Sintesi della Security Policy

INDICE

1 Premessa

Banca Generali, nell'ambito del contesto competitivo e del settore finanziario in cui opera, ha la primaria responsabilità di proteggere gli asset materiali e immateriali di cui dispone da ogni attacco ed accesso non autorizzato.

La Security Policy (di seguito anche la "*Policy*") descrive gli obiettivi, i principi di base e le principali responsabilità in materia di sicurezza all'interno di Banca Generali e comprende:

- *IT Security,* che riguarda la protezione dei dati e dei sistemi informativi da accessi non autorizzati, utilizzi, divulgazione, blocchi, modifiche o cancellazioni al fine di fornire riservatezza, integrità e disponibilità dei dati.
- *Cyber Security* che include la capacità di prevenire incidenti di sicurezza o vulnerabilità dei sistemi informatici e proteggere / difendere l'uso delle reti internet da attacchi cyber.
- *Physical Security,* che mira a garantire la protezione da accessi non autorizzati alle sedi, attrezzature e risorse, e alla protezione del Personale durante missioni e trasferte.
- *Corporate Security,* che attiene da una parte alla gestione degli aspetti di sicurezza nei più rilevanti eventi aziendali (per es. Assemblea degli azionisti) e dall'altra alle attività di *brand abuse*, di *social intelligence* e di *business intelligence*, anche a protezione della proprietà intellettuale da attacchi e danneggiamenti (es. spionaggio industriale e furto di dati) svolte anche in collaborazione con enti esterni, nonché autorità pubbliche nazionali e locali per raccogliere informazioni relative a specifiche minacce informatiche e fisiche legate ai brand monitorati.

La *Policy* si basa su standard internazionali, *framework* e *best practices* e completa il corpus normativo di Policy di cui la Banca si è dotata per determinare i principi e le linee guida di sicurezza degli applicativi informatici e di gestione integrata dei dati informativi, al fine di supportare in ottica *data driven* decisioni e strategie della Banca. Non rientrano in tale ambito le tematiche attinenti la salute e la sicurezza sul lavoro ex D.Lgs. 9 aprile 2008, n. 81.

2 Ambito di applicazione

La presente *Policy* si applica a tutti i dipendenti e collaboratori di Banca Generali e delle Società del Gruppo Bancario.

2.1 Ruoli e responsabilità

Il **Consiglio di Amministrazione**, quale organo con funzione di supervisione strategica, approva la strategia globale di sicurezza della Banca ed è tempestivamente informato di eventuali incidenti critici o eventi significativi in materia di sicurezza.

L'**Amministratore Delegato/Direttore Generale**, quale organo con funzione di gestione:

- su proposta del C.O.O., nomina il Chief Security Officer;
- definisce le misure di sicurezza, sulla base di quanto proposto dal Chief Security Officer;
- approva annualmente il Piano operativo della sicurezza e la Relazione sullo stato di attuazione delle iniziative di sicurezza;
- assume decisioni tempestive in merito a gravi incidenti di sicurezza o di significativi malfunzionamenti.

Il **Comitato Rischi** supporta l'Amministratore Delegato nella supervisione delle attività di attuazione e sviluppo della strategia di sicurezza della Banca.

Il ***Chief Security Officer*** (CSO) ha la principale responsabilità di definire la visione strategica della Security della Banca, implementare programmi a protezione degli asset informativi e volti a garantire la sicurezza delle Infrastrutture Informatiche e di identificare, sviluppare e implementare processi volti a mitigare i rischi derivanti dall'adozione delle tecnologie digitali.
Il Chief Security Officer è quindi responsabile di:

- sviluppare la strategia e la governance della *Security*;
- coordinare gli aspetti di sicurezza, con il supporto delle strutture organizzative coinvolte nei diversi processi;
- gestire gli aspetti della *Corporate Security*, in accordo con la funzione di Risk Management e in ottemperanza al *Framework* metodologico di gestione del rischio di reputazione e supportando su questo aspetto la struttura deputata nella gestione degli eventi aziendali più rilevanti;
- gestire gli aspetti della *IT & Cyber Security*, in accordo con la funzione di Risk Management e in ottemperanza al *Framework* metodologico di gestione dei rischi operativi, al cui interno sono ricompresi i rischi informatici;

- implementare il Piano di Sicurezza della Banca, in conformità e coerenza con il Piano strategico di sicurezza del gruppo assicurativo. Al fine di assicurare la corretta implementazione del Piano di Sicurezza il Chief security Officer valuta le specifiche esigenze della Banca, in termini di budget, pianificazione degli investimenti e risorse (finanziarie, umane, tecnologiche, ecc.);
- identificare i rischi per la sicurezza garantendo le opportune mitigazioni, promuovendo anche una cultura della sicurezza attraverso programmi di formazione e sensibilizzazione;
- monitorare e prevenire le attività di *Brand abuse* in ambito web e digitale;
- verificare la conformità ai requisiti di sicurezza informatica di tutte le modifiche sostanziali a sistemi e servizi IT;
- informare il C.O.O. e l'Amministratore Delegato in merito all'attuazione del Piano operativo di Sicurezza, relative risorse richieste e riguardo alle minacce alla sicurezza o incidenti critici che si sono verificati nel periodo di riferimento;
- promuovere e convocare di norma semestralmente un tavolo di confronto con le strutture responsabili per i relativi ambiti per un esame olistico delle varie componenti; al tavolo partecipano il C.O.O., che coordina il tavolo, il responsabile interno del Facility Management, il Chief Security Officer medesimo e il Responsabile Human Resources nonché il Responsabile Marketing e Relazioni esterne.
- gestire le attività volte all'aggiornamento del Business Continuity Plan (BCP) del Gruppo Bancario e alla realizzazione delle soluzioni di continuità individuate;
- garantire nell'ambito della sicurezza tutte le misure volte ad assicurare la protezione dei dati personali, raccordandosi in tal senso con il Data Protection Officer.

3 Missione e strategia di sicurezza

La missione della Banca è di proteggere l'insieme delle risorse fisiche, informatiche ed il patrimonio culturale dell'azienda, definendo un approccio comune per gestire gli elementi di sicurezza e promuovendo una cultura della sicurezza all'interno del Gruppo.

Per realizzare la sua missione e poter gestire efficacemente la crescente complessità dei rischi per la sicurezza, la Banca adotta un *approccio One-Security*, basato su una forte integrazione tra *IT Security, Cyber Security, Physical Security e Corporate Security*.

L'adozione di un approccio olistico è funzionale all'integrazione di processi, procedure e strumenti per l'identificazione, la valutazione e la gestione dei rischi per la sicurezza e per una efficace convergenza della sicurezza dove obiettivi di *IT Security, Cyber Security, Physical Security e Corporate Security* si sovrappongono e sono strettamente allineati. Questo approccio integrato della sicurezza riunisce le varie strutture della Banca che si occupano a vario titolo della sicurezza con altre parti dell'organizzazione consentendo la resilienza della Banca agli incidenti.

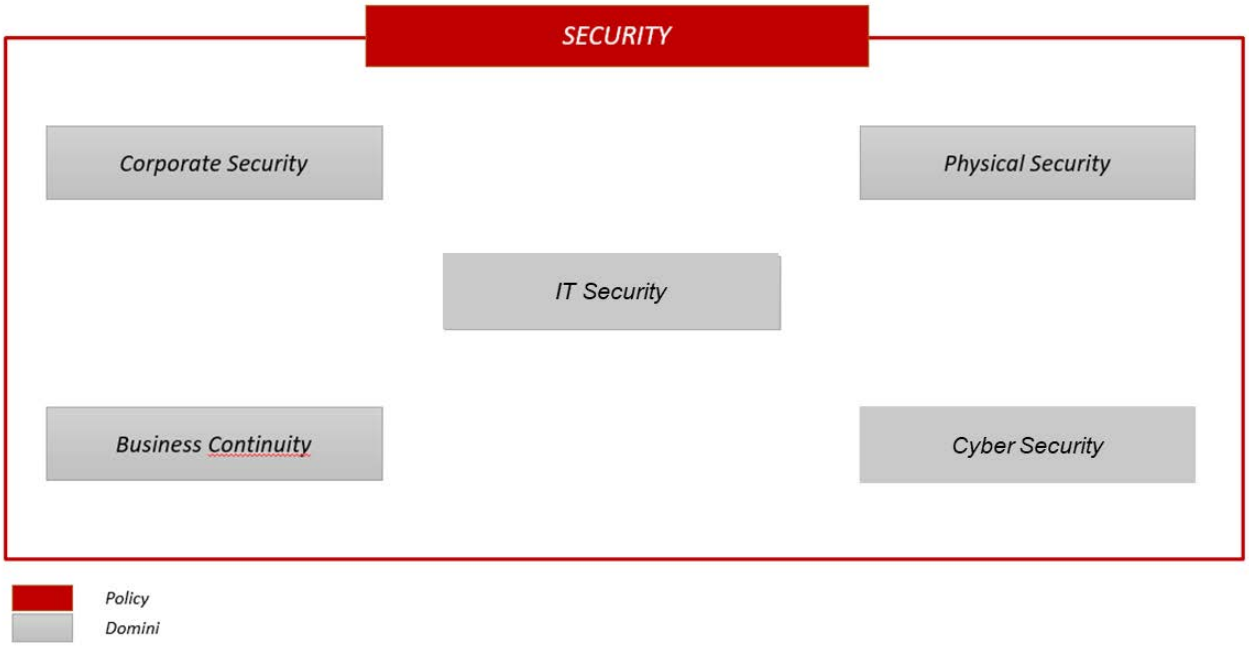
La strategia di sicurezza definisce un percorso per perseguire la mission di sicurezza dei beni aziendali, in linea con quella del Gruppo, e sfrutta i seguenti driver principali:

- *Prevenzione degli incidenti e protezione dalle minacce alla sicurezza:* il livello di esposizione ai rischi per la sicurezza, in particolare con riferimento ai rischi per la sicurezza informatica, deve essere costantemente monitorato, per attuare e migliorare adeguate misure di sicurezza che garantiscano la protezione delle risorse aziendali in termini di persone, informazioni e beni fisici;
- *Gestione dei rischi per la sicurezza con particolare attenzione ai fornitori di terze parti:* il livello di esposizione ai rischi per la sicurezza e in particolare il rischio relativo ai dati gestiti da terze parti richiede di valutare costantemente il loro comportamento, le prestazioni e i *Framework* di sicurezza su cui si basa la relazione;
- *Allineamento aziendale:* i nuovi servizi innovativi e digitali richiedono un livello di sicurezza e una resilienza dei servizi adeguati;
- *Conformità normativa:* la pressione esterna in termini di conformità e regolamentazione deve soddisfare requisiti normativi specifici, tra cui la protezione e la sicurezza dei dati personali.

4 Governance della sicurezza

4.1 Domini di sicurezza

La presente *Policy* include i seguenti domini di sicurezza, come descritto di seguito.



IT Security è un aspetto primario per garantire la continuità delle attività della Banca e per proteggere i dati di clienti, dipendenti e partner commerciali e riguarda la protezione di infrastruttura, applicazione, endpoints, dispositivi mobili e dati.

Cyber Security si occupa della prevenzione, identificazione e risposta a incidenti di sicurezza e vulnerabilità del sistema e della protezione dei dati e delle informazioni durante l'intero ciclo di vita da accessi non autorizzati, uso, divulgazione, distruzione, modifica o interruzione, tenendo anche conto della crescente rilevanza delle minacce informatiche a livello globale.

Corporate Security ha come obiettivo di preservare i beni e la proprietà intellettuale e include principi e requisiti per prevenire, scoraggiare, ritardare e mitigare possibili minacce,

minimizzare le conseguenze correlate e gestire in modo adeguato e tempestivo gli aspetti di sicurezza nei più rilevanti eventi aziendali (ad esempio l'assemblea dei Soci). Riguarda anche le attività di *business intelligence* eseguite in collaborazione con le autorità pubbliche locali e nazionali per raccogliere informazioni relative a specifiche situazioni economiche, politiche e finanziarie inerenti ai Paesi e/o a concorrenti e partner. La Corporate Security si riferisce inoltre alle attività di security intelligence per la protezione dei marchi e dei prodotti della Banca, monitorando la conversazione sui media digitali e le attività dannose sul web.

Physical Security include principi e requisiti per prevenire, scoraggiare, ritardare e mitigare possibili minacce, minimizzare le conseguenze correlate e gestire in modo adeguato e tempestivo potenziali incidenti di sicurezza relativamente alle sedi di lavoro e al personale. La Physical Security si riferisce alla definizione, attuazione e monitoraggio delle misure di sicurezza fisica necessarie per garantire un livello di sicurezza minimo degli edifici aziendali e degli spazi di lavoro interni, adottando un approccio basato sul rischio. Comprende la definizione e l'attuazione di azioni e misure da adottare al fine di garantire la sicurezza del Personale durante i viaggi di lavoro.

Business Continuity si riferisce all'individuazione delle priorità di un'organizzazione e alla preparazione di soluzioni per affrontare le minacce dirompenti, fornendo un quadro per una risposta efficace che salvaguardi gli interessi dei suoi *stakeholder* chiave, la reputazione e le attività di creazione di valore. Il dominio di continuità operativa comprende l'identificazione di operazioni e rischi critici, la predisposizione di piani per mantenere o ripristinare operazioni critiche durante una crisi e la creazione di piani per comunicare con le persone chiave durante la crisi.

4.2 Processo di Security Management

Per applicare correttamente ed efficacemente i principi di cui sopra, la Banca adotta un processo di gestione della sicurezza basato sui seguenti sotto processi:

A) identificazione,

B) protezione,

C) individuazione,

D) risposta,

E) ripristino.

Questi sotto processi dovrebbero essere eseguiti continuamente per formare una cultura operativa che indirizzi la sicurezza a livello operativo.

- *Identificare*

All'inizio del processo deve essere identificato il rischio per la sicurezza tenendo conto delle Risorse Aziendali e dei requisiti normativi rilevanti, definendo l'esposizione al rischio di sicurezza.

Il Chief Security Officer è incaricato di identificare i rischi per la sicurezza, nonché tutte le Misure di Sicurezza e le esigenze specifiche della Banca necessarie per mitigarle e riceve supporto e collabora con le altre strutture della Banca che presidiano particolari ambiti operativi di sicurezza.

- *Proteggere*

Questo processo consente di definire le misure di sicurezza da attuare al fine di proteggere le risorse della Banca durante l'esecuzione dei processi aziendali in base ai rischi e le azioni identificate nella fase precedente. Inoltre, è altresì necessario valutare le azioni da intraprendere per garantire la corretta attuazione del Piano operativo di Sicurezza della Banca e del Gruppo bancario. Le misure di sicurezza riguardano i seguenti ambiti:

- Gestione delle utenze e controllo degli accessi e delle autenticazioni
- Consapevolezza e formazione del personale sugli ambiti di sicurezza
- Sicurezza dei dati
- Processi e procedure di protezione delle informazioni
- Manutenzione e ripristino delle funzionalità e delle performance degli asset aziendali
- Tecnologie e sistemi di protezione al fine di garantire la sicurezza e la resilienza dei sistemi IT.

- *Individuare*

Questo processo consente di identificare il verificarsi di un evento di sicurezza, attraverso un rilevamento tempestivo di attività anomale e un monitoraggio continuo delle potenziali minacce e la valutazione dei potenziali impatti. In questa fase, il Chief Security Officer è incaricato di porre in essere le opportune attività per l'individuazione tempestiva di qualsiasi incidente di sicurezza che potrebbero interessare le Risorse Aziendali.

A tal fine, il Chief Security Officer è responsabile di coordinare il monitoraggio continuo delle potenziali minacce provenienti dall'ambiente esterno o da terzi e della valutazione dei potenziali impatti.

- *Rispondere*

A seguito del rilevamento di un evento di sicurezza, questo processo consente di definire attività appropriate da svolgere, al fine di attivare i processi di risposta e le attività di mitigazione con esecuzione tempestiva. L'apprendimento dalle attività di rilevazione/risposta fa parte di questo processo.

- *Ripristinare*

Questo processo consente di sviluppare e attuare attività appropriate per mantenere piani di resilienza e ripristinare tutte le capacità o servizi interessati da un evento di sicurezza, garantendo un ripristino tempestivo dei sistemi informativi e/o delle risorse fisiche interessati.