PIANO DI SICUREZZA

Revisioni e aggiornamenti del documento			
Revisione	**Data**	**Autore**	**Descrizione**
1.0	26/09/2022	Massimiliano Fazio	Stesura iniziale del documento
1.1	27/09/2022	Diego Tartari	Revisione a aggiornamento

Indice e Sommario

1. Premessa

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

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

Circolare AgID del 18 aprile 2017, n. 2.

Regolamento UE n. 679/2016 (GDPR).

3. Il piano della sicurezza

Il Piano della Sicurezza (PdS) rappresenta l'insieme delle indicazioni di natura tecnologica, organizzativa e procedurale che il Comune di Beinasco adotta per assicurare un adeguato livello di sicurezza informatica.
Il predetto piano si basa sull'analisi dei rischi a cui è esposto attualmente il sistema informatico dell'Ente nonché i relativi dati e documenti in esso contenuti.
Esso, inoltre:

- descrive le risorse e le configurazioni del sistema informatico e le politiche di sicurezza in essere;
- valuta minacce e vulnerabilità del sistema informatico (analisi dei rischi);
- gestisce il rischio, cioè individua le azioni da porre in atto o da adottare al fine di determinare il giusto livello di sicurezza da perseguire.

3.1 Revisione e modifica del piano di sicurezza e delle politiche della 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.

4. Componenti e configurazione del sistema informatico

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

4.1 Sistema di allarme e antincendio

Sistema di allarme - Presso alcune sedi è presente un impianto di allarme generale che comprende l'intero edificio. Dove non è presente l'impianto di allarme, le porte di ingresso sono chiuse con utilizzo di particolari serrature.

Le porte di ingresso dei singoli uffici vengono chiuse a chiave quando gli stessi non sono presidiati.

Sistemi antincendio - I sistemi antincendio sono costituiti da apposito allarme sonoro e da idranti presenti nel corridoio di accesso. In ciascuna zona è presente una planimetria che individua la specifica posizione e le relative vie di fuga previste dalle vigenti normative sulla sicurezza.

4.2 Caratteristiche di sedi e locali

Il Comune di Beinasco è composto da quattro sedi:

1. Sede 1 - Piazza Vittorio Alfieri 7 - Piazza Generale Carlo Alberto dalla Chiesa 1: è la sede principale del Comune, in essa sono presenti le terminazioni delle linee telefoniche-dati, sia per la parte voce sia per la parte dati. È presente una linea dati da 600 Mbps fornita dall'operatore Fastweb e una linea ISDN Primario 30 canali, che corrisponde alla numerazione del Comune 011.39891.
2. Sede 2 - Corso Cavour 1: è collegata alla sede principale tramite fibra ottica proprietaria. Non dispone di proprie terminazioni di linee telefoniche-dati, ma utilizza quelle della sede principale.
3. Sede 3 – Piazza Kennedy 37/a– Frazione Borgaretto: è una sede remota del Comune, essa dispone di una linea da 600 Mbps fornita dall'operatore Fastweb. È stato attivato un collegamento VPN con la sede principale sia per la parte fonia che per la parte dati.
4. Sede 4 – Viale Risorgimento 16 - Incubatore: è una sede remota del Comune, essa dispone di una linea da 200 Mbps fornita dall'operatore Fastweb. È stato attivato un collegamento VPN con la sede principale sia per la parte fonia che per la parte dati.

4.3 Locale CED e componenti server

Tutti i server sono posizionati all'interno di un apposito armadio Rack, che risiede all'interno di un apposito locale adibito a CED chiuso a chiave.

Il Servizio Informatico, composto dal Responsabile e referente interno dell'Ente, insieme alla società esterna specializzata a cui è stata affidata la consulenza e la manutenzione 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 e mantiene la documentazione descrittiva.

L'Ente, inoltre, ha dotato la parte server di gruppi di continuità, anch'essi ubicati nel locale CED, in modo da permettere la tenuta o lo spegnimento controllato dei dispositivi ad essi collegati in caso di mancanza di energia elettrica.

4.4 Connettività

Il Servizio informatico supporta l'Ente per l'individuazione delle caratteristiche tecniche che deve possedere ciascuna linea in base alle esigenze verificate. In caso di segnalazione di disservizi relativi alle connettività, il Servizio Informatico, previa verifica, provvede a segnalare il malfunzionamento al fornitore.

Il Servizio Informatico cura anche la documentazione tecnica di dettaglio che riporta schemi e descrizioni particolari di ciascun apparato Server, o apparato di rete e sicurezza, ubicato nei locali Comunali ed atto a erogare i servizi all'Ente.

4.5 Archivi

Gli utenti finali, ognuno per la loro funzione, aggiornano le basi dati dell'Ente (database) collegate agli applicativi in uso.
Il Servizio Informatico, in caso di segnalazione di malfunzionamento e anomalie riscontrate dagli utenti sulle basi dati dell'Ente, si attiva con i fornitori dei software per approntare le relative soluzioni.

4.6 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 consiste nella piattaforma Cloud di Microsoft Exchange on Line ed è raggiungibile dall'esterno attraverso un IP pubblico.

Ogni utente ha un indirizzo di posta nominale ed esistono, inoltre, delle caselle condivise e delle liste di distribuzione specifiche che fanno capo all'organizzazione dei servizi Comunali.

La creazione di una nuova casella avviene tramite apposita richiesta al Servizio Informatico, attraverso comunicazione ufficiale su canale email.

4.7 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 di fatturazione elettronica.

La continuità operativa e la manutenzione del servizio sono gestite a livello contrattuale con il fornitore.

4.8 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 opportune regole di content-filtering gestite ed avallate dal Servizio Informatico.

Per gestire ridondanza e continuità del servizio, in ciascuna sede è presente una coppia di firewall di rete in alta affidabilità, onde consentire l'entrata automatica in servizio del firewall secondario in caso di guasto del firewall principale.

Anche le configurazioni dei firewall sono mantenute dal Servizio Informatico che ne effettua una copia di backup prima di ogni modifica, oltre a prevedere e pianificare gli aggiornamenti e tenerne costantemente monitorato il corretto funzionamento.

I sistemi di sicurezza perimetrale sono coperti da apposito contratto di assistenza e manutenzione.

4.9 Sistemi di protezione da malware

Presso le postazioni di lavoro e i server dell'Ente è installato e attivo un sistema antivirus avanzato.

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 adotta le azioni ritenute opportune ed effettua le comunicazioni agli utenti in merito ai comportamenti da adottare.

4.10 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.

Il Servizio Informatico 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 e settimanali della corretta esecuzione dei processi di backup ed effettuare una verifica periodica della correttezza delle impostazioni dei sistemi di backup e dell'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 e il mantenimento di quali sono i dati facenti parte del sistema spetta al Servizio Informatico.

I backup vengono effettuati con cadenza giornaliera e settimanale presso supporti di rete NAS e copie su Cloud provider Veeam, che contengono copie giornaliere delle principali VM ospitate sul sistema di virtualizzazione dell'Ente.

I dettagli riguardanti i piani di backup, la loro schedulazione, l'ubicazione e la conservazione (definizione dei punti ripristino per ciascun piano), sono definiti in un apposito documento.

4.11 Log e tracciamento delle attività

Per quanto concerne i log applicativi, in caso di necessità, il Servizio Informatico contatta i fornitori degli applicativi per estrarre i log richiesti; tali log si ottengono aumentando il livello di debug degli applicativi in caso di necessità.

Per quanto concerne i log relativi ai sistemi operativi e apparati specifici, essi vengono disciplinati attraverso una specifica politica che regola i tempi e le modalità di creazione, gestione, eliminazione, salvataggio e conservazione.

4.12 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 provvisorie di accesso al sistema informatico, che vengono cambiate in autonomia dall'utilizzatore al primo accesso.

Nome utente e password sono strettamente personali.

L'utente è tenuto a:

- non comunicare a terzi la password
- 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 e, inoltre, viene automaticamente attivato il blocco dell'utenza che può nuovamente accedere unicamente reinserendo la propria password.

Le credenziali di accesso ai sistemi informatici sono rilasciate su richiesta dei responsabili dei servizi tramite e-mail, con la quale individuano le abilitazioni necessarie.

4.13 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.

4.14 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 dal Servizio Informatico 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.

Ove tecnicamente possibile, per l'accesso remoto di terze parti e manutentori esterni del sistema informatico, si utilizza preferibilmente la modalità VPN con doppio fattore di autenticazione, ovvero con un set di credenziali utente e password e in aggiunta un token che viene creato dal Servizio Informatico e comunicato attraverso canali sicuri, al destinatario.

4.15 Telelavoro – Smart Working

La modalità del telelavoro o smart working 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.

La modalità del telelavoro o smart working è consentita unicamente attraverso l'utilizzo di un PC portatile fornito dall'Ente e con l'utilizzo di VPN con doppio fattore di autenticazione.

4.16 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.

Inoltre, il predetto servizio definisce, aggiorna e utilizza delle configurazioni standard per l'installazione di tutti gli apparati (firewall, switch, ecc.), dei dispositivi (server, memorie di rete, ecc.) e delle 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 nuove postazioni, evitando così di rappresentare una minaccia alla sicurezza dell'Ente.

Le utenze e i privilegi agli utenti vengono gestiti a livello centralizzato dal Servizio Informatico, che li assegna a seconda delle effettive necessità e competenze concordate con i Responsabili di settore o servizio.

4.17 Notebook, smartphone e altri supporti mobili

Agli utenti possono essere forniti dispositivi mobili, quali notebook.

Il Servizio Informatico istruisce gli utenti finali sulla corretta gestione di questi strumenti, sulla loro custodia e sulle metodologie di protezione delle informazioni.
Ciò viene effettuato attraverso adeguate azioni di informazione agli utenti finali, evidenziando altresì i rischi che corrono utilizzando in modo errato tali strumenti.

Tutti i notebook, quando non vengono utilizzati, devono essere custoditi in un'area ad accesso controllato o in un ufficio, che viene chiuso quando non presidiato, o in un armadio/cassetto chiuso a chiave.

4.18 Responsabilità degli utenti e formazione

Nel piano formativo definito annualmente dall'Ente sono 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 dal Comune di Beinasco e 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	Alto
	Carenza di consapevolezza, disattenzione o incuria	Medio
	Comportamenti sleali o fraudolenti	Medio
	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 phishing o spamming	Medio
	Accessi non autorizzato a locali o risorse	Alto
Minacce derivanti da altre cause	Eventi distruttivi o limitanti per l'accesso o la fruizione delle risorse di cause naturali o artificiali	Medio
	Guasto a sistemi complementari (impianto elettrico, climatizzazione, etc.)	Basso
	Errori umano nella gestione della sicurezza fisica	Medio
	Malfunzionamento, indisponibilità o degrado degli strumenti	Basso
	Sottrazione di risorse e strumenti contenenti dati	Basso