# Sintesi della Security Policy

| Codice | Versione | Data di approvazione |
|---|---|---|
| PY059 | 004 | 10/02/2025 |

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

# INDICE

**1 PREMESSA ..... 3**

**2 AMBITO DI APPLICAZIONE ..... 4**

2.1 Ruoli e responsabilità ..... 4

**3 MISSIONE E STRATEGIA DI SICUREZZA ..... 10**

**4 GOVERNANCE DELLA SICUREZZA ..... 11**

4.1 Domini di sicurezza ..... 11

4.2 Processo di Security Management ..... 13

4.3 Relazione annuale sullo stato di attuazione delle iniziative di sicurezza e Rapporto sintetico sulla situazione del rischio ICT e di sicurezza ..... 16

4.4 Information Security Measuring and Reporting Performance ..... 16

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

# 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.
- *Business Continuity,* che include la capacità di garantire il mantenimento delle funzioni aziendali critiche a livelli definiti accettabili in caso di eventi con severity *High* o *Very High*.
- *Fraud Management,* che include la capacità di prevenire, rilevare e mitigare i rischi derivanti da attività fraudolente perpetrate da soggetti esterni sui canali di remote banking, garantendo l'implementazione di misure di sicurezza avanzate, tecnologie di monitoraggio in tempo reale, e una formazione continua del personale per riconoscere e rispondere tempestivamente a tentativi di frode.

La Policy si uniforma ed è coerente con le linee guida contenute nella politica di sicurezza del Gruppo Assicurativo, ove non in contrasto con le normative di settore che la Banca è tenuta ad osservare.

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.

I principi ed i requisiti in materia di IT Security sono declinati più compiutamente all'interno della normativa di secondo livello della Banca.

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

# 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 ***Chief Security Officer*** (CSO), ruolo attribuito al Responsabile di *Sicurezza e BCP*, 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:

- supportare la definizione della strategia di sicurezza della Banca, integrando le linee guida di evoluzione strategica della sicurezza definite a livello di Gruppo Generali e tenuta in considerazione la propensione al rischio fissata nel Risk Appetite Framework, le politiche di esternalizzazione, l'articolazione in essere e a tendere dei settori di operatività, dei processi e dell'organizzazione della Banca;
- redigere la Relazione sullo stato di attuazione delle iniziative di sicurezza, inclusiva del Piano Operativo delle iniziative di sicurezza e del Piano di formazione e sensibilizzazione sulla sicurezza dell'informazione da sottoporre all'approvazione dell'Amministratore Delegato/Direttore Generale;
- definire, di norma con cadenza annuale, il Piano Operativo delle iniziative di sicurezza per conseguire gli obiettivi definiti nella strategia;
- valutare le specifiche esigenze della Banca, in termini di budget, pianificazione degli investimenti e risorse (finanziarie, umane, tecnologiche, ecc.), al fine di assicurare la corretta implementazione del Piano Operativo delle iniziative di sicurezza;
- definire, di norma con cadenza annuale e di concerto con *Chief People Office*, il Piano di formazione e sensibilizzazione sulla sicurezza dell'informazione, da sottoporre all'approvazione dell'Amministratore Delegato/Direttore Generale;
- assicurare il monitoraggio dello stato di implementazione del Piano Operativo delle iniziative di sicurezza e informa, di norma con cadenza annuale, il Responsabile di C.O.O. & Innovation e l'Amministratore Delegato/Direttore Generale;
- promuovere con periodicità trimestrale (o ad evento su richiesta del Chief Risk Officer), un tavolo di confronto per un esame olistico delle varie componenti di sicurezza; al tavolo partecipano: Responsabile di C.O.O. & Innovation, Chief Risk Officer, Chief Compliance Officer, Chief Audit Officer, Responsabile IT & Operations e in base alle necessità il Responsabile di Assistenza territoriali Reti e Succursali bancarie e il Responsabile di Logistica, il Responsabile di Chief People Office e il Responsabile di Marketing, Formazione e Comunicazione. In tali incontri sono rappresentati, inter alia, a) lo stato di avanzamento delle principali iniziative ICT e di sicurezza, b) le eventuali azioni di rimedio pianificate e/o in corso sui punti di miglioramento evidenziati dalle funzioni di controllo di secondo livello e c) l'andamento del monitoraggio di controlli di primo livello su temi di sicurezza;

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

- implementare la governance della sicurezza in Banca, coerentemente con il processo di Security Management (di cui al Cap. 5) e con il supporto delle strutture organizzative coinvolte nei diversi processi;
- in accordo con Chief Risk Office e in ottemperanza al modello metodologico di gestione del rischio di sicurezza e reputazionale, identificare i rischi specifici, raccogliere le informazioni necessarie per la loro valutazione e verifica, garantendo l'adozione delle opportune attività di mitigazione, rispetto ai vari domini di sicurezza (di cui al Capitolo 5);
- promuovere, nell'ambito della sicurezza, l'adozione delle misure volte ad assicurare la protezione dei dati personali, raccordandosi in tal senso con il Data Protection Officer;
- definire le modalità di implementazione di un processo di gestione della sicurezza delle terze parti, in conformità con la Policy di esternalizzazione e gestione terze parti ICT e considerando le linee guida del Gruppo Generali;
- definire le modalità di implementazione delle misure di sicurezza, e assicurare che tali misure siano implementate sui sistemi gestiti da terze parti;
- definire le modalità di implementazione delle misure di controllo accessi ai sistemi informativi della Banca, ivi inclusi gli accessi di utenti privilegiati e assicurare che tali misure siano implementate sui sistemi gestiti da terze parti;
- definire le modalità di esecuzione di un piano di test di sicurezza annuale sui sistemi informativi gestiti dalla Banca e assicurare che tali verifiche siano eseguite per i sistemi gestiti da terze parti;
- definire le modalità di implementazione di un processo di Security by Design che consenta l'implementazione delle opportune misure di sicurezza e protezione durante la fase di acquisizione di una tecnologia innovativa, progettazione di un nuovo sistema informatico o in caso di modifiche sostanziali ai sistemi esistenti (change management);
- in caso di richiesta da parte dell'Autorità di Vigilanza di esecuzione di un Threat Led Penetration Test (TLPT), definire il documento di specifica dello scope del TLPT ed informare il Consiglio di Amministrazione della Banca. Il documento include: (i) l'elenco e le informazioni correlate sulle Funzioni Critiche o Importanti da coinvolgere e (ii) una descrizione di alto livello degli obiettivi delle attività di test;
- definire un processo di gestione degli incidenti di sicurezza per la Banca e informare tempestivamente, l'Amministratore Delegato, il Consiglio di Amministrazione della Banca e la funzione sicurezza del Gruppo Generali in caso di incidenti Major (incidenti con severity Alta o Molto Alta) e/o gravi minacce di sicurezza;
- garantire che siano attivate le procedure e le tecnologie, inclusi i servizi messi a disposizione dal Gruppo Generali (es. Security Operation Center, Group Cyber Threat Intelligence, Brand Abuse), atti a garantire l'identificazione di eventi di sicurezza e la rilevazione di incidenti di sicurezza;
- garantire l'adozione di un framework di sicurezza fisica e la sicurezza degli eventi, supportando in questo aspetto Eventi istituzionali, Corporate Communication e Immagine nella gestione degli eventi aziendali più rilevanti;
- definire le modalità di implementazione delle misure di controllo accessi alle sedi della Banca, e assicurare che tali misure siano implementate per la protezione dei data center gestiti da terze parti;
- garantire l'adozione di misure di prevenzione e assicurare il monitoraggio in ottica antifrode dei canali diretti (Home Banking e Mobile Banking), collaborando con le strutture preposte di informativa sulle perdite subite a Chief Risk Office;

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

- assicurare il reporting verso il Chief Security Officer del Gruppo Generali riguardante lo stato dei servizi di sicurezza secondo le modalità condivise dalla sicurezza del Gruppo Generali;
- garantire, con il supporto di Normativa e Regulatory Hub, l'aggiornamento della presente Policy e la predisposizione / aggiornamento delle Policy e normative operative di sicurezza da essa derivanti.

Il Chief Security Officer deve essere dotato delle risorse adeguate alle proprie responsabilità, non essere coinvolto nelle attività di business al fine di evitare conflitti di interesse e deve essere posto a diretto riporto del Responsabile dell'Area C.O.O. & Innovation.
In linea con i processi HR e i requisiti normativi di Banca Generali, il Modello di Governance della Sicurezza è declinato come segue:

- Sourcing: l'assunzione e il licenziamento del Chief Security Officer sono di competenza del Responsabile di C.O.O. & Innovation (sentito Chief People Office) in accordo con l'Amministratore Delegato/ Direttore Generale.

- Valutazione della performance: la definizione degli obiettivi e la valutazione degli obiettivi del Chief Security Officer sono di competenza del Responsabile di C.O.O. & Innovation in accordo l'Amministratore Delegato/Direttore Generale, secondo le procedure ed i processi di Gruppo tempo per tempo vigenti.

Il ***Chief People Office***, per quanto concerne la sicurezza fisica, si occupa, in coordinamento con il *Chief Security Officer*, degli aspetti operativi della sicurezza del Personale per quanto attiene missioni e trasferte. Inoltre, il *Chief People Office* supporta il *Chief Security Officer* nella implementazione delle iniziative di formazione e sensibilizzazione su tematiche di sicurezza.

Il **Vice Direttore Generale Distribution**, per il tramite di Assistenza territoriali Reti e Succursali bancarie e di Logistica, è responsabile di:

- implementare sulla base del Piano di Sicurezza gli aspetti operativi afferenti alla sicurezza fisica, in accordo con il Chief Security Officer;

- gestire, per le tematiche di competenza, gli outsourcer del Gruppo Assicurativo in materia di Facility Management;

- sulla base dei rischi per la sicurezza fisica identificati dal Chief Security Officer, garantire le opportune mitigazioni;

- verificare la conformità ai requisiti di sicurezza fisica di tutte le modifiche sostanziali a sedi, Dipendenze e locali della Banca;

- informare tempestivamente il Chief Security Officer sulle minacce alla sicurezza o incidenti critici (es. rapine) avvenute

Nell'ambito della sicurezza del personale (es. rapine), *Assistenza territoriale Reti e Succursali bancarie* riceve il supporto e la collaborazione di *Chief People Office*.

Il ***Chief Communication Office & External Relations***, relativamente alla *Corporate Security*, in coordinamento con il *Chief Security Officer*, si occupa delle tematiche degli aspetti operativi di sicurezza nell'ambito dell'organizzazione degli eventi aziendali.

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

Il Responsabile di C.O.O. & Innovation è responsabile di:

- sovrintendere all'attuazione del piano di Sicurezza e delle iniziative di sicurezza della Banca;
- supervisionare l'adeguata implementazione delle Misure di Sicurezza e informare periodicamente il Comitato Rischi sulla strategia di sicurezza degli ambiti di propria competenza, la definizione e implementazione del piano operativo di sicurezza e sulle minacce alla sicurezza o incidenti critici che si sono verificati nel periodo di riferimento;
- approvare e sottoporre, per il tramite dell'Amministratore Delegato, all'attenzione del Consiglio di Amministrazione linee guida, direttive, standard di gestione della Sicurezza Informatica in merito all'evoluzione del campo di attività, ai prodotti forniti ed alle tecnologie;
- assumere il più alto grado di responsabilità nella gestione delle situazioni ad alta criticità supportando la predisposizione di eventuali comunicazioni verso gli organi di Vigilanza e/o verso il corrispondente ruolo a livello di Gruppo.

Le responsabilità si applicano a IT Security (protezione infrastrutture e dati), Cyber Security (prevenzione e risposta a incidenti), Corporate Security (protezione IP, eventi e intelligence), Physical Security (protezione sedi e personale), Business Continuity (resilienza e risposta a crisi).

In linea con i processi HR e i requisiti normativi di Banca Generali, il Modello di Governance della Sicurezza è declinato come segue:

- Sourcing: l'assunzione e il licenziamento del CSO sono di competenza del Responsabile dell'Area C.O.O. & Innovation (sentita la Direzione Human Resources) in accordo con l'Amministratore Delegato/Direttore Generale.
- Valutazione della performance: la definizione degli obiettivi e la valutazione degli obiettivi del CSO sono di competenza del Responsabile dell'Area C.O.O. & Innovation in accordo l'Amministratore Delegato/Direttore Generale, secondo le procedure ed i processi di Gruppo tempo per tempo vigenti.

Il ***Chief Risk Office***, nell'ambito del proprio ruolo di controllo, si interfaccia con il Chief Security Officer per l'identificazione, la valutazione e la verifica delle misure da adottare per la mitigazione di rischi di sicurezza, in base alla propensione del rischio definito nel Risk Appetite Framework della Banca. Il *Chief Risk Office*, nell'ambito di gestione dei rischi di sicurezza e dei rischi reputazionali:

- promuove l'allineamento regolare con il Chief Security Officer ed esamina i rischi di sicurezza per la Banca;
- coopera con il Chief Security Officer per raccogliere le informazioni necessarie a quantificare l'esposizione ai rischi di sicurezza;
- è informato tempestivamente dal Chief Security Officer in caso di gravi incidenti di sicurezza o continuità operativa e in caso di qualsiasi evento che possa modificare significativamente il livello dei rischi di sicurezza identificati nel perimetro della Banca;
- è informato dal Chief Security Officer periodicamente sullo stato di implementazione delle misure di sicurezza nel perimetro di responsabilità e specificamente per quanto riguarda l'implementazione della strategia di sicurezza;

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

- è informato periodicamente riguardo i principali Key Performance Indicator (KPI) di sicurezza nel perimetro della Banca.

Il ***Chief Compliance Office***, nell'ambito del proprio ruolo di controllo, verifica periodicamente l'adeguatezza dei controlli di sicurezza in relazione ai requisiti normativi e regolatori.

Il ***Chief Audit Office***, nell'ambito del proprio ruolo di controllo, verifica periodicamente l'efficacia e l'efficienza degli standard, dei controlli, delle Policy e delle procedure definite.

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

Nell'ambito delle attività del Comitato Rischi, semestralmente, vengono trattate le tematiche attinenti la sicurezza per un esame olistico delle sulle varie componenti per garantirne una visione integrata sui vari ambiti specialistici e di competenza, a cura del Chief Security Officer, con la presenza del Responsabile di C.O.O. & Innovation, del Vice Direttore Generale *Distribution*, del Responsabile di *Chief People Office* nonché del Responsabile di *Chief Communication Office & External Relations*.

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

- su proposta del Responsabile della struttura C.O.O. & Innovation, nomina il Chief Security Officer;
- definisce i ruoli e le responsabilità per la gestione del rischio di sicurezza, nonché per le relative attività di continuità operativa;
- approva con cadenza annuale la Relazione sullo stato di attuazione delle iniziative di sicurezza, inclusiva del Piano Operativo delle iniziative di sicurezza e del Piano di formazione e sensibilizzazione sulla sicurezza dell'informazione;
- assicura che tutto il personale, incluso il personale che riveste ruoli chiave, riceva una formazione adeguata in materia di rischi ICT e di sicurezza;
- assume decisioni tempestive in merito a gravi incidenti di sicurezza informatica e, con il supporto delle Funzioni aziendali di Controllo, fornisce informazioni al Consiglio di Amministrazione in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti.

Il ***Consiglio di Amministrazione,*** quale organo con funzione di supervisione strategica, quale organo con funzione di supervisione strategica, è tempestivamente informato di eventuali incidenti critici o eventi significativi in materia di sicurezza. Inoltre, il Consiglio:

- approva la strategia ICT della Banca, comprendente le linee guida strategiche di sicurezza, su proposta dell'Amministratore Delegato / Direttore Generale;
- approva, con il supporto del Comitato Controllo e Rischi l'assetto organizzativo e di governo della Banca con riferimento al sistema informativo e alla gestione del rischio di sicurezza aziendali;

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

- assicura che il sistema di governo e controllo dei rischi di sicurezza sia costantemente adeguato, anche in termini di dimensionamento qualitativo e quantitativo del personale e di risorse finanziarie disponibili, alle esigenze operative e per l'attuazione della strategia di sicurezza;
- è informato dall'Amministratore Delegato/Direttore Generale riguardo la Relazione sullo stato di attuazione delle iniziative di sicurezza, inclusiva del Piano Operativo delle iniziative di sicurezza e del Piano di formazione e sensibilizzazione sulla sicurezza dell'informazione;
- è informato tempestivamente dall'Amministratore Delegato e/o dalle Funzioni aziendali di controllo coinvolte in caso di gravi incidenti di sicurezza e malfunzionamenti del sistema informativo con un impatto sulla continuità operativa della Banca.

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

# 3 MISSIONE E STRATEGIA DI SICUREZZA

La strategia di sicurezza adottata dalla Banca si basa su un modello integrato One-Security, che unisce in modo sinergico gli ambiti della IT Security, Cyber Security, Physical Security e Corporate Security, in linea con i più recenti orientamenti normativi nazionali ed europei.

Questo approccio trae fondamento da regolamenti come il Regolamento (UE) 2016/679 (GDPR) per la protezione dei dati personali, la Direttiva NIS 2 (Direttiva (UE) 2022/2555) per la sicurezza delle reti e dei sistemi informativi, e dal D.Lgs. 231/2001 in materia di responsabilità amministrativa degli enti, integrando i principi previsti da tali normative all'interno delle politiche e delle procedure aziendali di sicurezza.

Tra i driver strategici più rilevanti si evidenziano:

- Prevenzione degli incidenti e protezione dalle minacce: la Banca adotta misure tecniche ed organizzative adeguate a prevenire eventi dannosi e proteggere le informazioni, i beni fisici e le persone, conformemente all'art. 32 del GDPR e alle linee guida dell'ENISA (European Union Agency for Cybersecurity). Vengono effettuate periodiche attività di risk assessment e vulnerability assessment, in osservanza anche delle prescrizioni di Banca d'Italia in tema di sicurezza informatica.
- Gestione dei rischi, con particolare attenzione ai fornitori terzi: in ottemperanza all'art. 28 del GDPR e alle indicazioni dell'EBA (European Banking Authority) sulle esternalizzazioni, la Banca prevede una rigorosa valutazione dei fornitori di servizi terzi, sia sotto il profilo della sicurezza dei dati che della resilienza operativa. Ogni rapporto contrattuale include clausole specifiche su sicurezza, auditabilità e conformità regolamentare.
- Allineamento aziendale e resilienza dei servizi digitali: l'adozione di nuove tecnologie e servizi innovativi avviene nel rispetto dei requisiti di sicurezza applicabili, come previsto dalle normative del settore bancario e finanziario (ad esempio, le Disposizioni di Vigilanza di Banca d'Italia e la PSD2 per i servizi di pagamento digitali). La resilienza operativa è assicurata da piani di continuità operativa e disaster recovery, anch'essi definiti in conformità alle best practice internazionali (come lo standard ISO/IEC 27001).
- Conformità normativa e regolamentare: tutte le attività vengono costantemente monitorate e aggiornate per garantire l'aderenza ai requisiti delle normative di settore, quali GDPR, NIS 2, D.Lgs. 196/2003 e le linee guida emanate dalle autorità di vigilanza competenti. È inoltre prevista una formazione continua del personale sui temi della sicurezza e della privacy, come richiesto dalle disposizioni di legge.

In questo modo, la strategia di sicurezza della Banca si struttura come un sistema dinamico e proattivo, capace di rispondere tempestivamente alle evoluzioni normative e alle nuove minacce, assicurando la tutela del patrimonio aziendale e la fiducia di clienti e stakeholder.

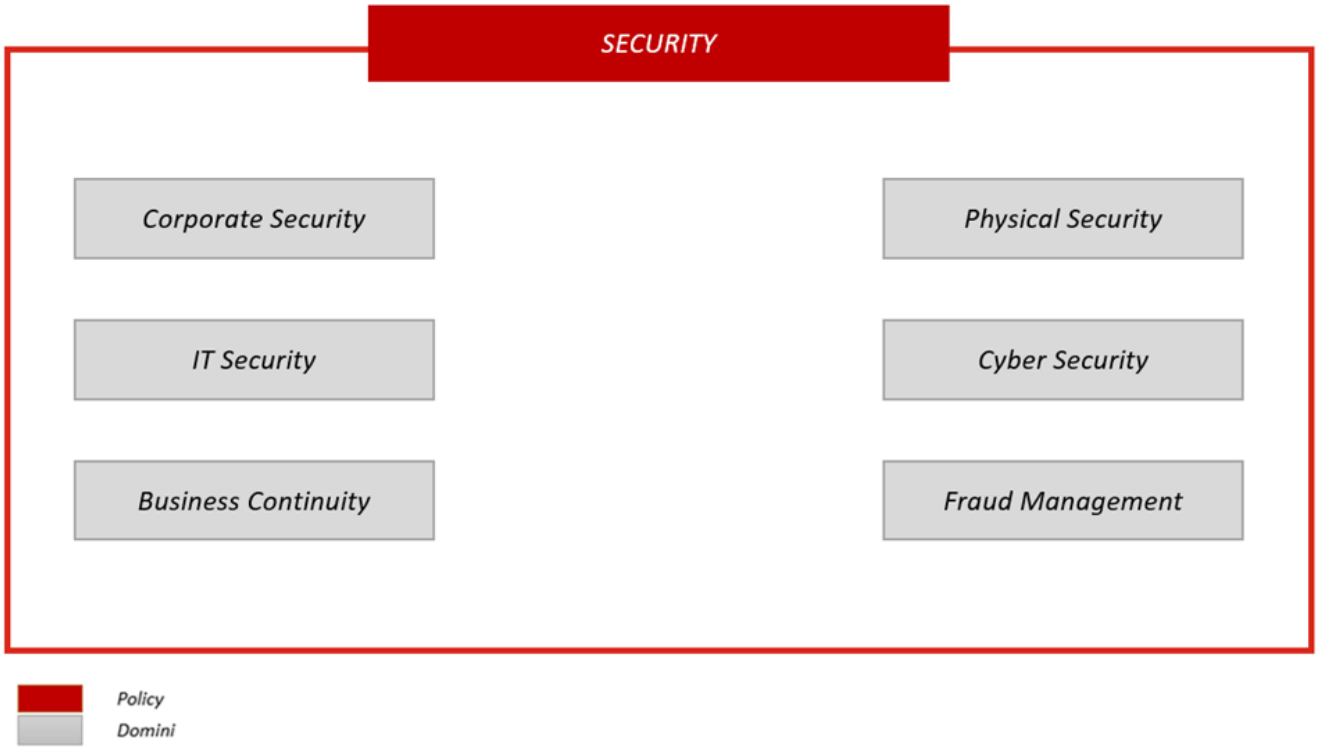
Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

# 4 GOVERNANCE DELLA SICUREZZA

## 4.1 Domini di sicurezza

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




**IT Security** ha l'obiettivo primario di proteggere i dati aziendali di clienti, dipendenti e partner commerciali e comprende l'attuazione di misure a salvaguardia delle infrastrutture, delle applicazioni, degli endpoints, dei dispositivi mobili e dei dati.

**Cyber Security** ha l'obiettivo primario di garantire la prevenzione, identificazione e risposta agli incidenti di sicurezza e vulnerabilità del sistema informativo, tenendo anche conto della crescente rilevanza delle minacce informatiche a livello globale.

**Corporate Security** ha come obiettivo primario 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 le autorità pubbliche locali e nazionali per raccogliere informazioni relative a specifiche situazioni economiche, politiche e finanziarie inerenti i 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** ha come obiettivo primario prevenire, scoraggiare, ritardare e mitigare possibili minacce, minimizzare le conseguenze correlate e gestire in modo adeguato e tempestivo potenziali

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

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** ha come obiettivo primario garantire la continuità operativa delle attività della Banca, l'individuazione delle priorità e 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.

**Fraud Management** ha come obiettivo primario la protezione dell'integrità delle operazioni bancarie, a salvaguardia della Banca e dei suoi clienti da attività fraudolente. Questo obiettivo viene raggiunto attraverso attività di sicurezza che consentono di prevenire potenziali vulnerabilità nei processi bancari e nelle transazioni, nonché adottando tecnologie per rilevare continuamente attività sospette, ed infine, attuando misure efficaci per limitare i danni derivanti da attacchi fraudolenti, proteggendo asset bancari e interessi della clientela.

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

## 4.2 Processo di Security Management

Il Chief Security Officer, in collaborazione con Risk Management e con il supporto della Direzione IT & Operations, mantiene aggiornato l'inventario delle terze parti ICT e le sottopone a valutazioni di sicurezza nell'ambito del processo di Third Party Security (TPS).

Il Chief Security Officer, figura centrale nella struttura di sicurezza aziendale, opera in stretta collaborazione con la funzione Risk Management e con il supporto attivo della Direzione IT & Operations. Questa sinergia consente di mantenere costantemente aggiornato l'inventario delle terze parti ICT, garantendo una mappatura accurata di fornitori, partner e collaboratori che accedono a risorse e dati sensibili della Banca.

All'interno del processo di Third Party Security (TPS), vengono effettuate regolari valutazioni di sicurezza sulle terze parti, sia in fase di onboarding sia durante il rapporto contrattuale. Queste valutazioni prevedono l'analisi dei rischi connessi all'esternalizzazione di servizi e all'utilizzo di tecnologie di terzi, la verifica della conformità ai requisiti normativi e agli standard di sicurezza aziendali e, ove necessario, l'introduzione di misure di mitigazione specifiche.

Il Chief Security Officer supervisiona inoltre la definizione e l'aggiornamento delle procedure relative alla gestione delle terze parti, promuovendo una cultura della sicurezza condivisa non solo all'interno dell'organizzazione, ma anche verso tutti i soggetti esterni coinvolti. Attraverso audit periodici, controlli e momenti formativi mirati, viene assicurato che tutte le parti rispettino gli standard previsti e che eventuali criticità siano prontamente individuate e gestite.

Queste attività, integrate nei processi aziendali, rafforzano la postura di security complessiva della Banca, riducendo il rischio di esposizione derivante dalle relazioni con fornitori e partner esterni e contribuendo a una gestione proattiva delle minacce nel sempre più complesso scenario digitale attuale.

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.

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

**A) <u>Identificazione</u>**

Questa fase ha l'obiettivo di identificare i rischi di sicurezza e valutarne l'esposizione, tenendo conto dell'evoluzione delle minacce, degli impatti aziendali in caso di incidenti o violazioni di sicurezza e dei requisiti normativi.Il Chief Security Officer collabora con *Chief Risk Office* nell'identificazione dei rischi di sicurezza, nonché nella valutazione di tutte le misure di sicurezza e delle esigenze specifiche della Banca necessarie per mitigare tali rischi.

Nella valutazione dei rischi di sicurezza devono essere tenuti in considerazione:

- **Il contesto aziendale** basato sulla mission e strategia della Banca, gli obiettivi in termini di resilienza operativa digitale, gli stakeholder e le attività principali;
- **Il censimento degli asset aziendali** basata sui dati, il personale, i dispositivi informatici, i sistemi IT e le infrastrutture che consentono alla Banca di realizzare la strategia di sicurezza ed assicurare la gestione degli aspetti di sicurezza;
- **La gestione della sicurezza delle terze parti** basata su ogni rischio di sicurezza connesso con tali parti. In merito, deve essere assicurata una corretta classificazione delle terze parti coinvolte, la loro conformità ai requisiti di sicurezza fissati dalla Banca, devono essere definite appropriate attività di monitoraggio ed identificato ogni rischio di sicurezza dovuto ad eventuali interruzioni del servizio o dell'accordo;
- **Le normative sulla sicurezza** basate sulle disposizioni di vigilanza esterne e sul corpus normativo interno in materia di sicurezza e le specifiche attività poste in essere per gestire e monitorare la conformità della Banca ai requisiti di sicurezza; a tal fine, *Chief Compliance Office* fornisce consulenza al Chief Security Officer nella definizione dei processi, delle procedure interne e dei presidi organizzativi in conformità ai regolamenti interni e alle disposizioni esterne

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

di sicurezza.

Inoltre, il Chief Security Officer deve:

- coordinare e supportare le strutture di sicurezza delle Controllate entro il perimetro di propria responsabilità in modo da garantire un allineamento con la metodologia in atto per identificare correttamente l'esposizione al rischio di sicurezza;
- condividere con le strutture di sicurezza delle Controllate, entro il perimetro di propria responsabilità, i rischi comuni identificati;
- informare Chief Risk Office e la funzione sicurezza del Gruppo Generali di eventuali rischi significativi identificati nel perimetro delle Controllate.

**B) <u>Protezione</u>**

Questa fase ha l'obiettivo di definire le misure di sicurezza da attuare al fine di proteggere le risorse della Banca, a fronte delle valutazioni di rischio effettuate nella fase precedente, aggiornando il *Piano operativo di Sicurezza* della Banca e il *Piano di formazione e sensibilizzazione sulla sicurezza dell'informazione*.

Le misure di sicurezza, anche nell'ottica di garantire una efficace resilienza operativa digitale, possono riguardare al minimo i seguenti ambiti:

- Gestione delle identità, autenticazione e controllo degli accessi logici e fisici
- Sicurezza dei dati
- Sviluppo sicuro dei servizi informativi
- Gestione sicura delle attività operative sui sistemi informativi
- Gestione dei log e delle tracce informatiche
- Misure di protezione dalle frodi informatiche sui canali diretti
- Formazione e awareness del personale sugli ambiti di sicurezza.

**C) <u>Rilevazione</u>**

Questa fase ha l'obiettivo di garantire un monitoraggio continuo delle potenziali minacce di sicurezza e identificare il verificarsi di un incidente di sicurezza, attraverso un rilevamento tempestivo di attività anomale, e consentire la valutazione dei potenziali impatti associati.

**D) <u>Risposta</u>**

Questa fase ha l'obiettivo di mettere in atto le attività appropriate per contenere gli impatti derivanti da incidenti di sicurezza, consentendo di definire strategie adeguate e attività di mitigazione tempestive.

**E) <u>Ripristino</u>**

Questa fase ha l'obiettivo di sviluppare e attuare attività appropriate per mantenere piani di resilienza e ripristinare tutte le capacità o servizi interessati da un incidente di sicurezza

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

## 4.3 Relazione annuale sullo stato di attuazione delle iniziative di sicurezza e Rapporto sintetico sulla situazione del rischio ICT e di sicurezza

Il Chief Security Officer predispone, entro il primo semestre successivo all'anno oggetto di analisi, la Relazione annuale sullo stato di attuazione delle iniziative di sicurezza, sugli incidenti critici occorsi e sulle iniziative di formazione poste in essere. Con particolare riferimento a quest'ultimo aspetto, la Relazione comprende anche il Piano Operativo di

Sicurezza e il Piano di formazione e sensibilizzazione sulla sicurezza dell'informazione. Al fine di garantire una visione integrata dei vari ambiti di sicurezza, il Chief Security Officer riceverà il supporto delle strutture coinvolte negli aspetti operativi della sicurezza.

Il Piano operativo di sicurezza è definito dal Responsabile di C.O.O. & Innovation, per il tramite del Chief Security Officer avvalendosi anche del supporto delle strutture coinvolte, ognuna per gli ambiti di competenza, e sottoposto in un documento congiunto al parere del Comitato Rischi al fine di declinarne un sunto con gli elementi fondamentali.

Il Piano ha cadenza annuale e viene riesaminato ogni volta che si verifica un cambiamento significativo (ovvero cambiamenti nel modello organizzativo, nella legislazione, nel mercato, nella regolamentazione, nel panorama delle minacce informatiche, ecc.).

La Relazione sullo stato di attuazione delle iniziative di sicurezza è preventivamente validata dal Responsabile di C.O.O. & Innovation che la presenta al Comitato Rischi per un parere in merito e quindi la sottopone, congiuntamente al Piano operativo di Sicurezza e al Piano di formazione e sensibilizzazione sulla sicurezza dell'informazione, all'approvazione dell'Amministratore Delegato2.

La Relazione è poi sottoposta all'attenzione del Consiglio di Amministrazione da parte dell'Amministratore Delegato.

il Chief Risk Office predispone, invece, il Rapporto sintetico sulla situazione del rischio ICT e di sicurezza informatica e la Relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai sistemi di pagamento, con il supporto del Chief Security Officer e di C.O.O. & Innovation, così come indicato nella Policy Analisi e Gestione del rischio ICT e di sicurezza informatica.

## 4.4 Information Security Measuring and Reporting Performance

L'ambito della misurazione e reportistica delle performance di sicurezza informatica è fondamentale per permettere alla Banca, grazie ai dati forniti sia dai partner esterni sia dalle risorse interne, di monitorare nel tempo l'efficacia del proprio modello di gestione della sicurezza.

Attraverso specifici indicatori chiave di performance (KPI), la Banca può identificare tempestivamente le aree di miglioramento e rafforzare processi, procedure, servizi e strumenti tecnologici a supporto delle proprie attività.

L'individuazione e la raccolta dei KPI sono affidate al Servizio Sicurezza e BCP, che su base trimestrale condivide il KPI "Cyber Risk" con la Direzione Risk Management, integrandolo nel RAF

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.

aziendale.

Nel quadro del sistema di gestione della sicurezza, la Banca adotta una serie integrata e coerente di misure volte a proteggere le informazioni e garantire la resilienza operativa contro le minacce esterne.

Un elemento chiave riguarda la sicurezza nella gestione delle risorse umane (OdS3). In questo contesto vengono formalizzati i requisiti di sicurezza nei processi di inserimento, permanenza e uscita di personale interno ed esterno, chiarendo ruoli e responsabilità, regolamentando l'onboarding e l'offboarding, assicurando la restituzione di dispositivi e la revoca di credenziali, promuovendo la formazione periodica continua e applicando, quando necessario, misure disciplinari per violazioni delle policy.

Per quanto riguarda la gestione dei rapporti con i fornitori (OdS12), la Banca inserisce requisiti di sicurezza specifici nei contratti e nelle convenzioni. In questo modo si assicura che i servizi forniti siano conformi agli standard interni e alle normative, favorendo il monitoraggio delle performance di sicurezza dei partner, la verifica periodica tramite audit, nonché la definizione di piani di risposta agli incidenti che coinvolgano servizi esternalizzati.

La gestione delle terze parti ICT prevede inoltre il mantenimento di un inventario aggiornato, in collaborazione con IT e Operations, e la valutazione periodica dei fornitori secondo criteri di rischio e sicurezza delle informazioni (TPS), così da rilevare prontamente eventuali criticità e pianificare le azioni correttive.

Complessivamente, queste misure, integrate in modo organico nel framework di sicurezza della Banca, non solo garantiscono la conformità normativa, ma rafforzano la protezione delle infrastrutture e delle informazioni condivise, consolidando la capacità dell'organizzazione di rispondere in maniera efficace e dinamica alle potenziali minacce.

Il contenuto del presente documento costituisce materiale riservato e soggetto a copyright.

Ogni violazione sarà punita ai sensi di legge.