7.

L’etica e l'integrità aziendale

Dichiarazione Non Finanziaria Consolidata 2023

Ci impegniamo a sviluppare e a diffondere la cultura e i valori aziendali, all'interno come all'esterno, e a portare avanti, con integrità, la lotta alla corruzione.

7.1 Integrità aziendale e lotta alla corruzione

[GRI 2-23]
[GRI 3-3]

Politiche e altra documentazione di riferimento

- Codice Etico di Gruppo
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001[54]
- Politica di Gruppo per la gestione delle segnalazioni delle violazioni (Whistleblowing)
- Politica Antiriciclaggio di Gruppo
- Linee di Indirizzo di Gruppo sul sistema di Controlli Interni
- Politica in materia di sistema di controlli interni (Ifis Finance I.F.N. S.A.)
- Manuale Antiriciclaggio Cap.Ital.Fin.
- Manuale Antiriciclaggio Banca Credifarma parte normativa/procedurale
- Manuale operativo Embargo e antiterrorismo: Controlli sui bonifici in entrata ed uscita (Banca Ifis)
- Manuale Operativo Liste Negative Antiriciclaggio
- Politica di distribuzione (Cap.Ital.Fin.)
- Politica creditizia di Gruppo
- Politica ESG di Gruppo

Il **Codice Etico di Gruppo**, parte integrante del Modello Organizzativo e di Gestione previsto dal D. Lgs. 231/2001, delinea l'insieme di principi, valori, diritti, doveri e responsabilità assunti e adottati nei confronti di tutti gli stakeholder di Gruppo Banca Ifis, e rappresenta il **"manifesto" della cultura aziendale** di Banca Ifis e delle altre società del Gruppo. 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. La violazione del Codice Etico da parte dei destinatari costituisce violazione del rapporto contrattuale tra Banca Ifis e/o le Controllate e il destinatario, e può attribuire a Banca Ifis e/o le Controllate il diritto di intimare la risoluzione o il recesso dal contratto per giusta causa.

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

[54] Adottato da tutte le società del Gruppo Banca Ifis che hanno nominato un Organismo di Vigilanza.

meccanismi di attuazione e di riportare al Consiglio di Amministrazione sull'attività svolta e sulle problematiche connesse all'attuazione del Codice Etico.

Il Codice Etico chiarisce che **l'assunzione di impegni con la Pubblica Amministrazione e con le pubbliche istituzioni** è riservata alle unità organizzative del Gruppo preposte e autorizzate, le quali sono tenute ad assolvere ai propri compiti con integrità, indipendenza e correttezza. È vietato promettere od offrire a pubblici ufficiali o a dipendenti in genere della Pubblica Amministrazione o di pubbliche istituzioni (incluse le Autorità di Vigilanza), pagamenti o beni per promuovere o favorire gli interessi del Gruppo in sede di stipulazione di contratti ed erogazione di servizi, 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, i quali valuteranno l'adozione di eventuali ulteriori iniziative.

La prevenzione della corruzione

Per la prevenzione del rischio di commissione dei reati di corruzione e concussione, le Società del Gruppo che hanno nominato un Organismo di Vigilanza si sono dotate del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 (MOG), oltre che delle linee guida espresse nel Codice Etico di Gruppo.

Nel corso del 2023 il Modello di Organizzazione, Gestione e Controllo della Capogruppo è stato aggiornato al fine di adeguare le Parti Generale e Speciale alle novità normative esterne intervenute nel corso del 2023, ovvero al d.lgs 24/2023 che recepisce la Direttiva UE 1937/2019, recanti disposizioni in materia di *whistleblowing* e alla normativa interna di nuova emanazione o soggetta ad aggiornamenti. Tale aggiornamento normativo è stato recepito anche nei Modelli di Organizzazione, Gestione e Controllo delle società controllate.

I Modelli di Organizzazione, Gestione e Controllo sono aggiornati secondo quanto stabilito dalla normativa interna nella quale vengono disciplinati i ruoli e le responsabilità relativamente all'attività di aggiornamento dei MOG. Nello specifico, il Gruppo si è dotato di una nota operativa con cui vengono disciplinate le modalità di aggiornamento del modello a seconda che lo stesso sia interessato da modifiche normative esterne, interne oppure da violazioni. Il Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 della Capogruppo 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;
- Peculato, peculato mediante profitto dell'errore altrui;
- Traffico di influenze illecite;
- Abuso d'ufficio.

Il Modello di Organizzazione, Gestione e Controllo ex. D. Lgs. 231/2001 della Capogruppo 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 2-24]
[GRI 205-2]

Il Consiglio di Amministrazione, in sede di approvazione del Codice Etico del Gruppo e del Modello di Organizzazione, Gestione e Controllo, viene a conoscenza delle procedure anticorruzione adottate.[55] **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 al Codice Etico di Gruppo, Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001, protocolli e procedure in materia.

Il Gruppo assicura che tutti i dipendenti delle sedi italiane ricevano, ciclicamente e in caso di aggiornamenti nella normativa, adeguata formazione sulle politiche e le procedure anticorruzione di cui al Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/01. Nello specifico, a dicembre 2023 è stato pubblicato nel portale Ifis Talent un nuovo corso e-learning di formazione obbligatoria "**Il Codice Etico di Banca Ifis**", nel quale vengono dettagliati i principi di condotta nei rapporti con dipendenti, collaboratori e altre parti interessate, nonchè gli strumenti di attuazione e vigilanza del codice etico. Il corso prevede un test finale. Rimane inoltre disponibile il corso di formazione obbligatoria sulla "Prevenzione e governo del rischio di reato (D.LGS. 231/2001).

La tabella seguente riporta il dettaglio del numero di dipendenti che hanno svolto almeno un corso in materia di anticorruzione. La **formazione sui temi dell'anticorruzione** riguarda unicamente il personale presente sul suolo italiano e non il personale delle sedi estere.

Numero e percentuale di dipendenti che hanno ricevuto formazione sulla lotta alla corruzione, suddivisi per categoria di inquadramento		2023[56]	2022	2021
	N.	**824**[57]	**1.557**	**543**
	%	**43%**	**83%**	**29,4%**
Dirigenti	N.	29	49	14
	%	26,6%	51,6%	15,7%
Quadri	N.	224	465	131
	%	37,2%	82,0%	24,0%
Impiegati	N.	571	1.043	398
	%	46,7%	86,1%	32,8%

I **membri del Consiglio di Amministrazione della Capogruppo** a luglio 2023 hanno approvato l'aggiornamento del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 di Banca Ifis che contiene anche le prescrizioni afferenti alla prevenzione del rischio di commissione dei reati di corruzione e concussione.

[55] Gruppo Banca Ifis ad oggi non ha svolto moduli formativi specifici sui reati corruttivi rivolti ai Consiglieri di Amministrazione. I membri del CdA vengono a conoscenza dei presidi attuati sul tema in occasione dell'approvazione del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01 e del Codice Etico.

[56] Nel conteggio sono stati considerati i dipendenti che hanno svolto almeno una di queste attività: Corso e-learning "Prevenzione e governo del rischio di reato (D. Lgs. 231/2001)", corso e-learning "Il codice etico di Banca Ifis", corsi di formazione realizzati dalla funzione Compliance per i colleghi assunti con contratto di apprendistato ("Apprendistato II Anno – Compliance") e per colleghi di specifiche funzioni ("Prevenzione e governo del rischio di reato D.lgs 231/2001 e whistleblowing").

[57] Il dato si riferisce al personale dipendente di Gruppo in forza al 31/12/2023. Includendo nel calcolo anche il personale dipendente che ha lasciato l'organizzazione durante il periodo di rendicontazione che ha ricevuto la formazione in oggetto nel corso dell'anno 2023 (29, di cui 27 impiegati e 2 quadri), le numeriche sono: totale n. 853 (44,3%); impiegati n. 598 (48,9%); quadri n. 226 (37,5%); le numeriche relative ai Dirigenti rimangono invariate.

Tra i presidi adottati per **garantire l'integrità dei comportamenti delle reti esterne** vi è l'obbligo di osservanza del Codice Etico e del Modello di Organizzazione e Gestione ex. D. Lgs. 231/01 all'atto della sottoscrizione del contratto. Infine, per quanto riguarda gli stakeholder del Gruppo, il Codice Etico di Gruppo e la "Parte Generale" del Modello di Organizzazione, Gestione e Controllo ex. D. Lgs. 231/01 sono resi noti attraverso la pubblicazione sul sito web di Gruppo[58].

[GRI 205-3]

Anche nel corso del 2023, 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.**

[GRI 206-1]

A conferma di un sistema di gestione efficace, si riporta come anche nel corso dell'anno 2023, in linea con i precedenti esercizi, Gruppo Banca Ifis **non è stato oggetto di azioni legali** in materia di **comportamento anticoncorrenziale, violazione delle normative antitrust e relative pratiche monopolistiche nelle quali il Gruppo è stato identificato come partecipante**.

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 e del Gruppo alla collaborazione attiva nei confronti dell'Autorità di Vigilanza. Il Gruppo rifiuta di intrattenere relazioni, in modo diretto o indiretto, con persone e aziende sanzionate, o delle quali sia conosciuta o sospettata l'appartenenza a organizzazioni criminali o comunque operanti al di fuori della liceità. In tali situazioni, inoltre, le Società del Gruppo collaborano attivamente con le autorità di Vigilanza avviando senza ritardo le attività collegate al processo di segnalazione di operazione sospetta. Questo principio si traduce in **specifiche procedure e verifiche** nelle diverse aree di business, che hanno l'obiettivo di assegnare alla controparte un profilo di rischio in base al quale viene attivato un processo di approvazione a livelli diversi della gerarchia aziendale. In caso di determinazione di un profilo di rischio alto, si procede con la verifica rafforzata e l'autorizzazione dell'Alto dirigente[59].

Nello specifico:

- nel settore **Leasing** vengono esaminate le liste e 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 della funzione Anti-Money Laundering;
- nel **Credito Commerciale** e nei prodotti di conto, 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 rischio di riciclaggio e la decisione di procedere o meno con l'apertura/prosecuzione del rapporto viene demandata all'appropriato livello gerarchico;
- in **Cap.Ital.Fin.** viene effettuato uno screening per l'individuazione dei soggetti esposti politicamente o a rischio terrorismo. La società ha inoltre in uso delle liste per lo screening delle informazioni reputazionali negative, che sono valutate volta per volta sui soggetti positivi, e strumenti per la verifica dei documenti di identità;
- in Banca **Credifarma** vengono verificati i possibili soggetti esposti politicamente o a rischio di terrorismo tramite la procedura Fastcheck, integrata negli applicativi di profilatura della clientela;

[58] Per ulteriori approfondimenti, si veda il capitolo 7.5 Relazione con la catena di fornitura.

[59] Con "Alto Dirigente" si fa riferimento ad una figura introdotta dalla normativa antiriciclaggio identificabile in un amministratore, direttore generale, o altro dipendente delegato dall'organo con funzione di gestione o dal direttore generale, a seguire i rapporti con la clientela a rischio elevato. Questa figura ha una conoscenza idonea del livello di rischio di riciclaggio o finanziamento del terrorismo cui è esposto il destinatario ed è dotato di un livello di autonomia sufficiente ad assumere decisioni in grado di incidere su tale livello di rischio.

- nel settore Npl viene effettuata una prima verifica nel momento di acquisto del portafoglio crediti, successivamente sono svolti controlli sulle singole controparti al momento della definizione dei piani di rientro e degli accordi transattivi.

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 all'Alto Dirigente per la decisione sul mantenimento del rapporto in essere.

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 fenomeni simili.

[GRI 2-24]

La funzione Anti-Money Laundering 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. La formazione antiriciclaggio è svolta sia attraverso corsi in aula (in presenza e/o modalità virtuale) sia online tramite il corso e-learning "La disciplina antiriciclaggio ed. 2022" della durata di 4 ore, attivato sulla piattaforma Ifis Talent.

Più specificamente, riguardo la formazione in aula, nel corso dell'anno è stato erogato un totale di 48,5 ore di formazione antiriciclaggio a 552 dipendenti.

Per Banca Ifis sono state organizzate:

- quattro sessioni per la presentazione dello strumento AMALTEA SOS (Modulo Segnalazione Interna di Operazioni Sospette) rivolte ai Responsabili di Primo Livello della Segnalazione e agli utenti della segnalazione interna;
- due sessioni di Istruzioni operative per la corretta identificazione del Titolare Effettivo (per Valutazione Fidi, Valutazione Leasing, Corporate Finance);
- una sessione di formazione per la presentazione dello strumento AMALTEA MONRAL rivolta ai Responsabili delle U.O. e agli alti Dirigenti;
- ulteriori sessioni formative previste nel processo di *onboarding* rivolte ai nuovi dipendenti della Banca.

Per Banca Credifarma sono state organizzate le seguenti sessioni formative aventi ad oggetto:

- la presentazione dello strumento AMALTEA SOS (Modulo Segnalazione Interna di Operazioni Sospette) rivolta ai Responsabili di Primo Livello della Segnalazione e agli utenti della segnalazione interna;
- il processo di Transaction Monitoring rivolto ai Sales Manager;
- lo screening delle liste negative: linee guida e aspetti operative rivolta alla U.O. Operations;
- formazione mirata e specifica per nuova risorsa spostata all'interno della U.O. Operations: verifica liste, AMLET, *transaction monitoring*, AUI, *payment filtering*, flussi SARA, SOS;
- istruzioni operative per la corretta identificazione del Titolare Effettivo rivolta ai Sales Manager e ai Sales Support.

Per Ifis Npl Servicing è stata erogata una sessione formativa riguardante lo screening liste negative alla U.O. Incassi e pagamenti. Inoltre, nel corso del 2023 sono state effettuate sessioni formative per presentare lo strumento AMALTEA SOS (Modulo Segnalazione Interna di Operazioni Sospette) rivolte ai Responsabili di Primo Livello della Segnalazione e agli utenti della segnalazione interna per le società Capitalfin, Ifis NPL Servicing e Ifis NPL Investing. Per Capitalfin è stato inoltre erogato il corso di formazione in aula virtuale "Prevenzione e governo del rischio di reato D. Lgs n. 231/2001 e whistleblowing.

La funzione Anti-Money Laundering ha partecipato alle sessioni formative organizzate dalla funzione HR legate ai programmi di formazione Business Accelerator e Formazione ai membri del Consiglio di Amministrazione di Capogruppo. Parimenti, la funzione Anti-Money Laundering ha erogato della formazione generale in materia di antiriciclaggio ai nuovi agenti e recuperatori di Ifis Npl Investing e Capitalfin; oltre a specifiche sessioni formative di un'ora ciascuna in tema di "Titolare Effettivo e Segnalazione di Operazioni Sospette" a tutta la rete terza di Ifis Npl Servicing (agenti in attività finanziaria iscritti all'OAM, società di recupero del credito,

recuperatori ex art.115 TULPS). Lo stesso corso verrà erogato a gennaio 2024 alla rete di Banca Ifis (agenti in attività finanziaria iscritti all'OAM che collocano il prodotto leasing) e di Capitalfin (agenti in attività finanziaria iscritti all'OAM, mediatori creditizi).

Gestione delle segnalazioni (Whistleblowing)

[GRI 2-26]

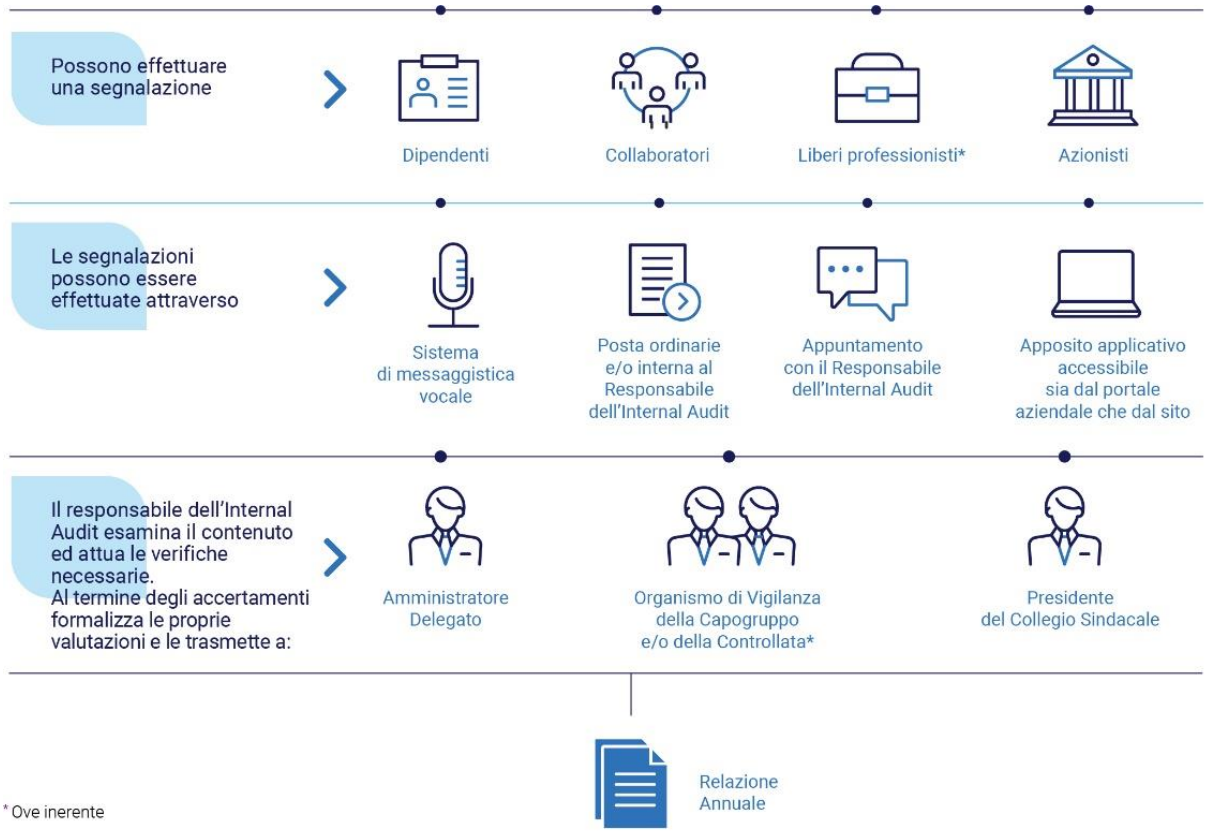
Banca Ifis, in qualità di Capogruppo, in coerenza con le disposizioni regolamentari, in particolare, da ultimo, con il d. lgs 24/2023 di attuazione della Direttiva UE 1937/2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali, e le best practice 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 dei Modelli Organizzativi delle Società del Gruppo Banca Ifis che ne sono dotate. Come più dettagliatamente indicato nella Politica in materia di gestione delle segnalazioni delle violazioni, possono fare una segnalazione i dipendenti di Gruppo Banca Ifis, i collaboratori e i liberi professionisti regolarmente iscritti ad un albo che prestano il loro operato 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 a Gruppo Banca Ifis. Possono rientrare in questa casistica, ad esempio, azioni od omissioni, commesse o tentate, che possano arrecare un danno patrimoniale al Gruppo, un danno alla salute o sicurezza del personale o dei clienti o un danno all'ambiente, oppure, come da ultimo introdotto con il d.lgs 24/2023, ledere gli interessi finanziari dell'Unione Europea.

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 della funzione Internal Audit formalizza le proprie valutazioni e le trasmette all'Amministratore Delegato (o al Presidente del Collegio Sindacale in caso di situazioni di potenziale incompatibilità), nonché, ove inerente, all'Organismo di Vigilanza della Capogruppo e, nel caso di segnalazione concernente una Controllata di diritto italiano, all'Organismo di Vigilanza della Controllata, che valuteranno le necessarie azioni correttive. La funzione 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 2023 non sono pervenute segnalazioni attraverso il sistema di segnalazione delle violazioni (Whistleblowing).



* Ove inerente

7.2 Sistema di controllo interno e di gestione dei rischi

[GRI 2-23]
[GRI 3-3]

Politiche e altra documentazione di riferimento

- Codice etico
- Modello di Gestione, Organizzazione e Controllo (ex. 231/2001)
- Politica di Gruppo per la gestione dei rischi ICT e di sicurezza
- Politica di Gruppo per del Risk Management per la gestione dei rischi creditizi
- Politica di Gruppo per la gestione dei rischi operativi e reputazionali
- Regolamento Risk Management di Gruppo
- Politica di Gruppo per del Risk Management per la gestione dei rischi di mercato
- Politica di Gruppo per del Risk Management per la gestione dei rischi di liquidità
- Politica di Gruppo del Risk Management per la gestione del rischio di tasso di interesse sul banking book
- Politica di gruppo per la gestione del rischio modello
- Politica Antiriciclaggio di Gruppo
- Politica di Gruppo per la gestione del Rischio di non conformità alle norme
- Politica di gestione del rischio di errata informativa finanziaria
- Politica di Gruppo per la gestione del rischio di non conformità alla normativa fiscale
- Politica di Risk Management per la gestione del rischio di controparte, di CVA e di regolamento
- Politica del Risk Management per la gestione dei rischi delle società controllate di diritto italiano facenti parte del gruppo bancario
- Politica di Gruppo per la gestione dei Conflitti di Interesse
- Regolamento Internal Audit Capogruppo

Il sistema di controllo interno e di gestione dei rischi

[GRI 2-24]

Il **sistema dei controlli interni** di Gruppo Banca Ifis è costituito dalle regole, dalle procedure e dalle strutture organizzative che mirano ad assicurare, tra gli altri, il rispetto delle strategie aziendali, l'efficacia ed efficienza dei processi e la conformità delle operazioni con la legge, la normativa di vigilanza, le politiche, le procedure e i codici di condotta adottati dal Gruppo. Le attività aziendali, laddove previsto, sono oggetto di **controlli da parte delle stesse funzioni o Aree di business**, *owner* dei diversi processi e attività (controlli di linea o di primo livello), di controlli da parte delle funzioni preposte di secondo livello (Risk Management, Compliance e Anti-Money Laundering) e di terzo livello (Internal Audit).

La funzione **Risk Management** identifica i rischi ai quali la Capogruppo e le società del Gruppo sono esposte e provvede alla misurazione e al monitoraggio periodico degli stessi attraverso specifici indicatori di rischio, pianificando le eventuali azioni di mitigazione per i rischi rilevanti[60]. L'obiettivo è garantire una visione unitaria e integrata dei rischi cui il Gruppo è esposto, assicurando un'adeguata informativa agli organi di governo. Le attività del Risk Management sono oggetto di periodica rendicontazione agli organi aziendali tramite il Tableau de Bord, e, ove previsto, anche a Banca d'Italia e a Consob.

La struttura complessiva di governo e gestione dei rischi a livello di Gruppo è disciplinata nel **Risk Appetite Framework** e nei documenti che ne discendono, tenuti costantemente aggiornati in base alle evoluzioni del quadro strategico del Gruppo stesso. Con riferimento alle evoluzioni societarie del Gruppo, si segnala che viene

[60] A fronte del 40^ aggiornamento della Circolare 285/2013 di Banca d'Italia il Gruppo Banca Ifis è si è dotato di una funzione di controllo di secondo livello responsabile della gestione e della supervisione dei rischi ICT e di sicurezza assegnando, come previsto dalla stessa Circolare, i compiti alle funzioni Compliance e Risk Management.

prontamente avviato un percorso di allineamento e integrazione delle metodologie di governo e gestione dei rischi, nel rispetto delle specificità dei singoli business.

In particolare, il Gruppo ha definito una Tassonomia dei Rischi all'interno della quale sono descritte le logiche seguite nell'identificazione dei rischi attuali e/o potenziali a cui il Gruppo potrebbe essere esposto nel conseguimento dei propri obiettivi strategici e, per ciascuna tipologia, gli strumenti di prevenzione e mitigazione previsti.

La Capogruppo effettua una prima identificazione dei rischi partendo dalla lista di rischi minimi identificati dalla normativa di vigilanza e ampliandola con ulteriori rischi significativi emersi dall'analisi del modello di business e dei mercati di riferimento in cui operano le diverse società del Gruppo, delle prospettive strategiche, delle modalità operative e delle caratteristiche degli impieghi e delle fonti di finanziamento.

L'individuazione dei rischi e l'aggiornamento periodico della Tassonomia dei Rischi sono frutto di un lavoro congiunto delle funzioni di Controllo di secondo livello (Risk Management, Compliance, Anti-Money Laundering) e di terzo livello (Internal Audit), che annualmente si riuniscono ed esaminano, sulla base dei risultati della gestione dei rischi dell'anno precedente, l'eventuale introduzione di nuovi eventi di rischio e/o una variazione nella valutazione dei rischi potenziali. L'Organismo di Vigilanza ha il compito di identificare e monitorare adeguatamente i rischi di cui al D. Lgs. 231/2001 assunti o assumibili rispetto ai reali processi aziendali, tenendo costantemente aggiornata la mappatura delle aree di rischio e dei "processi sensibili".

Il Comitato Controllo e Rischi, composto da membri del Consiglio di Amministrazione scelti tra gli Amministratori non esecutivi, la maggioranza dei quali indipendenti, ha il compito di supportare, con un'adeguata attività istruttoria, le valutazioni e le decisioni del Consiglio di Amministrazione relative al sistema di controllo interno e di gestione dei rischi.

In materia di gestione del rischio, viene favorito lo sviluppo e la diffusione a tutti i livelli di una cultura del rischio integrata in relazione alle diverse tipologie di rischio ed estesa a tutto il Gruppo. In particolare, vengono sviluppati e implementati programmi di formazione per sensibilizzare i dipendenti sulle proprie responsabilità di rischio in modo che il processo di gestione del rischio non sia limitato a specialisti o funzioni di controllo. La cultura del rischio viene propagata agli amministratori e ai sindaci attraverso apposite sessioni di formazione e induction. Anche nei confronti dei dipendenti vengono realizzati dei corsi di risk induction, tenuti periodicamente dalla funzione Risk Management.

Le attività di controllo effettuate dalla funzione Compliance (controlli continuativi e verifiche)[61], individuate sulla base della pianificazione approvata dal Consiglio di Amministrazione, mirano a verificare l'efficacia delle misure organizzative richieste, proposte e attuate ai fini della gestione del rischio di non conformità, pertanto, si applicano a tutti gli ambiti in cui sussiste tale rischio. Gli esiti dei controlli sono formalizzati in relazioni che vengono condivise con le strutture aziendali competenti, alle quali è richiesto di fornire riscontro sulle azioni di rimedio individuate e sulla tempistica di realizzazione. Tali adempimenti sono soggetti al monitoraggio della funzione e alla rendicontazione periodica agli organi aziendali tramite il Tableau de Bord e, ove previsto, anche a Banca d'Italia e a Consob.

Riguardo alle normative per cui sono già previsti presidi specializzati (sicurezza sul lavoro, trattamento dei dati personali, fiscale), i compiti della funzione Compliance possono essere graduati stabilendo, ad esempio, un coordinamento metodologico da parte dell'Unità Organizzativa, affinché questa possa fornire agli organi aziendali una visione complessiva dell'esposizione al rischio di non conformità. La funzione Compliance è comunque responsabile, in collaborazione con i presidi specialistici identificati, almeno della definizione delle metodologie di valutazione del rischio di non conformità, dell'individuazione delle relative procedure e della verifica della loro adeguatezza.

La funzione Compliance opera con due modalità di approccio:

[61] A fronte del 40^ aggiornamento della Circolare 285/2013 di Banca d'Italia il Gruppo Banca Ifis è si è dotato di una funzione di controllo di secondo livello responsabile della gestione e della supervisione dei rischi ICT e di sicurezza assegnando, come previsto dalla stessa Circolare, i compiti alle funzioni Compliance e Risk Management.

- ex ante: consulenza a supporto del business, sia pianificata a monte, su ambiti normativi identificati e aggiornati con approccio risk-based e in linea con il Piano Strategico del Gruppo, sia "a chiamata" per specifiche esigenze (e.g. nuovi prodotti o nuove attività);
- ex post: verifiche di conformità come previsto dal Piano di compliance annuale e controlli continuativi, i cui risultati vengono condivisi con le funzioni interessate, riportati al CdA nel Tableau de Bord e comunicati a Banca d'Italia.

FUNZIONE COMPLIANCE

Inoltre, ogni volta in cui venga dato avvio a un progetto rilevante (come acquisizioni, lancio di nuovi prodotti, avvio di nuove attività), la funzione Compliance partecipa attivamente fornendo indicazioni anche operative sulla gestione corretta del rischio di non conformità, ad esempio, in termini di presidi e controlli da istituire, normative di cui tenere conto, azioni di monitoraggio da attivare.

Per sviluppare una cultura diffusa basata sul principio di legalità, che coinvolga l'organizzazione a tutti i livelli, sono effettuati aggiornamenti e gestiti programmi di formazione per i dipendenti del Gruppo, al fine di assicurare l'acquisizione e lo sviluppo delle competenze necessarie per il rispetto di obblighi di legge, regole interne e normative di settore. I programmi di formazione sono stati messi a disposizione dei dipendenti del Gruppo anche per tutto l'esercizio 2023. La funzione Compliance informa le strutture interessate delle evoluzioni normative ritenute rilevanti al fine di dare avvio al processo di monitoraggio e di recepimento dei cambiamenti normativi, attua interventi formativi in autonomia o dà stimolo all'attivazione di eventi formativi più estesi con il coinvolgimento della funzione Human Resources.

La funzione Anti-Money Laundering effettua controlli sistematici di secondo livello in relazione al rischio di riciclaggio e di finanziamento del terrorismo, volti a verificare la corretta applicazione delle procedure ai processi operativi, produce Key Risk Indicator rappresentativi degli elementi di rischio più significativi da tenere monitorati ed effettua l'esercizio di autovalutazione dei rischi di riciclaggio e finanziamento del terrorismo con cadenza annuale. L'esito delle verifiche effettuate e il piano di azione sono condivisi con il Management di riferimento. Tali controlli e indicatori sono, inoltre, esposti trimestralmente nel Tableau de Bord e portati all'attenzione del Consiglio di Amministrazione e, ove previsto, anche a Banca d'Italia. La funzione Anti-Money Laundering monitora, inoltre, l'evoluzione normativa di competenza, dando informativa alle strutture impattate e attivandosi per i necessari adeguamenti compresi, se necessario, quelli ai processi e alla normativa interna. Al fine di garantire un'efficace applicazione della normativa antiriciclaggio, la funzione cura altresì la realizzazione di programmi di formazione del personale che garantiscano una piena consapevolezza delle finalità, dei principi degli obblighi e delle responsabilità aziendali in materia di contrasto al riciclaggio.

La funzione di revisione interna (Internal Audit) controlla, in un'ottica di controlli di terzo livello, il regolare andamento dell'operatività e l'evoluzione dei rischi aziendali e valuta la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle diverse componenti del Sistema dei Controlli Interni. L'attività di revisione condotta dalla funzione Internal Audit è trasversale a tutti i processi aziendali. Al fine di individuare eventuali andamenti anomali o violazioni della regolamentazione interna e di valutare la funzionalità del Sistema dei Controlli Interni nel suo complesso, alla funzione Internal Audit è attribuita, in particolare, la responsabilità delle verifiche sulla corretta applicazione delle disposizioni interne. In questo

specifico ambito, l'Internal Audit svolge verifiche annuali sulle attività di presidio dei rischi in capo alla funzione Risk Management del Gruppo.

La funzione Internal Audit opera sulla base della pianificazione approvata dal Consiglio di Amministrazione; a questa si aggiungono interventi non pianificati per specifiche necessità e/o richieste dei principali organi aziendali o di vigilanza esterni. Gli esiti degli audit sono condivisi con l'unità organizzativa di riferimento e con le funzioni di controllo di secondo livello, quindi inviati al Collegio Sindacale e al Comitato Controllo e Rischi. La funzione Internal Audit, inoltre, si relaziona periodicamente con gli organi aziendali anche tramite la presentazione di specifiche rendicontazioni di sintesi (Relazioni annuali e Tableau de Bord trimestrali) che, ove previsto, sono oggetto di trasmissione anche a Banca d'Italia o a Consob. Il ciclo di audit, come previsto dalla normativa di vigilanza, è triennale e prevede verifiche su tutti i principali processi aziendali.

Nel corso del 2023 la funzione Internal Audit ha pianificato e avviato, tra le altre, un'attività di verifica volta a garantire l'adeguatezza e conformità con le leggi e regolamenti sulla protezione e gestione dei dati personali della politica di Gruppo sulla privacy, in particolare per quanto concerne il Provvedimento del Garante n. 2 del 16/6/2004.

Il valore dell'etica: Il Codice Etico

[GRI 2-23]

Gruppo Banca Ifis aderisce alle finalità e alle indicazioni del Codice di Corporate Governance ed è dotata di un sistema di governance in linea con i principi contenuti nello stesso e con le raccomandazioni formulate da Consob in materia nonché, in generale, con le best practice, il cui obiettivo è garantire adeguate ripartizioni di responsabilità e poteri attraverso un corretto equilibrio tra funzioni di gestione e di controllo.

In ottemperanza alle disposizioni del Decreto Legislativo 231/2001 in materia di "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" Gruppo Banca Ifis rende disponibili il Codice Etico e il regolamento dell'Organismo di Vigilanza.

Il Codice Etico di Gruppo delinea l'insieme di principi, valori, diritti, doveri e responsabilità assunti e adottati nei confronti di tutti i portatori d'interesse con i quali le società del Gruppo entrano in relazione al fine di assicurare il perseguimento del proprio oggetto sociale.

Il Codice Etico fornisce un insieme di norme comportamentali fondate sui principi di correttezza, lealtà e coerenza, volte al rafforzamento, nel continuo, degli standard etico-comportamentali dei suoi destinatari e alla creazione di una cultura comune all'interno del Gruppo. Inoltre, rappresenta uno strumento in costante aggiornamento, fondamentale per preservare la reputazione fondata sulla fiducia e sull'affidabilità delle persone, garantire una creazione di valore sostenibile nel tempo e, quando necessario, riconoscere i nuovi principi che l'evoluzione socio-culturale impone di considerare. I valori in esso contenuti guidano le scelte e le iniziative adottate dal Gruppo, la definizione dei processi interni e le condotte dei soggetti che in esso operano.

Il Codice Etico di Gruppo ad oggi in vigore è stato approvato il 22 dicembre 2016 ed **è stato oggetto di costante aggiornamento, da ultimo in data13 luglio 2023**. Nello specifico, la revisione ha avuto come obiettivo l'aggiornamento del documento a fronte dell'adeguamento della normativa interna e dei canali di segnalazione (*whistleblowing*) a recepimento, con il d. lgs 24/2023, della Direttiva UE 1937/2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Le modifiche apportate al Codice Etico riguardano **l'elenco dei possibili canali di segnalazione interna**, con l'introduzione del sistema di messaggistica vocale, e la descrizione dei nuovi canali di segnalazione esterna (ANAC e Divulgazione pubblica).

Con particolare riferimento ai **fattori ESG**, Gruppo Banca Ifis intende diffondere e consolidare una cultura di rispetto dell'ambiente e della correttezza sociale, promuovendo comportamenti responsabili, dando adeguata informazione e formazione e chiedendo di segnalare tempestivamente le eventuali carenze o il mancato rispetto delle norme applicabili. Gruppo Banca Ifis ha quindi identificato nel Codice Etico uno strumento utile

alla diffusione di tali principi, in quanto chiede ai destinatari di considerare le conseguenze ambientali e sociali di ogni comportamento adottato durante la propria attività lavorativa, favorendo azioni responsabili[62].

In linea con i principi previsti dal Codice Etico, tutte le persone del Gruppo devono mantenere un comportamento eticamente corretto nei rapporti con dipendenti e collaboratori, clienti, debitori, fornitori, Pubblica Amministrazione, azionisti e con la comunità finanziaria. Non sono accettabili comportamenti illegali o eticamente scorretti, anche con riferimento a disposizioni di legge, codici e regolamenti adottati dal Gruppo.

Il Modello Organizzativo di Gestione

[GRI 2-24]

Gruppo Banca Ifis, con la volontà di assicurare condizioni di trasparenza e correttezza nella conduzione dell'attività aziendale, a tutela del proprio ruolo istituzionale e della propria immagine, delle aspettative degli azionisti e di coloro che lavorano per e con il Gruppo, ha scelto di adottare un Modello Organizzativo e di Gestione (MOG o Modello) in linea con quanto previsto dal D. Lgs. 231/2001.

Si tratta di un complesso organico di principi, regole, disposizioni, schemi organizzativi e relativi compiti e responsabilità funzionale alla realizzazione e alla gestione diligente di un sistema di controllo e monitoraggio delle attività sensibili al fine di prevenire la commissione dei reati previsti dal D. Lgs. 231/2001. Il Modello – adottato nel 2004 e mantenuto costantemente allineato alle novità normative – si inserisce nel più ampio sistema di controllo costituito principalmente da Sistemi dei Controlli Interni e dalle regole di Corporate Governance di Banca Ifis. Analoga impostazione è applicata dalle società del Gruppo.

Banca Ifis, ritenendo inoltre che il Modello costituisca parte fondamentale degli strumenti di politica aziendale di Gruppo, estende gli strumenti organizzativi presenti al suo interno alle società controllate, per quanto applicabili. A tal fine è prevista una funzione di supporto metodologico, nella Direzione General Counsel della Capogruppo, per le attività di tutti gli Organismi di Vigilanza del Gruppo con il compito di redigere e mantenere, previa validazione da parte della funzione di Compliance e con il supporto di eventuali altre funzioni coinvolte, il Regolamento dell'Organismo di Vigilanza. Inoltre, provvede a redigere ed aggiornare, con il supporto della funzione Compliance, la Parte Generale dei Modelli Organizzativi, mentre con riferimento alla Parte Speciale dei Modelli Organizzativi, coordina la funzione Organizzazione affinché apporti gli opportuni aggiornamenti di competenza.

Il Modello ricomprende, tra le fattispecie di illecito previste, anche tipologie di reato strettamente connesse a temi non finanziari, come reati societari (corruzione attiva e passiva), reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, reati ambientali e reati connessi alla tratta e allo sfruttamento di persone e all'impiego di cittadini stranieri il cui soggiorno è irregolare, nonché reati tributari, reati contro il patrimonio culturale e delitti in materia di mezzi di pagamento diversi dai contanti.

A fronte dell'aggiornamento della normativa esterna in materia di *whistleblowing* intervenuto nel corso del 2023, il Modello di Capogruppo e i Modelli delle Società controllate, sono stati oggetto di revisione, da ultimo a luglio 2023. In particolare, le modifiche effettuate, come previsto dagli iter deliberativi interni, sono state sottoposte ai rispettivi Organismi di Vigilanza e Consigli di Amministrazione, per verifica e successiva approvazione. La revisione risponde all'esigenza di tutela della Banca e del Gruppo, attraverso il recepimento delle novità normative e organizzative intervenute, innanzitutto attraverso l'informazione dei fruitori – cioè i dipendenti, dirigenti e collaboratori del Gruppo chiamati a conformare la loro attività a quanto in Modello – e, secondariamente, dei suoi lettori eventuali – cioè gli Inquirenti chiamati a valutarne effettività e adeguatezza.

Il compito di vigilare sul funzionamento e l'osservanza dei Modelli Organizzativi è affidato all'Organismo di Vigilanza della Capogruppo e agli Organismi di Vigilanza delle Controllate ove presenti, dotati di autonomi poteri di iniziativa e controllo. Una funzione fondamentale di coordinamento e integrazione, nonché di garanzia del mantenimento dei necessari flussi informativi da parte degli Organismi di Vigilanza delle società del Gruppo, è

[62] All'atto della formalizzazione di contratti o accordi con i fornitori il Codice potrà, secondo le indicazioni della normativa interna, essere espressamente richiamato quale documento vincolante, la cui violazione ha conseguenze anche di natura contrattuale.

attualmente svolta dal Responsabile della funzione Internal Audit e dal Responsabile della funzione Compliance di Gruppo Banca Ifis, componenti di tutti gli Organismi di Vigilanza.

Principali rischi legati ai temi non finanziari

Il Gruppo, nel corso degli anni e in linea con le richieste dell'art. 3 del D. Lgs. 254/2016, ha attivato processi e definito specifiche responsabilità per identificare e gestire i principali rischi connessi ai temi ESG. Di seguito viene presentato, per ciascun tema materiale, la natura dei rischi ad essi connessi e i principali rischi e le relative modalità di gestione attualmente realizzate. Nei successivi paragrafi vengono riportati degli approfondimenti specifici in riferimento ad alcuni temi e rischi riportati nella tabella sottostante.

Per ciascun tema materiale Gruppo Banca Ifis ha identificato la natura dei rischi ad essi connessi e le relative modalità di gestione attualmente realizzate, di cui si fornisce una sintesi nella tabella seguente.

Temi materiali	Natura dei rischi	Principali rischi	Principali presidi/azioni di mitigazione
Impegno per la comunità	Reputazionali	• Effetti reputazionali derivanti da eventi negativi con impatto sociale che riguardano i destinatari delle donazioni/ partner delle iniziative effettuate dal Gruppo	• Codice Etico • Presidio organizzativo accentrato per la gestione delle iniziative • Comitato Sostenibilità
Diversità, inclusione e benessere dei dipendenti	Reputazionali; Conformità / Operativi	• Richieste di risarcimento per eventuali forme di discriminazione motivate da identità di genere, disabilità, età, religione, nazionalità, razza, convinzioni personali, ecc. • Danni reputazionali e di immagine • Molestie e mobbing • Divario salariale o retributivo di genere parità di impiego e competenze • Difficoltà all'accesso a posizioni apicali e/o a processi di crescita professionale per il genere meno rappresentato • Infortunio di dipendente sul luogo di lavoro • Malattie professionali • Danni imputabili all'insufficiente sicurezza e/o salubrità di luoghi e strumenti di lavoro • Instabilità occupazionale (e.g. dei giovani dipendenti) a causa del ricorso a contratti a tempo determinato e/o di somministrazione	• Codice etico • Whistleblowing • Politiche in materia di remunerazione e di incentivazione • Politica di Gruppo per la gestione del personale dipendente • Politica per la promozione della diversità e dell'inclusività • Manuale regolamentare di gestione della parità di genere • Piano strategico per la parità di genere • Certificazione Uni PdR: 125 2022 "in miglioramento continuo" • Mantenimento della certificazione WWI (Winning Women Institute) • Controlli di secondo livello Operational Risk sul contenzioso in materia HR • Manuale integrato Sicurezza e Ambiente • Iniziative di formazione sulle pratiche e procedure in materia di salute e sicurezza • Documento di Valutazione dei Rischi (DVR) • Documento Unico di Valutazione dei rischi interferenziale (DUVRI) • Previsione del CCNL che determina i limiti di assunzione con contratti a termine/somministrazione e significativa conversione dei contratti a termine in contratti a tempo indeterminato • Controlli di secondo livello Operational Risk sul contenzioso in materia HR
Valorizzazione e sviluppo dei dipendenti	Reputazionali	• Contenziosi passivi legati alla gestione del rapporto di impiego o alla selezione del personale, relativamente allo svolgimento del rapporto di lavoro in tutte le sue articolazioni. A titolo esemplificativo ma non esaustivo: dagli aspetti retributivi ai livelli di inquadramento, allo sviluppo di carriera, alla formazione, ecc.	• Politica di Gruppo per la gestione del personale dipendente • Sistema di welfare aziendale • Politiche in materia di remunerazione e incentivazione • Ifis Academy • Supporto da legali esterni • Sistema di valutazione della performance • Controlli di secondo livello Operational Risk sul contenzioso in materia HR

Temi materiali	Natura dei rischi	Principali rischi	Principali presidi/azioni di mitigazione
Social Banking	Reputazionali; Conformità / Operativi; Credito	• Inadempienze ed errori nella gestione dell'operatività legata alle iniziative di inclusione finanziaria con conseguenti effetti reputazionali o in termini di rischio di credito	• Politica per la gestione del credito e procedure per la gestione della finanza agevolata • Iniziative di info/formazione territoriali
Transizione sostenibile delle imprese	Reputazionali; Conformità / Operativi; Credito	• Inadempienze ed errori nella gestione dell'operatività legata alle iniziative di inclusione finanziaria con conseguenti effetti reputazionali o in termini di rischio di credito	• Politica per la gestione del credito e procedure per la gestione della finanza agevolata • Iniziative di info/formazione territoriali
Innovazione digitale	Reputazionali Operativi ICT e di Sicurezza	• Rischio di perdita dovuta alla violazione della riservatezza, la carente integrità dei sistemi e dei dati, l'inadeguatezza o l'indisponibilità dei sistemi e dei dati o l'incapacità di sostituire la tecnologia dell'informazione (IT) entro ragionevoli limiti di tempo e costi nel caso di modifica dei requisiti del contesto esterno o dell'attività (ossia l'agilità) • Insoddisfazione della clientela con potenziali contestazioni o perdita della clientela stessa • Malfunzionamento o indisponibilità delle nuove tecnologie	• Politica per la pianificazione strategica ICT • Procedura di gestione degli Incidenti IT • Politica di gestione Change Management • Politica per la gestione progetti • Politica per il Monitoraggio e la misurazione delle performance • Procedura per il monitoraggio continuativo delle minacce e delle vulnerabilità di sicurezza • Politica di Gruppo per la Gestione del Rischio ICT e di Sicurezza
Finanziamenti e lotta al cambiamento climatico	Reputazionali; Credito	• Effetti reputazionali derivanti da eventi negativi che riguardano l'azienda (operante in settori ad alto impatto ambientale e/o sociale) finanziata dal Gruppo • Insolvenza o peggioramento del merito creditizio delle controparti verso cui il Gruppo è esposto	• Leasing: settori di attività esclusi • Identificazione di settori maggiormente a rischio reputazionale nell'ambito della politica delle OMR (Operazioni a Maggior Rilievo) • Comitato Sostenibilità
Impatti ambientali diretti	Reputazionali; Conformità / Operativi	• Danni ambientali provocati dal mancato rispetto delle norme in materia di gestione ambientale o dall'adozione di prassi ed operatività non appropriate • Percezione negativa dell'immagine e della reputazione del Gruppo derivante dagli eventi negativi sopra riportati • Rischi Climatici e Ambientali • Danni ad asset di proprietà di Gruppo Banca Ifis a seguito di eventi esterni (e.g.: terremoti, frane, inondazioni) che possono causare l'interruzione dell'operatività • Lamentele e contestazioni • Mancata riduzione dei target in termini di emissioni finanziate	• Manuale integrato Sicurezza e Ambiente • Politica del Gruppo in materia ambientale • La banca incorpora i rischi Climatici e Ambientali nelle proprie strategie aziendali, nella governance e nei framework RM, al fine di mitigare tali rischi e rispettare i requisiti normativi
Integrità aziendale	Reputazionali; Conformità / Operativi	• Frode interna, riconducibile ai dipendenti del Gruppo e agli Agenti che collaborano col Gruppo • Pratiche di recupero aggressive e/o comportamento anomalo da parte dei recuperatori esterni e degli agenti • Frode esterna, riconducibile alle Società di Recupero e/o agli Agenti in attività finanziaria • Coinvolgimento, anche inconsapevole, del Gruppo in attività di riciclaggio e di finanziamento del terrorismo	• Codice Etico • Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 • Politica di Gruppo per la gestione delle segnalazioni delle violazioni (Whistleblowing) • Presidi ad hoc rivolti agli agenti del Gruppo • Controlli sistematici in materia di riciclaggio e finanziamento al terrorismo • Formazione dei dipendenti • Controlli di secondo livello Operational Risk su prassi di business anomale da parte delle Reti Esterne di Recupero

Temi materiali	Natura dei rischi	Principali rischi	Principali presidi/azioni di mitigazione
Data protection	Reputazionali; Conformità / Operativi ICT e di Sicurezza	• Perdita o utilizzo inappropriato di dati del Gruppo derivanti da minacce interne o esterne che coinvolgono personale o sistemi informativi • Attacchi informatici mediante campagne di Phishing	• Presidio organizzativo accentrato per la gestione della Privacy e della Security del Gruppo • Misure tecniche e organizzative per la sicurezza delle informazioni • Misure tecniche e organizzative per la continuità operative • Procedure per la gestione degli incidenti informatici e IT • Procedure per la gestione degli incidenti informatici e di sicurezza • Politica di Gruppo per la Gestione del Rischio ICT e di Sicurezza • Campagne di Phishing Simulation • Piani di formazione volti al consolidamento di un'adeguata sensibilizzazione e di una cultura aziendale basata sulla sicurezza informatica
Trasparenza	Reputazionali; Conformità	• Aumento dell'insoddisfazione della clientela con conseguente turnover negativo • Riduzione della percezione di affidabilità e sicurezza nei confronti del Gruppo e dei servizi offerti • Rischi operativi e conseguenti effetti reputazionali in ambito trasparenza, idoneità, informativa e rapporto fiduciario con la clientela	• Processo per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività, l'inserimento in nuovi mercati • Comitato prodotti • Ricerca continua nell'efficientamento dei processi operativi al fine di ridurre i tempi di risposta alla clientela • Presidio organizzativo accentrato di gestione della comunicazione con la clientela • Meccanismi per la gestione di reclami • Procedura Organizzativa Trasparenza delle Operazioni e dei Servizi Bancari e Finanziari
Catena di fornitura	Reputazionali; Conformità /Operativi; Legali; ESG; di concentrazione; di sub-esternalizzazione	• Riduzione della qualità o interruzione dei servizi resi • Violazione di norme cogenti e conseguente sanzionamento • Perdita di quote di mercato • Rischi reputazionali derivanti dagli eventi di cui sopra (e.g. sanzioni rese pubbliche, incapacità di offrire i servizi contrattualizzati) • Perdite economiche (o necessità di accantonare somme di denaro) legate ai contenziosi di varia natura (e.g. contenziosi con clienti/fornitori)	• Definizione di una sourcing strategy aziendale • Analisi dei profili amministrativi, organizzativi, patrimoniali e reputazionali del fornitore • Analisi dei profili ICT e di sicurezza dei dati • Definizione di appositi standard contrattuali al fine di mitigare i rischi individuati (e.g. divieti di sub - esternalizzazione a determinate condizioni) • Analisi nel continuo dei livelli dei servizi erogati dal fornitore, alla luce di quanto garantito nel contratto • Definizione di exit strategy nel caso si rendesse necessario interrompere il rapporto con il fornitore • Controlli di secondo livello Operational Risk sulle funzioni esternalizzate, sulle terze parti ICT, sui fornitori con contratti superiori a 500K • Politica per l'esternalizzazione di funzioni aziendali • Politica di Gruppo per la gestione del ciclo passivo

7.3 Data protection

[GRI 2-23]
[GRI 3-3]

Politiche e altra documentazione di riferimento

- Politica di Gruppo per la gestione della sicurezza informatica
- Politica di Gruppo per la gestione dei rischi ICT e di sicurezza
- Procedura Organizzativa Gestione degli incidenti IT
- 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 (Gruppo Banca Ifis)
- 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
- Regolamento di Gruppo per l'utilizzo delle dotazioni aziendali
- Procedura Organizzativa per la Gestione Operativa dei sistemi e il controllo delle operazioni critiche
- Politica di Gruppo per la gestione della continuità operativa
- Politica di gruppo per la pianificazione strategica in ambito ICT (Gruppo Banca Ifis)
- Politica di gruppo per il monitoraggio e la misurazione delle performance (Gruppo Banca Ifis)
- Procedura Organizzativa per la gestione degli accessi logici
- Procedura Organizzativa per la gestione della Sicurezza Fisica delle risorse informative
- Politica di gruppo per la gestione e la sicurezza dei servizi di pagamento (Banca Ifis, Banca Credifarma)
- Procedura Organizzativa per il monitoraggio delle minacce e delle vulnerabilità di sicurezza
- Procedura Organizzativa per la Gestione dei log di Sicurezza delle informazioni
- Procedura Operativa Dismissione Dispositivi Elettronici (Gruppo Banca Ifis)
- Procedura Organizzativa Gestione dell'hardening e del patch management (Gruppo Banca Ifis)
- Politica classificazione e gestione delle informazioni (Gruppo Banca Ifis)
- Politica ESG di Gruppo

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.

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** del Gruppo, che comprende, tra gli altri, i dati di clienti, dipendenti, fornitori e ogni altro soggetto con cui il Gruppo intrattiene rapporti. Nel corso del 2023, Gruppo Banca Ifis ha condotto un'ampia e approfondita **revisione del compendio regolamentare interno** in materia di protezione dei dati personali e si è dotato di un ***tool*** **informatico** finalizzato alla gestione automatizzata dei principali adempimenti in tema di privacy.

Sicurezza informatica

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

Il **processo di gestione degli incidenti di sicurezza delle informazioni** è volto a garantire che eventuali eventi anomali con possibili ripercussioni sul livello di sicurezza aziendale (fisica e logica) e sulla disponibilità dei

Servizi IT siano tempestivamente riconosciuti come incidenti di sicurezza delle informazioni 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 Governance 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. Il Manuale e le norme e procedure per la 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 la funzione Human Resources** nello sviluppo di un'adeguata cultura aziendale in ambito privacy e svolge periodiche sessioni formative destinate al personale (dipendente e non).

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 2023, a livello di Gruppo, sono stati **registrati 2 reclami** presentati all'Autorità Garante per la protezione dei dati personali da parte di clienti, relativi ad asserite violazioni della privacy: in entrambi i casi, alla luce delle difese fornite in sede di riscontro, l'Autorità ha concluso le istruttorie disponendo l'archiviazione dei reclami.

Reclami documentati su violazioni della privacy e perdita di dati dei clienti		2023	2022	2021
Numero totale di reclami documentati ricevuti in merito a violazioni della privacy dei clienti	N.	2	4	4
da terzi e documentati dall'organizzazione	N.	2	4	4
da parte di organismi di regolamentazione	N.	0	0	0
Numero totale di eventi relativi a perdite e furti documentati dei dati dei clienti	N.	47[63]	57	46

Gli incidenti che hanno comportato la perdita, l'accesso o la divulgazione non autorizzata di dati personali nel 2023 riguardano soprattutto la perdita o il furto di dispositivi aziendali, l'errato invio di documentazione via posta ordinaria o via e-mail, lo smarrimento o il furto di documentazione cartacea. **Nessun incidente ha dato corso ad alcuna comunicazione verso l'Autorità Garante o verso gli interessati**.

[63] Il dato rappresenta il numero totale di incidenti occorsi nel 2023 che hanno comportato la perdita, l'accesso o la divulgazione non autorizzata di dati personali. Gli eventi sono suddivisibili tra le società del Gruppo come segue: 14 incidenti per Banca Ifis, 21 incidenti per Ifis Npl Servicing, 8 incidenti per Ifis Npl Investing, 2 incidente per Cap.Ital.Fin., 2 incidente per Banca Credifarma.

Al fine di mitigare l'esposizione a tali rischi, Gruppo Banca Ifis, nel corso del 2023, ha avviato delle campagne di sensibilizzazione interna sul tema della cybersecurity per sviluppare una maggiore attenzione circa l'identificazione e la segnalazione di incidenti riguardanti i dati personali.

La sensibilizzazione dei dipendenti e il programma sulla cybersecurity

Il Gruppo Banca Ifis, nel corso del 2023, ha dato corso a diverse campagne di sensibilizzazione sul tema della **cybersecurity** rivolte a tutti i dipendenti.

In continuità con il periodo di riferimento precedente, si è dato seguito ad alcune **campagne di *awareness*** sui dipendenti del Gruppo attraverso l'organizzazione di *webinar* e di sessioni formative in aula che hanno visto la partecipazione di autorevoli *speaker* nell'ambito della cybersecurity, oltre alla consueta newsletter mensile **"Flash Cyber News"**, per promuovere tra i dipendenti la conoscenza e la consapevolezza sulle più recenti minacce informatiche e azioni di *cyber crime*, fornendo informazioni aggiornate in materia di protezione cyber e utili suggerimenti per contrastarle.

È stata data continuità ai servizi di Cyber Intelligence e ricerche OSINT a supporto delle attività in capo alla struttura e a sostegno dell'*awareness* interna al Gruppo. Il Gruppo ha confermato l'adesione 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 interessate della Banca.

Infine, nel corso del 2023 sono state effettuate molteplici **campagne di simulazione di *phishing*** volte alla sensibilizzazione dei dipendenti sul tema della sicurezza informatica.

Le campagne in parola rientrano nell'ambito di un più ampio **programma di iniziative avviato dalla Banca al fine di aumentare il livello di compliance normativo e la *cyber security posture* necessaria al raggiungimento degli obiettivi di evoluzione digitale prefissati.**

7.4 Trasparenza

[GRI 2-23]
[GRI 3-3]

Politiche e altra documentazione di riferimento

- Codice Etico di Gruppo
- Politica di Gruppo per la gestione delle Contestazioni stragiudiziali della clientela
- Procedura Organizzativa Comunicazioni di Marketing alla Clientela (Banca Ifis)
- Procedura Organizzativa Gestione delle contestazioni indirizzate a Gruppo Banca Ifis
- Procedura Organizzativa Trasparenza delle Operazioni e dei Servizi Bancari e Finanziari (Banca Ifis)
- Procedura Organizzativa Trasparenza delle Operazioni e dei Servizi Bancari e Finanziari (Cap.Ital.Fin.)
- Procedura Organizzativa Trasparenza delle Operazioni e dei Servizi Bancari e Finanziari (Banca Credifarma)
- Procedura Organizzativa Gestione massiva delle condizioni economiche e contrattuali dei prodotti ex artt. 118 e 126-sexies tub (Banca Ifis, Banca Credifarma)
- Politica di Gruppo per la Gestione dei Rischi Operativi e di Reputazione
- Politica ESG di Gruppo

La trasparenza delle informazioni su prodotti e servizi

La **trasparenza nei confronti dei clienti** ha impatto sul senso di fiducia con il quale questi si affidano al Gruppo e rappresenta la base di un rapporto sano e duraturo e quindi **un asset da proteggere e far crescere**. Essa riguarda sia l'aspetto delle comunicazioni a vario titolo consegnate da parte della rete fisica, sia gli aspetti specifici della contrattualistica all'interno delle diverse linee di business.

Il Gruppo instaura relazioni dirette con la propria clientela e opera ispirandosi a **principi di professionalità, onestà e trasparenza,** fornendo informazioni circostanziate sugli impegni reciprocamente assunti e sugli eventuali rischi impliciti nella natura delle operazioni poste in essere.

Tutti i rapporti contrattuali, le comunicazioni e i documenti sono redatti in maniera chiara e comprensibile, permettendo al cliente la piena consapevolezza delle scelte che sta compiendo.

In ambito Npl, è previsto un meccanismo aggiuntivo che garantisca la trasparenza nel rapporto agente–cliente: il cliente può sottoscrivere, al termine di ogni visita dell'agente, un documento contenente la "Relazione di visita" che riepiloga quanto accaduto durante l'incontro e gli accordi stabiliti. Anche nella trasmissione di informazioni all'esterno, attraverso la pubblicità o altri canali, il Gruppo assicura che le **comunicazioni siano oneste, veritiere, chiare, trasparenti, documentabili e conformi alle politiche e ai programmi aziendali**.

Le unità organizzative afferenti all'area Operations gestiscono i processi di trasparenza verso la clientela e le condizioni applicabili ai prodotti offerti dal Gruppo, oltre a occuparsi delle attività disciplinate dalla **normativa sulla trasparenza** (come l'invio ai clienti della documentazione periodica) e a supportare le aree di business nel redigere le comunicazioni rivolte alla clientela.

La funzione Compliance vigila sull'applicazione della normativa bancaria sulla trasparenza ed è inoltre coinvolta nel processo di definizione delle comunicazioni che riguardano variazioni significative alle condizioni di un servizio o prodotto, al fine di garantirne la chiarezza espositiva.

[GRI 417-2]
[GRI 417-3]

Nel corso del 2023 **non sono stati rilevati episodi di non conformità** in merito a regolamenti e/o codici volontari relativi a informazioni su prodotti e servizi, né in ambito di comunicazioni di marketing.

Raccolta di segnalazioni e reclami

Il Gruppo adotta diversi **meccanismi volti a raccogliere feedback e segnalazioni** da parte di stakeholder chiave, in particolare, dipendenti, collaboratori, professionisti che operano in maniera continuativa per il Gruppo, nonchè i **reclami** di clienti e debitori. Tali meccanismi supportano il management nell'identificazione di eventuali inefficienze, anomalie o problematiche emergenti nei processi aziendali, e come tali costituiscono, insieme ai controlli, utili strumenti di verifica dell'efficacia dell'approccio di gestione sui diversi temi.

Gestione dei reclami

[GRI 2-25]
[GRI 2-26]

Oltre a rappresentare uno strumento utile per migliorare la qualità dei prodotti, dei servizi e della relazione con la clientela, **il reclamo rappresenta** anche **un canale di ascolto** più ampio che consente di monitorare la condotta delle funzioni aziendali e degli operatori interni ed esterni che operano per conto del Gruppo (come i front office e gli operatori delle reti esterne) e quindi di mantenere viva la fiducia reciproca fra il Gruppo e il Cliente. Possono rientrare nell'ambito dei reclami, infatti, oltre alle segnalazioni attinenti alla qualità di prodotti e dei servizi, anche segnalazioni relative al rispetto dei principi di integrità e correttezza, alla conformità normativa, alla non discriminazione e ad attività di sostegno all'imprenditoria e inclusione finanziaria.

Il processo di gestione dei reclami ha come **obiettivo gestire tempestivamente e con efficacia qualsiasi segnalazione di clienti** insoddisfatti dei prodotti e servizi erogati o offerti, attuando azioni correttive e preventive per evitare che qualsiasi disservizio si ripresenti. Tali azioni possono prevedere tanto iniziative specifiche rivolte al singolo reclamante quanto l'attivazione di soluzioni generalizzate, volte a risolvere le cause alla base del singolo reclamo o di più reclami attinenti allo stesso ambito. A tale proposito, tutto il personale addetto alla trattazione dei reclami ha ricevuto specifiche direttive in merito all'opportunità di agevolare la ricerca di una soluzione personalizzata mirata alla concessione di misure di sostegno su base volontaria dell'istituto.

Inoltre, sempre nell'ottica di favorire al cliente la risoluzione di problematiche legate all'accesso al credito, particolare rilevanza riveste nel processo di **formazione del personale addetto alla trattazione dei reclami** e nel **procedimento di gestione del reclamo**, l'attenzione al tema Segnaletico presso banche dati creditizie (Centrale dei Rischi e banche dati private), rispetto al quale l'Ufficio Reclami ha sviluppato delle competenza specialistiche che lo rendono un punto di riferimento, insieme al Servizio Segnalazioni di Vigilanza, per le altre funzioni aziendali.

La **politica di gestione delle contestazioni**, applicata a livello di Gruppo, definisce le linee guida per la corretta e tempestiva gestione dei reclami ricevuti dalle società del Gruppo, ispirandosi ai principi di equo trattamento dei clienti e nel rispetto della normativa vigente.

È stato costituito un **Ufficio Reclami della Capogruppo** che gestisce, in regime di accentramento, anche i reclami ricevuti dalle società controllate. Il presidio dedicato alla gestione dei reclami riceve e gestisce con la massima diligenza e imparzialità le contestazioni e informa e coinvolge le unità di business di volta in volta interessate. L'Ufficio Reclami riporta gerarchicamente al General Counsel e funzionalmente alla Compliance e opera secondo le linee guida fornite da queste.

Per quanto riguarda le **attività di controllo di secondo livello**, è prassi consolidata da parte dell'unità Rischi Operativi e di Reputazione effettuare un monitoraggio periodico riguardante le contestazioni nell'ambito del sistema dei controlli interni. Tale monitoraggio ha come obiettivo la verifica del rispetto delle tempistiche normativamente previste per il riscontro, la numerosità e quota di accettazione. L'esito di tali verifiche viene sintetizzato in apposita reportistica gestionale indirizzata a diverse strutture, tra cui l'Ufficio Reclami della Capogruppo, nonché all'interno del Tableau de Bord del Risk Management.

[GRI 2-16]

Con cadenza semestrale, il Responsabile dell'Ufficio Reclami elabora i dati statistici relativi ai reclami e alle altre tipologie di controversie stragiudiziali gestite dall'Ufficio Reclami e redige una relazione riassuntiva che presenti

la situazione del semestre di riferimento per ogni singola società. La relazione contiene altresì le ulteriori attività svolte dall'ufficio reclami nel periodo di riferimento, quali attività formativa, ispezioni, e simili.

L'elaborazione dei dati evidenzia tra l'altro, a titolo esemplificativo e non esaustivo, i seguenti indicatori:

- il totale reclami ricevuti;
- la percentuale reclami accolti;
- i tempi medi di risposta;
- la distribuzione territoriale dei reclami;
- la distribuzione dei reclami per categoria di clientela, per prodotto/servizio, per motivo del reclamo;
- le eventuali azioni correttive intraprese sul piano organizzativo a seguito dei reclami ricevuti nel periodo in esame.

Il Responsabile dell'Ufficio Reclami trasmette la relazione sui reclami ricevuti e le elaborazioni prodotte:

- all'Amministratore Delegato (laddove presente) della società del Gruppo Bancario;
- al Direttore Generale (laddove presente) della società.

Per il tramite del Responsabile degli affari societari:

- al Responsabile della funzione di controllo che gestisce il rischio di non conformità;
- al Responsabile della Direzione General Counsel;
- al Responsabile di Communication, Marketing, Public Affairs & Sustainability.

La relazione semestrale predisposta è successivamente portata a conoscenza del rispettivo Consiglio di Amministrazione.

Il Responsabile dell'ufficio reclami predispone altresì una relazione semestrale consolidata a livello di Gruppo Banca Ifis, afferente alla situazione complessiva delle contestazioni ricevute da tutte le società del Gruppo.

Reclami		2022[64]	2021	2020
Numero totale di reclami	**N.**	8.838	5.985	6.672
Accolti	N.	1.717	762	928
	%	19,4%	12,7%	13,9%
Parzialmente accolti	N.	254	267	342
	%	2,9%	4,5%	5,1%
Rigettati	N.	6.867	4.956	5.402
	%	77,7%	82,8%	81,0%

[64] I dati riferiti all'anno 2023 verranno consolidati e approvanti dal Consiglio di Amministrazione a marzo 2024 e successivamente pubblicati nel sito aziendale al seguente indirizzo: https://www.bancaifis.it/reclami/resoconto/.

7.5 Relazione con la catena di fornitura

[GRI 2-23]
[GRI 3-3]

Politiche e altra documentazione di riferimento

- Politica di Gruppo per la gestione del Ciclo Passivo
- Procedura Organizzativa Gestione degli Acquisti di beni e servizi aziendali
- Codice Etico di Gruppo
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 (Banca Ifis)
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 (ifis Npl Investing)
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 (Ifis Npl Servicing)
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 (Cap.Ital.Fin.)
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 (Ifis Rental Services)
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 (Banca Credifarma)
- Politica di gruppo per l'esternalizzazione di funzioni aziendali
- Procedura sulla gestione delle esternalizzazioni di funzioni aziendali
- Procedura Organizzativa – Analisi e monitoraggio fornitori ICT
- Politica ESG di Gruppo

La catena di fornitura

[GRI 2-6]

Gruppo Banca Ifis regolamenta i rapporti con la catena di fornitura attraverso politiche e procedure interne come la Politica di Gruppo per la gestione del Ciclo Passivo e la Procedura Organizzativa Gestione degli Acquisti di beni e servizi aziendali, aggiornate nel 2023.

In sede di formalizzazione di contratti o accordi di fornitura, fatte salve le esclusioni previste da Procedura, il Gruppo prevede la presa visione e accettazione dei principi contenuti all'interno del Codice Etico di Gruppo inteso come documento vincolante la cui violazione comporta conseguenze di natura contrattuale. Nel corso del 2021, a seguito dell'aggiornamento del Codice Etico, è stata prevista l'integrazione di una clausola contrattuale che richiama, secondo le indicazioni della normativa interna di riferimento, il Codice quale documento vincolante nei confronti di ciascun destinatario e in particolare dei fornitori. La violazione del Codice Etico da parte dei destinatari costituisce, nei casi previsti dalla normativa interna, violazione del rapporto contrattuale tra il Gruppo e il destinatario e attribuisce al Gruppo anche il diritto di intimare la risoluzione o il recesso dal contratto per giusta causa qualora, ad insindacabile giudizio del Gruppo, la violazione commessa sia tale da far venir meno il rapporto di fiducia ovvero venga arrecato un notevole pregiudizio per il Gruppo stesso. Resta ferma la facoltà della Capogruppo o delle sue Controllate di richiedere il risarcimento dei danni. Nei vari rapporti con i fornitori si sta pertanto introducendo, ove possibile, detta clausola nei testi contrattuali.

Inoltre, sempre in sede di formalizzazione di contratti o accordi di fornitura, secondo le indicazioni della normativa interna, il Gruppo richiede altresì la presa visione e accettazione del Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/01.

[GRI 204-1]

Nel corso del 2023 il Gruppo si è servito di 4.568 fornitori (4.524 nel 2022), prevalentemente nel territorio italiano, le cui principali categorie sono relative a servizi professionali e non professionali: in particolare servizi per consulenze o legali, servizi in outsourcing, servizi per informazione dei clienti e servizi collegati all'utilizzo o all'assistenza software.

Si riporta di seguito il totale del valore distribuito ai fornitori, suddiviso tra Italia ed Estero:

Proporzione di spesa verso i fornitori		2023	2022
Totale del valore distribuito ai fornitori	Valore monetario (mln di euro)	286,5	273,8
Totale del valore distribuito ai fornitori – Italia:	Mln di €	277,8	268,1
	%	97%	98%
Italia - Nord-est	Mln di €	91,5	96,5
	%	33%	36%
Italia - Nord-ovest	Mln di €	99,1	96,5
	%	36%	36%
Italia - Centro	Mln di €	65,8	50,9
	%	23%	19%
Italia - Sud e Isole	Mln di €	21,3	24,1
	%	8%	9%
Totale del valore distribuito ai fornitori – Estero:	Mln di €	8,7	5,6
	%	3%	2%

Il Gruppo **seleziona i propri fornitori** sulla base di procedure competitive, criteri trasparenti e valutazioni obiettive che interessano parametri quali la qualità, l'utilità, il prezzo, l'integrità, la solidità e la capacità di garantire un'efficace assistenza continuativa, nonché il rispetto degli standard etici che il Gruppo identifica come propri. I fornitori di servizi vengono selezionati valutandone altresì l'onorabilità, la correttezza e la lealtà nella conduzione degli affari, la capacità di far fronte agli obblighi del Codice Etico e di riservatezza, tenuto conto della natura del servizio offerto e la sensibilità alle tematiche di responsabilità sociale, ambientale e di impresa.

[GRI 403-7]

Nella gestione del rapporto con i fornitori Gruppo Banca Ifis, al fine di **minimizzare eventuali impatti negativi in materia di salute e sicurezza** derivati dall'interazione della propria attività con l'attività dei fornitori esterni[65], attua diversi presidi in funzione dell'opera/prestazione concordata. Nello specifico, qualora di caso in caso ritenuto necessario, il Gruppo:

- come prescritto dal D.Lgs 81/08, definisce le modalità ottimali di gestione delle interferenze e redige appositi documenti quali il Piano di sicurezza e coordinamento, PSC o il Documento di valutazione dei rischi di interferenza, DUVRI;
- richiede al fornitore di recepire la Politica della sicurezza della Banca dichiarando di adottarla e rispettarla;
- richiede al fornitore di presentare eventuali abilitazioni necessarie allo svolgimento delle attività, autocertificando i requisiti di idoneità professionale e inviando alla committente il documento unico di regolarità contributiva, DURC;
- adotta ulteriori misure di protezione i cui costi sono indicati nei singoli contratti (Costi della Sicurezza);
- verifica la presenza del Nominativo nelle liste antiriciclaggio;
- visura e iscrizione alla CCIAA in essere;
- richiede un'autodichiarazione di non trovarsi nei casi espressi nel d.p.r. 445 del 28/12/2000.

Per quanto riguarda le **attività di controllo** di secondo livello della supply chain, la funzione Risk Management è responsabile della gestione e supervisione dei rischi connessi agli accordi di esternalizzazione nell'ambito del sistema dei controlli interni. Inoltre, a valle del processo di revisione periodica delle attività esternalizzate, rendiconta annualmente gli esiti all'Organo con funzione di Supervisione Strategica. A partire dall'anno 2022-

[65] La presente metodologia viene adottata per tutti gli interventi che richiedono l'utilizzo di imprese appaltatrici, lavoratori autonomi, servizi e forniture.

2023, è stata altresì istituita una ulteriore attività di verifica e monitoraggio da parte dell'Unità Rischi Operativi e di Reputazione che riguarda specifici fornitori con singolo contratto superiore a una determinata soglia di materialità. I risultati di queste analisi vengono condivisi con il Chief Operating Officer al fine di identificare gli eventuali interventi necessari.