COMUNE DI SANTO STEFANO IN ASPROMONTE

Città Metropolitana di Reggio Calabria

Allegato 8
Piano di sicurezza informatica

Manuale di gestione documentale dell'archivio e del protocollo

Allegato 8 – Piano di sicurezza informatica

Premessa

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dal Comune per lo snellimento, l'ottimizzazione e una maggiore efficienza dei procedimenti amministrativi, comporta una serie di rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi. Tali rischi sono imputabili a due fattori caratteristici della tecnologia in questione: la non garanzia di corretto funzionamento sia nelle componenti hardware che in quelle software e l'esposizione alle intrusioni informatiche. In termini più operativi è bene intendere la sicurezza del Sistema Informativo non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali" ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".

Si evidenzia che la sicurezza del Sistema Informativo non dipende solo da aspetti tecnici ma anche, se non principalmente, da quelli organizzativi, sociali e legali. La sicurezza del Sistema Informativo è pertanto vista come caratteristica "globale", in grado di fornire dinamicamente, con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei servizi erogati.

Il presente Piano descrive le misure di sicurezza adottate con lo scopo di poter stabilire, attuare, mantenere e migliorare in modo continuo il sistema di gestione per la sicurezza delle informazioni.

Sono pertanto elencate le strategie ed i controlli adottati per assicurare al Sistema Informativo Comunale un adeguato livello di sicurezza.

Il presente Piano della Sicurezza (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) del Comune di Santo Stefano in Aspromonte.

Il sistema di gestione della sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità delle informazioni mediante l'applicazione di un processo di gestione del rischio e dà fiducia alle parti interessate sull'adeguatezza della gestione dei rischi.

Obiettivi

Scopo del presente documento è descrivere la strategia che il Comune intende adottare per poter soddisfare i seguenti requisiti di sicurezza:

Confidenzialità: l'accesso e la divulgazione delle informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, la probabilità che un'informazione riservata sia resa pubblica.

Integrità: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, le probabilità che l'informazione sia in qualche modo modificata. Devono essere altresì garantiti sia l'origine del dato (non ripudiabilità) che la sua conformità all'originale (autenticità).

Disponibilità: l'accesso all'informazione e ai sistemi deve essere sempre affidabile e tempestivo. Una perdita di disponibilità si verifica quando a fronte di un'intrusione un sistema diventa non più accessibile da parte

degli utenti, ovvero quando parte o tutte le informazioni in esso contenute vengono distrutte e/o rese inaccessibili.
Accountability (Tracciabilità): tutte le azioni che un'entità compie nell'ambito del sistema sono memorizzate in modo tale da poter essere, in tempi successivi, ricondotte in maniera inequivocabile all'entità stessa.

L'adozione di idonee e preventive misure di sicurezza garantisce che il trattamento dei dati personali comuni identificativi, sensibili e/o giudiziari venga effettuato 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, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

IL PIANO DI SICUREZZA
Le Pubbliche Amministrazioni, nell'ottica di sviluppare concretamente il Sistema di gestione informatica dei documenti, devono predisporre: "Il Piano per la sicurezza informatica relativo alla formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici.
Il suddetto Piano deve essere predisposto dal Responsabile della gestione documentale, d'intesa con il Responsabile della conservazione, il Responsabile dei sistemi informativi e il Responsabile del trattamento dei dati personali.
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 toccati dal documento sono:

- La descrizione delle risorse e delle configurazioni del sistema informatico e delle politiche di sicurezza in essere e delle responsabilità che ricadono su di esse.
- La valutazione delle minacce (analisi dei rischi), e delle vulnerabilità che incombono o possono incombere sulle risorse e configurazioni del sistema.
- La gestione del rischio, cioè le azioni adottate o da adottare al fine di determinare il giusto livello di sicurezza da perseguire.

Revisione e modifica del piano di sicurezza
Il presente Piano è soggetto a revisione, in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza.

Revisione e modifica delle politiche di sicurezza
Tutta la documentazione, ed in particolare le politiche di sicurezza, vengono riesaminate periodicamente mediante un'apposita pianificazione o quando al verificarsi di cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.
Il riesame comprende una valutazione delle opportunità di miglioramento delle politiche dell'organizzazione e dell'approccio alla gestione della sicurezza delle informazioni in risposta ai cambiamenti dell'ambiente organizzativo, dei servizi erogati, delle clausole legali o dell'ambiente tecnico.

Revisione delle politiche non pianificate vengono effettuate nei seguenti casi:

- Verificarsi di incidenti di sicurezza;
- Variazioni tecnologiche significative;
- modifiche all'architettura del sistema informatico;
- aggiornamenti delle prescrizioni normative;
- risultati delle eventuali attività di audit interni.

Componenti e configurazioni del sistema informativo Comunale

In questo paragrafo vengono descritte le risorse e le configurazioni in essere che compongono o supportano il sistema informatico.

4.1 Tipologia di servizi offerti

Il Sistema Informativo del Comune di Santo Stefano in Aspromonte è rivolto a soddisfare tutte le esigenze di carattere informativo- informatico, sia dal punto di vista delle esigenze "*interne*" cioè sostanzialmente provenienti dai servizi interni all'amministrazione stessa sia, quasi sempre indirettamente, provenienti dall'utenza della popolazione residente esterna all'amministrazione.

Nell'uno e nell'altro caso l'esigenza può essere soddisfatta o da un sistema effettivamente interno, fisicamente residente presso sistemi informativi strettamente Comunali, oppure tramite un sistema esterno, reso disponibile da altri enti e al Comune stesso accessibile con le opportune modalità.

4.2 Organizzazione

Ogni dipendente del Comune di Santo Stefano in Aspromonte deve collaborare, secondo le proprie specifiche funzioni, alla gestione del Sistema Informativo e alla gestione generale della sicurezza.

Tipologia Utenti	Compiti/Responsabilità	Note
Addetti società assistenza hardware e software	Attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alla sicurezza).	Vedi nomine ad Amministratore di Sistema
Dipendenti Comunali	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dei dati	Vedi incarichi specifici a Responsabile o incaricato del trattamento nei settori specifici

Nel contesto del Sistema Informativo ogni dipendente del Comune di Santo Stefano in Aspromonte è, in varia misura e con compiti diversi, corresponsabile del Sistema Informativo nel suo complesso. Per quanto concerne la gestione vera e propria della progettazione ed implementazione delle politiche di sicurezza informatica, si precisa che dovrà essere incaricata una società esterna specializzata in tale settore (non disponendo di personale adeguatamente formato al proprio interno), la quale svolge anche attività di assistenza hardware e software.

L'Ente ha adottato apposite politiche di sicurezza dei dati personali sia per il Servizio Informatico che per l'utilizzo dei dispositivi informatici da parte dei dipendenti e/o collaboratori.

4.3 Caratteristiche di sedi e locali

Il Comune di Santo Stefano in Aspromonte è composto da una sede presso la quale sono ospitati gli uffici dell'Ente. Le porte di ingresso agli uffici vengono chiuse quando non presidiate.

4.4 Infrastruttura tecnologica

L'Infrastruttura Tecnologica del Comune di Santo Stefano in Aspromonte può essere schematizzata come segue.

Tipologia di apparati	Descrizione
Apparati Server interni	Indichiamo in questa categoria tutti gli ambienti server di proprietà comunale o comunque gestiti direttamente, sia fisici che virtuali; tutti gli apparati server interni sono dislocati presso il locale Server Comunale
Apparati Server Esterni	Indichiamo in questa categoria tutti gli ambienti server, sia fisici che virtuali, gestiti da società o enti esterni, in virtù di contratti stipulati con il Comune
Apparati di Rete	Indichiamo in questa categoria tutti gli apparati (router, switch, etc.) che concorrono alla connettività fra gli ufficii Comunali (connettività interna), da e verso Internet (connettività pubblica verso l'esterno)
Apparati Storage, di Backup e Sicurezza	Indichiamo in questa categoria tutti gli apparati che concorrono specificatamente alla sicurezza ed alla protezione dei dati (storage per backup, apparati firewall)
Infrastruttura di Comunicazione	Intendiamo con questo termine l'insieme delle cablature che realizzano, per ogni sede, la connettività LAN, nonché l'infrastruttura di comunicazione fra le sedi (WAN), da e verso Internet
Apparati Client	In questa categoria raggruppiamo tutti gli apparati (PC, Notebook, etc.) utilizzati dall'utenza interna per la normale attività o in connettività mobile (telelavoro) per l'espletamento delle specifiche funzioni

4.5 Locale CED e componenti server

Tutti i server sono posizionati all'interno di un apposito armadio Rack chiuso a chiave, che a sua volta risiede all'interno di un apposito locale adibito a CED.
Il Servizio Informatico, composto dal Responsabile e referente interno dell'Ente, insieme alla società esterna specializzata a cui è stata affidata la consulenza e gestione del sistema informatico (d'ora in avanti Servizio Informatico), mantiene l'elenco dei server e dei dispositivi attivi presso l'Ente e lo aggiorna in caso di variazione, controllandone periodicamente lo stato e la correttezza al fine di garantirne l'affidabilità e la corrispondenza alla situazione esistente, specificando se i server presentano caratteristiche di sicurezza e continuità di mantiene la documentazione descrittiva.
L'ente inoltre ha dotato la parte server di gruppi di continuità, in modo da permettere la tenuta o lo spegnimento controllato dei dispositivi ad essi collegati in caso di mancanza di energia elettrica.

4.6 Connettività

La gestione delle linee dati è affidata all'operatore di settore, che ne tiene costantemente monitorato lo stato e ne tiene aggiornato l'elenco.
Tale elenco contiene la descrizione e le caratteristiche di ogni linea, le informazioni riguardo il fornitore che ne cura la manutenzione e gli eventuali dettagli contrattuali rilevanti, insieme alle eventuali specifiche di sicurezza.

4. 7 Archivi

Il Servizio Informatico tiene monitorato l'aggiornamento degli archivi e delle banche dati dell'Ente. In un elenco aggiorna le informazioni rilevanti e caratteristiche di ogni banca dati quali: funzione, fornitore, ubicazione, metodologie di backup, effettuando quindi verifiche di attendibilità e correttezza dell'elenco attraverso controlli a campione o verifiche complete.

4.8 Posta elettronica

Le caselle di posta elettronica sono gestite tramite un servizio di fornitura.
La creazione di una nuova casella avviene tramite apposita richiesta al Servizio Informatico, in seguito alla compilazione di modulistica concordata o attraverso comunicazione ufficiale su altri canali (cartacea, email).

4.9 Posta elettronica certificata

Anche le caselle di PEC sono gestite tramite un servizio di fornitura esterno.
Le caselle, rilasciate dal fornitore accreditato, sono direttamente integrate al software di protocollo informatico e fatturazione elettronica, quindi, il backup dei messaggi avviene seguendo il naturale percorso di integrazione con le procedure dell'ente.
La continuità operativa e la manutenzione del servizio sono gestite a livello contrattuale con il fornitore.

4.1O Sicurezza perimetrale

Il sistema informatico dell'ente è protetto tramite l'utilizzo di un firewall di rete dotato di servizi UTP, appositamente configurati per gestire la sicurezza perimetrale e per il controllo del traffico attraverso la configurazione dei servizi di Web e DNS Filtering, Application Contrai, lntrusion Pervention, etc.
Anche le configurazioni del firewall sono mantenute dal Servizio Informatico che ne effettua una copia prima di ogni modifica, oltre a prevedere e pianificare gli aggiornamenti e tenerne monitorato il corretto

funzionamento.

4.11 Sistemi di protezione da malware

Presso le postazioni di lavoro e i server dell'ente è installato e attivo un sistema di End Point Protection.
Tale software viene gestito a livello centralizzato attraverso un servizio SaaS in Cloud dal Servizio Informatico, che ne cura gli aggiornamenti, le installazioni sulle postazioni ed il monitoring delle segnalazioni e dei risultati delle scansioni.
In occasione di criticità relativa a virus o malware il Servizio Informatico convenzionato adotta le azioni opportune ed effettua le comunicazioni del caso, sia a livello di formazione che di consapevolezza.

4.12 Sistemi e politiche di backup

La gestione dei backup viene effettuata dal Servizio Informatico, per ciò che riguarda i dati che risiedono presso l'ente, e dai fornitori esterni per i servizi dati in concessione esterna o su cloud.
L'ente mantiene l'elenco delle risorse sottoposte a backup e delle relative procedure adottate per l'esecuzione delle copie di salvataggio, oltre ad effettuare verifiche giornaliere della corretta esecuzione dei processi di backup ed effettuare una verifica periodica della correttezza delle impostazioni dei sistemi di backup e della adeguatezza dei processi di backup.
Periodicamente viene effettuato un riesame delle risorse sottoposte a backup, in modo da assicurare che venga salvata la totalità dei dati facenti parte del sistema informatico.
La definizione ed il mantenimento di quali sono i dati facenti parte del sistema spetta al Servizio Informatico.
I backup vengono effettuati con cadenza giornaliera presso supporti di rete e su servizi esterni offline in Cloud.

4.13 Log e tracciamento delle attività

Il Servizio Informatico, tramite apposite richieste ai fornitori deve poter accedere ai log generati da applicativi, sistemi operativi e apparati specifici, disciplinati attraverso una specifica politica che regola i tempi e le modalità di creazione, gestione, eliminazione salvataggio e conservazione, nonché una specifica procedura che determini le modalità ed i tempi di definizione delle analisi e delle modalità di salvataggio e conservazione dei log delle nuove risorse messe a disposizione dall'ente .
Periodicamente il Servizio Informatico deve effettuare un riesame dell'elenco dei log e delle procedure adottate per la loro gestione.

4.14 Accesso logico alle reti e ai sistemi

L'accesso alla rete può avvenire esclusivamente tramite un processo di autenticazione che prevede un nome utente ed una password. La password è composta da almeno otto caratteri alfanumerici, essa non deve contenere riferimenti agevolmente riconducibili all'assegnatario.
Il Servizio informatico gestisce l'assegnazione delle password di accesso al sistema informatico. Nome utente e password sono strettamente personali. L'utente è tenuto a:

- Non comunicare a terzi la password
- A non annotare la password su supporti posti in vicinanza della propria postazione di lavoro o comunque incustoditi.

Tutte le password devono essere cambiate ogni 90 giorni.
In caso di assenza, anche temporanea, del personale incaricato dei trattamenti dei dati, sui P.C. devono essere chiuse le procedure di accesso ai dati o attivato il blocco attraverso lo screen saver con password.

Le credenziali di accesso ai sistemi informatici sono rilasciate su richiesta che avviene tramite la compilazione di moduli specifici a seconda dei servizi per i quali si richiede l'accesso. I processi di autorizzazione e di revoca sono illustrati ai paragrafi successivi.

4.15 Sistemi di autenticazione

Gli utenti autorizzati accedono alle risorse informative dell'Ente tramite diversi livelli di autenticazione, a seconda dei privilegi autorizzativi che vengono loro rilasciati.
In generale, l'accesso alle postazioni di lavoro, ai sistemi di navigazione internet e ai documenti residenti sul file server (cartelle di rete condivise), viene disciplinato in fase di rilascio delle credenziali da parte del Servizio Informatico, previa apposita richiesta fatta pervenire dal Responsabile di servizio o settore, nella quale vengono specificate, anche in maniera implicita, le funzioni dell'utente.

4.16 Modalità di accesso remoto

Il servizio informatico si occupa della gestione e del controllo degli accessi effettuati da terze parti e manutentori esterni del sistema informatico.
Le autorizzazioni di accesso vengono definite in sede contrattuale e vengono effettuate le apposite nomine in caso di accesso con profili di amministrazione .
Di volta in volta, in base alle specifiche attività da effettuare il Servizio Informatico autorizza l'accesso alle risorse, fisiche e logiche, del sistema informatico con credenziali identificate e con livelli di autorizzazione minimi per l'attività che deve essere effettuata.

4.17 Telelavoro

La modalità del telelavoro è abilitata in casi di emergenza o a seguito dell'attivazione di particolari progetti, per il periodo di tempo stabilito dall'emergenza o dai progetti stessi. Il Servizio Informatico, nei casi di telelavoro adibito per scopi non riguardanti il fronteggiamento di particolari emergenze, ma per l1attivazione di progetti concordati, fornisce gli strumenti necessari per permettere agli utenti di effettuare connessioni sicure con il sistema dell'Ente.

4.18 Inventario degli asset e postazioni di lavoro

Il Servizio Informatico mantiene aggiornato, tramite l'utilizzo e la configurazione di un apposito software, un inventario delle risorse hardware e software presenti presso l'ente.
Il servizio informatico definisce, aggiorna e utilizza delle configurazioni standard per l'installazione di tutti gli apparati (firewall, switch, etc..), dispositivi (server, memorie di rete, etc..) e postazioni di lavoro (fisse, mobili).
Le postazioni sono tenute in costante aggiornamento dal Servizio Informatico, che ha il compito, inoltre, di segnalare prontamente quando queste hanno bisogno di essere sostituite con delle nuove, evitando così di rappresentare una minaccia alla sicurezza dell'ente .
Le utenze ed i privilegi agli utenti vengono gestiti a livello centralizzato dal Servizio Informatico, che li assegna a seconda delle effettive necessità e competenze, concordate con gli appositi Responsabili di settore o servizio.

4.19 Notebook smartphone e altri supporti mobili

Agli utenti possono essere forniti dispositivi mobili, quali: notebook, supporti di memorizzazione esterna mobili quali chiavette USB, dischi esterni, e altro.

Il Servizio Informatico tiene aggiornato l'elenco degli strumenti di supporto mobile o memorizzazione esterna forniti in dotazione.
La corretta gestione di questi strumenti, la custodia e le metodologie di protezione delle informazioni in esse contenute sono gestite dal Servizio informatico stesso, attraverso adeguate azioni di informazione agli utenti finali sui rischi che corrono utilizzando tali strumenti.
Vengono inoltre effettuate periodicamente delle analisi sui dati presenti nei dispositivi mobili, anche potenziali, al fine di decidere l1applicazione o meno della crittografia dei dati sui dispositivi mobili analizzati.
Tutti i supporti mobili, nel momento del non utilizzo, devono essere custoditi in un1area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in un armadio/cassetto chiuso a chiave.

4.20 Responsabilità degli utenti e formazione

Nel piano formativo definito annualmente dall' Ente sono talvolta previste sessioni formative relative all'utilizzo sicuro delle risorse informatiche del personale.

5. Analisi delle minacce e delle vulnerabilità dell'infrastruttura informatica

Sulla base delle componenti del sistema e delle politiche di sicurezza adottate descritte al punto 4, viene effettuata un'analisi circa l'impatto che hanno, o possono avere, una serie di minacce e vulnerabilità, sulle risorse che fanno parte del sistema informatico o attraverso le quali il sistema informatico opera.

Rischi		Impatto sulla sicurezza:
Minacce derivanti dal comportament o degli utenti e amministratori	Sottrazione di credenziali di autenticazione	Basso
	Carenza di consapevolezza, disattenzione o incuria	Medio
	Comportamenti sleali o fraudolenti	Basso
	Errore materiale nell'utilizzo delle risorse	Basso
Minacce derivanti da terze parti	Minacce apportate da virus informatici, programmi suscettibili a	Medio
	Tentativi di fishing o spamming	Medio
	Accessi non autorizzati a locali o risorse	Basso
Minacce derivanti da altre cause	Eventi distruttivi o limitanti per l'accesso o la fruizione delle risorse di cause	Basso
	Guasti a sistemi complementari (impianto elettrico, climatizzazione, etc.)	Basso
	Errori umani nella gestione della sicurezza fisica	Basso
	Malfunzionamento, indisponibilità o degrado degli strumenti	Medio
	Sottrazione di risorse e strumenti contenenti dati	Basso

6. Misure adottate per la protezione e la sicurezza del sistema informatico, sulla base dei rischi considerati e del loro livello di impatto

Sulla base delle caratteristiche del sistema informatico e dei servizi con esso erogati, e delle minacce analizzate al par.5, vengono descritte qui le misure adottate per la protezione e la sicurezza dell'infrastruttura informatica e dei dati:

- ✓ Presidio in orario di lavoro dei locali e uffici. Tutti gli uffici vengono chiusi quando non presidiati.
- ✓ Autenticazione e autorizzazione degli accessi al sistema ed ai dati, attraverso l'utilizzo di profili nominali e credenziali adeguatamente complesse (in base alla rilevanza dei dati trattati).
- ✓ Segregazione delle reti LAN e WiFi esistenti attraverso il Firewall impedendo lo scambio di dati e la visibilità fra le stesse.
- ✓ Gestione adeguata e controllata dei profili di amministratore, secondo effettive necessità e competenze .
- ✓ Sistema di protezione gestito e a livello centralizzato con aggiornamento automatico delle minacce, installato su tutte le postazioni di lavoro e sui Server .
- ✓ Aggiornamenti software e applicazione delle patch periodiche e amministrate a livello centrale da parte del Servizio Informatico.
- ✓ Backup dei dati giornaliero dell'intero sistema informatico (macchine virtuali) sia su dispostivi di Rete (NAS) che su sistemi offline in Cloud.
- ✓ Sicurezza perimetrale e protezione dalle minacce erogati attraverso la gestione e configurazione di firewall di rete dotato di tutti i servizi UTP (Unified Threat Protection) necessari.
- ✓ Gestione controllata di connessioni sicure fra rete interna ed esterni: es. collegamento dei fornitori esterni per manutenzione o helpdesk o degli utenti interni per telelavoro.
- ✓ Protezione fisica: il locale CED è gestito interamente dal Servizio Informatico ed è stato messo in sicurezza dotando il locale di apposito armadio Rack per contenere la parte server e rete, protetto da gruppo di continuità; il locale è chiuso a chiave ed è ad accesso riservato.
- ✓ Formazione periodica del personale sulle tematiche della sicurezza e sui comportamenti da adottare nella normale operatività e in caso di situazioni di rischio.