3.

Ifis Integrity

3.1 Integrità aziendale e lotta alla corruzione

Politiche e altra documentazione di riferimento

- Codice Etico
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001
- Manuale tecnico-operativo Certificazione posizioni per match con liste negative antiriciclaggio e antiterrorismo
- La Politica di Gruppo per la gestione delle segnalazioni delle violazioni (Whistleblowing)
- Procedura Organizzativa Gestione della rete dei recuperatori stragiudiziali dei crediti distressed (Banca Ifis, IFIS NPL)
- Procedura Organizzativa Adeguata verifica e profilatura della clientela per classi di rischio – fase di onboarding (Banca Ifis)
- Procedura Organizzativa Adeguata verifica e profilatura della clientela per classi di rischio – nel continuo
- Politica di Gruppo per la gestione del rischio di riciclaggio e di finanziamento del terrorismo
- Procedura Organizzativa Adeguata verifica e profilatura della clientela NPL per classi di rischio (IFIS NPL)
- Istruzioni per la compilazione Agenti
- Istruzioni per la compilazione SDR
- Manuale Antiriciclaggio (Banca Ifis)
- Manuale Antiriciclaggio Cap.Ital.Fin.
- Manuale operativo “Embargo e antiterrorismo: Controlli sui bonifici in entrata ed uscita” (Banca Ifis)
- Procedura Organizzativa per la Gestione dei crediti erariali (Banca Ifis)
- Procedura Organizzativa attivazione Contomax (Banca Ifis)
- Procedura Organizzativa Rendimax (Banca Ifis)

Il modo in cui Banca Ifis conduce la propria attività di business è oggetto di grande attenzione da parte degli stakeholder. Il Gruppo Banca Ifis si impegna a sviluppare e a diffondere la cultura e i valori aziendali sia all’interno sia all’esterno e a competere con integrità e rispetto in tutti gli aspetti di compliance normativa, con particolare impegno nella lotta alla corruzione. Il Codice Etico rappresenta il “manifesto” della cultura aziendale di Banca Ifis e delle altre società del Gruppo, destinato sia alla informazione/formazione dei Collaboratori sia alla diffusione di tale cultura presso tutti gli stakeholder. Dato che l’efficacia del Modello Organizzativo e del Codice Etico presuppongono una piena diffusione della “cultura del controllo” presso tutti i dipendenti e la sensibilizzazione di tutte le strutture coinvolte, il Gruppo cura la formazione del personale sui contenuti del Modello Organizzativo ex D. Lgs. 231/01 e sul Codice Etico.

In relazione al Codice Etico l’Organismo di Vigilanza ha, tra gli altri, il compito di vigilare sul suo rispetto e applicazione, di attivare gli eventuali provvedimenti sanzionatori, di coordinare l’elaborazione delle norme e delle procedure che ne attuano le indicazioni, di promuovere la revisione periodica del Codice dei suoi meccanismi di attuazione e di riportare al Consiglio d’Amministrazione sull’attività svolta e sulle problematiche connesse all’attuazione del Codice Etico.

La prevenzione alla corruzione

Il Gruppo Banca Ifis si è dotato, per la prevenzione del rischio di commissione dei reati di corruzione e concussione, di linee guida espresse nel Codice Etico e del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001, quest'ultimo è stato aggiornato nel 2019 principalmente al fine di:

- specificare il ruolo della Capogruppo, prevedendo in capo a quest'ultima il potere di impartire criteri e direttive di carattere generale e di verificare, mediante le funzioni di controllo, la rispondenza dei Modelli delle società appartenenti al Gruppo a tali criteri e direttive;
- declinare i principi di indirizzo di Gruppo in materia di responsabilità amministrativa degli Enti e specificare in particolare, che ogni società appartenente al Gruppo è tenuta a: (i) adottare il proprio Modello, (ii) nominare l'Organismo di Vigilanza, assicurare il sistematico aggiornamento del Modello in funzione di modifiche normative e organizzative, (iii) predisporre piani di formazione, (iv) adottare un idoneo presidio dei processi sensibili al Decreto;
- in merito alle attività a rischio, introdurre talune ulteriori ipotesi esemplificative delle occasioni di reato e aggiornare le principali strutture e i soggetti coinvolti.

L'integrità della condotta degli agenti del Gruppo

Oltre a stabilire regole di condotta per il proprio personale, il Gruppo Banca Ifis ritiene fondamentale assicurare l'integrità della condotta anche degli agenti dell'area Leasing e della società Cap.Ital.Fin. nonché degli agenti e delle società di recupero di IFIS NPL.
Ad esempio, per garantire l'integrità dei comportamenti degli agenti e delle società di recupero vengono attuati diversi presidi, tra cui:

- l'obbligo di osservanza del Codice Etico e del Modello Organizzativo previsto dal decreto 231/01 all'atto della sottoscrizione del contratto;
- il controllo del numero dei mandati: la rete di agenti può avere al massimo tre mandati e solo di attività non in concorrenza;
- l'adozione di un sistema di incentivazione le cui logiche scoraggiano comportamenti scorretti o insistenti da parte degli agenti.

Relativamente alla gestione del call center della società IFIS NPL dedicato alla phone collection, sono aumentate ulteriormente le risorse disponibili, è stata ottimizzata l'organizzazione del lavoro interna e sono stati creati strumenti orientati al monitoraggio costante e analisi delle performance, che hanno, tra gli obiettivi, anche il contenimento del rischio di comportamenti "aggressivi" o pratiche commerciali scorrette da parte degli operatori. La società IFIS NPL adotta diverse modalità di verifica dell'efficacia dell'approccio di gestione adottato:

- verifiche da parte del call center "di monitoraggio", distinto da quello dedicato alla collection, che contatta tutti i clienti che abbiano risolto positivamente la propria posizione grazie ai piani di rientro proposti e, a campione, anche i clienti con i quali non viene raggiunto un accordo, al fine di verificare la correttezza e l'integrità dei comportamenti degli operatori di rete;

- richiesta agli agenti di predisporre, al termine di ogni visita al cliente, un “Verbale di visita” che riepiloga quanto accaduto e gli accordi stabiliti, che deve essere sottoscritto dal cliente stesso così da tenere una traccia trasparente e oggettiva di quanto concordato;
- revisione trimestrale dei reclami non accolti per identificare eventuali problematiche emergenti o aspetti di crescente interesse per i clienti, al fine di definire azioni correttive;
- monitoraggio continuo dei canali social della Banca;
- interviste a clienti che hanno risolto positivamente la pratica;
- ascolto continuo delle problematiche ed esigenze espresse dagli operatori della rete.

Il Codice Etico chiarisce che, nella gestione dei rapporti con la Pubblica Amministrazione, è vietato promettere od offrire a pubblici ufficiali o a dipendenti, pagamenti o beni per promuovere o favorire gli interessi del Gruppo in sede di stipulazione ed erogazione di contratti, aggiudicazione e gestione delle autorizzazioni, riscossione di crediti anche verso l’Erario, attività ispettive o di controllo o nell’ambito di procedure giudiziarie.

Chiunque riceva richieste o proposte di benefici da pubblici funzionari deve immediatamente riferire al proprio superiore e all’Organismo di Vigilanza.

Il Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 di Banca Ifis prevede le seguenti fattispecie di reato relative alla corruzione:

- Corruzione per l'esercizio della funzione;
- Corruzione per un atto contrario ai doveri d'ufficio;
- Corruzione in atti giudiziari;
- Corruzione di persona incaricata di un pubblico servizio;
- Concussione, induzione indebita a dare o promettere utilità e corruzione;
- Corruzione tra privati;
- Istigazione alla corruzione tra privati.

Il Modello di Organizzazione, Gestione e Controllo ex. D. Lgs. 231/2001 di Banca Ifis specifica che le strutture di controllo per quanto riguarda la commissione dei reati potenziali relativi alla corruzione sono, oltre alle funzioni di controllo di secondo e terzo livello, l’Organismo di Vigilanza e il Collegio Sindacale.

[GRI 205-2]

Il Consiglio di Amministrazione, in sede di approvazione del Codice Etico del Gruppo, viene a conoscenza delle procedure anticorruzione adottate. Tutti i dipendenti sono tenuti a conoscere e rispettare le regole in materia di contrasto alla corruzione, anche con riferimento alla tabella allegata al Modello che regola nel dettaglio le potenziali attività sensibili, le principali strutture e le tutele poste in atto in termini di politiche, regolamenti interni e strutture di controllo. Inoltre, tutti i dipendenti del Gruppo hanno accesso, attraverso la Intranet aziendale, alla normativa interna aziendale e in particolare il Codice Etico, MOG, protocolli e procedure in materia.

Il Gruppo assicura che tutti i dipendenti ricevano, ciclicamente e in caso di aggiornamenti nella normativa, adeguata formazione (diversamente dall’anno precedente, nel 2019 non sono stati riscontrati aggiornamenti normativi e relativa esigenza di formazione) sulle politiche e le procedure anticorruzione di cui al Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001. È infatti disponibile sulla piattaforma IFIS Talent, un corso e-learning ad hoc rientrante nel percorso di formazione obbligatoria del personale della Banca e per cui periodicamente si sollecita il completamento.

Nella tabella di seguito viene indicato il numero di dipendenti che hanno ricevuto formazione in materia, nel corso dei due esercizi precedenti, dall'implementazione della piattaforma IFIS Talent:

Numero e percentuale di dipendenti che hanno ricevuto formazione sulla lotta alla corruzione, suddivisi per categoria di inquadramento		**2019**[8]	**2018**
	N.	**476**	**798**
	%	**27,2%**	**48,7%**
Dirigenti	N.	8	5
	%	10,8%	8,2%
Quadri	N.	116	223
	%	22,7%	45,9%
Impiegati	N.	352	570
	%	30,1%	52,2%

Il Gruppo Banca Ifis ad oggi non ha svolto moduli formativi specifici sui reati corruttivi rivolti ai Consiglieri di Amministrazione. Tuttavia, occorre considerare che i membri del Consiglio di Amministrazione nel 2019 hanno approvato l'aggiornamento del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 che contiene anche prescrizioni afferenti alla prevenzione del rischio di commissione dei reati corruzione e concussione.

Come già descritto in precedenza, per garantire l'integrità dei comportamenti degli agenti e delle società di recupero vengono attuati diversi presidi, tra cui l'obbligo di osservanza del Codice Etico e del Modello Organizzativo previsto dal decreto 231/01 all'atto della sottoscrizione del contratto.

Infine, per quanto riguarda gli stakeholder della Banca, il Codice Etico e la "Parte Generale" del Modello di Organizzazione e Gestione ex. D. Lgs. 231/01 sono resi noti attraverso la pubblicazione sul sito web di Gruppo.

[GRI 205-3]

Anche nel 2019, analogamente all'esercizio precedente, non sono stati registrati casi di corruzione o cause legali che abbiano riguardato dipendenti del Gruppo o operatori delle reti esterne.

La prevenzione al riciclaggio e finanziamento al terrorismo

La prevenzione del rischio di riciclaggio è un elemento portante per la tutela della solidità finanziaria e, più in generale, della reputazione aziendale, e riflette l'impegno costante della Banca alla collaborazione attiva nei confronti dell'Autorità di Vigilanza. Il Gruppo rifiuta di intrattenere relazioni, in modo diretto o indiretto, con persone e aziende delle quali sia conosciuta o sospettata l'appartenenza a organizzazioni criminali o comunque operanti al di fuori della liceità. Di conseguenza:

- nel settore Leasing vengono esaminate le notizie negative di stampa tramite un processo automatizzato e integrato nella procedura dell'auto-delibera: se emergono riscontri la pratica viene bloccata e indirizzata verso la valutazione manuale, anche con il coinvolgimento dell'Antiriciclaggio. L'esito delle verifiche si traduce nell'assegnazione di un profilo di rischio in base al quale viene attivato un processo di approvazione a livelli diversi della gerarchia aziendale;
- nel Credito Commerciale il controllo sopra descritto è integrato nelle procedure di anagrafe. Anche in questo caso, in funzione dei riscontri ottenuti, alla controparte viene assegnato uno specifico livello di

[8] Nel conteggio sono stati considerati i dipendenti che hanno svolto almeno uno di questi corsi:
• Corso e-learning "La responsabilità degli enti ed. 2018" reso disponibile a partire da Luglio 2018.
• Due corsi di formazione esterna a cui hanno partecipato due dipendenti.

rischio di riciclaggio e viene demandata all'appropriato livello gerarchico la decisione di procedere o meno con l'apertura/prosecuzione del rapporto;

- nel settore NPL viene effettuata una prima verifica nel momento di acquisto del portafoglio crediti, e controlli successivi sulle singole controparti al momento della definizione dei piani di rientro.

Qualora venga attivato un rapporto su un cliente classificato a rischio alto sono previste revisioni più stringenti e frequenti della posizione, in termini di aggiornamento delle informazioni raccolte e di monitoraggio dell'operatività, ed un'escalation dell'Organo Deliberante competente.

Antiriciclaggio contribuisce alla definizione dei contenuti della formazione obbligatoria in materia di antiriciclaggio, in particolar modo per i dipendenti che hanno un contatto diretto con la clientela. Nel 2019 la formazione in merito all'antiriciclaggio è stata svolta attraverso corsi in aula ed il corso e-learning "La disciplina antiriciclaggio alla luce del recepimento della IV Direttiva ed. 2018" attivato sulla piattaforma IFIS Talent. Nel corso dell'anno è stato erogato un totale di 2.366 ore di formazione antiriciclaggio (circa 3.961 ore nel 2018) con il coinvolgimento del 38% della popolazione aziendale (62% nel 2018).

La formazione – oltre ad essere un obbligo normativo – è un importante strumento per aumentare la sensibilità e la cultura del personale sulla prevenzione del rischio di coinvolgimento inconsapevole della Banca in questo tipo di fenomeni.

Gestione delle segnalazioni (Whistleblowing)

Banca Ifis, in qualità di Capogruppo, in coerenza con le disposizioni regolamentari e le best practices del settore, ha definito un sistema interno volto a permettere la segnalazione di atti, fatti e omissioni che possono costituire una violazione delle leggi e delle procedure interne disciplinanti l'attività svolta dalla Capogruppo e dalle Controllate, garantendo al contempo la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione. Il sistema di segnalazione è disciplinato dalla Politica di Gruppo per la gestione delle segnalazioni delle violazioni (Whistleblowing), parte integrante del Modello Organizzativo di Banca Ifis e adottata dalle società del Gruppo. Possono effettuare una segnalazione i dipendenti del Gruppo Banca Ifis, i collaboratori e i liberi professionisti regolarmente iscritti ad un albo che prestano la loro opera in modo prevalente e continuativo per il Gruppo. La segnalazione può avere ad oggetto qualsiasi azione od omissione non conforme alle norme disciplinanti l'attività aziendale che arrechi o possa arrecare danno o pregiudizio al Gruppo Banca Ifis. Possono rientrare in questa casistica, ad esempio, azioni od omissioni, commesse o tentate, riconducibili ad atti o fatti penalmente rilevanti, che vìolino leggi e regolamenti, codici di comportamento come il Codice Etico o altre disposizioni aziendali sanzionabili in via disciplinare, suscettibili di arrecare un danno patrimoniale al Gruppo, un danno alla salute o sicurezza del personale o dei clienti o un danno all'ambiente.

Le segnalazioni possono essere effettuate attraverso diversi canali e sono gestite dal Responsabile dell'Internal Audit, che ne esamina il contenuto e attua le verifiche necessarie ad accertare la veridicità di quanto segnalato, nel pieno rispetto dei principi di imparzialità, riservatezza, dignità del dipendente e protezione dei dati personali.

Al termine degli accertamenti, il Responsabile dell'Internal Audit formalizza le proprie valutazioni e le trasmette all'Amministratore Delegato e al Direttore Generale (o al il Presidente del Collegio Sindacale in caso di situazioni di potenziale incompatibilità), che valuteranno le necessarie azioni correttive. Internal Audit redige una relazione annuale sul corretto funzionamento del processo, contenente anche informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, che viene approvata dal Consiglio di Amministrazione e messa a disposizione del personale.

Nel 2019, analogamente all'esercizio precedente, non si sono registrate segnalazioni tramite il sistema *Whistleblowing*.


POSSONO EFFETTUARE UNA SEGNALAZIONE
Dipendenti
Collaboratori
Liberi professionisti che collaborano in modo prevalente e continuativo con il Gruppo
LE SEGNALAZIONI POSSONO ESSERE EFFETTUATE ATTRAVERSO
Casella di posta elettronica dedicata
Via posta ordinaria e interna
Personalmente al Responsabile dell'Internal Audit
Apposito applicativo accessibile sia dal portale aziendale che dal sito
Il responsabile dell'Internal Audit esamina il contenuto ed attua le necessarie verifiche.
Al termine degli accertamenti, formalizza le proprie valutazioni e le trasmette a:
Amministratore Delegato
Direttore Generale
Presidente del Collegio Sindacale
RELAZIONE ANNUALE

3.2 Qualità del credito

Politiche e altra documentazione di riferimento

- Sistema delle deleghe di gruppo in materia di gestione del rischio di credito
- Politica di Gruppo per la gestione delle operazioni di maggior rilievo
- Politica di Gruppo per la valutazione delle attività aziendali
- Politica di gestione del credito ordinario (Banca Ifis)
- Politica di gestione dei portafogli di crediti acquistati a titolo definitivo e vantati verso gli enti della Pubblica Amministrazione (Banca Ifis)
- Politica di monitoraggio e recupero del credito ordinario (Banca Ifis, Credifarma)
- Politica di impairment
- Manuale metodologico: valutazione analitica del credito deteriorato (Banca Ifis)
- Procedura Organizzativa Gestione dei crediti erariali (Banca Ifis)
- NO 112 – BU Leasing - Processo di istruttoria Leasing (Banca Ifis)
- NO 111 – BU Leasing - Processo valutazione e settaggio Riscatti (Banca Ifis)
- NO 103 – BU Leasing - Valutazione qualità del credito soggettiva (Banca Ifis)
- Politica di monitoraggio e recupero del credito Leasing (Banca Ifis)
- Politica di gestione delle acquisizioni di portafogli di crediti distressed (IFIS NPL)
- Criteri di classificazione e gestione delle partite anomale (IFIS NPL)
- Procedura di Assegnazione delle pratiche NPL ai bacini di recupero (IFIS NPL)
- Procedura Organizzativa Recupero del credito attraverso azioni stragiudiziali (IFIS NPL)
- Procedura Organizzativa Recupero del credito attraverso azioni giudiziali (IFIS NPL)
- Procedura Organizzativa Gestione dei pagamenti associati al recupero dei crediti distressed (IFIS NPL)
- Procedura Organizzativa – Concessione e Gestione Finanza Strutturata
- Politica di gestione del credito ordinario (Cap.Ital.Fin.)
- Procedura Organizzativa Gestione della rete dei recuperatori stragiudiziali dei crediti distressed (Banca Ifis, IFIS NPL)
- Manuale Antiriciclaggio Cap.Ital.Fin.

La qualità del credito è strettamente connessa alla solidità patrimoniale, elemento chiave per la sostenibilità del modello di business del Gruppo ed una delle fondamenta della strategia del Gruppo Banca Ifis. Infatti, la qualità del credito e delle controparti può avere impatti significativi sul valore del titolo azionario, sul livello del rating creditizio della Banca, sul valore dei dividendi e sulla salvaguardia della solidità patrimoniale, rilevanti per azionisti, analisti finanziari, agenzie di rating, finanziatori e Autorità di Vigilanza, nonché sulla fiducia dei clienti nella capacità della Banca di fare fronte ai propri impegni, importante soprattutto per i risparmiatori retail delle business line Rendimax e Contomax.

Per il Credito Commerciale l'impegno aziendale alla tutela della solidità patrimoniale e alla qualità del credito si traduce in tre livelli di controllo sulle controparti, volti a prevenire sia i rischi di insolvenza sia il coinvolgimento in operazioni dai risvolti critici in termini reputazionali:

- controlli automatici sia sulle persone fisiche sia su quelle giuridiche, al fine di verificare la presenza del potenziale cliente nelle “watch list” (terrorismo, embarghi, ecc.) e nelle liste di “Persone Politicamente

Esposte", cui si aggiunge in relazione al livello di rischio un'analisi delle notizie di stampa effettuata dall'Antiriciclaggio;

- valutazione analitica, da parte dei team di Valutazione Operazioni e Valutazione Controparti, del cliente, dei clienti ceduti e del credito oggetto di cessione e sistema delle deleghe per l'assunzione del rischio di credito basato su importi e classi di rischio;
- continua interlocuzione con la rete territoriale, da cui possono provenire segnalazioni e riscontri sul potenziale cliente.

Per quanto concerne la cessione del quinto dello stipendio e/o pensione Banca Ifis, nel rispetto della privacy, considera anche la condizione del nucleo familiare nei casi in cui sia rilevante per valutare l'affidabilità del cliente.

Le politiche che regolano l'operatività del Leasing stabiliscono le verifiche sul futuro utilizzatore del bene rispetto a criteri di affidabilità e credibilità, attraverso un sistema di scoring e istruttorie svolte da team specializzati in cui vengono valutate, in particolare, la bontà della posizione creditizia della controparte e la congruità del bene richiesto con le sue attività.

Il controllo degli andamenti e il monitoraggio delle singole esposizioni vengono svolti con sistematicità, avvalendosi di procedure efficaci in grado di segnalare tempestivamente l'insorgere di anomalie e di assicurare l'adeguatezza delle rettifiche di valore e dei passaggi a perdita. La verifica del corretto svolgimento del monitoraggio andamentale sulle singole esposizioni, in particolare di quelle deteriorate, e la valutazione della coerenza delle classificazioni, della congruità degli accantonamenti e dell'adeguatezza del processo di recupero è svolta, a livello centrale e periferico, dal Risk Management.

Complessivamente, il Gross NPE ratio del Settore Imprese è invariato rispetto al 31 dicembre 2018 mentre il Net NPE Ratio è lievemente diminuito rispetto a fine 2018 (5,2% al 31 dicembre 2018).

GROSS E NET NPE RATIO	2019
Gross	9,5%
Net	5,1%

Per IFIS NPL, la cui specificità è l'acquisizione e la gestione di crediti deteriorati, la focalizzazione è sulla verifica della lavorabilità dei crediti e sul disegno di piani di rientro compatibili con la specifica situazione debitoria, attraverso diversi meccanismi lungo le fasi dell'acquisizione del credito:

- un primo controllo è volto a verificare che i crediti che si stanno acquisendo siano tutti lavorabili, al fine di escludere crediti inesistenti o prescritti e prevenire sia il rischio di inesigibilità sia il rischio reputazionale che si avrebbe nel richiedere crediti inesigibili. Una volta attivato il primo contatto con i clienti acquisiti, all'arrivo di eventuali reclami si verifica la fondatezza e, in caso di motivazioni fondate, si porta a perdita la posizione o se ne richiede la retrocessione/indennizzo alla società cedente se previsto contrattualmente;
- definizione di piani di rientro adeguati alle possibilità di spesa del cliente e contestualizzati rispetto a ogni singola pratica;
- valutazione del potenziale di rientro effettivo del cliente.

3.3 Data protection

Politiche e altra documentazione di riferimento

- Politica di Gruppo per la gestione della sicurezza informatica
- Politica di Gruppo per la valutazione e la gestione dei rischi informatici
- Procedura Organizzativa Gestione degli incidenti di sicurezza delle informazioni
- Procedura Organizzativa Gestione delle tematiche privacy attinenti ai diritti dell'interessato e al rapporto con il Garante
- Procedura Organizzativa Gestione dei Responsabili del trattamento dei dati personali
- Manuale metodologico per l'analisi del rischio dei trattamenti e la valutazione d'impatto sulla protezione dei dati (DPIA)
- Manuale regolamentare in materia di privacy
- Disciplinare tecnico per l'utilizzo delle dotazioni aziendali
- Politica di Gruppo per la gestione della continuità operativa
- Politica di gruppo per la pianificazione strategica in ambito ICT (Banca Ifis)
- Politica di gruppo per l'acquisizione di sistemi software e servizi IT (Banca Ifis)
- Politica monitoraggio performance ICT (Banca Ifis)
- Procedura Organizzativa per la gestione dei log (Banca Ifis)
- Procedura Organizzativa per la gestione degli accessi logici (Banca Ifis)
- Politica di gruppo Sistemi pagamento via internet (Banca Ifis)

La crescente diffusione di prodotti e servizi ICT basati sull'elaborazione di informazioni personali, ha accresciuto nel corso degli anni il ruolo strategico dei temi della privacy e della sicurezza informatica all'interno delle aziende.

Il Gruppo Banca Ifis considera la protezione dei dati personali un principio inderogabile, fondamentale per rafforzare la fiducia e il senso di sicurezza dei clienti e per tutelare la reputazione del Gruppo. Il Gruppo è inoltre impegnato nella prevenzione e gestione tempestiva di incidenti di sicurezza informatica a tutela del patrimonio informativo della Banca, che comprende, tra gli altri, i dati di clienti, dipendenti, fornitori e ogni altro soggetto con cui Banca Ifis intrattiene rapporti. Nel corso del 2019 il Gruppo ha ulteriormente consolidato i presidi richiesti dal Regolamento europeo in materia di protezione dei dati personali (General Data Protection Regulation, GDPR).

> L'area Privacy & Security ha consolidato il proprio ruolo di riferimento all'interno del Gruppo aziendale.
>
> La struttura conta dieci persone e si occupa di Privacy, Business Continuity e Cyber Security.

Laura Quaroni – Responsabile area Privacy & Security, DPO e BC Manager.

Sicurezza informatica

L'Unità Organizzativa Privacy & Security, attraverso l'Unità Organizzativa Information Security, presidia nel continuo la sicurezza informatica e partecipa alla valutazione del rischio informatico.

La sensibilizzazione dei dipendenti sulla cyber security

Per sensibilizzare tutti i colleghi sul tema della cyber security e delle novità normative ad esso correlate, nel corso del 2019 è stata lanciata una campagna di sensibilizzazione sui dipendenti del Gruppo attraverso la pubblicazione di news nella intranet aziendale finalizzate a far conoscere le informazioni inerenti campagne di email malevole relative alla diffusione di malware, phishing, tentativi di frode e ransomware. Sono stati attivati servizi di Cyber Intelligence e ricerche OSINT a supporto delle attività in capo alla struttura e a sostegno dell'awareness interno all'azienda. La Banca ha aderito al servizio CERTFin al fine di ricevere in tempo reale segnalazioni relative a tentativi di frode inerenti all'ambito bancario. Tali segnalazioni sono state condivise con i colleghi delle altre strutture della banca interessate.

Il processo di gestione degli incidenti di sicurezza informatica è volto a garantire che eventuali eventi anomali con possibili ripercussioni sul livello di sicurezza (fisica e logica) aziendale e sulla disponibilità dei Servizi IT siano tempestivamente riconosciuti come incidenti di sicurezza informatica e quindi correttamente gestiti dalle strutture competenti.

Le segnalazioni e gli eventi che possono determinare incidenti di sicurezza possono provenire da diversi canali interni (altre unità organizzative) ed esterni (clienti, fornitori e canali istituzionali). L'Unità Organizzativa Information Security gestisce tali segnalazioni in collaborazione con le eventuali altre parti coinvolte ed interessate, secondo l'entità e la tipologia dell'evento stesso.

Tutela dei dati personali

Il principale documento normativo interno in materia di protezione dei dati personali è rappresentato dal Manuale regolamentare in materia di privacy approvato dal Consiglio di Amministrazione di Banca Ifis in qualità di Capogruppo e recepito dalle controllate tramite Direttiva. Questo, insieme alle norme e procedure privacy, costituiscono il modello di gestione della privacy e l'insieme delle linee guida e delle regole che indicano come i dati personali sono protetti nel contesto aziendale.

La funzione **Privacy & Security**, in particolare attraverso l'unità dedicata alla Privacy:

- predispone e aggiorna la documentazione interna prevista dalla normativa in materia di privacy;
- monitora e controlla periodicamente l'osservanza della normativa e l'implementazione delle misure di sicurezza previste dalla legge;
- analizza le modalità di trattamento dei dati personali adottate dalla Banca e i rischi ad esse associati;
- valuta gli impatti in ambito privacy derivanti dal lancio di nuovi prodotti e servizi, dall'avvio di nuove attività, dall'ingresso in nuovi mercati e in tutti i casi in cui la Banca intenda realizzare internamente o acquistare un nuovo software;
- informa le unità organizzative della Banca, per gli ambiti di rispettiva competenza, in merito alle novità normative in tema privacy e fornisce supporto per garantirne l'adeguamento;
- supporta le Risorse Umane nello sviluppo di una adeguata cultura aziendale in ambito privacy.

Inoltre, nell'ambito della continuità operativa, attraverso l'Unità Organizzativa Business Continuity effettua l'analisi di impatto sui processi aziendali e ne redige il relativo piano.

[GRI 418-1]

Nel 2019, a livello di Gruppo, sono stati accolti 4 reclami relativi a violazioni della privacy a fronte dei 6 registrati nel 2018, legati per la quasi totalità ad errori operativi/umani che, in ogni caso, non hanno comportato la divulgazione di dati sensibili.

Nel corso dell'anno si sono verificati 10 eventi che hanno comportato la perdita, l'accesso o la divulgazione non autorizzata di dati personali (ad esempio furto di tablet o perdita di modulistica cartacea).

Reclami documentati su violazioni della privacy e perdita di dati dei clienti	**2019**	**2018**	**2017**
Numero totale di reclami documentati ricevuti in merito a violazioni della privacy dei clienti	**4**	**6**	**144[9]**
da terzi e documentati dall'organizzazione	4	6	144
da parte di organismi di regolamentazione	0	0	0
Numero totale di eventi relativi a perdite e furti documentati dei dati dei clienti	**10[10]**	**8**	**7**

[9] Nel 2017, a livello di Gruppo, sono stati accolti 144 reclami relativi a violazioni della privacy, legati per la quasi totalità ad un errore operativo commesso durante la predisposizione di un'indagine di mercato che, in ogni caso, non ha comportato la divulgazione di dati sensibili.

[10] Il dato rappresenta il numero di incident (non corrispondente al numero totale di dati esposti a perdite o furti). Per uno di questi incident si specifica che, nell'ambito delle attività di comunicazione periodica in materia di Trasparenza, a causa di un errore tecnico sono state inviate 60 raccomandate a soggetti che hanno prestato garanzie a favore della Banca contenenti dati di altri soggetti garanti e garantiti. A fronte delle analisi condotte, si è proceduto a notificare la violazione al Garante per la protezione dei dati personali. La Banca ha previsto misure atte a prevenire simili violazioni future come la revisione delle caratteristiche dei file contenenti i dettagli delle posizioni per permettere un maggior presidio ex ante del processo ed il rafforzamento dei controlli ex post effettuati sugli output della procedura informatica prima della postalizzazione delle comunicazioni.

3.4 Brand reputation

Politiche e altra documentazione di riferimento

- Investor Relations Policy
- Politica per la Gestione delle Informazioni Societarie
- Politica di Gruppo per la gestione dei rischi operativi e di reputazione

[GRI 102-15]

Il Gruppo Banca Ifis è cresciuto significativamente negli ultimi anni, anche a fronte del progressivo ampliamento delle aree di business presidiate e dell'articolazione dei brand offerti alla clientela, sia imprese che consumatori.

Pertanto, la brand reputation è diventata un fattore sempre più strategico al fine di garantire coerenza dei valori del Gruppo Banca Ifis nei confronti dei propri stakeholder.

Trasparenza e dialogo sono da sempre caratteristiche distintive nel processo di comunicazione delle informazioni relative alla Capogruppo e alle altre società. La Banca si interfaccia con clienti, investitori, azionisti, collaboratori riuscendo ad individuare esigenze diverse per mezzo, ad esempio, del customer care attraverso i social network, i siti web, progetti ed eventi. La Banca, inoltre cerca di indirizzare al meglio le proprie azioni, con l'obiettivo di offrire una miglior esperienza possibile ai propri interlocutori e di rispondere nel più breve tempo possibile a dubbi e richieste di informazioni. La brand reputation viene monitorata anche attraverso specifici tool dedicati.

Nello specifico, i rapporti con azionisti, investitori e analisti sono presidiati dalla funzione Investor Relations della Capogruppo e sono improntati a principi di correttezza, trasparenza, collaborazione e assoluto rispetto dell'indipendenza dei ruoli. L'attività di relazione e dialogo con il mercato finanziario rappresenta una componente strategica per il Gruppo: la Banca assicura la tempestività e la trasparenza delle comunicazioni al mercato e agisce in modo proattivo nei confronti dei propri stakeholder, illustrando e analizzando le informazioni di breve periodo, dando visibilità degli indirizzi strategici del Gruppo e sviluppando un rapporto di fiducia con gli operatori di mercato e la business community. Le modalità di relazione più significative con la comunità finanziaria sono: comunicati stampa, conference call con il mercato con cadenza trimestrale, incontri con gli investitori, comunicazione sul sito web ufficiale della Banca e nei social e diffusione del bilancio di Gruppo con modalità interattive per facilitarne la comprensione.

Il rischio di reputazione

Banca Ifis è impegnata nel monitoraggio e nella tutela della propria reputazione e delle società del Gruppo.

Al fine di valutare l'incidenza del rischio reputazionale, il Gruppo effettua un esercizio periodico di Risk Self Assessment prendendo in considerazione i fattori sia endogeni sia esogeni che potrebbero creare danni reputazionali al Gruppo ed agli stakeholder di volta in volta impattati.

Tra i principali fattori endogeni rientrano eventi di manifestazione del rischio operativo o di altri rischi non adeguatamente presidiati (es.: rischi di mercato, di liquidità, legali, strategici), violazione di leggi e regolamenti e norme di autoregolamentazione (come il Codice Etico), inefficace o errata gestione della comunicazione interna o esterna e comportamenti del management, dei dipendenti o dei collaboratori.

Fattori esogeni possono essere, invece, commenti e dibattiti che si sviluppano sui media, sui social network, sui blog o sugli altri strumenti di comunicazione digitale, riguardanti informazioni od opinioni lesive della reputazione del Gruppo o di singole società che lo compongono.

Gli stakeholder impattati dal rischio reputazionale possono essere diversi. Ad esempio:

- **Clienti**: possibile indebolimento della fiducia nella Banca nel Gruppo dovuta, ad esempio, ad inefficienze nelle prassi operative o a forzature commerciali;
- **Depositanti**: possibile indebolimento della fiducia nella Banca nel Gruppo con conseguente ritiro di parte dei depositi alla clientela;
- **Dipendenti e collaboratori**: perdita o diminuzione di fiducia / stima dei dipendenti e collaboratori nei confronti dell'azienda;
- **Azionisti e investitori**: perdita o diminuzione di fiducia / stima degli azionisti e dei mercati finanziari a causa di fattori quali, ad esempio, la presunta incapacità di raggiungere dei risultati soddisfacenti, comportamenti incoerenti rispetto a principi etici, percezione di non integrità manageriale, ecc.;
- **Territorialità e collettività**: perdite o diminuzione di fiducia / stima delle comunità territoriali e degli opinion maker;
- **Autorità di Vigilanza**: perdita o diminuzione di fiducia / stima delle Autorità di Vigilanza nei confronti dell'azienda a causa di omissioni o inadempienze derivanti dal mancato rispetto di obblighi previsti dalla legge o da disposizioni regolamentari;
- **Fornitori e controparti**: perdita o diminuzione di fiducia / stima dei fornitori e delle controparti.

Il Gruppo ha inoltre definito un set di indicatori in grado di evidenziare tempestivamente l'insorgenza di vulnerabilità nella esposizione della Banca e delle sue controllate ai rischi di reputazione e, ove necessario, relative soglie di attenzione ed allarme.

Attraverso un'attività di monitoraggio nel continuo, qualora vi siano risultati che superano le soglie predefinite, viene di volta in volta valutata la necessità di porre in essere eventuali azioni di mitigazione.