BANCA GENERALI

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

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

- approva, in funzione delle linee guida in materia di esternalizzazione assunte, le strategie di sviluppo del sistema informativo e la relativa architettura, in coerenza con l'articolazione in essere e a tendere dei settori di operatività, dei processi e dell'organizzazione aziendale;
- è informato tempestivamente dall'Amministratore Delegato e/o dalle Funzioni aziendali di controllo coinvolte in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo;
- approva la propensione al rischio informatico, avuto riguardo ai servizi interni e a quelli offerti alla clientela, in conformità con gli obiettivi di rischio fissati nel RAF – Risk Appetite Framework;
- assicura che il sistema di governance e, se applicabile, il sistema di gestione dei rischi e di controllo interno, gestiscano adeguatamente il rischio di sicurezza, all'interno del più ampio framework dei rischi operativi;
- assicura l'adozione e l'attuazione della strategia di sicurezza e del modello di governance di sicurezza di Banca Generali, in linea con le politiche del Gruppo Generali;
- assicura l'attuazione del piano strategico di sicurezza di Banca Generali, in linea con le politiche del Gruppo Generali.

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.
- approva, di norma con cadenza annuale, il piano operativo delle iniziative informatiche, verificandone la coerenza con le esigenze informative e di automazione delle linee di business nonché con le strategie aziendali;

- 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 **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 dell'Area C.O.O. & Innovation, del Responsabile dell'Area Canali Alternativi e di Supporto, del Responsabile della Direzione Human Resources nonché del Responsabile della Direzione Marketing e Relazioni Esterne.

La **Direzione Internal Audit**, nell'ambito del proprio ruolo di controllo, verifica periodicamente l'efficacia e l'efficienza degli standard, dei controlli, delle Policy e delle procedure definite e presenta al Consiglio di Amministrazione, con cadenza annuale, una specifica relazione sulla valutazione della sicurezza.

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;
- garantire, con il supporto del Servizio Normativa interna, l'aggiornamento della presente Policy.

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.

Il Responsabile dell'**Area 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.

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 Responsabile dell'**Area Canali Alternativi e di Supporto** è responsabile di:

- implementare sulla base del Piano di Sicurezza gli aspetti operativi afferenti alla Physical Security, 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;
- riguardo agli incidenti di Physical Security supportare il Chief Security Officer nella predisposizione della pertinente sezione dell'informativa.

Nell'ambito della sicurezza del personale (es. rapine), l'Area Canali Alternativi e di Supporto riceve il supporto e la collaborazione della Direzione Human Resources.

La **Direzione Human Resources**, per quanto concerne la Physical Security, si occupa, in coordinamento con il Chief Security Officer, degli aspetti operativi della sicurezza del Personale per quanto attiene missioni e trasferte.

La **Direzione Marketing e Relazioni Esterne**, 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.

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.

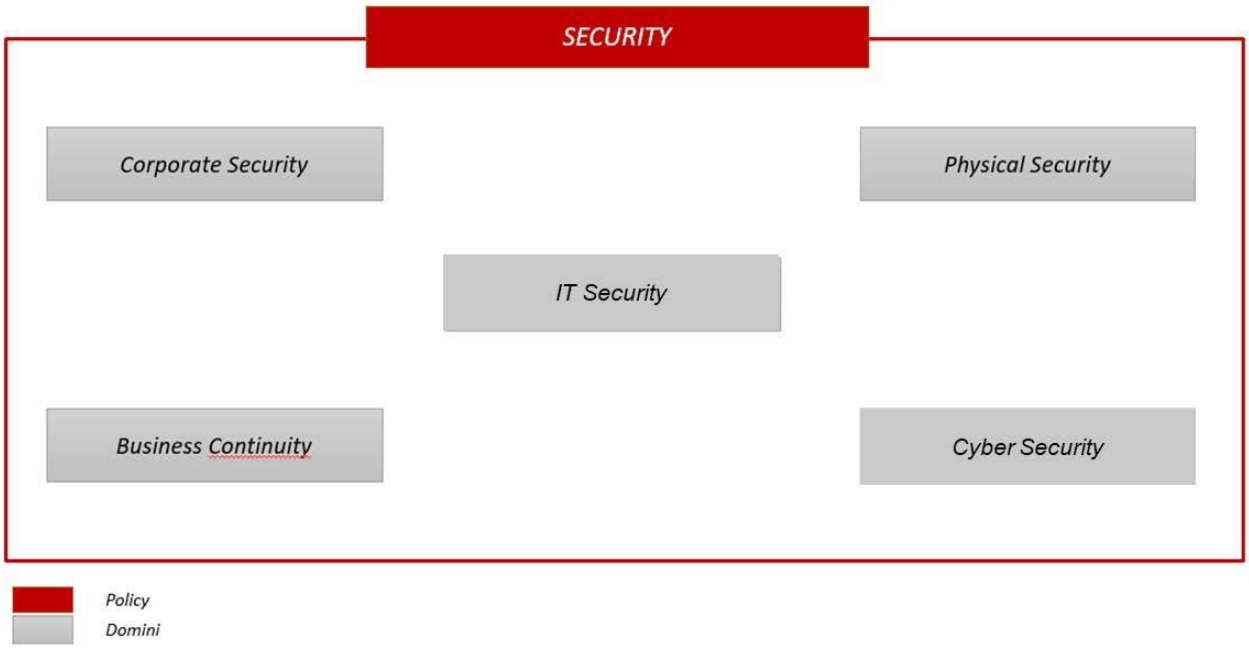
La strategia di sicurezza definisce un percorso per perseguire la mission di sicurezza dei beni aziendali, in linea con quella del Gruppo, e sfrutta i seguenti driver principali:

- *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.

- *Identificazione*

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.

Il Chief Security Officer deve considerare:

- i rischi di sicurezza relativi all'operatività della Banca (processi e sistemi IT), agli asset aziendali e al personale;
- 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;
- il contesto aziendale basato sulla mission e strategia della Banca, gli obiettivi, la tipologia di settore economico, gli stakeholders della banca e le attività principali;
- la gestione degli asset aziendali basata sui dati, il personale, i dispositivi informatici, i sistemi IT e le infrastrutture che permettono 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.

Pertanto, il CSO ha la responsabilità di implementare in stretta collaborazione con la funzione di Risk Management e con il supporto, ove necessario, della Direzione IT & Operations, la metodologia di gestione del rischio IT & Cyber Security e le relative attività di assessment e di provvedere ad un periodico confronto ed allineamento con la funzione di Risk Management al fine di riesaminare i rischi di sicurezza della Banca.

- *Protezione*

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: limitare l'accesso alle Risorse Aziendali (sia fisico che logico) a utenti, processi e dispositivi autorizzati.
- Consapevolezza e formazione del personale sugli ambiti di sicurezza
- Sicurezza dei dati: garantire un'adeguata protezione delle informazioni classificate, archiviate o trasmesse sia on-site che off-site.
- 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: garantire l'utilizzo di soluzioni tecniche adeguate, la protezione e la resilienza delle Risorse Aziendali e in particolare dei sistemi informatici.

- *Consapevolezza e formazione del personale sugli ambiti di sicurezza*

Gli interventi di "*awareness*" and "*education*" sono finalizzati alla generazione di una consapevolezza da parte del personale della Banca circa l'importanza di proteggere e trattare adeguatamente le informazioni sensibili prevenendo, intercettando e segnalando eventi o comportamenti che possono generare un danno per la Banca stessa.

In considerazione degli strumenti disponibili internamente e messi a disposizione a livello di Gruppo, dei piani formativi definiti dalla Direzione Human Resources o di altre modalità valutate di volta in volta opportune, è necessario prevedere periodicamente lo svolgimento delle seguenti attività:

- definizione della tipologia di interventi da attivare, il target dei partecipanti e / o dei destinatari di riferimento, le modalità di esecuzione (ad es. campagna mail, sessioni in aula, corsi tecnici, etc.);

- predisposizione, laddove non già disponibile, del materiale necessario all'esecuzione dell'intervento identificato;
- organizzazione degli eventi di "*awareness and education*", tra cui la predisposizione di un piano di formazione annuale per tutti i dipendenti e, per i soggetti incaricati di funzioni critiche (funzioni essenziali o importanti), predisposizione di un piano di formazione annuale ad-hoc sulla sicurezza delle informazioni;
- partecipazione di tutto il personale della Banca ai corsi di formazione, sensibilizzazione ed aggiornamento in materia di Sicurezza Informatica.

- *Individuazione*

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.In caso accada un Incidente di Sicurezza, il Chief Security Officer attiva prontamente le prime azioni necessarie per gestirlo, attivando l'appropriato Team di risposta agli Incidenti (IRT – Incident Response Team).

- *Risposta*

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.

In caso di Incidente Grave, il CSO deve attivare tempestivamente i processi di gestione delle crisi ed informare il Responsabile dell'Area C.O.O. & Innovation e l'Amministratore Delegato, che approverà le soluzioni al riguardo. Se necessario, devono essere prese in considerazione anche le misure pertinenti in materia di Business Continuity, previste dal piano di Business Continuity.

- *Ripristino*

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.

4.3 Piano operativo di sicurezza e Relazione annuale sullo stato di attuazione delle iniziative di sicurezza

Il *Piano operativo di sicurezza* è definito dall'Area 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 viene quindi trasmesso per approvazione all'Amministratore Delegato.

Il Chief Security Officer predispone una "*Relazione annuale sullo stato di attuazione delle iniziative di sicurezza*", sugli incidenti critici occorsi e sulle iniziative di formazione poste in essere. Al fine di garantire una visione integrata dei vari ambiti di sicurezza, il Chief Security Officer avrà il supporto delle strutture coinvolte negli aspetti operativi della sicurezza.

La *Relazione*, congiuntamente al *Piano operativo di sicurezza*, è sottoposta all'attenzione del Consiglio di Amministrazione da parte dell'Amministratore Delegato.

4.4 Relazione annuale sulla valutazione della sicurezza informatica

La Direzione Internal Audit, nell'ambito delle proprie competenze, predispone, entro il primo semestre successivo all'anno oggetto di analisi, la "*Relazione annuale sulla valutazione della sicurezza informatica*" focalizzata sulla governance ed organizzazione del sistema informativo, la sicurezza delle applicazioni e delle informazioni, i presidi di controllo, etc.

4.5 Information Security Measuring and Reporting Performance

L'ambito è finalizzato a consentire alla Banca, sulla base delle informazioni messe a disposizione dai fornitori e dalle risorse interne, di valutare nel tempo, anche attraverso opportuni KPI (Key Perfomance Indicators), l'efficacia del proprio modello di Gestione della Sicurezza. L'obiettivo è pertanto quello di facilitare l'identificazione delle misure di miglioramento ed il rafforzamento dei propri processi, delle procedure, dei servizi, delle attività e delle tecnologie e strumenti a supporto.

L'identificazione e la raccolta dei KPI è in carico al Servizio, Sicurezza e BCP.

Inoltre, su base trimestrale, il Servizio Sicurezza e BCP condivide con la Direzione Risk Management il KPI "Cyber Risk", che viene integrato all'interno del RAF.