Politica del Sistema di Gestione

per la Sicurezza delle Informazioni

Classificazione: Pubblico

Revisioni del documento				
Nome File: SGSI_00 - Politica SGSI - rev1.docx				
REV.	**Data**	**Descrizione della revisione**	**Redazione**	**Approvazione**
0	08/01/2019	Prima emissione	Gino Zuppella	Marco Cardelli
1	19/02/2020	Aggiornamento obiettivi	Gino Zuppella	Marco Cardelli

Sommario

1 Scopo e campo di applicazione

Scopo di questo documento è la definizione di tutte quelle che sono le linee guida che caratterizzano la determinazione, la struttura e i requisiti delle policy aziendali in materia di sicurezza informatica.

Il presente documento si applica ai metodi e agli strumenti utilizzati per il trattamento delle informazioni all'interno di SPEE.

2 Requisiti e riferimenti normativi

Le normative, gli standard e le leggi di riferimento sulle quali si basano le policy e la gestione informatica aziendale sono:

- Service Level Agreement (SLA) e requisiti di sicurezza stabiliti con tutte le Parti interessate;
- Regolamento UE 2016/679 e D. Lgs. 196/2003 (*) in materia di protezione dei dati personali;
- D. Lgs. 231/2001 (*) in materia di responsabilità amministrativa delle imprese;
- Legge 22 aprile 1941, n. 633 (*) in materia di diritto d'autore;
- Legge 23 dicembre 1993, n. 547 (*) in materia di antipirateria informatica;
- Legge 20 maggio 1970, n. 300 (*) meglio conosciuta come Statuto dei lavoratori;
- D. Lgs. 81/2008 (*) in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- CCNL settore Metalmeccanico e Vigilanza privata;
- ISO 27001:2013 – Requisiti di un Sistema di Gestione della Sicurezza delle Informazioni;
- ISO 27002:2013 – Linee guida per la Gestione della Sicurezza delle Informazioni.

(*) e successive modificazioni e/o integrazioni.

3 Significato di sicurezza delle informazioni

L'informazione è una risorsa che, come altre importanti risorse aziendali, è essenziale per lo svolgimento delle proprie attività di business, di conseguenza necessita di essere opportunamente regolamentata e protetta. Questo diventa particolarmente importante in un contesto aziendale sempre più interconnesso, dove le informazioni sono esposte ad un crescente numero e ampia varietà di minacce e vulnerabilità.

L'informazione è intesa in senso lato, dove non la si identifica come puro dato ma anche come l'insieme dei processi, dei sistemi e delle reti che ne consentono l'uso.

La sicurezza informatica rappresenta un elemento essenziale nell'organizzazione e nella gestione dell'infrastruttura informatica, sia al proprio interno, che in relazione ai servizi resi ai cittadini e alle imprese.

La definizione, l'implementazione, la gestione e il miglioramento della sicurezza informatica vestono un ruolo essenziale per lo svolgimento delle proprie attività di business, per il rispetto delle leggi e per l'immagine aziendale.

La sicurezza informatica costituisce di fatto una struttura di base mediante la quale si favorisce lo sviluppo di nuovi servizi e sistemi, e non un insieme di vincoli a cui sottostare. Questo avviene mediante una stretta sinergia tra gli obiettivi e gli sviluppi aziendali da una parte e dell'altra i principi che sono alla base della sicurezza.

4 Obiettivi per la sicurezza delle informazioni

L'informazione costituisce il patrimonio fondamentale su cui si basa il business dell'azienda, in quanto l'organizzazione le attribuisce un valore strategico per il conseguimento della propria missione.

L'informazione si esplicita in diverse forme: stampata o scritta su carta, memorizzata elettronicamente, trasmessa tramite posta o strumenti elettronici, mostrata in filmati, oppure espressa in conversazioni. Qualunque sia la forma presa dall'informazione, o il mezzo utilizzato per condividerla o memorizzarla, deve essere sempre adeguatamente protetta.

Una corretta gestione della sicurezza deve prevedere la protezione delle informazioni, indipendentemente dal tipo di registrazione e dal trattamento effettuato, da un'ampia gamma di minacce, assicurando la continuità della missione aziendale, minimizzando i danni in caso di incidenti e massimizzando l'efficienza negli interventi di sicurezza.

La sicurezza delle informazioni è assicurata dalla salvaguardia dei seguenti obiettivi:

- *Riservatezza*, che garantisce che un'informazione sia accessibile solo a chi è autorizzato;
- *Integrità*, che salvaguarda l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione;
- *Disponibilità*, che garantisce, quando richiesto e autorizzato, l'accesso alle informazioni e ai beni associati.

Gli obiettivi fissati sono conseguiti attraverso l'adozione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) aderente allo standard ISO/IEC 27001, che assicura il rispetto di tali requisiti, sulla base di un approccio sistematico, basato sull'analisi e il trattamento dei rischi, che stabilisce, realizza, attua, controlla, rivede, riadatta e migliora la sicurezza delle informazioni gestite da SPEE.

La politica generale enunciata si riferisce e si applica a tutte le informazioni gestite da SPEE, siano esse di origine interna o collegate ai servizi erogati ai clienti.

Con il SGSI si vogliono raggiungere le seguenti finalità:

- garantire la capacità di gestione della sicurezza, in linea con le aspettative delle parti interessate, con gli obiettivi aziendali e con gli standard internazionali;
- normalizzare i vari approcci, ottimizzando e coordinando le risorse disponibili;
- creare un'organizzazione della sicurezza condivisa, documentata, organica, efficiente e capillare;
- consentire un miglioramento continuo;
- armonizzare le procedure di sicurezza con i processi aziendali del Sistema di Gestione della Qualità (S.G.Q.), al fine di ottimizzare gli impatti sulle attività produttive;

- assicurare che le protezioni previste e attuate siano graduate in funzione della criticità dei beni tutelati, anche per ottimizzare l'aspetto economico.

5 Compliance

La legislazione cogente in materia di trattamento delle informazioni fa parte dei requisiti specifici che devono essere rispettati senza eccezioni.

È responsabilità del RSI, in collaborazione con eventuali altre aree preposte, individuare correttamente gli impatti delle normative con le attività svolte e predisporre, in collaborazione con le altre funzioni aziendali interessate, adeguate procedure e strumenti operativi.

6 Strategia per la sicurezza delle informazioni

Per un corretto ed efficace impiego della sicurezza informatica nella realtà aziendale, deve essere attuata una strategia che si basi sui seguenti punti.

Prevenzione

Condividere le informazioni con qualcun altro solo evitando le minacce prima che esse diventino dannose.

Salvaguardia

Proteggere i dati e il loro valore attraverso misure di sicurezza realmente efficaci e realizzabili.

Business Continuity

Ridurre l'indisponibilità di informazioni a fronte di eventi catastrofici che possono accadere.

Service Level Agreements

Definire gli indicatori chiave di prestazione (KPI) e le loro misurazioni per monitorare e gestire l'efficacia degli strumenti ICT.

Accordi con terze parti

Definire requisiti chiari e comprensibili nei contratti e negli ordini riguardanti la catena di fornitura dei sistemi di informazione.

Cultura della sicurezza

Elaborare i dati in sicurezza sfruttando la consapevolezza, la conoscenza e il comportamento di ogni membro dell'organizzazione. La sicurezza informatica deve appartenere al patrimonio culturale aziendale di base, affinché essa venga utilizzata, coinvolta e sfruttata sia nella definizione e attuazione delle strategie di business che nelle quotidiane attività.

7 Infrastruttura documentale

La documentazione è costituita da un gruppo di norme regolamentari, di ruoli e di regole che determinano il modo in cui le risorse, incluse le informazioni considerate sensibili, sono gestite, protette e distribuite all'interno dell'organizzazione.

Ciascun documento tratta in modo specifico un singolo aspetto di sicurezza, descrivendolo sotto tutti i possibili punti di vista di interesse e si distingue in:

- ✓ Documenti di sistema;
- ✓ Procedure organizzative;
- ✓ Procedure tecniche;
- ✓ Istruzioni operative.

A seguire la classificazione del documento, è riportato un numero progressivo che identifica in modo univoco il documento all'interno della corrispondente tipologia. Infine, si aggiunge un titolo esplicativo del contenuto del documento.

La documentazione è raccolta all'interno del sistema documentale aziendale ed è disponibile a tutto il personale nel rispetto delle regole di accesso stabilite.