Sommario

1.Piano di Sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dal Comune della Spezia siano resi disponibili, autentici e integri;
- i dati personali, i dati sensibili e quelli giudiziari vengono custoditi in modo da ridurre al minimo i rischi di distruzione o perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il piano di sicurezza, basato sui risultati dell'analisi dei rischi a cui sono esposti i dati personali e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno del Comune della Spezia;
- le modalità di accesso al sistema di protocollo e gestione documentale;
- le misure di sicurezza operative adottate sotto il profilo organizzativo, procedurale e tecnico;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Al fine di garantire la sicurezza dell'impianto tecnologico, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, il Comune della Spezia ha adottato le misure tecniche e organizzative di seguito specificate:

- protezione periferica dell'intranet dell'Amministrazione;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- piano di continuità del servizio che prevede:
    - l'esecuzione e la gestione delle copie di riserva dei dati e dei documenti effettuate con modalità sincrona e cadenza giornaliera;
    - la capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione, a cura dei Servizi informatici, delle copie di riserva dei dati e dei documenti, in locali diversi e lontani da quelli in cui è installato il sistema di elaborazione di esercizio;
- gestione delle situazioni di emergenza informatica attraverso risorse qualificate;
- impiego e manutenzione di un adeguato sistema antivirus;
- uso di soluzioni volte a rendere inintelligibili, a chi non è autorizzato ad accedervi, le particolari categorie di dati personali contenuti in elenchi, registri o banche di dati;
- impiego di adeguate misure di sicurezza anche nel caso di supporti analogici contenenti categorie particolari di dati;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultabili in caso di necessità per controlli da parte delle autorità competenti.

1.1 Gestione dei documenti informatici - Aspetti di sicurezza

I documenti del Comune della Spezia vengono gestiti attraverso il sistema di protocollo e gestione documentale p@doc, conforme alle specifiche previste dalla classe ITSEC F−C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata, in uscita e interni
- 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;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

1.1.1. Componente organizzativa della sicurezza

Tale componente consiste nella definizione di una struttura operativa dedicata alla gestione della sicurezza nell'ambito delle attività svolte dal sistema informatico p@doc.

In tale contesto la gestione della sicurezza si realizza con specifici interventi tecnici e organizzativi finalizzati a prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia e con attività di controllo e verifica essenziali ad assicurare l'eficacia nel tempo del sistema informatico.

Conseguentemente vengono adottate le seguenti misure di sicurezza, la cui competenza è posta a carico dei seguenti settori del Comune della Spezia:

Misure di sicurezza	Settore responsabile dei controlli
Sicurezza Fisica e infrastrutturale	- Lavori pubblici - Servizi Informatici
Sicurezza Logica	-Servizi Informatici

1.1.2 Componente fisica e infrastrutturale della sicurezza

La sicurezza fisica degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informativo è garantita dalle seguenti misure:

- porte blindate;
- armadi ignifughi;
- impianti elettrici dedicati;

- sistemi di condizionamento per il raffreddamento delle apparecchiature;
- gruppo di continuità elettrica;
- controllo periodico su efficienza del gruppo elettrogeno;
- estintori;
- piano di verifica periodica sull'efficacia dei sistemi di sorveglianza e degli estintori;
- impianto antincendio nella sala macchine presso i Servizi Informatici;
- accesso ai locali mediante sistema d'autenticazione tramite badge e chiave;
- impianto antintrusione autonomo per gli accessi al locale sala macchine.

1.1.3 Componente logica della sicurezza

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.

Tale componente, nell'ambito del sistema di gestione documentale, si realizza attraverso:

- identificazione e autenticazione utente;
- profilazione degli accessi (ACL);
- politica antivirus;
- firma digitale;
- monitoraggio sessioni di lavoro;
- disponibilità del software e dell'hardware;
- backup dei dati.

Nello specifico, p@doc è una *web-application* e come tale presenta una architettura di tipo *client-server*.

Il software è progettato e sviluppato secondo l'architettura *three-tier* (a tre livelli) che prevede la suddivisione dell'applicazione in tre diversi moduli (livelli):

1. interfaccia utente
2. logica funzionale/*business logic* (*application server*)
3. dati persistenti (*database* / *repository file*)

Le possibili interazioni fra i livelli sono vincolate secondo quanto segue:

- interfaccia utente ✕ logica funzionale
- logica funzionale ✕ dati persistenti

Il livello "interfaccia utente" non può quindi relazionarsi direttamente con il livello "dati persistenti" (e viceversa).
Gli utenti (*clients*) usufruiscono dell'applicazione interagendo con l'interfaccia utente per mezzo di un *browser* installato nella propria postazione di lavoro (PdL) e della rete locale (intranet) del Comune della Spezia.
Il software (logica funzionale) e le informazioni gestite (dati persistenti) risiedono in un sistema centralizzato presso i Servizi Informatici e costituito da server dedicati e sostanzialmente specializzati nelle seguenti funzioni:

- *application server;*

- *DBMS;*
- *repository file.*

Tale architettura permette di aumentare la modularità ed il livello di sicurezza del sistema.

L'utilizzo delle PdL e della rete intranet è garantito ai soli utenti dotati di credenziali d'accesso (user ID + password) al sistema informatico del Comune della Spezia.
L'operatore può accedere unicamente al livello "interfaccia utente" e solamente se dotato di specifiche autorizzazioni di accesso al sistema p@doc.
L'interfaccia viene generata in funzione delle autorizzazioni in possesso dell'utente connesso; funzioni e dati ai quali l'utente non è autorizzato ad accedere non vengono resi disponibili.

Agli utenti "generici" del Comune della Spezia non è quindi consentito:

- interrogare direttamente il DBMS;
- interagire direttamente con il repository dei file;
- accedere direttamente ai server fisici e virtualizzati.

Le precedenti operazioni sono possibili ai soli soggetti autorizzati ed appartenenti ai Servizi Informatici per le sole attività sistemistiche di amministrazione, aggiornamento e manutenzione delle componenti di sistema.

Nessun sistema, componente, servizio ed interfaccia inerente al sistema p@doc è direttamente accessibile e fruibile dalla rete pubblica *internet*.

1.2 Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) − presenti o transitati su p@doc o altri indipendenti sistemi di supporto − che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza possono essere costituite:

- 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 di p@doc.

Le registrazioni di sicurezza sono soggette alle seguenti misure:

- scrittura su database in modalità asincrona (scrittura logica che coincide con scrittura fisica sul disco);
- copie di backup realizzate su dischi RAID in mirroring e RAID 5;
- consegna di una copia di sicurezza dei back up in un locale diverso come previsto dalla normativa;
- accesso alle registrazioni limitato esclusivamente agli amministratori di sistema del sistema di protocollo, al Responsabile della gestione documentale e ai soggetti istruiti e autorizzati;
- conservazione dei supporti con le registrazioni di sicurezza all'interno di un locale con accesso limitato ai soli addetti.

1.3 Criteri di utilizzo degli strumenti tecnologici

Il sistema informatico garantisce agli utenti interni del Comune della Spezia l'accesso ai servizi previsti, mediante l'adozione di un insieme dei seguenti principi:

- ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi e dei programmi a cui ha accesso, nonché dei dati trattati ai fini istituzionali;
- ogni utente è responsabile, civilmente e penalmente, del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali, anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio e della normativa per la tutela dei dati personali;
- ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico;
- i dati archiviati informaticamente devono essere esclusivamente quelli attinenti alle proprie attività lavorative;
- la tutela dei dati archiviati su personal computer che gestiscono localmente documenti e/o dati è demandata all'utente finale, il quale dovrà effettuare con frequenza opportuna i salvataggi su supporti dedicati ed idonei, nonché la conservazione degli stessi in luoghi adatti;
- tutti i dati sensibili riprodotti su supporti informatici devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da terzi. Altrettanta cautela deve essere riposta in fase di stampa dei documenti contenenti dati sensibili: la stampa va effettuata su stampanti presidiate dall'addetto;
- l'account del sistema p@doc è costituito da un codice identificativo personale (username) e da una parola chiave (password);
- la password che viene associata a ciascun utente è personale, non cedibile e non divulgabile.