Tipologia Documento: *Policy*

Policy Sicurezza Informatica

Struttura Competente: CIO

Data: dicembre, 2021

Versione: N. 6

Internal Use Only

ANAGRAFICA

Tipologia Documento	Policy	
Struttura Responsabile del Documento	CIO	
Contatti	CIO: Filipe Teixeira Filipe.Teixeira@illimity.com	
	Responsabile operativo: Luca Dozio Luca.Dozio@illimity.com	
Strutture coinvolte nel processo di condivisione della presente versione	Compliance & AML; HR & Organization	
Destinatari della normativa	**Società Capogruppo**	**Altre Società**
	illimity Bank S.p.A.	Entità del Gruppo Bancario
Versione approvata da	Amministratore Delegato	
Data approvazione	13/12/2021	
Data validità	14/12/2021	

VERSIONI

Titolo normativa con # versione	Principali modifiche	Organo approvante e data
Policy di sicurezza informatica V.1	Redazione del documento	Consiglio di Amministrazione, 27 febbraio 2019
Policy di sicurezza informatica V.2	Inserimento allegato tecnico N.1 – Regole per l'utilizzo dei sistemi e strumenti informatici	Responsabile Direzione Digital Operations, 24 giugno 2019
Policy di sicurezza informatica V.3	Aggiornamento della Policy per recepire il nuovo perimetro di Gruppo	Amministratore Delegato, 15 novembre 2019
Policy di sicurezza informatica V.4	Aggiornamento dell'allegato tecnico della policy per avere un maggior dettaglio rispetto alle possibilità di utilizzo degli strumenti banca; aggiornamento di alcuni riferimenti nella parte normativa; approfondimento di dettagli e linee guida che afferiscono alle tematiche della sicurezza informatica nell'interazione con soggetti terzio nella scelta dei prodotti e di sviluppo dei progetti	Amministratore Delegato, 23 settembre 2020
Policy di sicurezza informatica V.5	Aggiornamento del paragrafo *"Gestione degli Asset Aziendali"* per avere un maggior dettaglio rispetto alle modalità di trasmissione all'esterno dei dati aziendali	Amministratore Delegato, 24 settembre 2021
Policy di sicurezza informatica V.6	Affidamenti operativi di minor rilievo, propedeutici alla pubblicazione sul sito istituzionale	Amministratore Delegato, 13 dicembre 2021

Indice

1 SCOPO E AMBITO DI APPLICAZIONE

La *Policy* di Sicurezza Informatica definisce gli obiettivi del processo di gestione della sicurezza ICT adottato dal Gruppo Bancario, in linea con la propensione al rischio informatico definito a livello aziendale, e descrive i principi generali di sicurezza inerenti alla gestione del sistema informativo nonché i ruoli e le responsabilità connessi e il quadro di riferimento organizzativo e metodologico dei processi di gestione dell'ICT deputati a garantire l'appropriato livello di protezione.

La *Policy* stabilisce, inoltre, le linee di indirizzo adottate per le attività di comunicazione, formazione e sensibilizzazione delle diverse classi di utenti del personale del Gruppo Bancario.

La *Policy* costituisce un insieme di obiettivi, principi di sicurezza e pratiche che il Gruppo Bancario adotta e recepisce nelle proprie procedure operative in ambito Sicurezza IT, per garantire il controllo e/o il governo del Sistema Informativo aziendale.

In conformità al modello di full outsourcing stabilito, il Gruppo Bancario definisce gli obiettivi del processo di gestione della sicurezza ICT adottata dal gruppo, gli indirizzi da perseguire, le responsabilità nonché i principi guida per la realizzazione ed il mantenimento dell'adeguato livello di sicurezza del Sistema Informativo aziendale, in linea con la propensione al rischio aziendale, secondo regole e requisiti minimi stabiliti a livello aziendale e nel rispetto della normativa rilevante e dagli standard nazionali ed internazionali di riferimento.

Tale approccio permette costantemente al Gruppo Bancario di:

- soddisfare i bisogni della propria clientela;
- creare valore nel tempo per i soci;
- offrire un servizio di qualità caratterizzando le proprie azioni con professionalità, competenza, comprensione delle esigenze di ciascun cliente e trasparenza;
- assicurare la rigorosa osservanza delle norme;
- valorizzare la crescita professionale e personale delle risorse;
- tutelare la reputazione ed il patrimonio aziendale.

La definizione e l'implementazione di processi e procedure di Sicurezza Informatica sono finalizzate ad indirizzare le strutture preposte nel conseguimento degli obiettivi di seguito riportati:

- tutelare la riservatezza delle informazioni, evitando la loro consultazione e divulgazione non autorizzata;
- garantire l'integrità delle informazioni gestite dai sistemi e dalle altre risorse informatiche utilizzate per il loro trattamento, al fine di assicurare la loro correttezza e coerenza;
- garantire la disponibilità delle risorse informatiche per assicurare la continuità di erogazione dei servizi informatici/telematici, secondo le modalità ed i tempi prestabiliti dagli SLA contrattualmente definiti;
- garantire la conformità ed il rispetto delle disposizioni di legge in materia di sicurezza ICT, ottemperando alle normative cogenti in materia di data protection quali GDPR e circolare 285 di Banca d'Italia;
- assicurare l'autenticità e la provenienza dei dati e mantenere traccia degli aggiornamenti (non ripudio);
- garantire la sicurezza del Sistema Informativo aziendale sulla base dei risultati dell'analisi del rischio.

1.1 AMBITO DEL DOCUMENTO

Il Sistema Informativo del Gruppo Bancario costituisce una risorsa strategica del patrimonio aziendale e, analogamente a quanto avviene per i beni "materiali", deve essere adeguatamente protetto dai rischi che possono arrecare danni economici e d'immagine al Gruppo Bancario e/o compromettere il regolare svolgimento delle attività aziendali.

L'Amministratore Delegato e tutte le strutture aziendali devono quindi contribuire e concorrere alla realizzazione ed al mantenimento di un adeguato livello di Sicurezza Informatica.

La presente *Policy* di Sicurezza Informatica fornisce l'indirizzo in materia di sicurezza del Sistema Informativo aziendale e, pertanto, rappresenta il principale strumento di comunicazione e condivisione delle direttive aziendali in materia di governo della Sicurezza IT, attraverso la definizione di:

- principi e criteri generali di sicurezza che devono essere garantiti e rispettati nei processi di gestione della Sicurezza IT;
- linee guida per adempiere agli obblighi imposti dalle normative e dai regolamenti esterni a cui l'azienda si sottopone in materia di Sicurezza IT;
- ruoli, responsabilità e personale coinvolto nella gestione della Sicurezza IT.

Tale *Policy* è portata all'attenzione di tutto il personale dipendente e dei Fornitori/*Outsourcer* IT del Gruppo Bancario, al fine di garantirne il rispetto.

Le linee guida descritte nel presente documento si applicano a tutte le entità del Gruppo Bancario illimity, sottoposte alla direzione ed al coordinamento della Capogruppo illimity Bank S.p.A., per le parti di competenza e in funzione della natura dell'attività svolta dalla singola società controllata. Le entità del Gruppo sono tenute pertanto a recepire tali linee guida e ad adeguare, ove necessario, la propria normativa interna secondo le indicazioni della Capogruppo.

1.2 ALLINEAMENTO CON IL PROCESSO DI GESTIONE DEL RISCHIO IT

Il processo di gestione dei rischi adottato dal Gruppo Bancario valuta periodicamente i rischi IT cui esso è esposto e permette di individuare misure di sicurezza e controlli finalizzati a ridurne l'entità, in relazione agli obiettivi elencati nel precedente paragrafo. La presente *Policy* di Sicurezza Informatica fornisce indirizzi direttivi anche in relazione ai risultati di tale processo.

Le informazioni aziendali devono essere protette mediante l'adozione di tutte le misure di sicurezza, che si reputano necessarie per la mitigazione dei rischi individuati dalle apposite analisi del rischio.

La struttura dei processi e l'intensità dei presidi da porre in atto è commisurata alle risultanze del processo di analisi dei rischi. Ogni rischio che non sia adeguatamente mitigato da meccanismi di protezione deve essere portato all'attenzione degli Organi della Banca, del Responsabile della Funzione designata alla supervisione dei rischi IT o dell'Unità Operativa, in funzione del relativo livello di rischio.

La gestione della sicurezza informatica abilita la corretta gestione del rischio informatico, mediante un'adeguata gestione di processi quali *Change Management*, *Incident Management* e *Business Continuity Management*, al fine di identificare i vettori di minaccia e le vulnerabilità sui processi e sistemi.

1.3 PRINCIPI GENERALI

I principi generali che fondano ed indirizzano l'approccio del Gruppo Bancario nei confronti della gestione della sicurezza sono riconducibili ai seguenti criteri:

- riservatezza – protezione dei dati da modalità di fruizione non autorizzate e/o non in linea con il livello di classificazione degli stessi (es: accesso ai dati da parte di soggetti non autorizzati, comunicazione di dati non autorizzata);
- integrità – protezione dei dati da attività volte alla loro modifica non autorizzata o indesiderata (es.: modifica volontaria o involontaria non autorizzata delle informazioni);
- disponibilità – protezione dei dati da possibili eventi in grado di ridurre la capacità dell'azienda di renderli disponibili (es: non raggiungibilità dei sistemi);
- conformità – gestione dei dati in modo conforme alle leggi ed alle normative di settore in tema di sicurezza;
- non ripudio – la garanzia che le persone o i processi che hanno dato origine alle informazioni siano effettivamente quelli riconosciuti dai meccanismi di identificazione;
- verificabilità - la garanzia di poter ricostruire, all'occorrenza e anche a distanza di tempo, eventi connessi all'utilizzo del sistema informativo e al trattamento di dati;
- minimo privilegio (*least privilege*) – il principio che stabilisce che a ciascun utente o amministratore di sistema siano assegnate le abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati;
- segregazione dei compiti (*segregation of duties*) – il principio che stabilisce che l'esecuzione di operazioni di particolare criticità sia svolta attraverso la cooperazione di più utenti o amministratori di sistema con responsabilità formalmente ripartite;
- *need to know* – la regolamentazione dell'accesso logico a reti, sistemi, basi di dati sulla base delle effettive esigenze operative;
- *zero trust* – la gestione del perimetro che prevede barriere all'ingresso viene meno perché si rafforza la partecipazione alla realtà informativa del gruppo legata all'identificazione univoca dei soggetti.

2 GLOSSARIO

Definizioni	
Banca	illimity Bank S.p.A. con sede legale in Milano, via Soperga n. 9 - 20127
Gruppo	Indica la Banca e le società controllate rientranti nel Gruppo Bancario illimity iscritto all'Albo dei gruppi bancari
Analisi del rischio	Insieme delle attività atte ad identificare i possibili rischi (attacchi e vulnerabilità) a cui può essere sottoposto un sistema con l'obiettivo di individuare le contromisure di sicurezza a protezione del sistema medesimo
Asset	Ogni tipologia di bene che abbia un valore per l'organizzazione
Autenticazione	Procedura di verifica dell'identità di un utente da parte di un sistema o servizio
Autorizzazione	Procedura che verifica se un cliente o un altro soggetto interno o esterno ha il diritto di compiere una certa azione, ad es. di trasferire fondi o accedere a dati sensibili
Backup	Salvataggio di flussi informativi (librerie di programmi, procedure ed archivi di dati) e creazione di copie di riserva allo scopo di garantire comunque la disponibilità del loro contenuto informativo anche nel caso di distruzione degli originali
Componente critica del sistema informativo	Sistema o applicazione per i quali un incidente di sicurezza informatica può pregiudicare il regolare e sicuro svolgimento di funzioni operative importanti per la Banca, tra cui l'efficace espletamento dei compiti degli organi aziendali e delle funzioni di controllo
Crittografia	Processo di conversione di un'informazione in un formato codificato (cifratura) che non potrà essere interpretata senza un processo di riconversione al formato originale. Tale processo viene eseguito tramite algoritmi ed una password di cifratura/decifrazione chiamata Chiave
Dati personali	Informazioni relative a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale
Disaster recovery	Insieme delle attività volte a garantire la disponibilità e a ristabilire i processi critici e i servizi IT in caso di interruzioni dei sistemi
Esternalizzazione (*outsourcing*)	Accordo in qualsiasi forma tra la Banca e un fornitore di servizi in base al quale il fornitore realizza un processo, un servizio o un'attività della stessa Banca
Grave incidente di Sicurezza Informatica	Un incidente di sicurezza informatica da cui derivi almeno una delle seguenti conseguenze: • perdite economiche elevate o prolungati disservizi per l'intermediario, anche a seguito di ripetuti incidenti di minore entità; • disservizi rilevanti sulla clientela e altri soggetti (ad es., intermediari o infrastrutture di pagamento); la valutazione della gravità considera il numero dei clienti o controparti potenzialmente coinvolti e l'ammontare a rischio; • il rischio di inficiare la capacità della banca di conformarsi alle condizioni e agli obblighi di legge o previsti dalla disciplina di vigilanza

	• danni reputazionali, nel caso venga reso di pubblico dominio (ad esempio attraverso i media e gli organi di stampa).
Incidente	Qualsiasi evento che non rientri nella normale operatività dei servizi e che causa, o può causare, un'interruzione e/o una riduzione della qualità di erogazione degli stessi e che corrisponde a un cambio di stato significativo ovvero a un cambio di stato che ha rilevanza ai fini delle attività di business della Banca
Incidente di Sicurezza informatica	Ogni evento, o serie di eventi collegati, non pianificati dalla Banca che interessa le sue risorse informatiche e che i) ha o potrebbe avere un impatto negativo sull'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi o dei processi dell'intermediario; oppure ii) comunque implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi)
Manuali/Procedure/Istruzioni Operative di sicurezza	Descrivono in dettaglio le modalità operative da seguire per l'attuazione di una norma o di una direttiva di sicurezza
Norme/Normativa	Regole, direttive e standard che, coerentemente alle Politiche di Sicurezza, devono essere seguiti per il conseguimento degli obiettivi di sicurezza prefissati. Sono da considerarsi un'estensione diretta delle Politiche di Sicurezza
Organo con Funzione di Gestione (OFG)	L'Organo aziendale o i componenti di esso a cui - ai sensi del codice civile o per disposizione statutaria – spettano o sono delegati compiti di gestione corrente, intesa come attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica. Nell'attuale modello adottato da illimity, esso è individuato nell'Amministratore Delegato (di seguito anche AD), il quale, in qualità di vertice della struttura interna, partecipa alla funzione di gestione
Organo con Funzione di Supervisione Strategica (OFSS)	L'Organo aziendale a cui - ai sensi del codice civile o per disposizione statutaria - sono attribuite funzioni di indirizzo della gestione dell'impresa, mediante, tra l'altro, esame e delibera in ordine ai piani industriali o finanziari ovvero alle operazioni strategiche. Esso è individuato nel Consiglio di Amministrazione (di seguito anche CdA)
Outsourcer/Fornitore	Soggetto esterno a cui viene assegnata la realizzazione di un processo, di un servizio o di un'attività della Banca stessa, sulla base di specifici accordi contrattuali
Password	Parola chiave attraverso la quale può essere implementato il meccanismo dell'autenticazione (riconoscimento certo) di un utilizzatore del Sistema Informativo
Rischio informatico	Rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (Information and Communication Technology – ICT). Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici
Risorsa ICT	bene dell'azienda afferente all'ICT che concorre alla ricezione, archiviazione, elaborazione, trasmissione e fruizione dell'informazione gestita dall'intermediario

Trattamento	Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati
Utente	Colui che crea o utilizza, in quanto autorizzato a farlo, l'informazione
Utente responsabile	Figura aziendale identificata per ciascun sistema o applicazione e che ne assume formalmente la responsabilità, in rappresentanza degli utenti e nei rapporti con le funzioni preposte allo sviluppo e alla gestione tecnica
Strutture organizzative (o Strutture)	Si intendono le tipologie di strutture organizzative che compongono l'Organigramma di illimity, cui sono attribuite le responsabilità di dettaglio come descritto nel "Regolamento Struttura Organizzativa".

3 RUOLI E RESPONSABILITÀ

La predisposizione ed il mantenimento della Policy di Sicurezza Informatica coinvolgono le seguenti Strutture Aziendali, che risultano parte attiva nei processi di indirizzo, gestione e controllo della sicurezza del Sistema Informativo.

3.1 CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione, quale Organo di supervisione strategica come definito dalla Circolare n. 285 di Banca d'Italia, ha la responsabilità di indirizzo e controllo del sistema informativo. In tale ambito:

- approva le strategie di sviluppo del sistema informativo;
- approva la presente *Policy* di sicurezza informatica;
- approva le linee di indirizzo in materia di selezione del personale con funzioni tecniche e di acquisizione di sistemi, *software* e servizi, incluso il ricorso a Fornitori esterni[1];
- promuove lo sviluppo, la condivisione e l'aggiornamento di conoscenze in materia ICT all'interno dell'azienda;
- è informato tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti del sistema informativo.

Con specifico riguardo all'esercizio della responsabilità di supervisione della analisi del rischio informatico, lo stesso organo:

- approva il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico;
- approva la propensione al rischio informatico;
- è informato con cadenza almeno annuale sulla situazione di rischio informatico rispetto alla propensione al rischio.

3.2 AMMINISTRATORE DELEGATO

L'Amministratore Delegato, quale Organo con funzione di gestione come definito dalla Circolare n. 285 di Banca d'Italia, ha il compito di assicurare la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema informativo. In particolare:

- definisce l'architettura organizzativa della Struttura ICT assicurandone nel tempo la rispondenza alle strategie e ai modelli definiti;
- definisce l'assetto organizzativo, metodologico e procedurale per il processo di analisi del rischio informatico, in collaborazione con la funzione aziendale deputata alla gestione del rischio;
- approva tutta la documentazione del Gruppo Bancario rilevante in ambito ICT, anche in raccordo con le procedure del Fornitore di servizi, verificandone la coerenza con le esigenze informative e di business nonché con le strategie aziendali;
- valuta almeno annualmente le prestazioni della funzione ICT rispetto alle strategie e agli obiettivi fissati, in termini di rapporto costi/benefici o utilizzando sistemi integrati di misurazione delle prestazioni, assumendo gli opportuni interventi e iniziative di miglioramento;
- approva almeno annualmente la valutazione del rischio delle componenti critiche nonché la relazione sull'adeguatezza e costi dei servizi ICT, informando a tale riguardo l'organo con funzione di supervisione strategica;
- monitora il regolare svolgimento dei processi di gestione e di controllo dei servizi ICT e, a fronte di anomalie rilevate, pone in atto opportune azioni correttive;
- assume decisioni tempestive in merito a gravi incidenti di sicurezza informatica.

3.3 FUNZIONE ICT

L'articolazione organizzativa della funzione ICT del Gruppo Bancario, all'interno della quale è inquadrata la funzione deputata alla gestione della sicurezza informatica si ispira a criteri di funzionalità, efficienza e sicurezza, definendo compiti e responsabilità, tenuto conto di fattori quali la complessità della struttura societaria, la dimensione, i settori di attività, le strategie di *business* e gestionali. In particolare, la funzione di sicurezza informatica:

- segue la redazione e l'aggiornamento delle policy di sicurezza e delle istruzioni operative;
- assicura la coerenza dei presidi di sicurezza con le policy approvate;
- partecipa alla progettazione, realizzazione e manutenzione dei presidi di sicurezza dei data center;
- partecipa alla progettazione del software applicativo della banca;

[1] Si veda in proposito la Circolare di Banca d'Italia 285/2013, Parte Prima, Titolo IV, Capitolo VI.

- partecipa alla valutazione dei prodotti informatici a supporto dei processi della banca;
- partecipa alla valutazione del rischio potenziale nonché all'individuazione dei presidi di sicurezza nell'ambito del processo di analisi del rischio informatico;
- assicura il monitoraggio nel continuo delle minacce applicabili alle diverse risorse informatiche;
- segue lo svolgimento dei test di sicurezza prima dell'avvio in produzione di un sistema.

Nello svolgimento delle suddette attività di competenza, la funzione ICT – per il tramite della funzione deputata alla gestione della sicurezza informatica – coinvolge nel continuo o laddove opportuno le funzioni aziendali di controllo.

3.4 RISK MANAGEMENT

Il CRO è parte attiva nel processo di gestione della Sicurezza IT della Banca.

La valutazione dei rischi informatici, basata sulla definizione di opportuni flussi informativi continui all'interno del Gruppo Bancario in merito ai mutamenti del contesto operativo ed all'efficacia delle misure di protezione delle risorse ICT, è propedeutica all'individuazione di eventuali misure di sicurezza da introdurre al fine di mitigare/ridurre il rischio IT sugli asset aziendali analizzati. La valutazione dei rischi è effettuata con cadenza almeno annuale e, comunque, in occasione di cambiamenti rilevanti.

Il CRO è altresì incaricato della conduzione dell'analisi del rischio sui fornitori di servizi, ovvero il processo del monitoraggio del rischio delle terze parti, al fine di produrre una valutazione olistica e omnicomprensiva dell'esposizione al rischio informatico del Gruppo Bancario.

3.5 COMPLIANCE & AML

Compliance & AML monitora nel continuo la conformità di sistemi e processi agli obblighi normativi rilevanti in materia di ICT, garantendo:

- l'assistenza su aspetti tecnico-organizzativi che possono implicare un rischio di non conformità come tematiche relative al trattamento dei dati personali;
- la coerenza degli assetti organizzativi rispetto alla normativa esterna, per le parti relative al sistema informativo;
- la verifica degli ambiti sottoposti a requisiti normativi inclusi nei contratti con Terze Parti e Società facenti parti del Gruppo (inclusi i contratti di esternalizzazione di funzioni essenziali importanti e componenti critiche del sistema informativo).

3.6 INTERNAL AUDIT

La struttura Internal Audit, secondo un approccio *risk-based* e *process-oriented*, svolge l'attività di revisione interna (c.d. "controlli di terzo livello") volta a garantire un'adeguata copertura delle varie applicazioni, infrastrutture e processi di gestione, incluse le eventuali componenti esternalizzate; nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni.

3.7 OUTSOURCER E FORNITORI INFORMATICI

La Banca si avvale di *Outsourcer* e Fornitori IT a cui ha affidato, in modalità *as-a-service*, il Sistema di *Core Banking*, l'infrastruttura cloud nonché i diversi Sistemi di Pagamento. Gli *Outsourcer* e i Fornitori hanno individuato, all'interno delle rispettive organizzazioni, figure e strutture atte a garantire i presidi di Sicurezza IT sulla base delle necessità identificate dal "business" de Gruppo Bancario. Il rapporto con gli *Outsourcer*/Fornitori è contrattualizzato anche tramite la formalizzazione di SLA e KPI, per il monitoraggio nel continuo delle componenti IT esternalizzate, e prevede il rispetto delle politiche di sicurezza del Gruppo Bancario.

4 LINEE GUIDA

4.1 POLITICHE DI SICUREZZA INFORMATICA

Le politiche operative del Gruppo Bancario che attengono a tematiche di Sicurezza Informatica – oltre alla presente – hanno come obiettivo la gestione e la salvaguardia del Sistema Informativo aziendale, assicurando che dati ed informazioni, durante il loro intero ciclo di vita, siano adeguatamente protetti, in conformità con i requisiti normativi in materia di protezione dei dati personali e di salvaguardia degli asset aziendali.

A tal fine, il Gruppo Bancario pubblica ed aggiorna periodicamente tali politiche[2], a cui la presente *Policy* di Sicurezza Informatica offre indirizzi, linea guida da seguire ed obiettivi da perseguire. In particolare, il presente documento viene aggiornato almeno annualmente e, comunque, ogni qual volta si rilevi l'introduzione o la variazione significativa di normative di riferimento, standard di sicurezza, processi e tecnologie del Gruppo Bancario. È necessario garantire il costante aggiornamento ed il conseguente allineamento tra la normativa del Gruppo Bancario e l'eventuale variazione/introduzione di nuovi processi da parte degli *Outsourcer*.

4.2 ORGANIZZAZIONE DELLA SICUREZZA INFORMATIVA

Per assicurare un'adeguata gestione della sicurezza informatica, sono definiti presidi organizzativi e relativi *framework* di sicurezza ed indicatori per l'indirizzo, il controllo e il monitoraggio delle misure di protezione e di salvaguardia dei principi generali di cui al paragrafo 1.3.

L'organizzazione della sicurezza informatica e le relative procedure/misure di protezione sono sottoposte a revisione periodica, eventualmente anche da terze parti, con lo scopo di assicurare il mantenimento di adeguati livelli di efficienza e protezione nella gestione del sistema informativo aziendale.

4.3 GESTIONE DELLE RISORSE UMANE

Le politiche di Sicurezza IT supportano le Risorse Umane prevedendo i seguenti aspetti:

- Definizione degli obblighi e delle prassi comportamentali cui attenersi nell'utilizzo delle credenziali e dei dispositivi aziendali assegnati, che sono comunicati al nuovo personale del Gruppo Bancario (nel momento in cui entra in Azienda) dalla funzione HR & Organization;
- Sensibilizzazione e responsabilizzazione di tutto il personale aziendale e delle eventuali terze parti coinvolte nei processi aziendali (consulenti, Fornitori, etc.) relativamente al corretto e sicuro utilizzo delle risorse ICT che costituiscono il Sistema Informativo aziendale;
- Definizione della corretta gestione dei processi di chiusura del rapporto lavorativo, prevedendo la restituzione/cessazione degli asset e la chiusura formale del rapporto di lavoro tra le parti;
- Definizione e supporto alla gestione dell'intero ciclo di vita delle utenze e delle relative credenziali di accesso ai sistemi informativi della Banca;
- Supporto nell'organizzazione di programmi di formazione rivolti al personale in materia di sicurezza informatica.

Tutti gli utenti (dipendenti e personale esterno), come parte dei loro obblighi contrattuali, accettano e sottoscrivono i termini e le condizioni in merito alle loro responsabilità e quelle dell'organizzazione rispetto alla Sicurezza Informatica.

Il personale è costantemente formato ed aggiornato sulle tematiche di sicurezza in modo che sia a conoscenza delle principali misure di sicurezza tecnologiche ed organizzative attuate dal Gruppo Bancario.

Tale obiettivo è raggiunto attraverso l'offerta di momenti formativi e di norme per i dipendenti che ne indirizzino le attività quotidiane.

A tal fine, i dipendenti devono frequentare la formazione offerta che copre le tematiche di sicurezza, per essere aggiornati sulle novità normative introdotte, in modo da comprendere l'importanza della Sicurezza Informatica, e sulle loro responsabilità ed i danni che un uso non corretto del Sistema Informativo aziendale potrebbe provocare al Gruppo Bancario.

La responsabilità e gli obblighi di protezione delle informazioni aziendali sono parte fondamentale del compito assegnato alle singole persone, e rimangono validi anche dopo il termine del rapporto contrattuale, garantendo così la riservatezza delle informazioni afferenti al Gruppo Bancario.

Eventuali violazioni delle disposizioni presenti nella *Policy* di Sicurezza Informatica devono essere portate a conoscenza del proprio responsabile, e tramite il servizio di whistleblowing fornito internamente.

[2] Costituiscono esempi di tali politiche la Policy sulla Gestione degli Incidenti e la Procedura sulla Gestione dei Cambiamenti.

4.4 GESTIONE DEGLI ASSET AZIENDALI

Tutte le risorse IT (*hardware*, *software*, procedure e dati) appartenenti all'organizzazione aziendale sono censite e registrate, favorendo in questo modo l'identificazione ed il riconoscimento dei soggetti responsabili della sicurezza di tali risorse.

In questo ambito, rientra l'attività di censimento e monitoraggio degli strumenti sviluppati con strumenti di informatica di utente[3].

Il Gruppo Bancario ha in essere un processo che assicura che tutti gli strumenti (fisici e logici) siano correttamente dismessi nel momento in cui perdono la loro valenza operativa, e siano correttamente riassegnati nel momento in cui i soggetti responsabili lasciano il proprio ruolo nell'organizzazione.

Tutte le informazioni devono essere classificate, sulla base del loro livello di criticità e degli impatti derivanti da una violazione delle loro proprietà di riservatezza, integrità e disponibilità, con l'obiettivo ultimo di identificare ed implementare misure di protezione adeguate.

Il personale è tenuto a seguire le regole per la corretta gestione e protezione dei dati e delle informazioni aziendali definite nel rispetto della loro classificazione. Qualora sia necessario condividere ed inviare le informazioni aziendali verso l'esterno, il personale deve adottare le misure di sicurezza per la trasmissione dei dati definite all'interno della Policy di Classificazione dei Dati, utilizzando solo gli strumenti di lavoro certificati dal Gruppo Bancario. Eventuali deroghe alle modalità di trasmissione previste devono essere autorizzate dalla funzione ICT Security.

4.5 GESTIONE E CONTROLLO DEGLI ACCESSI

Obiettivo di questo dominio è quello di normare le modalità di accesso alle varie componenti di sistemi, reti ed applicazioni gestite ed utilizzate dal Gruppo Bancario coerentemente con il ruolo svolto dagli utenti e nel rispetto delle misure di sicurezza definite, a partire dall'analisi del rischio.

Più specificatamente, rientrano in tale ambito gli obiettivi seguenti:

- garantire l'autorizzazione degli accessi ai sistemi aziendali mediando tra le esigenze dettate dall'efficienza lavorativa e le buone politiche di sicurezza e privacy che impongono di limitare tali accessi solo agli operatori che hanno realmente la necessità di accedervi per finalità lavorative; in particolare garantire che l'accesso alle informazioni riservate sia essere ispirato al principio di reale necessità di utilizzo (*need to know*) e al principio di adeguata suddivisione dei compiti (*separation of duties*);
- verificare periodicamente il mantenimento delle esigenze lavorative che giustificano le autorizzazioni di accesso ai sistemi ed eventualmente procedere con la loro eliminazione parziale/totale;
- controllare il corretto utilizzo da parte dell'utenza delle autorizzazioni di accesso ricevute.

In particolare, il ciclo di vita delle utenze è gestito da un opportuno processo di Identity Governance definito dalla funzione ICT Security e che prevede macroscopicamente le seguenti attività:

- **creazione delle utenze** – la richiesta di creazione di una nuova utenza (assunzione nuovo dipendente, esigenza del Gruppo Bancario, etc.) è tracciata ed autorizzata da personale responsabile autorizzato. Ogni utenza deve essere associata a profili autorizzativi caratterizzanti il ruolo che assume nell'organizzazione bancaria;
- **modifica dei profili** – per ogni modifica al profilo dell'utente è necessaria una richiesta formale da personale responsabile autorizzato con l'indicazione delle modifiche e delle motivazioni (variazione organizzative, cambiamento di mansione, etc.) da apportare, inclusi gli eventuali diritti di scrittura, di lettura e di modifica da revocare;
- **disabilitazione delle utenze** – è prevista la disattivazione delle credenziali nel caso in cui il possessore non abbia più la necessità di utilizzarle a causa del cambiamento delle proprie mansioni lavorative o in casi di assenza prolungata (ad esempio in caso di maternità). I sistemi sono configurati per disattivare automaticamente le credenziali di autenticazione in caso di inutilizzo superiore ai 6 mesi;

[3] Lo sviluppo di applicazioni direttamente in carico alle unità operative e di controllo è sottoposto a misure di natura organizzativa e metodologica, tese a garantire un livello di sicurezza comparabile con le applicazioni sviluppate dalla struttura ICT. Un periodico monitoraggio censisce le applicazioni sviluppate con strumenti di informatica d'utente e ne verifica la rispondenza alla policy di sicurezza, in particolare se utilizzate in attività rilevanti quali la predisposizione dei dati di bilancio, del risk management, della finanza e del reporting direzionale, al fine di contenere il rischio operativo

- **gestione dei profili applicativi** – a ciascun utente è assegnato un profilo di autorizzazione in linea con le proprie mansioni lavorative conformemente al Modello definito. Su motivata richiesta possono essere concesse deroghe che devono essere opportunamente documentate;
- **monitoraggio e verifica delle utenze e dei profili abilitativi assegnati** – periodicamente, e comunque almeno annualmente, è prevista una revisione delle utenze e dei profili per verificarne la pertinenza, con particolare attenzione alle deroghe concesse.

I principi generali per l'autorizzazione ai sistemi sono basati sui seguenti aspetti:

- segregazione dei ruoli e delle responsabilità (*separation of roles/duties*);
- attribuzione delle abilitazioni strettamente necessarie allo svolgimento dei compiti assegnati a ciascun utente o amministratore di sistema (*least privilege*);
- regolamentazione degli accessi logici ai sistemi sulla base delle effettive esigenze operative (*need to know*).

Sono inoltre in essere le seguenti misure tecniche di sicurezza nell'implementare il sistema di autenticazione al Sistema Informativo aziendale:

- *password* – la parola chiave richiesta per accedere ai sistemi è gestita nel rispetto delle "*Good Practice*" internazionali, ad esempio non può contenere il codice identificativo o il nome dell'utente e deve essere modificata al primo utilizzo. È responsabilità dell'utente assegnatario delle credenziali di accesso garantirne la riservatezza ed un utilizzo coerente con la propria attività lavorativa;
- codici identificativi – i codici identificativi assegnati agli utenti sono univoci, personali, non cedibili e non riassegnati.

Il Gruppo Bancario implementa anche soluzioni di autenticazione forte per tutti gli utenti (Multi Factor Authentication) e riconoscimento di accesso condizionato (Conditional Access); gli utenti del gruppo possono accedere agli strumenti informatici sono quando sono in possesso di credenziali valide, che vengono ulteriormente validate da apparti fisici gestiti dalla ICT del gruppo (Laptop e Mobile), che fanno parte della dotazione assegnata a tutti i dipendenti.

Relativamente alle utenze tecniche e/o con privilegi amministrativi sono attive procedure specifiche e controlli in linea che soddisfano quanto previsto dal Provvedimento dell'Autorità Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008".

Per questa tipologia di utenze è attivo un sistema di gestione dell'accesso privilegiato che prevede un workflow approvativo nel caso queste utenze avessero bisogno di un elevamento dei loro privilegi minimi. Il workflow approvativo scatena una richiesta alla funzione ICT Security che la valuta e la accetta o rifiuta di conseguenza.

4.6 SICUREZZA FISICA ED AMBIENTALE

In conformità con le vigenti disposizioni di legge in materia di sicurezza degli ambienti di lavoro, tutti i locali destinati ad ospitare le risorse tecnologiche impiegate per l'erogazione dei servizi informatici sono predisposti per garantire un'idonea protezione contro le minacce di eventi naturali, intenzionali ed accidentali che possono arrecare danni alle persone e ai beni aziendali e/o pregiudicare il corretto e continuo funzionamento delle risorse stesse.

Sono a tal fine definiti i processi ed i controlli da attivare per l'accesso fisico ai locali al fine di prevenire accessi non autorizzati, come ad esempio, la registrazione degli ospiti in ingresso e uscita dagli stabili della banca. Il coinvolgimento di terze parti è indispensabile per garantire una corretta protezione dell'azienda da potenziali eventi, quali incidenti, allagamenti, etc.

Il Gruppo Bancario è impegnato nel proteggere adeguatamente i propri sistemi informativi anche con l'utilizzo di misure di sicurezza fisica. Tale obiettivo è perseguito attraverso:

- la sicurezza delle aree fisiche e dei *data center*;
- la protezione delle apparecchiature informatiche;
- i processi di distruzione o eliminazione sicura di strumenti ed informazioni;
- norme per la conservazione e protezione degli strumenti a disposizione dell'utente.

Gli impianti di elaborazione delle informazioni aziendali critiche o delicate sono ubicati in aree sicure, protetti da perimetri di sicurezza definiti, con appropriate barriere per la sicurezza e controlli per l'ingresso.

4.7 CRITTOGRAFIA

La crittografia rappresenta uno degli strumenti applicati a garanzia della sicurezza della memorizzazione dei dati nonché della loro relativa gestione e comunicazione.

L'utilizzo di meccanismi di crittografia quali protocolli di comunicazione sicura (ad esempio HTTPS) o la gestione di certificati emessi da una CA (*Certificate Authority*) interna od esterna, al fine di proteggere le informazioni di business ritenute critiche, sono normati da processi aziendali che definiscano ruoli e responsabilità in tale ambito.

In particolare, sono separate le funzioni che gestiscono l'operatività delle chiavi crittografiche e le funzioni addette al controllo e alla definizione degli standard di crittografia da adottare.

4.8 GESTIONE DELL'OPERATIVITA'

L'obiettivo del presente dominio è quello di assicurare che i servizi informatici garantiscano adeguati livelli di riservatezza, integrità e disponibilità dei dati, e di tutti i principi elencati nel par. 1.3, nel rispetto delle esigenze aziendali e delle leggi vigenti, anche nel caso in cui sia esternalizzata la gestione di componenti ICT del Gruppo Bancario presso terze parti.

I processi operativi sono opportunamente formalizzati in apposite procedure e/o istruzioni operative che definiscano ruoli e responsabilità, attività, controlli e flussi informativi.

Tutte le postazioni con un accesso alla rete aziendale sono dotate di meccanismi di sicurezza che riducono il rischio di attacchi informatici/virus che potrebbero provocare gravi perdite aziendali.

L'utente deve provvedere ad informare immediatamente la funzione ICT Security in tutti i casi in cui le misure di sicurezza non siano applicate correttamente e/o gli strumenti a disposizione non si rivelino adeguati.

Nonostante le misure di sicurezza implementate, è necessario che l'utente utilizzi i servizi a disposizione (*mail*, *web*, etc.) in maniera responsabile e conforme alla normativa interna evitando la divulgazione di informazioni aziendali. È necessario, ad esempio, evitare di scaricare file da internet e/o aprire/inoltrare allegati di *e-mail* di dubbia provenienza, etc.

Gli asset aziendali in dotazione (ad esempio computer, *mail*, cellulare) sono da utilizzare per fini lavorativi e/o ad uso promiscuo, ove previsto.

È vietata l'installazione di *software* non autorizzato dalla struttura responsabile della gestione del *software* aziendale. Eventuali installazioni ad hoc devono essere giustificate da esigenze di business e vagliate dai referenti responsabili della gestione del *software*.

Le operazioni di *backup* consentono di garantire la disponibilità delle informazioni e dei sistemi anche a seguito di incidenti di sicurezza informatica o di eventi di disastro. Durante tutte le fasi previste dal processo di gestione dei *backup* è comunque garantita la riservatezza, l'integrità e la disponibilità dei dati trattati.

Così come definito dalla normativa vigente (tracciatura dati bancari, amministratori di sistema, etc.) sono previsti, per garantire la piena conformità, meccanismi di tracciatura degli accessi e delle operazioni critiche garantendone la riservatezza, l'inalterabilità e la disponibilità in linea con le richieste dei singoli provvedimenti.

Per comprendere i futuri requisiti aziendali, le operazioni dell'organizzazione, l'infrastruttura informatica e garantire le prestazioni e l'efficienza delle capacità attuali e future dei sistemi, sono definite delle attività di *capacity management*. Nello svolgimento di tali attività il Gruppo Bancario considera i requisiti relativi all'operatività dell'azienda, dei servizi erogati e delle risorse IT al fine di implementare un processo iterativo in conformità con i piani strategici aziendali, che valuti il corretto bilanciamento dei vincoli di costo con le necessità dell'organizzazione.

Il Gruppo Bancario effettua, delegando a terze parti sotto la propria supervisione, l'esecuzione periodica, di attività di *Vulnerability Assessment* e *Penetration Test* (VA/PT) sul Sistema Informativo aziendale ed in particolare sui sistemi ritenuti più critici dal business. L'individuazione del perimetro da sottoporre a tali attività è definita anche sulla base di un'analisi del rischio IT che potrebbe evidenziare criticità sui sistemi del Gruppo Bancario. Tali attività permettono di eseguire una certificazione periodica della sicurezza dei sistemi, garantendo nel tempo efficaci contromisure rispetto alle nuove minacce individuate e la gestione del rischio associato. In concomitanza con le verifiche il Gruppo Bancario provvede a generare la reportistica di dettaglio con l'esito dei test ottenuti e a programmare eventuali azioni di *remediation* da intraprendere.

4.9 SICUREZZA DELLE COMUNICAZIONI

La Sicurezza delle Comunicazioni si prefigge lo scopo di salvaguardare la trasmissione dei dati sulle reti di telecomunicazioni private e pubbliche, con particolare attenzione a tutte le componenti fisiche (dispositivi *hardware*) e logiche (*firmware* e *software*) che costituiscono l'infrastruttura di rete utilizzata dal Gruppo Bancario. Al fine di minimizzare i rischi che possono compromettere l'integrità e la disponibilità delle funzioni di trasmissione dati, le principali attività da svolgere sono le seguenti:

- censimento e classificazione della tipologia delle reti;
- gestione corretta delle componenti dell'infrastruttura di rete, con particolare attenzione agli aspetti di *capacity planning*, *business continuity*, *disaster recovery* e Sicurezza Informatica;
- specificare formalmente le regole aziendali che normano il comportamento del personale interno/esterno nell'utilizzo e nella gestione dell'infrastruttura di rete utilizzata dal Gruppo Bancario.

A tale proposito, i principali aspetti da prendere in considerazione sono i seguenti:

- disponibilità, modalità e strumenti per garantire la continuità nell'erogazione dei servizi di rete;
- monitoraggio, modalità e strumenti da utilizzare per il controllo del traffico in transito sulle reti, con lo scopo di individuare eventuali scostamenti rispetto all'operatività definita;
- segregazione della rete di telecomunicazione, meccanismi di separazione e filtraggio del traffico tra sottoreti interne al perimetro aziendale;
- modalità e processi di trasferimento delle informazioni sia verso l'interno che verso l'esterno. In particolare, la comunicazione delle informazioni deve avvenire attraverso l'utilizzo di protocolli sicuri in base a criteri che garantiscano la riservatezza e l'integrità delle informazioni trasmesse e ricevute dal Gruppo Bancario.

L'utilizzo di internet e della posta elettronica aziendale è consentito a tutto il personale. Il Gruppo Bancario ispeziona il traffico internet (anche SSL) per applicare filtri atti ad aumentare la protezione da malware o impedire azioni potenzialmente dannose per la reputazione. L'abilitazione all'accesso ai presenti strumenti è consentita ai singoli utenti, tramite le autorizzazioni base, in seguito a segnalazione di assunzione da parte dell'ufficio del personale.

4.10 ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEL SISTEMA INFORMATIVO

Lo scopo di tale dominio di sicurezza è di garantire la realizzazione, l'acquisizione e la manutenzione di sistemi applicativi affidabili e sicuri, in termini di:

- correttezza dei trattamenti elaborativi dei dati gestiti dall'applicazione;
- controllo di autorizzazione all'utilizzo delle funzionalità e dei dati dell'applicazione;
- salvaguardia dell'integrità dei dati memorizzati negli archivi dell'applicazione;
- salvaguardia della riservatezza dei dati gestiti;
- tracciatura e storicizzazione degli aggiornamenti dei dati effettuati;
- conformità di trattamento dei dati alle disposizioni di legge fiscali e alle normative;
- prevenzione e minimizzazione dei rischi di business associati all'utilizzo dell'applicazione.

In tale contesto è responsabilità del Gruppo Bancario richiedere ad eventuali terze parti che sono coinvolte nelle attività di sviluppo e manutenzione *software*/*hardware*, di seguire processi definiti ed in linea con le politiche di sicurezza del Gruppo. Il Gruppo Bancario inoltre provvede a controllare la correttezza dei processi seguiti verificando la documentazione prodotta ed approvando formalmente le attività del processo di sviluppo (analisi funzionale, piano dei test UAT, passaggio in produzione, etc.).

4.11 SVILUPPO SICURO DEL SOFTWARE

Il *software* prodotto deve essere progettato e sviluppato in modo da garantire la massima efficienza, efficacia ed un livello di sicurezza coerente con le informazioni trattate e gli obbiettivi di business. Occorre quindi tenere in considerazione i seguenti requisiti generali:

- lo sviluppo sicuro del *software* deve garantire la riservatezza, disponibilità ed integrità delle informazioni trattate e gestite, e in coerenza con i principi generali elencati nel par. 1.3;
- gli ambienti utilizzati per la gestione del ciclo di vita del software (*development*, *test*, UAT, preproduzione e produzione) devono essere tenuti, per quanto possibile, segregati l'uno dall'altro;
- il codice sviluppato deve tenere presente tutte le normative vigenti, in particolare per quanto riguarda la protezione dei dati personali, favorendo i principi di *Security/Privacy by Design & by Default*;
- le buone pratiche di settore inerenti alla sicurezza del processo di sviluppo (quali OWASP top 10) devono essere favorite;
- il personale coinvolto nella progettazione e sviluppo deve essere adeguatamente formato e sensibilizzato sulla sicurezza informatica.

4.12 SICUREZZA DELLE TERZE PARTI

La gestione del Sistema Informativo – anche quando componenti di esso vengono gestite e/o affidate a Terze Parti – deve avvenire nel rispetto dei principi guida e delle misure di sicurezza definite nella presente *Policy* di Sicurezza Informatica. È dunque fondamentale prevedere a livello contrattuale quanto previsto nella *Policy* in materia di esternalizzazione di funzioni aziendali.

La gestione e/o esternalizzazione di determinati servizi ICT deve prevedere il rispetto delle misure di sicurezza definite dal Gruppo Bancario. A tale scopo, sono definiti i requisiti minimi di sicurezza che devono essere rispettati per la regolamentazione contrattuale e gestionale dei rapporti con terze parti che, per erogare i servizi concordati, hanno necessità di accedere alle risorse informative del Gruppo Bancario o ne trattano i dati.

A garanzia dell'effettivo rispetto delle misure di sicurezza sono previste all'interno dei contratti specifiche attività di audit sulla terza parte, richiedendo formalmente la conformità a leggi e regolamenti quali quelli relativi alla protezione dei dati; in funzione delle evidenze raccolte sul fornitore viene lavorato un Third Party Security Risk Score che qualifica l'adeguatezza delle misure di sicurezza e della postura della terza parte.

Le informazioni aziendali devono quindi essere protette in conformità anche con gli eventuali vincoli contrattuali sottoscritti con le terze parti che concorrono al trattamento di parte del Sistema Informativo aziendale, nel rispetto della riservatezza, integrità, disponibilità delle informazioni e proprietà intellettuale.

4.13 GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

Il processo di gestione degli incidenti rappresenta l'insieme delle attività e degli strumenti che il Gruppo Bancario adotta per prevenire o individuare e rispondere tempestivamente ed efficacemente al presentarsi di incidenti che interessano i servizi erogati, con l'obiettivo di salvaguardare i sistemi informativi societari, in linea con le *best practices* del settore e le normative vigenti, attraverso le seguenti attività:

- individuazione tempestiva degli impedimenti e delle violazioni al corretto funzionamento del sistema e delle relative cause;
- classificazione degli incidenti di sicurezza secondo una metodologia strutturata;
- identificazione della modalità di trattamento dell'incidente di sicurezza;
- definizione delle modalità di gestione degli incidenti di sicurezza sia interna (*escalation*), che esterna attraverso un opportuno coordinamento con gli *Outsourcer* IT e attivazione di eventuali comunicazioni a Banca d'Italia, *broker* assicurativi, autorità, forze dell'ordine, ecc.;
- rapporto e condivisione di indicatori con gruppi specialistici per un pronto rilevamento delle minacce;
- raccolta delle informazioni necessarie (evidenze) per supportare un'eventuale azione legale;
- analisi dell'incidente di sicurezza individuando gli errori, le debolezze e le strategie adottate per gestirlo, migliorando la tempestività di intervento e la risposta ad analoghi eventi futuri.

Ogni soggetto che venga in contatto con le risorse informative aziendali è responsabile di segnalare eventi e incidenti di sicurezza qualora si verifichino. La segnalazione, da censire in un apposito strumento di *ticketing*, deve essere effettuata al responsabile diretto che provvederà, se necessario, ad attivare il processo di escalation. La segnalazione deve includere data e ora in cui è avvenuto l'incidente, l'asset informativo colpito (applicazione, *database*, PC, componente di rete, etc.) e descrizione dell'accaduto.

I gravi incidenti di sicurezza informatica sono comunicati tempestivamente al Consiglio di Amministrazione, a Banca d'Italia e, laddove previsto, ad altre autorità di vigilanza e/o forza dell'ordine, previo l'invio di un rapporto sintetico recante una descrizione dell'incidente e dei disservizi provocati agli utenti interni e alla clientela. Gli incidenti che riguardano i sistemi di pagamento e i *personal data breach* devono ottemperare agli obblighi di notifica previsti dalle normative specifiche di riferimento.

Maggiori informazioni sono contenute nella Policy sulla Gestione degli Incidenti.

4.14 GESTIONE DELLA CONTINUITÀ OPERATIVA

Il Gruppo Bancario pianifica, implementa ed aggiorna costantemente tutte le misure di Sicurezza IT atte ad assicurare la continuità dei servizi ICT anche in presenza di eventi catastrofici.

Il Piano di Continuità Operativa definisce gli attori, le strategie e le soluzioni di continuità adottate, proponendosi i seguenti principali obiettivi:

- garantire la salvaguardia del personale;
- rispettare i requisiti normativi e legali;

- minimizzare i tempi di reazione e ripristino dei processi considerati vitali per il business al verificarsi di eventi critici;
- evitare o limitare il più possibile gli impatti economici derivanti dalla mancata attività;
- evitare o limitare il più possibile i danni all'immagine della Società.

Annualmente e/o in caso di variazione strutturale dei sistemi il piano è collaudato, controllato e revisionato, anche con l'ausilio di Outsourcer esterni.

ALLEGATI

4.15 ALLEGATO 1: NORMATIVA COLLEGATA

NORMATIVA INTERNA COLLEGATA

illimity way
Policy Privacy

NORMATIVA ESTERNA COLLEGATA

Disposizioni di vigilanza prudenziale per le banche - Circolare n° 285 di Banca d'Italia del 17 dicembre 2013 e successivi aggiornamenti
Codice in materia di protezione dei dati personali - Decreto Legislativo 30 giugno 2003, n° 196 (Gazzetta Ufficiale del 29 Luglio 2003), integrato con le modifiche introdotte dal Decreto Legislativo 10 Agosto 2008, n.101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati"
Linee guida del Garante per posta elettronica e internet (Gazzetta Ufficiale n. 58 del 10 marzo 2007 e s.s.m.m.)
Misure ed accorgimenti prescritti al titolare dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (Gazzetta Ufficiale n. 300 del 24 dicembre 2008 e s.s.m.m.
Provvedimento in materia di videosorveglianza - 8 aprile 2010 (Gazzetta Ufficiale n. 99 del 29 aprile 2010 e s.s.m.m.)
Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (Provvedimento n.192 del 12 Maggio 2011 del Garante, pubblicazione su Gazzetta Ufficiale n. 127 del 3 Giugno 2011 e s.s.m.m.
Legge 231 - Responsabilità di Impresa, Codice Etico e Responsabilità delle persone Giuridiche ex D.Lgs. 231/2001
Gazzetta Ufficiale n. 99 del 29 aprile 2010 e s.s.m.m.
Gazzetta Ufficiale n. 127 del 3 Giugno 2011 e s.s.m.m.
Linee guida in tema di riconoscimento biometrico e firma grafometrica (Avvio della consultazione – Gazzetta Ufficiale n. 118 del 23 Maggio 2014 e s.s.m.m.)
General Data Protection Regulation - Regolamento UE 2016/679 (GDPR - Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio 2018 e s.s.m.m.)

Payments Service Directive 2 - (EU) 2015/2366 (PSD2 – 13 gennaio 2018) e decreti legislativi di recepimento nell'ordinamento italiano - d. lgs 27 gennaio 2010 n. 11 – nonché norme tecniche di regolamentazione e linee guida emanate dalla European Banking Authority (EBA).

4.16 ALLEGATO 2: STANDARD E METODOLOGIE DI RIFERIMENTO

La comunità internazionale ha sviluppato nel tempo diverse metodologie, alcune delle quali sono state ratificate da Enti di standardizzazione (BS, ISO/IEC, Enti governativi, ecc.) e sono quindi diventate degli standard di riferimento.

Gli standard, le linee guida e le *best practices* più diffuse e riconosciute dalla comunità internazionale sono state prese in considerazione per individuare i requisiti del sistema di gestione della sicurezza maggiormente aderenti allo specifico contesto tecnologico, organizzativo e di business del Gruppo Bancario, in modo da avere un punto di riferimento autorevole ed esaustivo, anche in presenza di outsourcing del sistema informativo.

Si riportano di seguito gli standard e le metodologie di riferimento a cui la presente *Policy* di Sicurezza Informatica si ispira:

- ISO/IEC 27001:2017 - *Information technology - Security techniques - Information security management systems - Requirements*;
- ISO/IEC 27002:2013 - *Information technology - Security techniques - Code of practice for information security controls*;
- *The Standard of Good Practice for Information Security - June* 2014 - *Information Security Forum*;
- COBIT 2019 (*Governance, Control and Audit for Information and Related Topics*) from ISACF (*Information Systems Audit and Control Foundation*) and ITGI (*IT Governance Institute*);
- *Payment Card Industry Data Security Standard* (PCI DSS);
- NIST *Cybersecurity Framework* v1.1 - *National Institute of Standards and Technology*
- SCF – *Secure Control Framework*