

Policy di Sicurezza Informatica - Estratto

 Banco di Desio e della Brianza S.p.A.

1. Premessa

Questo documento rappresenta un estratto della *Policy di Sicurezza Informatica* e descrive l'approccio generale in termini di governance, principi e sistemi adottati dal Gruppo al fine di garantire la sicurezza delle informazioni. Le politiche e le misure di sicurezza sono definite e applicate nel rispetto delle normative vigenti e delle migliori pratiche di settore.

2. Ruoli e responsabilità

Il Gruppo ha definito un modello strutturato di **governance della sicurezza delle informazioni**, volto a garantire un presidio efficace, integrato e coerente con le strategie di business e con il quadro normativo di riferimento.

La **responsabilità di indirizzo e supervisione strategica** in materia di sicurezza delle informazioni è attribuita agli Organi Aziendali di vertice, che approvano le politiche di sicurezza e ne monitorano periodicamente l'attuazione. La governance della sicurezza è integrata nei processi di **ICT governance**, di gestione dei rischi e di continuità operativa a livello di Gruppo.

Le funzioni specialistiche dedicate alla sicurezza informatica e alla continuità operativa operano in coordinamento con le funzioni di controllo e con le strutture operative, nel rispetto del principio di **separazione dei compiti**, assicurando un presidio costante dei rischi ICT e di sicurezza delle informazioni.

Il modello di governance adottato consente una **supervisione continua**, flussi informativi strutturati e un reporting periodico verso gli Organi competenti, favorendo un processo di miglioramento continuo del sistema di sicurezza delle informazioni.

3. Indirizzi e principi del "Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)"

Il Gruppo riconosce le informazioni e i dati come **asset strategici** per il conseguimento dei propri obiettivi di business e si impegna a garantirne un utilizzo sicuro, conforme e responsabile lungo l'intero ciclo di vita.

In particolare, il Gruppo si impegna a:

- **Migliorare continuamente** i sistemi di sicurezza delle informazioni, adottando un approccio basato sul rischio e ispirato alle best practice e agli standard internazionali di riferimento;
- **Garantire l'integrità, la riservatezza e la disponibilità dei dati**, assicurando che le informazioni siano protette da accessi non autorizzati, alterazioni indebite e indisponibilità;
- **Monitorare e gestire le minacce** alla sicurezza delle informazioni attraverso attività strutturate di prevenzione, rilevazione e risposta agli eventi di sicurezza;
- **Definire e diffondere responsabilità individuali** in materia di sicurezza delle informazioni per l'intera forza lavoro, promuovendo comportamenti consapevoli e conformi alle politiche aziendali;

- **Stabilire requisiti di sicurezza per le terze parti**, inclusi fornitori e partner, assicurando che il trattamento dei dati e l'erogazione dei servizi avvengano nel rispetto di adeguati livelli di protezione e delle normative applicabili.

Tali impegni si applicano a tutte le società del Gruppo e a tutti i soggetti che, a vario titolo, trattano o accedono alle informazioni aziendali.

Il Gruppo ha adottato un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** strutturato e coerente con i principali standard internazionali, finalizzato alla protezione del patrimonio informativo e alla resilienza operativa.

Il programma di gestione della sicurezza delle informazioni comprende, tra l'altro:

- **Piani di continuità operativa e disaster recovery**, volti a garantire la continuità dei servizi essenziali e il ripristino delle funzionalità critiche in caso di eventi avversi;
- **Processi di identificazione e gestione delle vulnerabilità**, basati su attività di monitoraggio, analisi e trattamento dei rischi di sicurezza;
- **Attività di audit interni** sull'infrastruttura ICT e sui presidi di sicurezza, svolte da funzioni indipendenti di controllo;
- **Audit esterni indipendenti**, anche in riferimento a standard internazionali quali ISO/IEC 27001, al fine di valutare l'adeguatezza e l'efficacia del sistema di sicurezza adottato;
- **Processi strutturati di segnalazione ed escalation**, che consentono a dipendenti e collaboratori di segnalare incidenti, vulnerabilità o attività sospette in materia di sicurezza delle informazioni;
- **Programmi di formazione e sensibilizzazione**, destinati a tutto il personale, con l'obiettivo di rafforzare la cultura della sicurezza e la consapevolezza dei rischi informatici.

Il sistema è oggetto di **riesame periodico** e di aggiornamento continuo per assicurare l'allineamento all'evoluzione del contesto tecnologico, normativo e delle minacce cyber.