Cybersecurity e Privacy

La **protezione** e la **riservatezza** dei dati dei nostri clienti e stakeholder, così come la **sicurezza** della nostra operatività, sono tra le nostre priorità massime. Ecco perché sono parte integrante della strategia di sostenibilità della Banca.

Siamo consapevoli di operare in un settore economico essenziale per le imprese, le famiglie e tutto il Paese. Questo ci spinge a innovare e aggiornare le nostre modalità di lavoro per garantire i più elevati livelli di servizio e sicurezza.

Abbiamo avviato un **Piano d'Azione ESG (Environmental, Social & Governance)** in cui la **cybersecurity** riveste un ruolo rilevante. In particolare, abbiamo predisposto piani specifici per la **business continuity** e la **sicurezza**, oltre a procedure costantemente aggiornate. Nella gestione ci basiamo sugli **standard ISO 27014**, realizziamo continue attività di formazione e ci avvaliamo di partnership esterne qualificate.

La strategia di trasformazione digitale

La nostra strategia di trasformazione digitale è avviata già da diversi anni e si è accelerata in risposta alle esigenze sorte con l'emergenza pandemica: abbiamo migliorato interazioni, autonomia e flessibilità e – al contempo – poniamo sempre maggiore attenzione alla gestione dei rischi legati al mondo dei servizi bancari online, come illeciti e frodi digitali.

Per quanto riguarda la continuità operativa, la cybersecurity e la privacy, il nostro modello di gestione si fonda su due pilastri: l'ambito della Data Governance e IT Security garantisce la gestione e la sicurezza di dati e informazioni, assicurando la continuità operativa, mentre l'ambito Privacy promuove la tutela del patrimonio informativo a disposizione del Gruppo.

Tanto nelle attività quotidiane come nel definire le strategie di innovazione del servizio, seguiamo con attenzione e scrupolo le direttive e le politiche nazionali e internazionali sulla sicurezza.

Un ambiente digitale più sicuro

Il nostro obiettivo è garantire la sicurezza dei dati e delle operazioni. E, per costruire un ambiente digitale più sicuro, lavoriamo su tre aspetti sinergici e complementari: innovazione, adozione di nuove tecnologie, miglioramento continuo.

Implementiamo innanzitutto nuove modalità di lavoro, come l'estensione dell'Open Banking, gli Advanced Analytics o la Blockchain, e abbiamo attivato un sistema SIEM (Security Information and Event Management) di nuova generazione.

Inoltre, introduciamo costantemente nuove protezioni, quali la doppia autenticazione nelle app o la Strong Customer Authentication per pagamenti online tramite carte, e promuoviamo la consapevolezza

tra i clienti fornendo informazioni attraverso tutti i canali di comunicazione, in particolare digitali (app, web ed e-mail, messaggistica e bancomat).

Partecipiamo infine a numerose partnership per prevenire il cybercrime: tra queste il CERTFin (CERT Finanziario Italiano), un'iniziativa pubblico-privata finalizzata a innalzare la capacità di gestione e la resilienza del sistema finanziario, mentre nell'ambito del progetto OF2CEN (Online Fraud Cyber Centre Expert Network), è attiva una collaborazione con la Polizia di Stato per lo scambio in tempo reale di informazioni.

Il nostro Security Operation Center

Per intervenire tempestivamente sugli incidenti informatici, è costantemente operativo un Security Operation Center che prende in carico e analizza le segnalazioni di cybersecurity. Una volta identificato il tipo di incidente, il Centro avvia azioni di contenimento e risoluzione coinvolgendo le strutture aziendali pertinenti e, se necessario in relazione al livello di gravità, anche le funzioni apicali.

Il nostro sistema IT è sottoposto a controlli secondo la normativa di Banca d'Italia, con una frequenza relativa alle criticità ed esigenze. Per la gestione del sistema di sicurezza, il Gruppo segue lo standard ISO 27001.

La gestione degli incidenti rientra nel processo di crisis management, che definisce le strategie e i soggetti da coinvolgere. Per i casi più rilevanti, è prevista la comunicazione dell'incidente alle autorità di controllo, come la stessa Banca d'Italia.

Come ulteriore garanzia, abbiamo stipulato due polizze assicurative per una completa copertura degli incidenti informatici.

Approfondimenti

La protezione dei dati, la sicurezza informatica e la continuità operativa sono valori che portiamo avanti ogni giorno, attraverso un approccio strutturato e iniziative mirate.

Il sistema informativo rispetta gli standard europei e italiani ed è sottoposto a verifiche periodiche. Collaboriamo inoltre con qualificati partner esterni indipendenti.

In un'ottica di responsabilità aziendale, la sicurezza informatica e la privacy sono presidiate da tre funzioni che rispondono direttamente al Condirettore Generale e all'Amministratore Delegato: Data Governance e Sicurezza IT, Information Technology e Compliance (Data Protection Officer).

Per identificare i potenziali rischi alle attività aziendali e sviluppare strategie adeguate a minimizzarli, conduciamo una business impact analysis. I risultati dell'analisi d'impatto permettono di sviluppare il Piano di continuità operativa che assicura la business continuity del Gruppo definendone princìpi, le procedure e le risorse.

Per affrontare i diversi scenari definiti dalla normativa, il Piano si articola in piani specifici come quello di disaster recovery, che individua siti alternativi per consentire il funzionamento delle procedure rilevanti. Il Piano di continuità operativa viene testato almeno una volta l'anno e i risultati vengono sottoposti al Consiglio di Amministrazione della Capogruppo e delle altre società coinvolte.

Relativamente al Piano di Sicurezza svolgiamo regolarmente valutazioni in linea con lo standard NIST Cybersecurity Framework e in collaborazione con partner qualificati. Il sistema informativo aziendale rispetta gli accreditamenti esterni (PCI-DSS, SWIFT CSP, etc.) e lo standard europeo e italiano.

Per garantire la continuità operativa definiamo principi, procedure e risorse e abbiamo predisposto piani specifici per proteggere l'operatività anche in presenza di eventi avversi.

La centralità della formazione

Con l'obiettivo di diffondere consapevolezza sulle tematiche di sicurezza e privacy, realizziamo iniziative formative tramite lezioni interattive in aula virtuale, corsi di formazione a distanza (o in presenza), consigli e raccomandazioni veicolati a clienti e colleghi tramite il sito web, i nostri canali social e la intranet aziendale.

Le iniziative toccano tutti i più importanti aspetti della cybersecurity e privacy, a partire dalle tematiche generali fino agli approfondimenti sulle normative, come il GDPR. Sono inoltre previste iniziative di formazione specifiche su questi temi mirate a supportare i neoassunti ad acquisire consapevolezza in questi ambiti.

Con l'obiettivo di innalzare l'attenzione dei dipendenti verso questa tipologia di rischi, vengono attuate simulazioni di un piano di phishing con l'invio di mail che ricreano le caratteristiche di questa frode informatica, mettendo i collaboratori in grado di riconoscerla più facilmente.

Il modello di protezione dei dati

Il nostro modello di protezione dei dati guarda costantemente ai diritti e alle libertà degli interessati, mantenendo un equilibrato bilanciamento tra questi e le esigenze di business.

Il Responsabile della Protezione dei dati (anche Data Protection Officer/DPO) è il Responsabile della Funzione Compliance e riporta direttamente all'Amministratore Delegato, con accesso diretto agli organi sociali.

A supporto del DPO abbiamo costituito un ufficio dedicato al mondo della privacy così da poter presidiare il rispetto della normativa sulla protezione dei dati in tutti gli ambiti della nostra attività, privilegiando un approccio che possa garantire un utilizzo dei dati rispettoso dei diritti e delle libertà degli interessati.

La nostra policy sulla protezione dei dati definisce: i) i principi e le regole a cui attenersi nello svolgimento delle attività quotidiane e ii) ruoli e responsabilità nel presidio del ciclo di vita dei dati.

Tutti i dipendenti ricevono le istruzioni su come trattare e custodire i dati nonché le indicazioni sui comportamenti da tenere o evitare per garantire la riservatezza delle informazioni.

Per le attività di organizzazione, acquisizione, progettazione e sviluppo di una componente IT, prodotto o servizio è prevista la valutazione anche in termini di impatto privacy, trattamento e protezione dei dati personali. Le misure tecniche e organizzative, per impostazione predefinita, devono garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento, tenendo conto della quantità di dati personali raccolti, del tipo di trattamento e della loro accessibilità.

La nostra policy dedicata alla gestione dei diritti degli interessati prevede: i) l'aggiornamento costante dell'Informativa privacy e l'individuazione delle funzioni aziendali a cui compete la corretta individuazione delle basi giuridiche dei trattamenti; ii) la definizione del processo di ricezione, valutazione ed evasione delle richieste degli interessati; iii) la sinergia con le funzioni commerciali e tecniche competenti per garantire la tenuta del processo.

I nostri fornitori garantiscono la loro conformità alle norme sulla protezione dei dati e l'eventuale assenza di adeguate garanzie ne comporta l'esclusione dalle collaborazioni.

Promuoviamo la conoscenza e consapevolezza dei dipendenti tramite iniziative formative articolate in sessioni di formazione sia a distanza sia in aula virtuale: soluzioni che, combinate fra loro, consentono di coinvolgere il maggior numero di "Stakeholder" (i dipendenti).

Il nostro processo di gestione delle violazioni dei dati personali prevede il coinvolgimento tempestivo di tutte le funzioni competenti per le analisi e la classificazione degli eventi e definisce i requisiti per gli eventuali obblighi di comunicazione all'Autorità competente e agli interessati.

I nostri clienti possono gestire in completa autonomia le loro preferenze in ambito privacy, grazie a una sezione *ad hoc* nell'area riservata del proprio home banking (App e Web). In tale sede possono autonomamente modificare i consensi e selezionare i canali di contatto più graditi. Per coloro che invece non hanno la disponibilità dell'home banking sono previsti l'intervento della filiale e il supporto dell'ufficio dedicato del DPO.

Per ogni altra informazione puoi consultare la nostra sezione dedicata alla privacy:

https://gruppo.bancobpm.it/privacy