Politica della Sicurezza delle Informazioni

Versione	Descrizione	Modifica	Approvazione
01	Prima emissione	RGSI 02/07/2019	CDA 02/07/2019
02	Revisione a seguito di audit di terza parte	RSGSI 07/05/2020	CDA 07/05/2020

La Direzione, riconoscendo l'importanza strategica degli asset organizzativi di ***SMC Treviso srl***, siano essi di natura materiale (risorse umane, dispositivi informatici e infrastrutture) o immateriale (patrimonio delle informazioni), ha deciso di tutelarne la salvaguardia in tutte le fasi dei processi aziendali considerando **l'Information Security** uno strumento che permette la ***condivisione sicura delle informazioni***, ***il miglioramento delle prestazioni rese ai Clienti*** e ***della propria immagine.***

La Direzione, inoltre, in considerazione del fatto che il proprio personale si trova anche a svolgere attività lavorativa presso la sede dei Clienti, ha deciso di estendere tale tutela anche alle informazioni affidate, durante il rapporto contrattuale, dalle terze parti a ***SMC Treviso srl***, o ai suoi rappresentanti.

Obiettivi di ***SMC Treviso srl*** sono quindi:

1. **Riduzione delle vulnerabilità dei propri asset aziendali da minacce quali virus, software nocivo ecc. tramite interventi di monitoraggio e protezione ad ampio spettro che interessano:**
   - sistemi hardware e software (personal computer, workstation, server, supporti di memorizzazione, apparecchiature di rete, sistemi di comunicazione elettronica);
   - informazioni (banche dati, documenti digitali e dati in transito su sistemi di comunicazione);
   - servizi (posta elettronica e accessi al portale).
2. **Caratterizzazione della propria offerta di servizi ai Clienti con la garanzia della salvaguardia delle informazioni condivise mediante il monitoraggio sistematico del rispetto delle regole di protezione delle informazioni vigenti in *SMC Treviso srl* o definite in sede contrattuale.**

Per garantire la continuità operativa delle attività di ***SMC Treviso srl***, è necessario che le opportune forme di protezione siano applicate in modo sistematico in tutte le aree che risultino critiche sulla base di una valutazione dei rischi associata a quella del valore delle informazioni trattate.

SMC Treviso srl in qualità di erogatore di servizi cloud, al fine di proteggere le informazioni dei Clienti archiviate e gestite in cloud, considera:

- le informazioni archiviate nell'ambiente del Cloud cui il Cliente può avere accesso e che sono gestite dal Provider del Cloud;
- gli asset mantenuti sul Cloud, come le applicazioni;
- i processi in multi-tenant che si possono svolgere nel Cloud virtuale;
- gli utenti del Cloud ed il contesto in cui essi utilizzano il servizio;
- gli amministratori del servizio Cloud dei Clienti che hanno un accesso privilegiato;
- la localizzazione geografica del Provider del Cloud ed i Paesi in cui quest'ultimo può archiviare i dati relativi al Cloud (anche temporaneamente).
- i requisiti base di sicurezza delle informazioni applicabili alla progettazione ed alla implementazione del servizio Cloud;
- i rischi derivanti da addetti ai lavori autorizzati;
- accesso agli asset del Cliente da parte del Provider
- procedure per il controllo accessi, come la strong authentication per l'accesso amministrativo al Cloud;

- comunicazioni con il Cliente durante il change management;
- sicurezza virtuale;
- accesso ai dati del Cliente del servizio Cloud e loro protezione;
- gestione del ciclo di vita dell'account del Cliente;
- comunicazione di Data Breach e linee guida per la condivisione delle informazioni, per aiutare le investigazioni.

In tale ambito, il percorso definito dalla Direzione prevede le seguenti tappe:

- Certificazione del Sistema di Gestione della Sicurezza delle Informazioni con estensione ai controlli 27017 e 27018 e mantenimento della stessa nel triennio successivo;
- Rilevazione di specifici indicatori di sicurezza per l'adozione di idonee azioni atte a mantenere il rischio residuo a livelli accettabili;
- Attuazione, ove necessario, di idonee azioni correttive per ridurre a livelli ritenuti accettabili l'incidenza di condizioni anomale sul funzionamento complessivo del sistema;
- Definizione di reazioni idonee al manifestarsi di incidenti di sicurezza per garantire la continuità dell'operatività in sicurezza (business continuity);
- Stabilizzazione e progressivo miglioramento del livello di sicurezza, anche attraverso l'attuazione di idonee azioni preventive, rispetto agli indicatori misurati negli anni precedenti.

Al fine di perseguire gli obiettivi prefissati dalla Direzione di ***SMC Treviso srl***, saranno messe in atto iniziative finalizzate a:

- Definire, implementare e mantenere aggiornato ed operativo il Sistema di Gestione della Sicurezza delle Informazioni, conforme allo standard internazionale ISO/IEC 27001:2013, alla legislazione vigente e alla tutela dei copyright;
- Sensibilizzare e formare lo staff sul detto Sistema di Gestione della Sicurezza delle Informazioni (SGSI), sui relativi sistemi di riferimento e sulle sanzioni previste in caso di violazione delle regole di Sicurezza delle Informazioni aziendali;
- Ottenere la certificazione di conformità allo standard indicato come mezzo di verifica oggettiva del sistema di gestione realizzato, di stimolo al continuo miglioramento dello stesso e di garanzia di tutte le parti interessate.
- Migliorare continuamente il livello di Sicurezza, sia "logica" (ad es. attraverso l'analisi per identificare potenziali minacce, garantendo in qualsiasi situazione la disponibilità e la capacità di almeno una copia dei dati per finalità di recovery, riducendo al minimo gli incidenti di sicurezza, aggiornando le patch di sicurezza, ecc.) che "organizzativa" (ad es. attraverso incontri di awareness periodica, training delle nuove risorse, training su nuove policy e procedure, NDA, ecc.), rispettando le strategie di business, in conformità ai requisiti legali, normativi e contrattuali, tenendo presente i requisiti delle terze parti interessate.
- Assegnare e monitorare opportuni ruoli e responsabilità per la gestione della sicurezza delle informazioni;
- Valutare periodicamente i rischi di sicurezza delle informazioni, di tutte le parti interessate, al fine di ridurli a livelli accettabili;
- Aumentare il livello di consapevolezza della popolazione aziendale sugli aspetti relativi alla sicurezza delle informazioni;

- Aumentare il livello di competenza della popolazione aziendale sugli aspetti relativi alla sicurezza delle informazioni;
- Proteggere il proprio patrimonio informativo e quello delle parti interessate in termini di Riservatezza, Integrità e Disponibilità;
- L'Azienda si impegna a verificare periodicamente l'efficacia e l'efficienza del sistema di gestione per la sicurezza delle informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie, al fine di consentire l'attivazione di un processo continuo che terrà sotto controllo il variare delle condizioni a contorno o degli obiettivi di business aziendali al fine di garantirne il suo corretto adeguamento;
- Preservare al meglio l'immagine aziendale;
- Evitare ritardi nell'erogazione dei servizi (rispetto degli SLA);
- Assicurare e monitorare i requisiti di sicurezza all'interno degli accordi con le parti interessate;
- Ridurre il numero di incidenti di sicurezza delle informazioni;
- Soddisfare tutti i requisiti normativi relativi alla Sicurezza delle Informazioni vigenti e cogenti;
- Raggiungere la conformità alla legislazione applicabile in materia di protezione delle informazioni personali;
- Raggiungere la conformità rispetto alle condizioni contrattuali concordate con il Provider del Cloud pubblico che tratta Informazioni Personali Identificabili e con i Clienti del servizio Cloud.

Il Sistema di Gestione identifica e tiene conto dei requisiti derivanti dall'evoluzione del contesto interno e del contesto esterno, in particolare dei requisiti delle terze parti interessate, e identifica gli obiettivi di sicurezza da perseguire. L'Alta Direzione si impegna ad allocare le risorse necessarie alla realizzazione del predetto sistema e mantiene un "commitment" adeguato sulle tematiche della sicurezza, assicurando che gli obiettivi di sicurezza siano integrati nei processi aziendali e conseguiti.

Sono state inoltre individuate e messe a disposizione le opportune risorse e definite specifiche responsabilità assegnate al Responsabile della Sicurezza delle Informazioni, che avrà il compito di predisporre e aggiornare il Sistema di Gestione della Sicurezza delle Informazioni, verificarne l'efficacia e relazionare la Direzione sul relativo stato di attuazione.

Lo stato del SGSI e la valutazione della sua efficacia sono discussi in appositi Riesami della Direzione, che sono riunioni periodiche (almeno una volta l'anno) cui partecipa la Direzione e il Responsabile del Sistema per la Sicurezza delle Informazioni con il compito di analizzare, discutere e fornire indicazioni relativamente a:

- Eventuali variazioni subite dai fattori che determinano l'esito dell'analisi dei rischi: incremento, variazione delle minacce, modifiche valutazione degli impatti, ecc.;
- Risultanze di Rapporti di Incidenti di sicurezza;
- Rapporti di Audit interni.

In considerazione dell'importanza degli obiettivi da raggiungere e dell'impegno necessario per il loro ottenimento, si invita tutto lo Staff a prestare la propria disponibilità e collaborazione nell'attuazione ed aggiornamento del Sistema e ad attenersi scrupolosamente alle prescrizioni contenute nel Manuale di Gestione della Sicurezza delle Informazioni, nelle Procedure Operative e nelle altre disposizioni in merito eventualmente fornite dal management.