POLITICA PER LA SICUREZZA DELLE INFORMAZIONI
- UNI EN ISO 27001 -

Sesa S.p.A. (di seguito “Sesa” o “Società”) considera la tutela della Riservatezza, Integrità e Disponibilità del patrimonio informativo aziendale e dei dati gestiti tramite la propria infrastruttura ad alta affidabilità un presupposto imprescindibile per la competitività e la reputazione della Società. Le informazioni costituiscono beni aziendali che hanno un valore per la Società e devono essere protetti in modo adeguato. Questo documento stabilisce la Politica per la Sicurezza delle Informazioni (di seguito “Politica”), secondo le indicazioni dello standard ISO 27001 a cui Sesa ha aderito in forma volontaria. Costituisce il riferimento, al più alto livello, del Sistema di Gestione per la Sicurezza delle Informazioni (di seguito “SGSI”) definito e attuato in Sesa al fine di assicurare adeguata protezione alle informazioni in linea con le aspettative dei diversi stakeholders.

Il tema della sicurezza delle informazioni ha acquisito ormai un’importanza centrale sia a livello nazionale sia internazionale. Il quadro normativo di riferimento comprende, oltre allo standard ISO sopra citato, anche la normativa europea applicabile, in particolare la Direttiva NIS2, recepita in Italia con il Decreto Legislativo 138/2024, e il Regolamento Europeo DORA (Digital Operational Resilience Act) 2022/2554, relativo alla resilienza operativa digitale, per quanto pertinenti alle attività di Sesa.

La presente Politica è destinata a tutti i dipendenti e collaboratori della Società (di seguito “Destinatari”); sarà inoltre applicata anche alle parti interessate coinvolte nel trattamento delle informazioni alle quali si richiede di implementare parte delle politiche definite. Tutti i soggetti Destinatari sono responsabili dell'attuazione della presente Politica, allo scopo di proteggere il patrimonio informativo dell’azienda da tutte le minacce, interne o esterne, intenzionali o accidentali.

La sicurezza delle informazioni ha il compito di proteggere le informazioni da un ampio numero di minacce in modo da assicurare la continuità del business aziendale, minimizzare i danni e massimizzare il ritorno degli investimenti e delle opportunità commerciali. Secondo lo standard ISO 27000, essa si basa sulla tutela di tre principi fondamentali: riservatezza, integrità e disponibilità delle informazioni.

Garantire un adeguato livello di protezione di un sistema significa:
- ridurre ad un valore accettabile la probabilità che vengano violati i parametri di sicurezza informatica;
- individuare tempestivamente quando ed in quale parte del sistema questo accade;
- limitare i danni e ripristinare i requisiti violati nel minor tempo possibile.

In accordo con le indicazioni dello standard ISO 27001, la protezione viene effettuata attraverso un SGSI, con il quale si intende l’insieme delle misure tecniche ed organizzative volte ad assicurare la protezione della riservatezza, integrità e disponibilità delle informazioni.

I principi che l'azienda sceglie di seguire ed applicare nel perseguire la sicurezza delle informazioni sono:

- gestione dei rischi ICT secondo Framework robusti che ne garantiscano governance e controllo;
- gestione degli incidenti di ogni genere e in particolare degli incidenti ICT, con processi strutturati e noti e con reportistica il più possibile standardizzata, in modo da velocizzare i tempi di risposta;
- controllo continuo della sicurezza e rilevazione e gestione degli incidenti;
- Business Continuity Management e pianificazione di test di resilienza operativa adeguati alla realtà aziendale, periodici e supportati da piani di test di diverso livello di complessità correlati alle valutazioni formalizzate nell'Analisi di Impatto sul Business (BIA) e supportati di procedure di recovery;
- allineamento delle misure di sicurezza ai requisiti di business aziendali, conformi alle normative vigenti e agli obblighi contrattuali;
- gestione del rischio dei fornitori di servizi ICT e dei collaboratori esterni, in modo da stabilire solide relazioni contrattuali di impegno e responsabilità con le terze parti che operano nella filiera di fornitura del servizio ICT erogato;
- individuazione delle misure di sicurezza (controlli) da adottare a seguito del processo di valutazione del rischio, sulla base di criteri condivisi di accettazione, al fine di mantenere un adeguato equilibrio tra il costo dei controlli e quello del rischio associato;
- formazione e sensibilizzazione di tutto il personale aziendale, quale elemento fondamentale del processo di sicurezza, finalizzate ad accrescere la consapevolezza individuale e promuovere un utilizzo responsabile delle risorse, contribuendo al raggiungimento degli obiettivi prefissati;
- definizione di misure di sicurezza chiare e facilmente comprensibili, al fine di favorirne una corretta e diffusa applicazione;
- integrazione della sicurezza nell'ambito dei servizi erogati, da pianificare e applicare in tutte le fasi, a partire da quelle iniziali di progettazione e sviluppo;
- definizione delle autorizzazioni di accesso alle informazioni secondo il principio del need-to-know, in coerenza con le esigenze operative e di business aziendali;
- promozione della condivisione delle informazioni e delle analisi sulle minacce informatiche tra le aziende appartenenti allo stesso perimetro, in linea con le indicazioni delle autorità competenti, quale elemento di rafforzamento della capacità collettiva di risposta a tali minacce.

La sicurezza delle informazioni, intesa come tutela dei principi di riservatezza, integrità e disponibilità (continuità del servizio), rappresenta un fattore critico di successo al quale l'azienda attribuisce la massima attenzione, in relazione sia alla natura dei servizi erogati sia al proprio posizionamento sul mercato. A tal fine Sesa si è dotata di un SGSI che, in accordo con i principi sopraelencati e con lo scopo di contenere tali rischi a livelli accettabili e di risultare competitivi nei costi, prevede il raggiungimento dei seguenti obiettivi:

- essere conformi alle normative di legge (a titolo esemplificativo e non esaustivo, al D.Lgs. 196/03, al Regolamento UE 2016/679, al D.Lgs. 231/01 e ss.mm.ii., al Decreto NIS2 e al Regolamento UE DORA), agli standard e regolamenti di settore e ai requisiti contrattuali dei clienti;
- mantenere un sistema di sicurezza aziendale allineato a buone pratiche e standard internazionali, dandone evidenza alle parti interessate;

- verificare, mediante un processo di valutazione e gestione del rischio, il continuo allineamento strategico degli obiettivi di sicurezza con il business aziendale;
- diffondere in azienda una cultura della sicurezza delle informazioni;
- considerare il miglioramento continuo quale pratica per il mantenimento di un adeguato livello di sicurezza.

La Società è impegnata a promuovere la comprensione e la diffusione della Politica per la Sicurezza delle Informazioni a tutti i portatori di interesse.

Sesa ha cura di verificare e valutare costantemente il livello di sicurezza delle informazioni raggiunto e l'efficacia del proprio sistema di gestione nell'ottica del miglioramento continuo, anche mediante il conseguimento e il mantenimento delle certificazioni previste dai più avanzati standard internazionali di settore, allo scopo di consolidare, per tale ambito, la propria efficienza, qualità e affidabilità nella prestazione dei servizi e nella protezione sicura dei dati delle pubbliche amministrazioni.

La politica sulla sicurezza delle informazioni viene costantemente aggiornata e verificata, attraverso un riesame annuale e ogni qual volta se ne ravvisi la necessità, per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione e messa a disposizione dei clienti, degli stakeholders, dei soci e delle terze parti.

Empoli, lì 30/04/2025

Sesa S.p.A.