POLITICA DELLA PRIVACY

Scopo e obiettivi

Con la politica della privacy **Sereni Orizzonti 1 S.p.A.** intende proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dal Regolamento (UE) 27/04/2016, n. 679 e dal Decreto Legislativo n. 196 del 30/06/2003 e s.m.i.

Campo di applicazione

La politica della privacy si applica a tutti gli organi e i livelli dell'azienda. La sua attuazione è obbligatoria per tutto il personale ed è inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno coinvolto con il trattamento di informazioni che rientrano nel campo dei Sistema di Gestione della Privacy.

Sereni Orizzonti 1 S.p.A. consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per le finalità connesse al corretto svolgimento delle attività aziendali nel rispetto delle regole e delle norme vigenti.

La nostra policy in tema di sicurezza delle informazioni

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate all'interno delle procedure aziendali, rispetto alle quali **Sereni Orizzonti 1 S.p.A.** assicura l'integrità, la protezione e l'accesso solo a chi è autorizzato.

La mancanza di adeguati livelli di sicurezza comporta principalmente il danneggiamento dell'immagine aziendale, la mancata soddisfazione degli ospiti o dei loro famigliari, senza escludere il rischio di incorrere in sanzioni legate alla violazione della normativa vigente nonché danni di natura economica e finanziaria.

Sereni Orizzonti 1 S.p.A. ha istituito e mantiene aggiornato un registro dei trattamenti.

L'azienda identifica tutte le esigenze di sicurezza tramite la valutazione di impatto sulla protezione dei dati che consente di acquisire consapevolezza del livello di esposizione a minacce dei propri sistemi di gestione dei dati. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità che tali minacce identificate diventino atti concreti. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

- I principi generali della gestione della sicurezza delle informazioni si basano su alcuni punti fondamentali.
- Esiste una catalogazione aggiornata degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuna è individuato un responsabile funzionale.
- Le informazioni sono classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza e integrità coerenti e appropriati.

- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi è sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo e agli incarichi ricoperti dai singoli utenti, in modo che ognuno di essi possa accedere alle sole informazioni di cui necessita; le autorizzazioni sono periodicamente sottoposte a revisione.
- Sono definite delle procedure per l'utilizzo sicuro dei beni strumentali volti alla gestione delle informazioni aziendali.
- È incoraggiata una consapevolezza adeguata da parte del personale delle problematiche relative alla sicurezza delle informazioni.
- Per poter gestire in modo tempestivo gli incidenti e le relative conseguenze, tutti sono invitati a notificare qualsiasi problema relativo alla sicurezza al responsabile protezione dati.
- È stata posta particolare cura nel prevenire l'accesso non autorizzato ai locali e alle apparecchiature dove sono gestite le informazioni.
- È posta particolare cura alla conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- È predisposto un piano di continuità che permette all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative rispetto alla missione aziendale. Gli aspetti di sicurezza sono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Viene fatto tutto il possibile al fine di garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni.

Responsabilità di osservanza e attuazione

L'osservanza e l'attuazione della policy sono responsabilità di:

- tutto il personale che, a qualsiasi titolo, collabora con l'azienda ed è in qualche modo coinvolto con il trattamento di dati e informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Privacy (il personale è responsabile 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 e che devono garantire il rispetto dei requisiti contenuti in questa politica.
- il Responsabile della Privacy che deve:
  - condurre l'analisi dei rischi con le opportune metodologie e dare l'indicazione al fine di adottare le misure per la gestione del rischio;
  - promuovere le norme necessarie alla conduzione sicura delle attività aziendali, verificando le violazioni relative alla sicurezza dei dati e di conseguenza promuovere l'adozione delle contromisure necessarie e controllare l'esposizione dell'azienda alle principali minacce e rischi;
  - dare disposizioni per l'organizzazione della formazione e la promozione della consapevolezza del personale per tutto ciò che concerne la sicurezza delle informazioni;
  - verificare periodicamente l'efficacia e l'efficienza del Sistema di Gestione della Privacy.

Il personale dell'azienda è istruito e sensibilizzato al rispetto di tutte le regole di sicurezza dei dati stabilite da **Sereni Orizzonti 1 S.p.A.**. Sono previsti percorsi di aggiornamento finalizzati a mantenere alta l'attenzione del personale verso il rispetto della normativa riguardante la privacy.

Riesame

La direzione aziendale verifica almeno una volta all'anno l'efficacia e l'efficienza del Sistema di Gestione della Privacy, in modo di assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e di favorire l'attivazione di un processo di aggiornamento continuo.

Il Responsabile della Privacy ha il compito di riesaminare questa politica. Il riesame deve verificare lo stato delle azioni correttive e di miglioramento, nonché l'aderenza dell'organizzazione alla Politica della Privacy in funzione dell'evoluzione dell'azienda. Deve pertanto tenere conto di tutti i cambiamenti che possono influenzare l'approccio dell'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 include tutte le revisioni procedurali e le azioni relative al miglioramento dell'approccio aziendale alla gestione della sicurezza delle informazioni.

Impegno della direzione

La direzione sostiene attivamente le attività inerenti la gestione della privacy aziendale tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.

L'impegno della direzione si attua tramite una struttura i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che questi incontrino i requisiti aziendali;
- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del Sistema di Gestione della Privacy;
- gestire le risorse aziendali messe a disposizione per la pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema di Gestione della Privacy;
- controllare che il Sistema di Gestione della Privacy sia integrato in tutti i processi aziendali e che le procedure e i controlli siano sviluppati efficacemente;
- approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni
- promuovere programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

Sereni Orizzonti 1 S.p.A. riconosce la propria responsabilità e si impegna a proteggere i dati personali che gli utenti affidano all'azienda da perdita, uso improprio o accesso non autorizzato. Per la protezione dei dati personali degli utenti, l'azienda si avvale di una serie di tecnologie, istruzioni operative e procedure aziendali di protezione.

Il Responsabile della Privacy
Dott. Alessandro Conte

Il Responsabile della Protezione dei Dati
Dott.ssa Micol Noacco