Policy di Sicurezza

Consiglio di Amministrazione del 12 dicembre 2023

Owner della Policy: IT Operation Security & Governance

flowe

Indice

1 PREMESSA

Scopo del presente documento è descrivere i principi di carattere generale, gli obiettivi, il modello organizzativo ed i processi adottati da Flowe S.p.A. Società Benefit, (di seguito anche la Società) in materia di sicurezza delle informazioni (che comprende la sicurezza informatica), nonché di sicurezza fisica e di continuità operativa.

1.1 CONTESTO DI RIFERIMENTO

L'adozione del presente documento risponde alle Disposizioni di Vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019 e alle disposizioni contenute negli Orientamenti dell'EBA sulla gestione dei rischi ICT e di sicurezza, che prevedono la necessità per gli intermediari di dotarsi di una policy di sicurezza (sia in tema di sicurezza delle informazioni che di sicurezza relativa alla prestazione dei servizi di pagamento e di emissione della moneta elettronica.

1.2 AMBITO DEL DOCUMENTO

La presente policy conformemente alla policy di sicurezza della Capogruppo Banca Mediolanum SpA (di seguito anche la Capogruppo), descrive i principi relativi alla sicurezza al fine di garantire, in particolare, che i sistemi informatici siano appropriati rispetto alla natura, portata e complessità dell'attività dell'impresa, nonché dei conseguenti rischi.

Inoltre, la presente Policy presidia il patrimonio materiale e il capitale intellettuale di proprietà della Società oltre alla sicurezza delle informazioni, al fine di difendere gli interessi del personale e dei terzi[1], perseguendo i seguenti obiettivi:

- garantire la conformità e il rispetto delle disposizioni di legge in materia di sicurezza delle informazioni e delle infrastrutture;
- garantire la sicurezza degli asset aziendali, riservando l'accesso agli stessi solo al personale autorizzato;
- tutelare la riservatezza delle informazioni, evitando la loro consultazione e divulgazione non autorizzata;
- garantire l'integrità delle informazioni gestite dai sistemi e delle altre risorse informatiche utilizzate per il loro trattamento;
- garantire la disponibilità nel tempo delle risorse informatiche per assicurare la continuità di erogazione dei servizi applicativi;
- garantire l'attribuzione delle attività eseguite sui sistemi informatici a soggetti univocamente identificabili ed assicurarne la tracciabilità in accordo con i requisiti normativi di riferimento.

[1]Le tematiche relative alla sicurezza fisica dei dipendenti, intese come safety del personale dipendente, non sono oggetto della presente Policy.

1.3 SICUREZZA DELLE INFORMAZIONI

La sicurezza delle informazioni si articola in principi (ad esempio Segregation of Duties), strumenti (ad esempio anti-malware), processi (ad esempio distruzione dei dati) e scelte organizzative individuate al fine di proteggere le informazioni della Società, che sono gestite mediante tecnologie informatiche a seguito di azioni deliberate o accidentali, in relazione alle specifiche esigenze di:

- riservatezza, intesa come la capacità di rendere disponibili o rivelare le informazioni solo e soltanto a individui, entità o processi autorizzati ad accedervi;
- integrità, intesa come la capacità di salvaguardare l'autenticità, la consistenza e la completezza delle informazioni;
- disponibilità, intesa come la capacità di rendere accessibili e utilizzabili le informazioni secondo tempi e modi richiesti da un'entità autorizzata;
- accountability, intesa come la capacità di attribuire in maniera univoca gli accadimenti sul sistema informativo a soggetti univocamente identificabili;
- verificabilità, intesa come la capacità di ricostruire gli eventuali accadimenti avvenuti sul sistema informativo;
- tracciabilità: misure e regole di tracciabilità delle operazioni per consentire la verifica a posteriori delle operazioni, se specificatamente richiesto dalla normativa di settore.

1.4 SICUREZZA FISICA

La sicurezza fisica si articola in principi, strumenti, processi e scelte organizzative finalizzate alla protezione di beni patrimoniali aziendali, di valori gestiti e custoditi per conto della clientela a seguito di azioni deliberate o accidentali, in relazione alle specifiche esigenze di:

- incolumità, ovvero la capacità di tutelare l'integrità e l'indennità fisica dei beni patrimoniali della Società ed i valori gestiti e custoditi per conto della clientela;
- esclusività, ovvero la capacità di rendere disponibile, solo e soltanto a individui, entità o processi autorizzati ad avvalersene, i beni patrimoniali della Società e i valori gestiti e custoditi per conto della clientela;
- proprietà, ovvero la capacità di tutelare il possesso dei beni patrimoniali della Società e i valori gestiti e custoditi per conto della clientela.

1.5 CONTINUITÀ OPERATIVA

La continuità operativa, si articola in principi, strumenti, processi e scelte organizzative finalizzate ad assicurare la continuità dei processi aziendali in caso di eventi di disastro, ivi inclusi il malfunzionamento o l'interruzione prolungata di risorse e servizi ICT, in relazione a specifiche esigenze di:

- resilienza, ovvero la capacità di assicurare il ripristino dell'operatività in un intervallo temporale adeguato, sulla base delle aspettative degli utilizzatori del processo o del servizio;
- qualità, intesa come la capacità di garantire un livello qualitativo e quantitativo adeguato

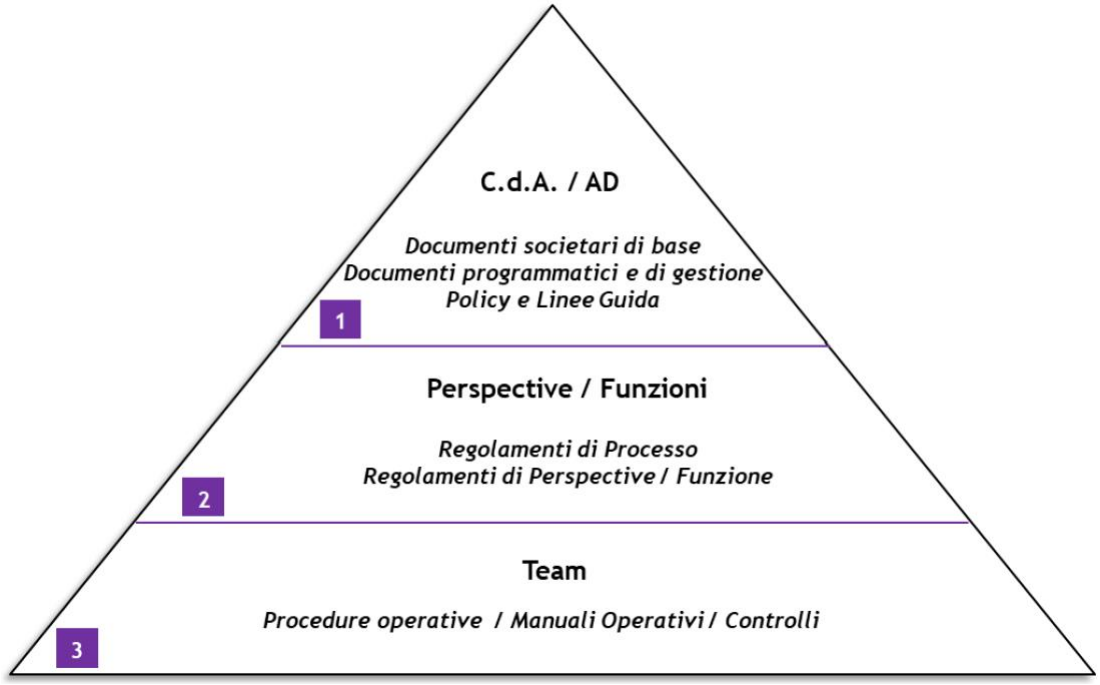
in relazione alle aspettative degli utilizzatori del processo o del servizio.

La definizione e gestione del piano di continuità operativa della Società è svolta in outsourcing dalla Capogruppo Banca Mediolanum, in virtù di un apposito contratto di prestazione di servizi aziendali. Il Piano di continuità operativa della Società è contenuto all'interno del piano di continuità operativa del Gruppo Mediolanum, approvato dal Consiglio di Amministrazione di Banca Mediolanum, oltre che, per quanto di competenza, dal Consiglio di Amministrazione di Flowe.

I principi richiamati nella presente Policy trovano attuazione nella normativa interna di livello inferiore (policy operative, regolamenti di processo), nella quale saranno meglio declinati i compiti, le attività operative e di controllo, alla base del presidio della sicurezza, descrivendone gli attori coinvolti, i loro ruoli e le responsabilità.

Con riferimento alla "Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna", il presente documento si colloca al primo livello (di vertice) della piramide documentale richiamata nello schema seguente.

Figura 1. Modello della normativa aziendale



2 APPLICABILITÀ

2.1 DESTINATARI DEL DOCUMENTO

Il presente documento è approvato dal Consiglio di Amministrazione di Flowe S.p.A. e si applica a

tutte le Perspective della stessa incluse nel perimetro di intervento.

I principi definiti si applicano a:

- tutto il personale (dipendente o che intrattiene rapporti di lavoro di altra natura);
- collaboratori esterni ed outsourcer che accedono a siti o sistemi di proprietà della Società.

2.2 RESPONSABILITÀ DEL DOCUMENTO

L'aggiornamento e la revisione periodica del presente documento sono di responsabilità di IT Operation Security & Governance.

3 DEFINIZIONI

Ai fini della presente Policy si intendono per:

Ambiente di produzione: infrastruttura tecnologica aziendale utilizzata per installare e configurare il nuovo hardware/software, sviluppato in ambiente di sviluppo, al fine di erogare i servizi.

Ambiente di sviluppo: infrastruttura tecnologica aziendale destinata allo sviluppo di nuove componenti hardware/software destinate ad essere adottate in azienda.

Autenticazione: la procedura di verifica dell'identità di un utente da parte di un sistema o servizio.

Autorizzazione: la 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.

Comunicazione Telematica: trasferimento di informazioni attraverso una rete, da un punto di origine ad un punto di destinazione.

Credenziali: le informazioni – generalmente riservate – utilizzate da un utente a fini di autenticazione ad un sistema o servizio. Sono inclusi nella definizione gli strumenti fisici che forniscono o memorizzano le informazioni (ad es., generatori di password non riutilizzabili, smart card) o qualcosa che l'utente ricorda (ad es., password) o rappresenta (ad es., caratteristiche biometriche);

Dato: elemento di cui si dispone per svolgere un'attività aziendale. I dati possono costituire input, output o elaborazioni interne di ciascun processo aziendale e possono essere classificati in base alla propria natura.

Disaster Recovery: l'insieme delle tecniche, delle tecnologie e delle modalità per ripristinare i servizi informatici erogati da un Centro di Elaborazione Dati colpito da disastro e non più funzionante, su un Centro di Elaborazione Dati alternativo e fisicamente separato dal primo.

Hardening: processo avente l'obiettivo di eliminare o ridurre la superficie di attacco dei sistemi e dispostivi aziendali, ad esempio eseguendo patching delle vulnerabilità, disattivando servizi non essenziali o adottando configurazioni di sicurezza specifiche.**IMEL**: Istituti di Moneta Elettronica, imprese che svolgono in via esclusiva l'attività di emissione di Moneta elettronica.

Incidente operativo o di sicurezza: ogni evento, o serie di eventi collegati, non pianificati dagli istituti che ha, o probabilmente avrà, un impatto negativo sull'integrità, la disponibilità, la riservatezza, e/o l'autenticità dei servizi;

Informazione: nell'ambito della trasmissione e ricezione di comunicazioni o nozioni, ritenute utili o anche indispensabili per la definizione e l'attuazione dei processi aziendali, per informazione si intende il dato elettronico, il documento cartaceo ma anche le comunicazioni telefoniche o tramite videoconferenze o altri strumenti informatici e le conoscenze del personale.

Log: registrazione sequenziale e cronologica delle operazioni e degli eventi di sicurezza, generati dagli utenti, dai servizi e dai processi su sistemi informatici, database, applicazioni o dispositivi di rete che vengono memorizzati all'interno di apposite Piattaforme di monitoraggio.

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.

PSD2: acronimo che identifica la direttiva (EU) 2015/2366 Payment Service Directive.

Resilienza: capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura, in modo da garantire la disponibilità dei servizi erogati.

Rischio ICT e di sicurezza (o rischio ICT): il rischio di incorrere in perdite dovuto alla violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell'informazione (IT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell'attività (agility), nonché i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguata. Nella rappresentazione integrata dei rischi aziendali, tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici.

Risorsa informativa: una raccolta di informazioni, tangibile o intangibile, che merita protezione.

Risorsa informatica (o ICT): qualsiasi software o hardware presente nel contesto aziendale.

Risorse (supporti): le risorse che possono "trattare" o "influire" sulle informazioni, in altre parole tutte quelle risorse che possono incidere sui parametri di disponibilità delle informazioni o sul loro uso per finalità non autorizzate o non legali. Di seguito si pone l'attenzione sulle tipologie di risorse che normalmente sono presenti in azienda:

- Edifici e locali: sedi nelle quali sono contenute e/o trattate informazioni e risorse aziendali della Società;
- Attrezzature: includono tutti gli equipaggiamenti e le infrastrutture che veicolano le informazioni appartenenti al patrimonio informativo aziendale o che le contengono. In particolare, sono compresi tutti i dispostivi hardware per l'elaborazione (personal computer, server, workstation, laptop, etc.) e la trasmissione delle informazioni (apparati e infrastrutture TLC, networking, fonia, etc.), nonché gli equipaggiamenti per i controlli di sicurezza e d'accesso fisico agli edifici e locali di cui al punto sopra. Sono, infine, inclusi gli apparati per il controllo ambientale dei data center;
- Applicazioni: comprendono tutto il software utilizzato per il trattamento di dati aziendali, sia che sia stato sviluppato internamente alla Società, sia che sia acquistato da terzi. In particolare, sono inclusi, a titolo di esempio: sistemi operativi e relativo software di supporto, sistemi di gestione dei database e applicativi di business;
- Documenti: includono tutte le informazioni aziendali, sia su supporto digitale che cartaceo, o comunque registrate su un qualsiasi altro supporto fisico;
- Personale: comprendono i dipendenti, i fornitori, i consulenti/collaboratori e tutte le persone fisiche che hanno accesso al patrimonio informativo aziendale

- Risorsa informatica (o risorsa ICT): un bene dell'azienda afferente all'ICT che concorre alla ricezione, archiviazione, elaborazione, trasmissione e fruizione dell'informazione gestita dalla Capogruppo.

Segregation of duty (Segregazione dei ruoli): 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;

Tecniche crittografiche: tecniche atte a garantire la riservatezza e l'integrità delle informazioni, rendendole illeggibili attraverso trasformazioni delle informazioni originali o la generazione di sequenze uniche di caratteri, basate sul contenuto delle informazioni stesse. Le tecniche crittografiche si basano sull'utilizzo di specifici algoritmi e utilizzano chiavi crittografiche con cui vengono elaborate le informazioni.

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.

Vulnerabilità Tecniche: punti deboli presenti all'interno di elaboratori e programmi / nella configurazione degli stessi, che potrebbero essere sfruttati da una potenziale minaccia per ottenere l'accesso a informazioni o per ostacolarne il funzionamento.

4 RUOLI E RESPONSABILITÀ

Il modello organizzativo adottato da Flowe S.p.A. per la gestione della sicurezza prevede il coinvolgimento delle seguenti strutture della società stessa e delle strutture organizzative della Capogruppo Banca Mediolanum, che svolgono in outsourcing servizi aziendali, in virtù di apposito accordo di esternalizzazione, le quali si impegnano, per quanto di competenza, ad applicare rigorosamente i principi generali di sicurezza (cfr. cap. 6) contenuti nella presente policy.

4.1 CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione della Società ha la responsabilità di indirizzo e controllo del sistema informativo aziendale, al fine di perseguire in modo ottimale le strategie aziendali di sicurezza. In particolare, ha la responsabilità di approvare la presente policy e deliberare i successivi aggiornamenti.

4.2 L'AMMINISTRATORE DELEGATO

L'Amministratore Delegato di Flowe S.p.A. SB ha la responsabilità di:

- definire la struttura organizzativa a supporto della sicurezza, assicurandone nel tempo la rispondenza alla strategia aziendale;
- garantire il corretto dimensionamento quali-quantitativo del personale impiegato nelle attività di presidio della sicurezza informatica;
- definisce e attua il disegno dei processi di gestione della sicurezza, garantendo l'efficacia e l'efficienza dell'impianto nonché la complessiva completezza e coerenza;
- assumere decisioni tempestive in merito a gravi incidenti di sicurezza informatica.

4.3 IT OPERATION SECURITY & GOVERNANCE

IT Operation Security & Governance garantisce, ispirandosi a criteri di funzionalità, efficienza e sicurezza, la gestione e lo sviluppo dei sistemi informativi e di comunicazione della Società.

In particolare, ha la responsabilità di:

- presidiare, con il supporto dell'ufficioIT Security e della Funzione Risk Management di Banca Mediolanum, il governo dei Rischi ICT e della sicurezza informatica;
- sviluppare ed attuare le strategie ed i piani complessivi di Sicurezza Informatica, in conformità alle politiche aziendali e agli obblighi normativi di settore;
- supportare la Funzione Risk Managementdi Banca Mediolanum, alla definizione del modello di valutazione e gestione del rischio ICT e di sicurezza;
- effettuare, nella figura del Control Owner, la valutazione dei presidi di competenza ICT che contribuiscono alla definizione della probabilità di accadimento degli scenari di Rischio ICT, fornendo inoltre i dati storici degli incidenti informatici;
- supportare la Funzione Risk Management, nella fase di Trattamento e nella definizione di misure compensative / alternative da integrare nei Piani di Trattamento;
- ;
- in accordo con la Direttiva (UE) 2015/2366 (PSD2) del Parlamento Europeo, svolge analisi del rischio ICT di dettaglio per i servizi di pagamento;
- definire, con il supporto dell'ufficioIT Security Governance di Banca Mediolanum, il quadro di riferimento metodologico e di controllo di primo livello per il presidio e governo della Sicurezza Informatica, condividendolo con le strutture del Gruppo;
- curare, con il supporto dell'ufficioIT Security Governance di Banca Mediolanum, la redazione e l'aggiornamento delle policy di sicurezza informatica raccordandosi con le altre unità deputate alla gestione della sicurezza informatica;
- verificare, con il supporto dell'ufficioIT Security di Banca Mediolanum, la coerenza dei presidi di sicurezza informatica con le policy approvate;
- definire, con il supporto dell'ufficio IT Security di Banca Mediolanum, i requisiti e le guideline di sicurezza per le esternalizzazioni e per la realizzazione di nuovi servizi ICT (security by design), in coerenza con i dati trattati;
- analizzare, con il supporto dell'ufficio IT Security di Banca Mediolanum, i requisiti e validare le soluzioni architetturali e tecnologiche relativamente alla sicurezza informatica;
- presidiare, con il supporto dell'ufficio IT Security di Banca Mediolanum, il monitoraggio, nel continuo, delle minacce applicabili alle risorse informatiche e monitorare/controllare i relativi programmi di mitigazione;
- presidiare, con il supporto dell'ufficio IT Security Governance di Banca Mediolanum, il recepimento delle evoluzioni normative in materia di sicurezza informatica;
-
- definire e aggiornare, con il supporto dell'ufficio IT Security di Banca Mediolanum, le policy operative di sicurezza delle informazioni, le relative procedure operative e metriche di controllo e i processi correlati, verificandone la corretta applicazione anche da parte degli outsourcer, esercitando opportuni controlli e garantendo il presidio attività degli stessi per

quanto riguarda l'erogazione dei servizi forniti;

- verificare il corretto funzionamento dei servizi informatici anche al fine di garantire la capacità e la continuità operativa dei sistemi della Società;
- definire, governare e controllare le specifiche per il piano di Disaster Recovery della Società, predisporre e mantenere le infrastrutture in linea con il suddetto piano;
- programmare, con il supporto del Business Continuity Office della Capogruppo, i test di Disaster Recovery;
- garantire, con il supporto dell'ufficio IT Security di Banca Mediolanum, il processo comunicativo verso le Forze dell'Ordine degli accadimenti relativi alla sicurezza (Incidenti di sicurezza);
- presidiare, con il supporto dell'ufficio IT Security di Banca Mediolanum, il soddisfacimento da parte dei fornitori dell'infrastruttura cloud, con i quali è in essere un contratto di servizi, dei principi di Sicurezza definiti dal presente documento per le fasi di analisi, progettazione, sviluppo, gestione e dismissione delle componenti infrastrutturali.
- supportare le Perspective della Società che gestiscono lo sviluppo applicativo e la realizzazione dei progetti IT nel rispetto dei vincoli di costo, di tempo e di qualità definiti;
- supportare le Perspective della Società che coordinano lo sviluppo e l'evoluzione tra canali, garantendone integrazione e sinergie;
- individuare le opportunità o le necessità di intervento nelle applicazioni/servizi gestiti, al fine di assicurare i livelli di servizio definiti;
- presidiare lo svolgimento dei test di sicurezza, prima dell'avvio in produzione di un sistema nuovo o modificato;
- proporre e supportare le iniziative di formazione e sensibilizzazione in materia di sicurezza delle informazioni, in collaborazione con le competenti strutture aziendali;
- gestire lo sviluppo e il disegno applicativo relativo all'interazione cliente-piattaforma con il supporto di IT Operation Security & Governance nel rispetto dei vincoli di costo, tempo e qualità definiti, garantendo i principi e i presidi di sicurezza adottati dalla Società.

4.4 ORGANIZATION & BUSINESS CONTINUITY

Organization & Business Continuity ha la responsabilità di:

- definire e gestire, con il supporto della struttura IT Operation Security and Governance e dei Perspective Leader, i processi di sicurezza logica legati alla definizione dei profili per l'accesso a reti, sistemi e base dati, ivi comprese le autorizzazioni degli utenti privilegiati, in conformità con i processi aziendali. IT Operation Security & Governance viene coinvolto per supportare il processo di gestione dei processi di sicurezza logica;
- gestire il processo di ricertificazione dei profili assegnati con il supporto della struttura IT Operation Security and Governance.

4.5 PERSPECTIVE BANKING SERVICES & CONTROLS

La Perspective ha la responsabilità di:

- difendere i clienti dai tentativi di frodi (es. phishing, crimeware);
- monitorare l'utilizzo dei sistemi di autenticazione ed eventualmente bloccarne l'uso improprio;
- gestire le operazioni disconosciute dal cliente;
- gestire le informative provenienti da altre banche circa le presunte contraffazioni e attivare le procedure previste a fronte di smarrimento/furto delle carte di debito, contattando il Cliente per il blocco e restituzione carta, eventualmente con il supporto dei fornitori esterni;
- supportare il processo comunicativo verso le Forze dell'Ordine nei casi di tentativi di frode / frodi conclamate perpetrate nei confronti dei clienti della Società.

4.6 FUNZIONE RISK MANAGEMENT DI BANCA MEDIOLANUM

La Funzione Risk Management di Banca Mediolanum, o la facente funzione, è responsabile del processo di gestione e definizione del rischio ICT e di sicurezza e in particolare:

- definisce e manutiene il framework di controllo e gestione del rischio ICT e di sicurezza;
- svolge campagne periodiche di analisi del rischio ICT e di sicurezza, al fine di identificare, analizzare e valutare il rischio ICT residuo connesso alle risorse informatiche utilizzate da Flowe, identificando le azioni necessarie al trattamento del rischio;
- redige e aggiorna la policy di Gestione del Rischio ICT e di Sicurezza e il Rapporto Sintetico sulla situazione del Rischio ICT e di sicurezza;
- effettua valutazioni del rischio ICT e di sicurezza riveniente dalle nuove iniziative/cambiamenti rilevanti e dalle esternalizzazioni con significativo impatto IT, in collaborazione con l'ufficio IT Security di Banca Mediolanum e con il team IT Operation Security and Governance, che svolge nel continuo un'attività di analisi e identificazione dei presidi da adottare;
- effettua il monitoraggio, nel continuo, dei valori assunti dai Key Risk Indicator, integrandoli nella valutazione finale del rischio ICT e di sicurezza;
- partecipa al processo di classificazione, analisi e segnalazione dei gravi incidenti di Sicurezza Informatica;
-
- nell'ambito dei processi di esternalizzazione, riveste il ruolo di Funzione di Esternalizzazione.

Inoltre, la Funzione Risk Management si occupa di:

- contribuire alla definizione dei principi e delle regole ad alto livello in ambito Sicurezza Informatica, indicate nel presente documento;
- coinvolgere il team IT Operation Security and Governance nell'ambito delle analisi relative

al rischio ICT e di sicurezza previste dal framework di valutazione e gestione del rischio ICT e di sicurezza;

- interagire con il team IT Operation Security and Governance nella valutazione delle perdite operative derivanti da incidenti gravi o rilevanti;
- ricevere i dati da Flowe per il calcolo degli indicatori di rischio ICT, previsti dal framework di gestione del rischio ICT e di sicurezza;
- interfacciarsi con le strutture del team IT Operation Security and Governance per le attività riconducibili al processo di gestione e valutazione dei rischi di una nuova esternalizzazione e di monitoraggio con riferimento alle LE servite e con cui risultano vigenti accordi di servizio dedicati.

4.7 FUNZIONE COMPLIANCE DI BANCA MEDIOLANUM

La Funzione Compliance di Banca Mediolanum è responsabile del processo di verifica della conformità alle norme e presiede la gestione dei rischi di non conformità alle norme, secondo un approccio risk based. Alla Funzione competono attività di consulenza specialistica, ai fini della valutazione del rischio di conformità, il costante monitoraggio del contesto normativo esterno (alert normativo), la valutazione dell'impatto delle normative (gap analysis) sui processi aziendali, le verifiche di adeguatezza (attraverso l'identificazione di proposte di modifiche, anche organizzative e procedurali, derivanti anche da gap analysis, valutazioni e pareri) e di funzionamento di assetti e processi aziendali atte a prevenire la violazione di norme imperative o di autoregolamentazione e il monitoraggio dell'adozione delle misure correttive proposte.

Nell'ambito della presente policy, inoltre, la Funzione Compliance:

- contribuisce alla redazione in conformità alla normativa vigente dei principi e delle regole ad alto livello in ambito Sicurezza Informatica, indicate nel presente documento;
- mediante l'Unità Framework, Reporting & Coordinamento di Gruppo riceve i rapporti di segnalazione di grave incidente informatico dalle Unità Organizzative preposte e li inoltra, in forma elettronica tramite posta elettronica certificata, a Banca d'Italia.

4.8 FUNZIONE INTERNAL AUDIT DI BANCA MEDIOLANUM

La Funzione Internal Audit di Banca Mediolanum ha la responsabilità di:

- verificare, mediante opportune attività di audit ed in collaborazione con le strutture organizzative che hanno un ruolo in materia di sicurezza sia all'interno della Società che all'interno del fornitore Banca Mediolanum o di altro fornitore esterno al gruppo, e con il supporto di IT Operation Security & Governance, l'adeguata applicazione delle misure necessarie al soddisfacimento dei principi di sicurezza definiti dalla presente Policy, eventualmente suggerendo le misure necessarie a colmare eventuali scoperture rilevate.

4.9 DIVISIONE ORGANIZZAZIONE E BUSINESS CONTINUITY OFFICE DI BANCA MEDIOLANUM

La Divisione Organizzazione e Business Continuity Office di Banca Mediolanum, in virtù del contratto di esternalizzazione in essere, attraverso l'unità Business Continuity Office, ha la responsabilità di supportare operativamente il Consiglio di Amministrazione della Società nella

stesura e aggiornamento del piano di continuità operativa aziendale e garantisce un presidio continuativo delle misure di continuità operativa.

Inoltre, per tutti gli aspetti di sicurezza logica attinenti gli asset IT proprietari di Banca Mediolanum, la Divisione Organizzazione e Business Continuity Office di Banca Mediolanum ha la responsabilità di confermare le abilitazioni richieste dal personale Flowe.

4.10 UFFICIO IT SECURITY DI BANCA MEDIOLANUM

Il Settore IT Security della Divisione ICT di Banca Mediolanum, in virtù del contratto di esternalizzazione in essere, supporta IT Operation Security & Governance nel:

- definire e gestire, i processi di attuazione e governo della sicurezza informatica secondo le linee guida del Gruppo Bancario;
- accertare che, nell'ambito dei processi di progettazione, realizzazione e manutenzione dei servizi IT, i requisiti di sicurezza forniti siano rispettati, coerentemente con quanto stabilito dalle policy in ambito;
- definisce almeno annualmente, in collaborazione con la Direzione Risorse Umane di Banca Mediolanum, piani di formazione e sensibilizzazione sulla sicurezza dell'informazione da somministrare ai dipendenti ed alle terze parti.

4.11 UFFICIO IT SECURITY GOVERNANCE DI BANCA MEDIOLANUM

L'ufficio IT Security Governance della Divisione ICT di Banca Mediolanum supporta IT Operation Security & Governance nel:

- definire il quadro di riferimento metodologico e di controllo di primo livello per il presidio e per il governo della Sicurezza Informatica, condividendolo con le strutture del Gruppo interessate;
- la redazione e l'aggiornamento delle policy di sicurezza informatica;
- recepimento delle evoluzioni normative in materia di sicurezza informatica;

4.12 SETTORE CORPORATE SERVICES DI BANCA MEDIOLANUM

Il Settore Corporate Services di Banca Mediolanum, in virtù del contratto di esternalizzazione in essere, ha la responsabilità di:

- garantire il soddisfacimento dei principi di Sicurezza definiti dal presente documento per le fasi di analisi, progettazione, sviluppo, gestione e dismissione delle componenti infrastrutturali di sicurezza fisica;
- gestire le strutture di reception e vigilanza (security) e – sotto il coordinamento del Responsabile della Sicurezza – gli impianti antintrusione e controllo accessi fisici;
- identificare ed implementare, in accordo con le strutture organizzative che si occupano di sicurezza, le misure e le soluzioni tecnologiche e procedurali necessarie al soddisfacimento

dei principi espressi dal presente documento;

- gestire, per le parti di competenza, le relazioni istituzionali e con le Forze dell'Ordine e con altri istituti / associazioni di categoria in materia di sicurezza fisica;
- gestire le iniziative di formazione e sensibilizzazione in materia di sicurezza fisica, anche in collaborazione con le competenti strutture aziendali;
- supportare le Funzioni interne di Controllo durante le attività di analisi e verifica.

4.13 Divisione Gestione e Sviluppo Risorse Umane di Banca Mediolanum

La Divisione Gestione e Sviluppo Risorse Umane di Banca Mediolanum, in virtù del contratto di esternalizzazione in essere, ha la responsabilità di:

- curare il processo di reclutamento e di selezione del personale, curare la gestione e la cessazione del rapporto di lavoro, nel rispetto dei principi di sicurezza, così come definiti dal presente documento.

5 PRINCIPI GENERALI DI SICUREZZA

La gestione della sicurezza avviene attraverso il recepimento delle linee guida dettate dalla Capogruppo allo scopo di proteggere il patrimonio informativo, materiale, del capitale intellettuale e dei processi aziendali della Società e dell'interno Gruppo. La Società, allo scopo di gestire la sicurezza fisica, delle informazioni e la continuità operativa, recepisce e ove ritenuto necessario integra strumenti, processi e soluzioni di sicurezza atti a garantire il pieno soddisfacimento dei seguenti principi:

- Classificazione delle informazioni: individuare le informazioni rilevanti e le risorse che, direttamente o indirettamente, se mal gestite o non correttamente utilizzate, potrebbero danneggiare la Società e/o la Capogruppo. L'obiettivo è assegnare il grado di criticità delle informazioni e delle risorse informative anche in base alle conseguenze derivanti da eventuali danni / eventi fraudolenti;
- Conformità normativa: garantire la conformità alle leggi nazionali, alle leggi internazionali, alle Istruzioni di Vigilanza e, più in generale, a eventuali normative in materia di sicurezza e continuità operativa;
- Cooperazione con le Autorità Pubbliche: supportare le Forze dell'Ordine, le Autorità Giudiziarie e altre Autorità Pubbliche ed istituzionali nel perseguimento e nella risoluzione di eventi criminosi, che sono stati realizzati contro o mediante l'utilizzo di risorse della Società e/o della Capogruppo;
- Rapporti istituzionali: verificare, certificare, controllare e tracciare le informazioni e i dati che sono rilasciati / pubblicati all'esterno in modo ufficiale (quindi verso "istituzioni"), attraverso opportuni presidi di sicurezza, al fine di limitare l'insorgere di rischi, sia informatici che reputazionali;
- Rapporti con i fornitori: garantire che il coinvolgimento di soggetti terzi nella gestione dei dati e delle informazioni non determini un livello di sicurezza inferiore a quello garantito dalle funzioni interne. È auspicabile applicare, ove possibile, i principi definiti per i soggetti interni, anche nei confronti dei soggetti esterni, mediante opportune clausole

contrattuali;

- Segregazione dei ruoli (c.d. “segregation of duty”): definire misure organizzative idonee a garantire la segregazione funzionale tra i diversi ruoli/attori coinvolti nei processi;
- Monitoraggio e controllo: garantire, in base all’evoluzione del contesto operativo e tecnologico di riferimento, il monitoraggio ed il miglioramento continuo delle misure di sicurezza;
- Trattamento e protezione dei dati custoditi: definire le responsabilità (proprietà del dato) per tutti coloro che, all’interno della Società, a vario titolo, possono accedere alle informazioni e ai dati in base alle proprie competenze e alla tipologia di operazioni condotte (i dipendenti, i fornitori, i collaboratori, i prestatori di servizi);
- Gestione della documentazione: produrre documentazione a supporto delle fasi di analisi, progettazione, implementazione e gestione delle misure di sicurezza al fine di consentire le verifiche da parte delle strutture organizzative competenti;
- Adeguatezza dei presidi del rischio ICT e di sicurezza: graduare le misure di sicurezza, in funzione delle minacce e delle vulnerabilità, in modo da contenere il rischio potenziale a cui le risorse sono esposte. Tale attività è svolta mediante un processo di analisi e gestione del rischio, mentre il livello di priorità degli interventi è determinato dall’esposizione e dalla propensione al rischio[2];
- Gestione del personale: gestire il personale in modo coerente con gli obiettivi di sicurezza in ogni fase del rapporto di lavoro (in fase di assunzione, nel corso del periodo di assunzione e al momento della conclusione/variazione del rapporto di lavoro).

Gli interventi derivanti da tali principi, in particolare, devono essere finalizzati a:

- implementare le misure di sicurezza in accordo al principio di proporzionalità, ovvero tenuto conto della dimensione e della complessità operative, della natura dell’attività svolta, della tipologia dei servizi prestati;
- assicurare l’adeguata vigilanza e reporting relativamente agli incidenti di sicurezza in corso o passati;
- garantire l’adeguata formazione e sensibilizzazione del personale sugli aspetti di sicurezza;
- perseguire il continuo miglioramento dei processi organizzativi e la ricerca di soluzioni tecnologiche e / o organizzative adeguate alle evoluzioni delle minacce;
- distribuire le misure di sicurezza su diversi livelli, così che un’eventuale falla in una linea di difesa sia coperta dalla successiva (“difesa in profondità”);
- garantire che l’implementazione di ogni controllo di sicurezza includa le modalità ed i meccanismi adeguati a verificarne l’efficacia e la corretta attuazione nel tempo.

6 MISURE DI SICUREZZA

La Società in accordo con la policy di Capogruppo recepisce principi e soluzioni organizzative in

[2]La propensione al rischio IT viene approvata dal Consiglio di Amministrazione.

materia di sicurezza fisica, delle informazioni e di continuità operativa. In aggiunta, ove ritenuto necessario considerando il cambiamento del contesto rispetto alla Capogruppo, la Società integra quanto recepito con misure addizionali.

6.1 ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

Organizzazione interna

La Società si impegna a:

- definire ruoli e responsabilità relative alla sicurezza delle informazioni in modo chiaro;
- evitare di creare conflitti tra compiti delle figure responsabili in tema di sicurezza con altre aree di responsabilità per ridurre al minimo le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset dell'organizzazione;
- mantenere in modo appropriato i contatti con le Autorità competenti;
- indirizzare nell'ambito della gestione delle iniziative, la sicurezza delle informazioni, a prescindere dal tipo di progetto.

Dispositivi portatili e Lavoro Agile

La Società stabilisce che:

- siano predisposte misure per il corretto utilizzo, da parte del personale interno ed esterno, dei sistemi di elaborazione aziendali, quali postazioni di lavoro, device mobili, sistemi di posta elettronica, sistemi applicativi, reti di comunicazione, ecc.;
- siano comunicate, a coloro che usufruiscono del sistema e dei servizi informativi aziendali, le regole di comportamento e gli standard di condotta per il corretto utilizzo, dei sistemi di elaborazione; in particolare:
    - le modalità di accesso ed utilizzo delle postazioni di lavoro;
    - l'atteggiamento da adottare in caso di eventi criminosi (rapina, furto o situazioni particolari) per ridurre gli impatti e allertare, prontamente, le Forze dell'Ordine e le funzioni di sicurezza competenti, al termine della eventuale azione criminosa compiuta;
    - le modalità di utilizzo delle apparecchiature portatili messe a disposizione dall'azienda esposte in modo particolare al rischio di furti.

La Società, in accordo con le normative vigenti, prevederà la possibilità per i suoi dipendenti di lavorare al di fuori degli edifici societari, in modalità "Lavoro Agile" al fine di garantire la sicurezza delle informazioni e degli asset aziendali, la Società implementerà presidi di protezione e tracciamento delle attività sui devices aziendali mobili (PC e smartphones) quali sistemi di Mobile Device Management (MDM).

Gestione dei dispositivi informatici

La Società si basa esclusivamente su un sistema di archiviazione gestito sul cloud e, pertanto, non prevede la consegna di dispositivi informatici di archiviazione e trasmissione di informazioni esterni. Qualora utilizzati viene fatto divieto al personale di esportare la documentazione

aziendale su tali dispositivi removibili.

Gli unici dispositivi previsti in dotazione dalla Società sono i laptop, i quali vengono consegnati come nuovi o rigenerati.

In caso di dimissioni o di restore dei device, la Società provvederà alla rimozione dei dati presenti all'interno del laptop attraverso la procedura di ripristino alle impostazioni di fabbrica con cancellazione completa dei dati (wipe) effettuata in modalità remota.

6.2 SICUREZZA DELLE RISORSE UMANE

La Società esternalizza le funzioni relative alla gestione delle risorse umane a Banca Mediolanum, in virtù del contratto di esternalizzazione in essere, che se ne occupa sulla base delle misure definite per l'intero Gruppo Bancario. In tale ambito Flowe adotta le misure definite dalla Banca e di seguito descritte.

In particolare, la Società stabilisce che:

- i livelli di conoscenza e competenza adeguati ai ruoli e alle responsabilità siano definiti, in vista delle attività di selezione e assunzione del personale;
- le modalità di chiusura e variazione del rapporto di lavoro con la Società debbano essere coerenti con gli obiettivi di sicurezza aziendale. In particolare, la Società deve comunicare e definire, a livello contrattuale, le responsabilità del personale per quanto concerne la sicurezza del patrimonio informativo aziendale al termine o al variare del rapporto lavorativo;
- per quanto concerne il personale adibito a compiti di sicurezza, tali mansioni siano assegnate al personale, il quale deve essere opportunamente formato ed informato circa le proprie responsabilità sulla sicurezza dei dati e delle risorse informatiche;
- siano definite procedure e misure, atte a garantire e controllare che le attività operative del personale adibito a compiti di sicurezza informatica, vengano svolte in conformità alle normative interne ed esterne.

Misure per la comunicazione, formazione e sensibilizzazione

La Società, per tramite della Capogruppo, provvede a identificare gli obiettivi dei training di Sicurezza Informatica per gli utenti aziendali, differenziandoli sulla base dei ruoli e delle mansioni lavorative coperte, definendone i contenuti e predisponendo i relativi strumenti, nonché le modalità di erogazione periodica.

Devono essere pertanto definiti almeno annualmente da parte dell'ufficio IT Security di Banca Mediolanum, in collaborazione con la Direzione Risorse Umane di Banca Mediolanum, piani di formazione e sensibilizzazione sulla sicurezza dell'informazione da somministrare ai dipendenti e alle terze parti sulla base della specificità dei servizi offerti. Le specifiche esigenze formative che dovranno essere attuate da parte dei fornitori saranno esplicitate nell'ambito degli accordi di servizio sottoscritti con le terze parti.

Tali piani devono essere approvati dall'Amministratore Delegato di Banca Mediolanum previa condivisi per revisione al Direttore Generale di Banca Mediolanum e condivisi infine con l'Amministratore Delegato della Società.

La Società recepisce le iniziative di carattere formativo e di sensibilizzazione in materia di

Sicurezza Informatica promosse da Banca Mediolanum (ad esempio incontri di Board Induction con l'Alta Direzione, pubblicazione di materiale informativo, erogazione di pillole formative, erogazione di corsi online,…) e ne monitorano l'evoluzione e l'aggiornamento, verificandone la fruizione da parte del personale aziendale e l'efficacia degli stessi, anche tramite erogazione periodica di test e/o utilizzo di eventuali simulazioni "controllate" di scenari di attacco (ad esempio simulazione di un attacco di phishing, al fine di verificare il livello di comprensione dei fenomeni da parte degli utenti), monitorando come gli utenti reagiscono in tali frangenti, al fine di poter indirizzare eventuali ulteriori azioni, quali ad esempio campagne di training/sensibilizzazione mirate, ove necessario, anche per specifiche categorie di utenti.

6.3 GESTIONE DEGLI ASSET

Misure per la custodia dei beni, dei valori e dei segreti aziendali

La Società stabilisce che:

- beni, valori e segreti aziendali siano adeguatamente protetti al fine di salvaguardarne l'integrità, evitarne l'utilizzo improprio, impedire l'interruzione dell'operatività aziendale e ridurre i rischi provenienti da minacce e pericoli ambientali; rientrano tra questi:
    - i beni appartenenti al patrimonio artistico e di interesse storico-culturale per l'azienda;
    - le informazioni riservate e/o sensibili, custodite in aree dichiarate ad accesso riservato;
    - le apparecchiature informatiche e i supporti di memorizzazione presenti nelle aree tecnologiche, se esistenti.
- norme interne siano definite per:
    - l'adeguata collocazione degli asset informatici;
    - la messa a disposizione delle risorse necessarie al funzionamento;
    - la predisposizione di un livello di manutenzione adeguato;
    - la gestione e duplicazione delle chiavi e delle combinazioni dei mezzi forti, garantendo la custodia e l'utilizzo delle chiavi solo al personale autorizzato.

Misure per la classificazione e gestione delle informazioni

La Società stabilisce che:

- per la protezione delle informazioni gestite, siano definite:
    - responsabilità degli asset: le risorse informative devono essere direttamente associate ad un proprietario;
    - classificazione delle informazioni per rilevanza: identificazione del livello di rilevanza delle informazioni rispetto ai criteri di riservatezza, integrità e disponibilità. Inoltre, ulteriori parametri quali accountability e verificabilità devono essere considerati per alcune casistiche più specifiche, ove richiesto dalla normativa;
    - classificazione delle informazioni per livello di riservatezza: corretta gestione dei dati attraverso una gerarchia di riservatezza delle informazioni articolata su cinque

livelli:

- **Pubbliche**: sono le informazioni destinate ad essere divulgate all'esterno. La divulgazione non deve causare danni o problemi di alcun tipo alla Società o alla Capogruppo, ai suoi clienti o ai suoi partner, deve essere sempre realizzata su supporti che riportino il logo della Società e deve essere sempre autorizzata;
- **Ad uso interno**: sono informazioni che possono essere diffuse senza alcuna limitazione all'interno della Società o della Capogruppo. La divulgazione di tali informazioni all'esterno della Società o della Capogruppo deve essere autorizzata e deve essere giustificata da esigenze di carattere operativo;
- **Confidenziali**: sono informazioni la cui diffusione deve essere circoscritta a coloro che ne hanno necessità per motivi di carattere professionale, strettamente connesse con le attività svolte in qualità di collaboratori della Società o della Capogruppo;
- **Sensibili/Price Sensitive**: sono le informazioni più sensibili la cui diffusione potrebbe determinare rilevanti danni alla Società o alla Capogruppo o effetti sul valore del titolo della Capogruppo. Devono essere custodite con meccanismi che ne tutelino la riservatezza e l'integrità e nel rispetto dei principi di circolazione delle informazioni riservate e privilegiate (rif. "Policy per il contrasto degli abusi di informazioni privilegiate e manipolazione di mercato - market abuse" in vigore);
- **Segrete**: informazioni ad uso esclusivo di un ambito ristretto di persone, la cui compromissione può ragionevolmente determinare severi danni, di varia natura, alla Società o alla Capogruppo. Tali informazioni devono essere sottoposte a misure di protezione adeguate (ristretta accessibilità) per garantire la loro custodia e il loro alto livello di riservatezza.

- le misure di sicurezza per l'elaborazione, l'archiviazione, la trasmissione ed il controllo delle informazioni siano definite ed implementate. Le modalità di gestione e di protezione delle informazioni devono essere coerenti con il livello di rilevanza identificato;
- L'implementazione di misure a protezione dei dati riguardino la totalità del loro ciclo di vita (includendo la loro locazione, l'accesso a questi, il loro utilizzo e la loro eventuale distruzione).

6.4 CONTROLLO DEGLI ACCESSI

Misure per il controllo degli accessi al sistema informativo

La Società stabilisce che:

- siano adottati appropriati meccanismi di registrazione e controllo degli accessi, commisurati ai rischi associati alle informazioni trattate;
- le norme e le procedure di controllo degli accessi al sistema informativo siano definite, documentate e revisionate periodicamente, in linea con le esigenze di business ed i criteri di necessità di conoscere ("need to know") e del minimo privilegio ("need to do");
- l'accesso al sistema informativo sia controllato mediante meccanismi di autenticazione degli utenti al fine di consentirne l'accesso ai soli utenti autorizzati;

- la gestione dei diritti di accesso degli utenti al sistema informativo sia regolamentata da procedure formali che definiscono tutto il ciclo di vita dei privilegi, dall'attivazione delle credenziali di autenticazione, alla loro gestione, revisione periodica, disattivazione o eventuale cancellazione/revoca.

Misure per il controllo degli accessi ai siti e alle risorse aziendali

La Società stabilisce che:

- le modalità di abilitazione all'accesso (dentro e fuori il normale orario di lavoro) e le modalità di accesso (mediante strumenti di riconoscimento, es. badge) del personale siano definite; siano fissati i requisiti necessari per la concessione di tale abilitazione e le modalità di revoca delle abilitazioni qualora non sussistano più le condizioni contrattuali; la sussistenza delle condizioni necessarie per la concessione dell'abilitazione sia verificata periodicamente; la definizione delle autorizzazioni all'accesso alle aree critiche (ad esempio archivi, aree tecnologiche, aree di carico e scarico, parcheggi) avvenga in base al ruolo e, per personale e/o tecnici esterni, solo mediante una specifica autorizzazione;
- l'accesso avvenga mediante varchi ad apertura controllata (ad esempio porte, tornelli), assicurandone il costante e corretto funzionamento; l'accesso alle aree critiche preveda ulteriori misure di controllo (es. il monitoraggio della permanenza nei locali, etc.), commisurate al rischio, al fine di prevenire accessi fisici non autorizzati, danneggiamenti e interferenze.

6.5 CRITTOGRAFIA

La Società stabilisce che:

- le comunicazioni tra sistemi informativi avvengano sempre attraverso protocolli sicuri, sia per la Società stessa che per tutti gli outsourcer coinvolti;
- esista un processo definito e sicuro per la gestione delle chiavi di accesso di tutti gli utenti, sia per la Società stessa che per tutti gli outsourcer coinvolti.

6.6 SICUREZZA FISICA E AMBIENTALE

Misure per la protezione dei siti e delle risorse aziendali

La Società stabilisce che:

- adeguate misure di sicurezza passiva per la protezione dei perimetri e degli ingressi principali e secondari (ad esempio pareti resistenti ad urti accidentali o deliberati, vetrate blindate, cancelli, tornelli) siano predisposte;
- vi siano adeguate misure di sicurezza attiva quali:
    - impianti di allarme (ad esempio sensori volumetrici, perimetrali, sismici, rilevatori fumi e microfonici), eventualmente collegati con apposite sale controllo;
    - impianti di videoregistrazione, in grado di monitorare i perimetri, gli accessi principali, gli accessi secondari e le aree critiche e rilevare eventuali eventi dannosi di origine naturale, accidentale o dolosa. Gli impianti di videoregistrazione, gestiti a livello centralizzato dalla Capogruppo, devono garantire la riservatezza delle

attività svolte dal personale, non riprendendo direttamente il personale della Società, nel rispetto dei limiti previsti dalla normativa in materia di Privacy.

- il corretto funzionamento degli impianti di allarme e degli impianti di videoregistrazione sia garantito, mediante una verifica periodica della loro funzionalità, da parte di personale autorizzato.

Misure per la gestione degli eventi criminosi

La Società stabilisce che:

- le misure di natura tecnica, normativa ed organizzativa siano definite e descritte al fine di prevenire o minimizzare gli impatti in caso di eventi di rapina, furto o situazioni particolari (ad esempio allarme bomba, dimostrazioni di piazza, tumulti), garantendo l'incolumità di persone, beni e valori eventualmente coinvolti;
- l'immediato coinvolgimento delle Forze dell'Ordine e delle funzioni di sicurezza sia garantito, in caso di segnalazioni di azioni sospette o al termine dell'evento criminoso;
- il personale sia sensibilizzato ed istruito alle problematiche correlate agli eventi criminosi di rapina, furto o altre situazioni particolari, illustrando le misure di natura tecnica, normativa ed organizzativa che devono essere osservate per la gestione di tali eventi.

6.7 SICUREZZA DELLE ATTIVITÀ OPERATIVE

Misure per la gestione dei cambiamenti

La Società stabilisce che:

- le regole per il passaggio in produzione delle applicazioni informatiche siano definite e documentate; devono essere previste specifiche procedure di storicizzazione e versioning delle modifiche;
- la predisposizione e il costante aggiornamento nel tempo di un inventario o mappa del patrimonio informatico sia garantita;
- la valutazione dell'impatto dei cambiamenti sul sistema e dei rischi correlati sia garantita;
- un adeguato meccanismo di gestione della configurazione di sistema (software) sia previsto per l'implementazione dei cambiamenti.

Misure per la protezione delle infrastrutture tecnologiche e delle applicazioni informatiche

La Società stabilisce che:

- le procedure per la gestione operativa delle infrastrutture tecnologiche siano definite, documentate e revisionate periodicamente;
- le infrastrutture tecnologiche siano progettate e gestite per assicurare la riservatezza, l'integrità e la disponibilità delle informazioni trattate;
- la separazione degli ambienti di sviluppo e di produzione sia attuata al fine ridurre il rischio di uso improprio dei sistemi;
- prima di mettere in esercizio un'infrastruttura tecnologica o una sua componente, deve

essere eseguito un piano di test comprensivo degli aspetti di sicurezza;

- la conformità dei servizi erogati sia controllata nel rispetto delle normative interne ed esterne con gli accordi intrapresi con terze parti;
- le prestazioni di ogni infrastruttura tecnologica in esercizio siano monitorate al fine di prevenire problemi dovuti a riduzioni o interruzioni dei livelli di servizio; in particolare, devono essere effettuate valutazioni periodiche di efficienza e capacità anche a fronte di prevedibili maggiori carichi (c.d. "capacity planning");
- le copie di salvataggio (backup) delle informazioni e delle applicazioni siano regolarmente effettuate e verificate al fine di mantenere l'integrità e la disponibilità dei sistemi informativi e dei servizi di comunicazione;
- le infrastrutture tecnologiche di loro utilizzo siano monitorate al fine di rilevare vulnerabilità tecniche (configurazioni non corrette, componenti software non aggiornate, etc.) e attività non autorizzate;
- le registrazioni delle attività degli operatori e dei malfunzionamenti debbano essere effettuate, nel rispetto della normativa vigente, al fine di identificare i problemi insorti, verificare l'efficacia delle misure di protezione adottate e rispondere ad eventuali esigenze legali;
- le misure per la configurazione sicura del sistema debbano essere previste nelle fasi di installazione (es. hardening/modifica di eventuali credenziali di default);
- nel corso di tutte le fasi del ciclo di vita di un nuovo sistema/servizio informatico l'utilizzo di dati personali debba sempre essere limitato allo stretto necessario, secondo le necessità operative ed in conformità con la normativa vigente (es. i dati personali utilizzati per le verifiche formali e funzionali devono essere fittizi e/o anonimi);
- le appropriate misure siano previste all'interno delle applicazioni per soddisfare i requisiti di sicurezza e per assicurare il corretto trattamento delle informazioni (acquisizione, elaborazione interna e produzione risultati).

L'infrastruttura tecnologica su cui si basa la piattaforma applicativa che garantisce la fruizione dei servizi della Società è stata costituita sulla base del principio Privacy by Design con la partecipazione dell'outsourcer Microsoft, garantendo così i migliori standard di sicurezza e la completa ottemperanza rispetto ai regolamenti vigenti.

La Società si impegna inoltre a seguire i principi dettati dal Secure System Development Lifecycle (SSDLC) allo scopo di mantenere un adeguato livello di sicurezza per ogni applicazione sviluppata internamente.

Misure per la tracciabilità delle operazioni svolte

La Società stabilisce che:

- i criteri per la tracciabilità delle operazioni critiche siano definiti;
- le norme e le procedure per la gestione e conservazione delle informazioni registrate siano definite;
- i controlli da eseguire per il monitoraggio degli eventi, anche mediante l'analisi dei log, siano definiti e documentati, al fine di prevenire e gestire gli incidenti di sicurezza informatica;

- i log per tutti gli eventi correlati ad attività critiche, eccezioni o errori sui controlli di sicurezza ed eventi di sicurezza siano definiti, generati, analizzati ed archiviati, in conformità alle normative vigenti. I log possono essere utilizzati anche per raccogliere le evidenze necessarie per eventuali attività forensi, a seguito di un incidente di sicurezza.

Gestione dei log

La gestione dei log deve essere realizzata dalla Società con modalità tali da consentire di condurre controlli di sicurezza informatica e di monitorare i guasti di tutti i sistemi informatici. Pertanto, i sistemi devono essere configurati per:

- produrre log di controllo con le necessarie informazioni sugli eventi;
- avere la capacità di trasmettere i dati dei log di controllo a un server di aggregazione dei log.

6.8 SICUREZZA DELLE COMUNICAZIONI

Misure per la protezione degli strumenti di comunicazione

La Società stabilisce che:

- la riservatezza e la disponibilità delle informazioni in transito sulle reti e la protezione delle infrastrutture tecnologiche di supporto sia assicurata;
- la separazione delle reti interne da quelle di altre organizzazioni o da quelle pubbliche sia prevista; in particolare devono essere inoltre implementate adeguate misure atte a garantire la sicurezza delle comunicazioni che la Società espone.

6.9 END USER DEVELOPED APPLICATION (EUDA)

Gli strumenti EUDA, essendo parte integrante di processi di Business o di Governance, devono essere rilevati in sede di mappatura dei processi interessati: ogni soluzione EUDA presente in azienda deve essere censita e le informazioni relative devono essere mantenute aggiornate.

Prima di dar corso allo sviluppo di una soluzione EUDA, va attentamente valutata la possibilità di individuare una soluzione alternativa di tipo centralizzato, mediante il coinvolgimento del team IT Operation Security and Governance; solo nel caso in cui tale soluzione non sia attuabile e/o conveniente, sarà possibile avviare il processo di sviluppo di una soluzione EUDA.

L'avvio della realizzazione di una soluzione EUDA deve iniziare con una fase di definizione dei requisiti funzionali, seppur minimi, esplicitando le motivazioni che ne hanno portato allo sviluppo al di fuori della competente funzione della Perspective Augmented Intelligence.

I rischi di sicurezza ricollegabili alla soluzione EUDA individuata devono essere identificati, analizzati e validati dall'unità richiedente, congiuntamente al team IT Operation Security and Governance; i rischi individuati dovranno essere documentati ed indirizzati prima del rilascio della soluzione stessa. Qualora la soluzione EUDA presenti un rischio consistente, si consiglia di rivolgersi alla Perspective Augmented Intelligence, al fine di individuare una soluzione alternativa di tipo centralizzato (si sconsiglia infatti, in tal caso, l'utilizzo di un approccio EUDA).

Nel caso la soluzione EUDA preveda l'elaborazione di dati personali o dati sensibili, devono essere rispettate tutte le misure di protezione dei dati previste dalla normativa in essere (es. accesso alla soluzione, utilizzo password, cifratura dei dati, etc.); la gestione dei diritti di accesso alle soluzioni EUDA è a carico della funzione di business che la gestisce.

Le soluzioni Terze devono essere documentate e la relativa documentazione dovrà essere conservata sia da chi ha sviluppato la soluzione, sia dal team o dalla Perspective non ICT richiedente.

Il rilascio in produzione deve essere autorizzato dal team o dalla Perspective che usufruisce dei relativi servizi.

Per gli strumenti individuali, devono essere documentati gli aspetti funzionali (acquisizione, elaborazione e gestione dei dati); prima del rilascio dell'applicazione in produzione l'utente deve effettuare un test finale.

Sia per gli Strumenti individuali "critici" che per le soluzioni Terze, deve essere prevista per gli utenti la continuità nel supporto per la gestione delle anomalie, la manutenzione e le eventuali implementazioni successive.

La Società ha incaricato il team IT Operation Security and Governance di gestire gli EUDA ed in particolare, il team deve:

- predisporre l'inventario delle soluzioni EUDA, da conservare in un Registro EUDA dedicato (contenente i dati relativi alle soluzioni EUDA presenti in azienda);
- attivare l'identificazione delle misure minime di sicurezza da applicare alle soluzioni EUDA (es. controllo accessi, conservazione e manutenzione dei sorgenti ed esecuzione dei backup, per le soluzioni Terze e per gli Strumenti individuali critici, ecc);
- attivare la verifica dell'applicazione delle misure minime di sicurezza stabilite;
- attivare eventuali valutazioni in merito alla possibilità/opportunità di un passaggio alla gestione centralizzata della soluzione EUDA.

Si specifica che è responsabilità dei team o delle Perspective richiedenti un nuovo EUDA di fornire al team IT Operation Security and Governance le informazioni relative alle soluzioni EUDA in essere o da sviluppare

6.10 RELAZIONI CON I FORNITORI

Misure per la gestione dei rapporti con i fornitori

La Società stabilisce che:

- le relazioni con soggetti terzi debbano essere definite mediante contratti che chiariscano i requisiti di sicurezza (conformità alle normative vigenti, accordi di non divulgazione, eventuale richiesta di specifiche attività di controllo, etc.), in base a quanto definito dalla normativa interna in tema di esternalizzazione e dalle normative esterne applicabili;
- il fornitore di servizi garantisca la sicurezza delle informazioni relative alle attività svolte per la Società, sotto l'aspetto della disponibilità, dell'integrità, della riservatezza, dell'accountability e della verificabilità;
- la gestione dei dati e delle informazioni da parte dei fornitori esterni debba essere soggetta a limitazioni (accesso alle informazioni, permessi autorizzativi concessi, etc.) e preventivamente valutata sul piano dei rischi a cui le informazioni potrebbero essere

esposte (es. accordi di riservatezza con i fornitori di servizi ICT);

- sia esercitato il monitoraggio della conformità dell'outsourcer rispetto ai requisiti contrattuali in tema di sicurezza, per identificare eventuali misure da adottare in caso di gravi mancanze;
- il fornitore di servizi comunichi tempestivamente alla Società il verificarsi di incidenti di sicurezza, anche al fine di consentire la pronta attivazione delle relative procedure di gestione degli incidenti o di emergenza.

Misure per la gestione del Cloud

La Società recepisce le raccomandazioni in applicazione dell'articolo 16 del regolamento (UE) n. 1093/2010 in tema di esternalizzazione di servizi in cloud. In particolare, la Società:

- si impegna a valutare i rischi ai fini dell'identificazione di quali attività siano rilevanti;
- si impegna ad informare adeguatamente le autorità competenti circa le attività rilevanti che si esternalizzano in Cloud;
- si impegna a tenere un registro aggiornato delle informazioni su tutte le attività esternalizzate a fornitori di servizi Cloud;
- deve poter avere diritto di controllo sui fornitori ed esercitarne i diritti secondo modalità basate sui rischi verificando inoltre che il personale che lo effettua abbia le giuste capacità e conoscenze;
- deve garantire tramite apposite sezioni contrattuali la riservatezza delle informazioni trasmesse e salvate su Cloud;
- deve tener conto di eventuali rischi connessi all'esternalizzazione "a catena" (ad esempio, se il fornitore di servizi cloud fa parte di una catena di subesternalizzazione);
- deve pianificare e attuare provvedimenti atti a garantire la continuità operativa aziendale anche in caso di interruzione o deterioramento inaccettabile dell'erogazione dei servizi da parte di un fornitore Cloud;
- deve accertarsi di avere la possibilità, ove necessario, di recedere da accordi di esternalizzazione tramite Cloud senza che ciò comporti un'indebita interruzione della sua erogazione di servizi o pregiudichi la conformità al regime normativo.

6.11 GESTIONE DEGLI INCIDENTI

Misure per la gestione delle situazioni di crisi

Allo scopo di una più dettagliata descrizione delle attività, è stato ritenuto necessario suddividere il processo di gestione degli incidenti in due sotto-processi: gestione operativa degli incidenti, compresi gli incidenti valutati e classificati come "gravi" in base alle istruzioni di Banca d'Italia e gestione della crisi. La gestione operativa di tutti gli incidenti è in carico alla Società. In caso di crisi sarà invece la Capogruppo, in qualità di outsourcer dei servizi di gestione della continuità operativa, a coordinare il processo di gestione.

La Società, in adesione ai principi di Gruppo, stabilisce che:

- le strutture organizzative coinvolte nei processi di gestione delle emergenze siano definite, all'interno del Piano di Continuità Operativa, identificandone ruoli e responsabilità;

- le modalità di rilevazione e classificazione dell'evento di crisi, le modalità di attivazione dei processi per la gestione delle emergenze (escalation) e di attivazione delle necessarie soluzioni di continuità operativa siano definite e descritte all'interno del Piano di Continuità Operativa;
- le modalità di ripristino dell'operatività ordinaria, a seguito dell'emergenza e di analisi delle modalità gestionali implementate, siano definite e descritte, all'interno del Piano di Continuità Operativa, al fine di identificare eventuali interventi migliorativi.

Misure per la gestione degli incidenti di sicurezza

La Società stabilisce che:

- le procedure di gestione degli eventi e delle debolezze, segnalate rilevanti per la sicurezza, siano definite, documentate e revisionate periodicamente (c.d. "incident management");
- per assicurare l'efficace e tempestiva attivazione di tali procedure in caso di eventi di sicurezza, opportuni ruoli e responsabilità debbano essere definiti e assegnati, per la gestione ed il monitoraggio degli incidenti all'interno dell'organizzazione;
- le procedure di segnalazione degli incidenti di sicurezza siano rese disponibili al personale designato;
- siano definite opportune procedure e canali di comunicazione per la segnalazione tempestiva, qualora sia necessario, di gravi incidenti di sicurezza alle Autorità competenti;
- per tutti gli incidenti di sicurezza devono essere adottate specifiche azioni correttive.

Misure per la gestione delle frodi sulla multicanalità e sui sistemi di pagamento

La Società stabilisce che:

- per l'accesso, da parte dei clienti, ai servizi di pagamento via internet e mobile si debbano prevedere meccanismi di *strong authentication* che consentano alla Società di verificare l'identità del cliente;
- siano previste misure di sicurezza specifiche nell'ambito delle procedure di attivazione e consegna al cliente degli strumenti di autenticazione;
- un processo di monitoraggio dei comportamenti sospetti, sui servizi erogati dai canali telematici adottati per l'offerta e dagli strumenti di pagamento elettronico, sia definito, al fine di identificare le operazioni anomale effettuate, stabilendo appropriati strumenti, ruoli e responsabilità a supporto delle suddette attività; per l'autorizzazione delle transazioni di pagamento e per il relativo monitoraggio, si devono definire processi efficaci, al fine di identificare schemi di pagamento sospetti e prevenire eventuali frodi;
- sia definito un processo di verifica delle segnalazioni provenienti da Forze dell'Ordine o da altre funzioni competenti interne ed esterne, correlate a comportamenti sospetti, finalizzato a:
    - esaminare segnalazioni pervenute;
    - comunicare i risultati dell'accertamento alle controparti interne ed esterne interessate, stabilendo appropriati strumenti, ruoli e responsabilità a supporto delle suddette attività.

- al fine di prevenire eventuali frodi, le transazioni di pagamento siano tracciate, monitorate e analizzate tramite opportune soluzioni tecnologiche, in modo da garantire l'identificazione tempestiva e l'eventuale blocco di ordini di pagamento anomali;
- le procedure di segnalazione dei diversi tipi di eventi che possono essere correlati ad attività fraudolente siano rese disponibili a tutto il personale coinvolto, interno o esterno, e alla propria Clientela (ove necessario), identificando i referenti designati alla raccolta e diffusione di tali segnalazioni;
- siano previste informative agli utenti finali sui requisiti necessari (ad esempio: tecnologici oppure procedurali) per l'esecuzione di operazioni di pagamento in modalità sicura su canale internet e mobile e sui rischi inerenti a tali operazioni di pagamento.

6.12 MISURE PER LA CONTINUITÀ OPERATIVA

La Società recepisce le linee guida in termini di Continuità Operativa definite dalla Capogruppo.

Misure per la continuità operativa

La Società adotta i seguenti principi definiti dalla Capogruppo e stabilisce che:

- siano presi in considerazione i seguenti aspetti:
  - i principali scenari di crisi (ad esempio eventi naturali, attività umana, danneggiamento grave da parte dei dipendenti, etc.);
  - le strutture organizzative che gestiscono processi con requisiti di continuità mandatori o che sono ritenuti critici, per l'impatto economico, normativo e reputazionale;
  - le risorse informatiche e non informatiche necessarie all'erogazione dei processi critici.

per cui predisporre, in base ad una analisi preliminare di impatto, soluzioni di Continuità Operativa. L'obiettivo è garantire l'operatività minima, soluzioni di alta affidabilità e di Disaster Recovery proporzionali al livello di criticità;

- il "Piano di Continuità Operativa" di Gruppo, integrato con le specificità della Società, sia predisposto, aggiornato e distribuito all'interno della Società. Questo deve contenere l'insieme delle soluzioni di continuità predisposte ed esplicitare il modello di gestione della Continuità Operativa (ruoli e responsabilità) nonché i processi per la gestione in ordinario e in emergenza.

Misure per il Disaster Recovery

La Società adotta i seguenti principi definiti dalla Capogruppo e stabilisce che siano identificate all'interno del Piano di Continuità Operativa di Gruppo le applicazioni e le infrastrutture informatiche della Società per le quali garantire soluzioni di alta affidabilità e di Disaster Recovery, tali da garantire requisiti di ripristino proporzionali alla criticità del processo; siano predisposte le misure tecnologiche atte a garantire tali requisiti di ripristino di applicazioni e infrastrutture;

- le soluzioni di ripristino definite siano testate periodicamente, al fine di garantirne

l’efficacia nel tempo e di identificare eventuali necessità di revisione o aggiornamento.

La Società esternalizza i servizi ad outsourcer esterni al Gruppo: per questo motivo, i piani di Disaster Recovery di ciascun outsourcer dovranno costituire allegato al Piano di Continuità Operativa di Gruppo, nel quale vengono identificate le misure adottate da tutte le società appartenenti al Gruppo.

7 NORMATIVA DI RIFERIMENTO

Di seguito si riportano i principali riferimenti normativi e regolamentari in tema di sicurezza utilizzati per la stesura del presente documento:

Normativa esterna:

- Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d’Italia il 23 luglio 2019 e successive modifiche;
- "Orientamenti finali sulla sicurezza dei pagamenti via internet" emanati dall’European Banking Authority (EBA), 19 dicembre 2014 i seguenti aspetti;
- Direttiva (UE) 2015/2366 (PSD2) per le misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento del 12 gennaio 2018 i seguenti aspetti;
- Decreto Legislativo 9 aprile 2008 nr. 81 Testo Unico sulla salute e sicurezza sul lavoro i seguenti aspetti;
- Norme UNI 10459:2017 in tema di Security Management.
- Regolamento (UE) n. 1093/2010 del Parlamento Europeo e del Consiglio e successive modifiche

Normativa interna:

Policy di Incident Management