

POLITICA DELLA SICUREZZA DELLE INFORMAZIONI

Sommario

1. SCOPO, AMBITO E DESTINATARI DEL DOCUMENTO	3
2. DOCUMENTI DI RIFERIMENTO	3
3. TERMINI E DEFINIZIONI DI BASE RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI.....	3
4. GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI	4
4.1. OBIETTIVI PRINCIPALI E MISURAZIONI	4
4.2. REQUISITI DELLA SICUREZZA DELLE INFORMAZIONI	5
4.3. CONTROLLI DELLA SICUREZZA DELLE INFORMAZIONI.....	5
4.4. COMUNICAZIONE DELLA POLITICA.....	5
5. SUPPORTO PER L'IMPLEMENTAZIONE DELL'ISMS	5
6. VALIDITÀ E GESTIONE DEL DOCUMENTO	6

1. Scopo, Ambito e Destinatari del Documento

L'intento di questa Politica strategica è quello di definire lo scopo, la direzione, i principi e le regole base per la gestione della sicurezza delle informazioni.

Questa Politica si applica all'intero Information Security Management System (ISMS) di Proxima Informatica SpA, come definito nel documento di descrizione dell'Ambito dell'ISMS.

I destinatari di questo documento sono tutto il personale interno ed esterno di Proxima Informatica SpA, nonché le parti esterne rilevanti.

2. Documenti di Riferimento

- Standard ISO/IEC 27001, clausole 5.2 e 5.3
- Lista dei requisiti Legali, Regolatori e Contrattuali
- Documento della Descrizione dell'Ambito dell'ISMS
- Metodologia della Valutazione del Rischio e del Trattamento del Rischio
- Dichiarazione di Applicabilità (SoA)
- Piano di Formazione e Consapevolezza
- Procedura di Risposta e Notifica agli Incidenti di Sicurezza delle Informazioni
- Piano di Disaster Recovery

3. Termini e Definizioni di base relativi alla Sicurezza delle Informazioni

Riservatezza – proprietà di una informazione di non essere disponibile a individui, entità e processi non autorizzati.

Integrità – proprietà di una informazione di essere protetta relativamente alla sua accuratezza e completezza.

Disponibilità – proprietà di una informazione di essere accessibile e utilizzabile, entro i tempi previsti, su richiesta di un'entità autorizzata.

Sicurezza delle Informazioni – protezione della confidenzialità, integrità e disponibilità delle informazioni.

Information Security Management System – quella parte del Sistema di Gestione di un'organizzazione che si occupa della pianificazione, implementazione, manutenzione, revisione e miglioramento continuo della Sicurezza delle Informazioni.

4. Gestione della Sicurezza delle Informazioni

PROXIMA INFORMATICA considera la Sicurezza delle Informazioni un aspetto primario per la protezione del proprio Business e dei propri Clienti. Lo scopo dell'ISMS è quello di proteggere gli asset informativi dell'azienda, sia su supporti elettronici che cartacei, da minacce, interne ed esterne, deliberate e accidentali.

La Direzione di PROXIMA INFORMATICA riconosce che la protezione dei suoi asset informativi, all'interno dell'ambito dell'ISMS scelto, è la chiave per proteggere i dati in essi contenuti da perdite e danni. Perciò la Direzione si impegna a stabilire, mantenere e migliorare continuamente un Information Security Management System che soddisfi i seguenti obiettivi generali.

4.1. Obiettivi principali e Misurazioni

PROXIMA INFORMATICA si impegna a soddisfare i requisiti applicabili alla Sicurezza delle Informazioni e si impegna al continuo miglioramento del suo ISMS e all'efficacia dei controlli di sicurezza.

In linea con la sua missione, gli obiettivi principali dell'ISMS di PROXIMA INFORMATICA sono i seguenti:

- Proteggere la riservatezza, l'integrità e la disponibilità delle informazioni che sono critiche per il soddisfacimento della qualità dei servizi offerti ai Clienti e la reputazione di Proxima Informatica come Partner affidabile;
- L'ISMS definisce metodi e responsabilità per la gestione delle informazioni per preservarne:
 - Riservatezza: per prevenire la divulgazione delle informazioni a persone non autorizzate
 - Integrità: per assicurare che le informazioni siano corrette, complete e affidabili
 - Disponibilità: per assicurare che le informazioni siano rese disponibili a chi ne necessita e quando ne necessita
- Mantenere la conformità a leggi e regolamenti pertinenti e ai contratti dei Clienti (SLA);
- Valutare i rischi su base continua e stabilire misure di mitigazione commisurate all'impatto sul business;
- Fissare delle regole per il processamento e la gestione delle informazioni, che siano comunicate a tutti i dipendenti, all'interno dell'ambito scelto. Queste regole coprono politiche e procedure, relativamente alla sicurezza fisica, tecnologica e del personale;
- Formare il personale sulla Sicurezza delle Informazioni, attraverso dei piani di formazione annuali, e renderlo consapevole dell'importanza che il suo ruolo ha sulle performance dell'ISMS. Il personale dovrà essere formato, attraverso training per esempio, e dovrà essere valutato il suo livello competenza;
- Fissare regole per gestire incidenti di sicurezza, effettivi o sospetti, e vulnerabilità in modo da ridurre i loro effetti e i costi associati, sui Clienti, e preservare la reputazione dell'azienda;
- Stabilire un Business Continuity Management Framework e produrre piani di Business Continuity per contrastare interruzioni alle attività di business e per proteggere i processi di business critici dagli effetti di major failure o disastri. I piani saranno mantenuti e testati;

- Creare una migliore immagine di Proxima Informatica sul mercato, aumentandone il vantaggio competitivo;
- Essere conforme ai requisiti della ISO27001 e ottenerne la certificazione come tale.

Tali obiettivi sono in linea con la strategia e i piani di business dell'organizzazione. Il Responsabile dell'ISMS insieme alla Direzione di PROXIMA INFORMATICA è incaricato di rivedere questi obiettivi generali dell'ISMS regolarmente e di impostarne nuovi in caso di cambiamenti significativi, questo per garantire che siano e restino adeguati, efficaci e idonei.

PROXIMA INFORMATICA verificherà gli obiettivi e misurerà il loro raggiungimento almeno una volta l'anno.

Verranno effettuati Audit interni, ivi incluse verifiche sulla validità e l'efficacia dei controlli di continuità dell'information security, per ottenere informazioni su come viene implementato e mantenuto l'ISMS, sulla sua efficacia e per mettere in atto azioni correttive per il suo miglioramento continuo.

4.2. Requisiti della Sicurezza delle Informazioni

Questa Politica e l'intero ISMS devono essere conformi ai requisiti legali e regolatori rilevanti per PROXIMA INFORMATICA relativamente alla sicurezza delle informazioni e agli obblighi contrattuali.

Una lista dettagliata di tutti i requisiti legali e contrattuali è fornita nella Lista dei Requisiti Legali, Regolatori e Contrattuali.

4.3. Controlli della Sicurezza delle Informazioni

Il processo di selezione dei controlli è definito nella Metodologia della Valutazione del Rischio e del Trattamento del Rischio.

I controlli selezionati e il loro stato implementativo sono elencati nel Documento Dichiarazione di Applicabilità (SoA).

4.4. Comunicazione della Politica

Il responsabile dell'ISMS deve assicurare che tutto il personale di Proxima Informatica, così come le parti interessate esterne, per quanto appropriato, conoscano questa Politica.

5. Supporto per l'implementazione dell'ISMS

Con la presente Politica di Sicurezza delle Informazioni, la Direzione di Proxima Informatica si impegna a supportare l'implementazione dell'ISMS, la sua efficacia e il suo continuo miglioramento attraverso adeguate risorse al fine di raggiungere tutti gli obiettivi fissati in questa Politica e di soddisfare tutti i requisiti identificati.

6. Validità e gestione del Documento

Questo documento è valido dal 01/02/2022.

L'owner di questo documento è il Direttore Internal Operation che deve controllarlo e, se necessario, aggiornarlo almeno una volta l'anno.

Direttore Internal Operation