Politica per la sicurezza dei dati e delle informazioni

La Società Scala Virgilio & Figli S.p.A. ha per oggetto l'attività di costruzioni edili, stradali e ferroviarie mediante assunzione in appalto e subappalto delle relative prestazioni. Specializzata nella realizzazione di opere infrastrutturali ferroviarie, opera pertanto nel settore dei lavori pubblici nel rispetto delle normative che ne disciplinano procedure di qualificazione e di esecuzione. La Direzione è convinta che la sicurezza dei dati e delle informazioni sia un fattore abilitante strategico per la continuità operativa, il successo del *business* e il mantenimento della fiducia di Clienti e *stakeholder*.

La tutela del patrimonio informativo è una responsabilità prioritaria a tutti i livelli dell'organizzazione e un pilastro irrinunciabile per l'adempimento degli obblighi legali e regolamentari, inclusa la Direttiva NIS 2, data l'operatività in un settore ad alta criticità.

La presente Politica definisce l'impegno della Società e le direttive generali per l'istituzione e il mantenimento del Sistema di Gestione per la Sicurezza dei Dati. Lo scopo è garantire la tutela e la protezione da tutte le minacce (interne o esterne, intenzionali o accidentali) dei dati e delle informazioni.

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi della Società. La mancanza di un adeguato livello di sicurezza può comportare gravi danni economici, finanziari, e di reputazione, oltre al rischio di sanzioni legali.

Il Sistema di Gestione adottato dalla Società persegue il mantenimento dei tre pilastri fondamentali della sicurezza dei dati e delle informazioni:

- Riservatezza (confidenzialità): le informazioni devono essere accessibili esclusivamente da chi è autorizzato.
- Integrità: protezione della precisione e della completezza delle informazioni e dei metodi per la loro elaborazione, impedendo modifiche non autorizzate o accidentali.
- Disponibilità: gli utenti autorizzati devono poter accedere effettivamente alle informazioni e ai beni collegati nel momento in cui lo richiedono, garantendo la continuità operativa dei servizi.

Scala Virgilio & Figli S.p.A. si impegna a gestire la sicurezza delle informazioni attraverso un approccio basato sul rischio, che è il fondamento del Sistema di Gestione per la Sicurezza dei Dati e delle Informazioni:

- Identificare tutte le esigenze di sicurezza tramite l'analisi dei rischi, che valuta il livello di esposizione a minacce del proprio sistema informativo;
- Valutare le potenziali conseguenze e i danni derivanti dalla mancata applicazione di misure di sicurezza e la probabilità di attuazione delle minacce;
- Utilizzare i risultati di tale valutazione per determinare le azioni necessarie per gestire i rischi individuati e per implementare le misure di sicurezza più idonee.

I principi generali della gestione della sicurezza delle informazioni sono applicati attraverso l'implementazione dei seguenti controlli:

- Asset management: mantenere un catalogo aggiornato degli asset aziendali rilevanti e individuare un responsabile per ciascuno di essi. Classificare le informazioni in base al loro livello di criticità.
- Controllo degli accessi: ogni accesso ai sistemi è sottoposto a identificazione e autenticazione. Le autorizzazioni devono essere differenziate in base al ruolo e agli incarichi (principio del minimo privilegio) e sottoposte a revisione periodica.
- Gestione degli incidenti: tutto il personale è tenuto a notificare tempestivamente qualsiasi problema relativo alla sicurezza. Ogni incidente è gestito secondo procedure stabilite, garantendo la capacità di risposta rapida in ottemperanza ai requisiti di notifica previsti dal D.Lgs. 138/2024 e s.m.i. che impongono l'inoltro di un *early warning* entro 24 ore e di una notifica dettagliata entro 72 ore dalla conoscenza dell'incidente significativo.

- Continuità operativa: predisposizione e test di un Piano di Continuità Operativa e un piano di *Disaster Recovery* per affrontare efficacemente eventi imprevisti e garantire il ripristino dei servizi critici in tempi e modalità che limitino le conseguenze negative.
- Sicurezza fisica: prevenire l'accesso non autorizzato alle sedi e ai locali aziendali dove sono gestite le informazioni, garantendo la sicurezza delle apparecchiature.
- Sviluppo sicuro: includere gli aspetti di sicurezza in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
- Conformità e terze parti: assicurare la conformità con i requisiti legali, statutari e contrattuali. Includere requisiti di sicurezza e clausole contrattuali specifiche con i fornitori (terze parti) che trattano dati aziendali, per mitigare i rischi della catena di approvvigionamento (*supply chain security*).
- Risorse umane e consapevolezza: incoraggiare la piena consapevolezza delle problematiche di sicurezza in tutto il personale (dipendenti e collaboratori), a partire dalla selezione e attraverso programmi di informazione e formazione continua. La formazione è estesa in modo specifico agli organi di amministrazione e direzione per garantire la comprensione della gestione del rischio di cybersecurity e delle relative conseguenze.

Tutto il personale che collabora con la Società ed è coinvolto nel trattamento di dati e informazioni è tenuto all'osservanza e all'attuazione della presente politica. Allo stesso modo, tutto il personale è responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza

Chiunque, dipendente, consulente o collaboratore esterno, disattenda in modo intenzionale o per negligenza le regole di sicurezza stabilite e provochi un danno all'azienda, potrà essere perseguito nelle opportune sedi legali e contrattuali.

La Direzione sostiene attivamente la sicurezza delle informazioni 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 concretizza attraverso una struttura i cui compiti sono:

- Garantire che siano identificati tutti gli obiettivi di sicurezza dei dati 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 Sicurezza dei Dati e delle Informazioni.
- Fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema di Gestione della Sicurezza dei Dati e delle Informazioni.
- Controllare che il Sistema di Gestione della Sicurezza dei Dati e delle Informazioni sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente.
- Approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni.

La Direzione si impegna inoltre a verificare periodicamente, regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza dei Dati. Ciò è volto ad assicurare il miglioramento continuo e l'adeguamento della Politica in risposta ai cambiamenti dell'ambiente operativo, del business e delle condizioni legali.

Montevarchi, 20 novembre 2025

La Direzione
SCALA VIRGILIO & FIGLI spa
Amministratore Delegato