POLITICA DELLE AZIENDE DEL GRUPPO SOL IN MATERIA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI E DELLA CONTINUITÀ OPERATIVA

Premessa

I fattori di successo della strategia del Gruppo SOL sono:

- l'internazionalizzazione del business per competere su un mercato globale;
- la capacità di anticipare le nuove esigenze della domanda;
- la diversificazione e valorizzazione delle nuove opportunità di mercato;
- l'orientamento al Cliente;
- il miglioramento continuo e l'innovazione del prodotto e del servizio, visto sempre più come impegno a fornire soluzioni "tailor made".

In considerazione dell'importanza strategica che risiede nella gestione della sicurezza delle informazioni e della continuità operativa, delle reti e dei sistemi IT, per il proprio Business, il Gruppo SOL, si dota di una politica adeguata alle esigenze attuali e future.

SOL è consapevole che la gestione della sicurezza delle informazioni e della continuità operativa è un processo culturale complesso che deve coinvolgere a tutti i livelli ed in modo pervasivo l'operatività individuale di tutte le risorse umane assegnate a tutte le unità organizzative all'interno del perimetro di certificazione (nel seguito denominato "ambito").

Obiettivi

Per consentire al Gruppo SOL di sviluppare e consolidare la posizione di leadership sui mercati, è necessario garantire:

- la redazione, l'aggiornamento ed il controllo di piani di sviluppo affinché le infrastrutture ed i servizi IT siano di supporto alle attività di business, adottando opportune politiche di sicurezza e di continuità operativa;
- la qualità e l'affidabilità dei servizi IT erogati;
- la conservazione sicura delle informazioni gestite;
- la continuità operativa dei servizi IT erogati.

SOL riconosce la necessità di sviluppare, mantenere, controllare e migliorare in modo costante l'Information Security and Business Continuity Management System (nel seguito indicati come ISMS e BCMS), in conformità alle norme ISO/IEC 27001, estesa in conformità alle linee guida ISO/IEC 27017 e ISO/IEC 27018, e ISO 22301 e al General Data Protection Regulation (GDPR).

L'ISMS e il BCMS si concretizzano assicurando:

- la riservatezza del patrimonio informativo gestito, patrimonio reso disponibile ai soli individui e/o entità autorizzate;
- l'integrità del patrimonio informativo gestito, tutelandone la proprietà, la attendibilità e la completezza;
- la disponibilità del patrimonio informativo gestito, il quale deve essere accessibile ed utilizzabile da parte delle entità autorizzate;
- la continuità operativa dei servizi IT erogati sulla base delle necessità del business;

ed attraverso:

- l'ottemperanza ai requisiti cogenti del quadro normativo di riferimento e contrattuali (compliance);
- l'ottemperanza ai requisiti previsti in tema di trattamento dei dati personali, dalla legge (es. GDPR, d.lgs 101/2018, ecc.), dalle norme di riferimento (es. ISO/IEC 27018, ecc) e dai requisiti contrattuali;
- la definizione appropriata dei requisiti di sicurezza condivisi con i clienti dei servizi cloud, in conformità alla norma ISO/IEC 27017;

- l'adeguata formazione in tema di sicurezza delle informazioni e di continuità operativa del personale;
- l'efficacia e l'efficienza dei controlli atti ad evitare, contrastare, gestire e registrare, azioni e/o eventi, che possano violare la sicurezza delle informazioni e ostacolare la continuità operativa.

L'implementazione dell'ISMS e del BCMS prevede di:

- identificare una metodologia di valutazione dei rischi, nell'ambito del Sistema di Gestione Integrato, derivanti dalla gestione delle informazioni richieste e dai requisiti del business; in base a tale metodologia identificare le minacce alle quali il proprio patrimonio informativo possa essere soggetto;
- ricondurre i rischi ad un livello accettabile, allineato alle strategie di gestione dei rischi dell'organizzazione;
- definire e rendere effettive le linee operative, le regole, le funzioni, gli strumenti, gli oggetti e controlli, che garantiscano in ogni struttura organizzativa, ambiente informatico, singolo elaboratore, il rispetto degli standard definiti da SOL;
- controllare, cogliendo ogni spunto di miglioramento, il sistema attuato.
- assicurare il rispetto dei requisiti di sicurezza previsti per i servizi cloud concordati con i clienti.

Applicabilità

La Politica per la sicurezza delle informazioni e della continuità operativa è applicata a tutto il personale SOL in ambito, alle aziende Partner, ai Fornitori, Clienti o Terze Parti sotto contratto temporaneo o permanente, coinvolti nel trattamento degli asset informativi aziendali in ambito o che abbiano accesso ai locali in ambito.

Responsabilità

La presente politica viene emessa e riesaminata dall'Alta Direzione del Gruppo SOL.

Il Responsabile ISMS e BCMS, designato dall'Alta Direzione, facilita l'attuazione della presente politica attraverso norme e procedure appropriate. Tutto il personale ed i fornitori in ambito devono seguire le procedure stabilite da SOL per la politica della sicurezza delle informazioni e della continuità operativa.

Tutto il personale in ambito, in base alle proprie conoscenze, ha la responsabilità di riferire al Responsabile ISMS e BCMS qualsiasi punto debole individuato. Qualsiasi azione, che in modo intenzionale provochi o possa provocare un danno a SOL, dovrà essere perseguita nelle opportune sedi.

Riesame

La presente politica viene riesaminata annualmente in occasione del CGSQ ed ogni qual volta ve ne sia l'esigenza a seguito dell'attuazione di modifiche che la influenzano, per accertarsi che permanga idonea alle finalità del Gruppo SOL, alle aspettative degli utenti e di tutte le parti interessate.

Presidente
(Aldo Fumagalli Romario)

Direttori Generali
(Giulio Mario Bottes - Andrea Monti)

Direttore Centrale Qualità,
Sicurezza, Ambiente & Affari Regolatori
(Daniele Valtolina)

Maggio 2020

SOLGROUP
a breath of life