Principi generali in tema di sicurezza

PRINCIPI GENERALI

La rapida evoluzione dei sistemi informativi, delle procedure a loro connesse e delle minacce nel contesto globale, richiedono una sempre maggiore attenzione alla natura dei rischi che incombono sul patrimonio informativo, sui servizi erogati e, conseguentemente, sulle persone, il loro patrimonio e la loro privacy.

Il Gruppo FinecoBank attribuisce grande importanza alla sicurezza delle informazioni e del proprio sistema informativo in quanto costituisce:

- una risorsa strategica, elemento rilevante per lo sviluppo e la gestione del business e parte integrante del proprio patrimonio;
- un fattore chiave di successo per lo sviluppo del business e per il rafforzamento dell'immagine del Gruppo;
- un elemento distintivo per garantire la qualità e l'affidabilità dei servizi erogati e a supporto della corretta gestione dei dati.

In tale ottica **la sicurezza delle informazioni è, per il Gruppo FinecoBank, un elemento fondamentale per garantire gli interessi dei propri clienti e di tutti gli stakeholder, la continuità dei sistemi a supporto del business, oltre che per assicurare la conformità alla normativa vigente**: in questo contesto, il Gruppo indirizza e governa la sicurezza delle informazioni ispirandosi agli standard e ai principali framework e best practice internazionali.

Tali riferimenti devono trovare attuazione nel **Sistema di Gestione della Sicurezza del Gruppo**, ovvero nell'articolazione di regole interne, politiche, procedure, manuali, presidi organizzativi e tecnici, nonché in **un modello organizzativo strutturato volto ad assicurare che tali presidi siano periodicamente rivisti alla luce dell'evoluzione delle minacce**, sia interne che esterne, secondo il principio di miglioramento continuo.

I processi e le attività di governo e gestione della sicurezza informatica e del relativo rischio devono essere quindi organizzate secondo un modello che coinvolge gli Organi aziendali della Banca e le diverse funzioni aziendali, secondo le rispettive competenze ed in linea con i presidi relativi alle tre tipologie di controlli previste dal Sistema dei Controlli Interni, al fine di assicurare una corretta interazione tra tutte le funzioni e organi con compiti di controllo.

L'esito di tutte le attività descritte definisce un quadro di riferimento per la sicurezza delle informazioni nell'ambito del quale devono essere periodicamente valutati, rivisti e rafforzati gli interventi e le azioni volte ad assicurare:

- il **governo** e l'evoluzione della sicurezza in linea con gli obiettivi aziendali e con la **strategia ICT & Security** del Gruppo;
- la creazione di **un'organizzazione della sicurezza** condivisa, documentata, organica, efficiente, ed efficace;
- il **monitoraggio continuo** del panorama **delle minacce di sicurezza** applicabili al contesto in cui opera il Gruppo;

- il coordinamento e l'ottimizzazione delle **risorse** disponibili;
- l'implementazione di **misure di sicurezza preventive e reattive** per il contrasto alle minacce secondo un modello di sicurezza multilivello coerente con il principio di "**difesa in profondità**";
- l'integrazione delle procedure di sicurezza con i differenti processi aziendali, al fine di assicurare che le attività di identificazione e gestione dei rischi di sicurezza siano aspetti integranti delle iniziative condotte, anche in un'ottica di security by design e default;
- lo sviluppo e la crescita delle **competenze** e della **sensibilità sui rischi e sulle minacce di information & cyber security**, tramite attività periodiche di formazione e sensibilizzazione;
- il **monitoraggio attivo dei sistemi e degli eventi di sicurezza,** nonché il **presidio delle vulnerabilità tecniche**, tramite attività di **threat intelligence**, **vulnerability assessment e penetration test**, al fine di prevenire e identificare eventuali attacchi informatici verso il Gruppo;
- la **gestione degli eventi di sicurezza** rilevanti tramite un processo strutturato di **gestione degli incidenti e delle crisi**;
- la **conformità alle normative** applicabili;
- la **sicurezza nei rapporti con le terze parti e nelle attività esternalizzate**, tramite opportuni presidi da attuare sia a livello contrattuale sia durante il rapporto di collaborazione e la verifica del possesso di valutazione delle terze parti.