistema e tutti i documenti e dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici mediante l'attivazione di software antivirus e firewall.
Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dall'ente, vengono costantemente tenuti aggiornati, per mezzo dell'istallazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Backup e ripristino dell'accesso ai dati

Il servizio BB è il servizio base offerto per la esternalizzazione della gestione del server. Esso comprende il costante e continuo monitoraggio, da remoto tramite un apposito pannello di controllo (Dashboard), che evidenzia lo stato di funzionamento dei servizi offerti realizzato tramite un apparato dedicato, chiamato concentratore, che permette di avere hardware e software sempre aggiornati.
Sono incluse l'esecuzione giornaliera delle copie dati effettua automaticamente di notte sull'hard disk interno e sul supporto magnetico esterno (NAS o hard disk) presso l'Ente e gli aggiornamenti degli applicativi software.
La procedura di esecuzione dei backup quotidiani settimanali mensili e annuali consente comunque di avere un archivio storico di 60 giorni, consultabile in modo retroattivo ogni giorno, con esecuzione programmata di controlli remoti di corretta effettuazione e integrità delle copie.
Il Servizio di DR non è incluso ma acquistabile separatamente e prevede una copia remota, giornaliera ed automatica dei programmi e dei dati Halley, e/o dei dati che l'Ente sceglie di inserire nell'apposita cartella denominata "Disaster Recovery" fornita in abbinamento con il Servizio Storage (dati non Halley), trasferite e conservate in modalità cifrata con garanzia di fruibilità ed utilizzabilità dei dati e dei programmi contenuti nei Datacenter di Matelica e/o Roma, con una latenza massima di allineamento di 8 ore lavorative precedenti alla rilevazione del disastro o di altra esigenza di recupero dati.

Conservazione dei documenti

I documenti informatici registrati sul Sistema sono affidati per la conservazione digitale al Polo di

Conservazione DIGIP della Regione Marche, soggetto conservatore accreditato ai sensi del DPCM 03/12/2013 "regole tecniche per il sistema di conservazione".
Il trasferimento in conservazione avviene in automatico con cadenza giornaliera direttamente tramite il Sistema Halley.

Disaster recovery e continuità operativa

Il Comune di Sant'Angelo in Vado, conformemente a quanto disposto dall'art. 50 -bis del D. Lgs. 82/05, **prevede di dotarsi** di un piano di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività, definendo a tali fini il piano di continuità operativa e quello di disaster recovey.
In caso gravi danni al sistema locale sarà possibile accedere alla copia remota del server e in seguito ripristinare il sistema locale.

Accesso di Utenti esterni al Sistema

L'esercizio del diritto di accesso da parte di utenti esterni al Sistema viene effettuato nel rispetto di quanto sancito dalla legge 241/90 e del D. Lgs. 196/03.
Qualora l'utente esterno decida di esercitare il proprio diritto di accesso rivolgendosi direttamente all'URP o ad altro sportello allo scopo predisposto, la consultazione deve avvenire in modo che siano resi visibili soltanto dati o notizie che riguardino il soggetto interessato ed adottando gli opportuni accorgimenti volti ad evitare la diffusione di informazioni di carattere personale.

Piani formativi del personale

Ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, il Comune predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo applicativi software per la gestione dei documenti informatici;
- utilizzo del Sistema di Gestione Informatica dei Documenti;
- fascicolazione dei documenti informatici;
- gestione dei fascicoli informatici;
- aggiornamento sui temi suddetti.

Monitoraggio periodico del funzionamento del Sistema

Il Responsabile della gestione documentale dell'Ente effettua periodiche verifiche sul corretto funzionamento del Sistema di Gestione Informatica dei Documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale.