SCOPO

Lo scopo della presente Politica per la Sicurezza delle Informazioni è garantire la tutela e la protezione delle Informazioni dalle minacce, interne o esterne, intenzionali o accidentali.

La presente Politica per la Sicurezza delle Informazioni definisce le linee guida che indirizzano la gestione di tutti i processi e delle prassi aziendali affinchè siano coerenti con l'implementazione del proprio Sistema di Gestione per la Sicurezza delle Informazioni in conformità ai requisiti previsti dalla norma ISO/IEC 27001.

La Direzione Aziendale ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente Politica per la Sicurezza delle Informazioni.

CAMPO DI APPLICAZIONE

La presente Politica per la Sicurezza delle Informazioni si applica indistintamente a tutti gli organi e i livelli dell'Azienda.

L'attuazione della presente Politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel Campo di Applicazione del Sistema di Gestione per la Sicurezza delle Informazioni.

L'azienda consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

"POLICY" AZIENDALE PER SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda.

È necessario assicurare:

- ✓ **RISERVATEZZA/CONFIDENZIALITÀ** delle informazioni: deve essere garantito che le informazioni siano accessibili solo a chi è autorizzato
- ✓ **INTEGRITÀ** delle informazioni: deve essere garantita la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione
- ✓ **DISPONIBILITÀ** delle informazioni: deve essere garantito che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La mancanza di adeguati livelli di Sicurezza delle Informazioni può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.

Un adeguato livello di Sicurezza delle Informazioni è altresì basilare per la condivisione delle informazioni stesse.

L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo.
La valutazione dei rischi relativi alla Sicurezza delle Informazioni permette di valutare le potenziali conseguenze che possono derivare dalla mancata applicazione di misure di gestione della sicurezza e quale sia la realistica probabilità di attuazione delle minacce identificate.

I risultati della suddetta valutazione del rischio determinano le azioni di miglioramento necessarie per prevenire i rischi individuati.

I principi generali della gestione della sicurezza delle informazioni coinvolgono vari aspetti:

- ✓ Deve esistere un elenco costantemente aggiornato degli Asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile.
- ✓ Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
- ✓ Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base

al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.

- ✓ Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- ✓ Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- ✓ Per poter gestire in modo tempestivo gli incidenti (sia potenziali che effettivi) relativi alla Sicurezza delle Informazioni, tutti coloro che collaborano con l'azienda devono segnalare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere registrato e gestito come indicato nella procedura specificamente predisposta.
- ✓ È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- ✓ Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- ✓ Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- ✓ Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- ✓ Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

RESPONSABILITA' DI OSSERVANZA E ATTUAZIONE DELLE PROCEDURE

L'osservanza e l'attuazione delle procedure per garantire la Sicurezza delle Informazioni sono responsabilità di tutti coloro che, a qualsiasi titolo, collaborano con l'azienda e sono in qualsiasi modo coinvolti con il trattamento di dati e di informazioni che rientrano nel Campo di Applicazione del Sistema di Gestione per la Sicurezza delle Informazioni.

I collaboratori sono inoltre responsabili della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.

Tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda devono garantire il rispetto dei requisiti contenuti nella presente Politica per la Sicurezza delle Informazioni.

Il Responsabile del Sistema di Gestione della Sicurezza delle Informazioni, tramite procedure e prassi appropriate, deve:

- ✓ Eseguire periodicamente la valutazione dei rischi relativi alla Sicurezza delle Informazioni e adottare tutte le misure per la gestione del rischio
- ✓ stabilire tutte le procedure e prassi necessarie alla conduzione di tutte le attività aziendali garantendo la Sicurezza delle Informazioni
- ✓ verificare le eventuali violazioni al Sistema di Gestione della Sicurezza delle Informazioni e adottare le contromisure necessarie e controllare l'esposizione dell'azienda a minacce e rischi
- ✓ organizzare la formazione e promuovere la consapevolezza del personale per tutto ciò che concerne la Sicurezza delle Informazioni.
- ✓ verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione Sicurezza delle Informazioni.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole e procedure stabilite per la corretta Gestione della Sicurezza delle Informazioni ed in tal modo provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

RIESAME PERIODICO

La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione della Sicurezza delle Informazioni, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della presente Politica per la Sicurezza delle Informazioni in risposta agli eventuali cambiamenti dei fattori del Contesto, delle aspettative delle Parti Interessate, dell'ambiente aziendale, del business, delle condizioni legali.

Il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni ha la responsabilità della periodica verifica e riesame della presente Politica per la Sicurezza delle Informazioni.

Il Riesame dovrà verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica.

Il Riesame dovrà tenere conto di tutti i cambiamenti che possono influenzare l'approccio della azienda alla gestione della Sicurezza delle Informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

Il risultato del riesame dovrà includere tutte le decisioni e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni.

IMPEGNO DELLA DIREZIONE

La Direzione sostiene attivamente il Sistema di Gestione per la Sicurezza delle Informazioni:

- ✓ garantendo che siano identificati tutti gli obiettivi relativi alla Sicurezza delle Informazioni e che gli obiettivi siano coerenti con le risorse disponibili per permettere l'effettivo raggiungimento degli obiettivi stessi
- ✓ definendo chiaramente i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del Sistema di Gestione per la Sicurezza delle Informazioni
- ✓ rendendo effettivamente disponibili le risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema di Gestione per la Sicurezza delle Informazioni
- ✓ controllando che il Sistema di Gestione per la Sicurezza delle Informazioni sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
- ✓ approvando e sostenendo tutte le iniziative volte al miglioramento della sicurezza delle informazioni
- ✓ attivando programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

Schio, 18/01/2022

Direzione DEEPSER SRL Via Luigi dalla Via 3/B 36015 Schio (VI) - ITALIA P.IVA e C.F. IT04232140246 REA: VI-389342 www.deepser.com