Piano di Sicurezza

Comune di Vignate

Edizione 01/2015 – Rev. 01

Sommario

1. Premessa

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

Lo scopo del documento è quello di poter stabilire, attuare, mantenere e migliorare in modo continuo il sistema di gestione per la sicurezza delle informazioni.
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.

2. Riferimenti normativi

- DPR 20 ottobre 1998, n. 428 - Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD) e in particolare art. 50 bis;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 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, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 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 ex al Decreto Legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

3. 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, nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del D.Lgs. 196/2003 «Codice della Privacy»".
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.

3.1 Revisione e modifica del piano di sicurezza

Annualmente l'Ente effettua la revisione del piano sicurezza al fine di assicurarne la continua idoneità, adeguatezza ed efficacia o, in ogni caso,
Le modifiche al piano di sicurezza vengono approvate dall'Ente stesso.

3.2 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 estemporanee vengono effettuate nei seguenti casi:

- verificarsi di incidenti di sicurezza
- variazioni tecnologiche significative;
- modifiche all'architettura informatica;
- aggiornamenti delle prescrizioni normative;
- risultati delle eventuali attività di audit interni.

4. Componenti e configurazioni del sistema informatico

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

4.1 Caratteristiche di sedi e locali

Il Comune di Vignate è composto da due sedi: Municipio e Biblioteca, quest'ultima collegata logicamente al Municipio, tramite un'apposita rete VPN che ne permette lo scambio informatico di dati e configurazioni.

Presso la sede del Municipio è presente un impianto di allarme generale che comprende l'intero edificio. Le porte di ingresso agli uffici vengono chiuse quando non presidiate.
Sistemi antincendio - I sistemi antincendio sono costituiti da idranti presenti nel corridoio di accesso.
.

4.2 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.

4.3 Connettività

Anche la gestione delle linee dati è affidata al Servizio Informatico, 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.

4.4 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.

4.5 Posta elettronica

Le caselle di posta elettronica vengono gestite attraverso un servizio in Cloud, tramite il quale il Servizio

Informatico cura, per quanto di competenza, sia la gestione amministrativa delle caselle e di configurazione del sistema, sia la gestione degli aspetti legati alla sicurezza. Gli aspetti di tenuta dell'infrastruttura, di backup e di continuità di servizio sono in carico al fornitore del servizio cloud.
Il Servizio Informatico mantiene l'elenco con le caratteristiche del sistema di posta e delle caselle.

Il server di posta è posizionato all'interno dell'Ente convenzionato e raggiungibile dall'esterno attraverso un IP pubblico, ed è gestito attraverso la piattaforma software Microsoft Exchange.

Ogni utente ha un indirizzo di posta nominale.
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).

4.6 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.

4.7 Sicurezza perimetrale

Il sistema informatico dell'ente è protetto tramite l'utilizzo di firewall di rete, appositamente configurati per gestire la sicurezza perimetrale e, nel caso, l'applicazione di opportuni content filtering gestiti ed avvallati dal Servizio Informatico.
Anche le configurazioni dei 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.
I sistemi di sicurezza perimetrale sono coperti da apposito contratto di assistenza e manutenzione.

4.8 Sistemi di protezione da malware

Presso le postazioni di lavoro e i server dell'ente è installato e attivo un sistema antivirus.
Tale software viene gestito a livello centralizzato (presso macchina virtuale) 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 e consapevolezza.

4.9 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 supporti esterni offline.

4.10 Log e tracciamento delle attività

Il Servizio Informatico, tramite apposite richieste ai fornitori deve poter accedere ai dei 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.

4.11 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.

La password di accesso alla rete viene cambiata autonomamente ogni 3 mesi secondo quanto stabilito dalla normativa vigente.
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.

4.12 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.

4.13 Modalità di accesso remoto

Il servizio informatico si occupa della gestione e del controllo degli accessi effettuati da parte di 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.

4.14 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 l'attivazione di progetti concordati, fornisce gli strumenti necessari per permettere agli utenti di effettuare connessioni sicure con il sistema dell'Ente.

4.15 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.

4.16 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.
Inoltre vengono effettuati periodicamente delle analisi sui dati presenti nei dispositivi mobili, anche potenziali, al fine di decidere l'applicazione o meno della crittografia dei dati a porzioni delle memorie analizzate sui dispositivi mobili.

Tutti i supporti mobili, nel momento del non utilizzo, devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in un armadio/cassetto chiuso a chiave.

4.17 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 da ATO 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: alto/medio/basso
Minacce derivanti dal comportamento 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 recare danno	Basso
	Tentativi di fishing o spamming	Basso
	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 naturali o artificiali	Basso
	Guasti a sistemi complementari (impianto elettrico, climatizzazione, etc.)	Basso
	Errori umani nella gestione della sicurezza fisica	Medio
	Malfunzionamento, indisponibilità o degrado degli strumenti	Basso
	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:

- Presenza di antifurto presso la sede. 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).
- Centralizzazione del sistema attraverso il collegamento in VPN della sede bibliotecaria
- Gestione adeguata e controllata dei profili di amministratore, secondo effettive necessità e competenze.
- Antivirus gestito e a livello centralizzato con aggiornamento automatico delle minacce, da parte del Servizio Informatico.
- 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) con tenuta di copie offline separate settimanali.
- Sicurezza perimetrale e content filtering gestiti attraverso la gestione e configurazione di firewall di rete.
- 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 dagruppi di continuità e sistemi di condizionamento dell'aria.