



3.

Ifis 4 Integrity

Dichiarazione non finanziaria
consolidata 2022



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.

Ifis 4 Integrity rappresenta l'integrità del Gruppo, il nostro costante impegno per diffondere la **cultura e i valori aziendali** all'interno e all'esterno del Gruppo. Promuoviamo comportamenti virtuosi e coerenti con i valori del Gruppo, quali la **lotta alla corruzione**, la **tutela della privacy** dei nostri clienti e l'attenzione alla sostenibilità.

3.1 Integrità aziendale e lotta alla corruzione

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

Politiche e altra documentazione di riferimento

- Codice Etico di Gruppo
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 della Banca
- 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
- 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

Il **Codice Etico**, 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 attribuisce 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

ORGANISMO DI VIGILANZA



le indicazioni, di promuovere la revisione periodica del Codice dei suoi 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, il Gruppo si è dotato del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 (MOG), oltre che delle linee guida espresse nel Codice Etico.

Nel corso del 2022 il Modello di Organizzazione, Gestione e Controllo della Capogruppo è stato aggiornato al fine di adeguare le Parti Generale e Speciale al modello di *Governance* adottato dalla Banca, alle novità normative esterne intervenute nel corso del 2022 e alla normativa interna di nuova emanazione o soggetta ad aggiornamenti.

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, la banca si è dotata 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.

L'integrità della condotta degli agenti del Gruppo

Oltre a stabilire regole di condotta per il proprio personale, 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 Investing.

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**: ai sensi di quanto previsto dall'art. 128 quater comma 4 TUB l'agente in attività finanziaria può svolgere l'attività su mandato di un solo intermediario o di più intermediari appartenenti al medesimo Gruppo. In determinati casi, l'agente può assumere due ulteriori mandati purché per prodotti diversi da quelli già in essere;
- l'adozione di un **sistema di incentivazione** le cui logiche **scoraggiano comportamenti scorretti o insistenti** da parte degli agenti;
- l'osservazione del **Codice di Condotta** redatto dal forum Unirec – Associazioni Consumatori.

Con riferimento alla rete distributiva di Cap.Ital.Fin. e Banca Ifis, le Funzioni di Controllo svolgono verifiche periodiche in merito al rispetto della normativa di riferimento in materia di trasparenza e antiriciclaggio. Sulla base delle evidenze che emergono dalle verifiche svolte, vengono quindi adottate iniziative specifiche (e.g. sessioni di formazione su determinate tematiche) al fine di garantire un elevato standard qualitativo e professionale da parte della rete distributiva.

Relativamente alla gestione del call center della società Ifis Npl Servicing S.p.A. dedicato alla phone collection, è stata ottimizzata l'organizzazione del lavoro interna e sono stati creati **strumenti orientati al monitoraggio costante e all'analisi delle performance**, i quali presentano tra gli obiettivi anche il contenimento del rischio di comportamenti "aggressivi" o

“pratiche commerciali scorrette” da parte degli operatori. La società Ifis Npl Servicing S.p.A adotta diverse modalità di verifica dell'efficacia dell'approccio di gestione implementato:

- 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, quando è possibile, al termine di ogni visita al cliente, una “**Relazione 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 società;
- **interviste a clienti** che hanno risolto positivamente la pratica di cui al punto primo;
- **ascolto continuo** delle problematiche ed esigenze espresse dagli operatori della rete con incontri realizzati ad hoc.

In linea con quanto previsto per la Rete distributiva di Cap.Ital.Fin. e Banca Ifis, le Funzioni di controllo svolgono **verifiche periodiche nei confronti della Rete Esterna** (Società di Recupero, Agenti ex 115 TULPS e Agenti in attività finanziaria) in merito al rispetto delle disposizioni legislative e regolamentari nonché alle procedure condivise in sede di sottoscrizione del mandato e oggetto di periodico aggiornamento, al fine di ridurre i rischi operativi, legali e reputazionali collegati all'attività di intermediazione del credito. Sulla base delle evidenze che emergono dalle attività svolte vengono adottate iniziative specifiche.

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.¹⁹ **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.

¹⁹ 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.

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, da giugno 2022 è stato pubblicato nella Intranet aziendale la nuova edizione del 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		2022 ²⁰	2021	2020
	N.	1.557 ²¹	543	691
	%	83%	29,4%	40,0%
Dirigenti	N.	49	14	14
	%	51,6%	15,7%	17,9%
Quadri	N.	465	131	179
	%	82,0%	24,0%	35,3%
Impiegati	N.	1.043	398	498
	%	86,1%	32,8%	43,6%

Nel corso del 2022, la struttura Human Resources Learning and Development ha predisposto **incontri formativi destinati ai membri del Consiglio di Amministrazione** delle società del Gruppo di diritto italiano. Uno degli interventi formativi è stato dedicato agli aspetti regolamentari da monitorare per i componenti di un CdA del settore bancario. Inoltre, i membri del Consiglio di Amministrazione 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. Nel corso del periodo di rendicontazione, hanno ricevuto una formazione in tema anticorruzione il 31% dei membri del Consiglio di Amministrazione²².

I membri del Consiglio di Amministrazione della Capogruppo a marzo e a ottobre 2022 hanno approvato l'aggiornamento del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 che contiene anche le prescrizioni afferenti alla prevenzione del rischio di commissione dei reati di corruzione e concussione.

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 Gruppo²³.

[GRI 205-3]

Anche nel corso del 2022, 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 2022, 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. Questo principio si traduce in **specifiche procedure e verifiche** nelle diverse aree di business, che hanno

²⁰ Nel conteggio sono stati considerati i dipendenti che hanno svolto almeno una di queste attività: Corso e-learning "La responsabilità degli enti ed. 2020" reso disponibile a partire da ottobre 2020; "Prevenzione e governo del rischio di reato (D. Lgs. 231/2001)", reso disponibile da giugno 2022 in aggiornamento e sostituzione del corso precedentemente citato.

²¹ Il dato si riferisce al personale dipendente di Gruppo in forza al 31/12/2022. 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 2022 (26, di cui 22 impiegati e 4 quadri), le numeriche sono: totale n. 1583 (84%); impiegati n. 1065 (87,9%); quadri n. 469 (82,7); le numeriche relative ai Dirigenti rimangono invariate.

²² Il dato considera esclusivamente il Consiglio di Amministrazione di Banca Ifis.

²³ Per ulteriori approfondimenti, si veda il capitolo "3.4 Relazione con la catena di fornitura".

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 dirigente²⁴; in caso di presenza confermata nelle liste terroristi si provvede all'immediato rigetto della richiesta nonché all'invio di una eventuale segnalazione di operazione sospetta.

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;
- 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.

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 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 51,5 ore di formazione antiriciclaggio a 742 dipendenti** (nel 2021 46 ore per 496 dipendenti).

Per **Banca Ifis** sono state organizzate:

- 6 sessioni formative in aula virtuale da due ore ciascuna su "Intercettazione di elementi di anomalia e segnalazione di operazioni sospette", dirette ai dipendenti delle funzioni di gestione e sviluppo commerciale della Banca, per un totale di 248 dipendenti;
- specifiche sessioni formative dedicate alle funzioni sviluppo & gestione Crediti Commerciali, Servizio Clienti Leasing, Anagrafe, Recupero Crediti, Corporate Finance (per un totale di 156 dipendenti) sul tema degli "Obblighi di Adeguata Verifica nel continuo";
- specifiche sessioni formative dedicate alle funzioni Valutazione operazioni e Grandi rischi e monitoraggio (per un totale di 59 dipendenti) sulla nuova versione dell'applicativo di profilatura "GIANOS 5.5"²⁵;
- ulteriori sessioni formative sono state organizzate per l'*onboarding* di 14 nuovi dipendenti della Banca tra apprendisti e nuovi sviluppatori commerciali;

²⁴ 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.

²⁵ Tool integrato nel sistema informativo di Core Banking della Banca del fornitore CEDACRI che permette di calcolare il profilo di rischio di riciclaggio e di finanziamento del terrorismo della clientela, sia in on-boarding sia nel continuo.

Per **Banca Credifarma** sono state organizzate:

- due sessioni formative in aula virtuale da due ore ciascuna su “Intercettazione di elementi di anomalia e segnalazione di operazioni sospette” dedicate ai dipendenti delle funzioni Commerciale, Operations e Monitoraggio, per un totale di 46 dipendenti;
- due sessioni di formazione specialistica sui nuovi applicativi antiriciclaggio (AMLET) e sulla gestione delle certificazioni nelle liste negative Fastcheck e i flussi SARA.

Per **Capitalfin** è stata offerta una sessione formativa alle funzioni Marketing & Recruiting (4 persone) sull'utilizzo del Tool KYC; mentre tutte le UO sono state chiamate in aula per il corso di “Adeguata verifica della clientela e segnalazione di operazioni sospette” (36 persone).

Infine, le funzioni di Incassi conto terzi, Collection conto terzi e Master Servicing Npl di Ifis Npl Servicing (14 persone) hanno ricevuto una formazione specifica sul processo di rinnovo del profilo di rischio e di transaction monitoring (Portafoglio Elipso); mentre gli addetti delle funzioni Top Loan e Contenzioso sono stati chiamati in aula per un corso su Adeguata verifica della clientela e segnalazione di operazioni sospette (44 persone).

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 delle società controllate.

Parimenti, la funzione Anti-Money Laundering ha erogato della formazione generale in materia di antiriciclaggio ai nuovi agenti e recuperatori di Ifis Npl Investing; oltre a specifiche sessioni formative di un'ora ciascuna in tema di “Adeguata verifica senza la presenza fisica del cliente” 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 febbraio 2023 alla rete di Banca Ifis (agenti in attività finanziaria iscritti all'OAM che collocano il prodotto leasing).

Gestione delle segnalazioni (Whistleblowing)

[GRI 2-26]

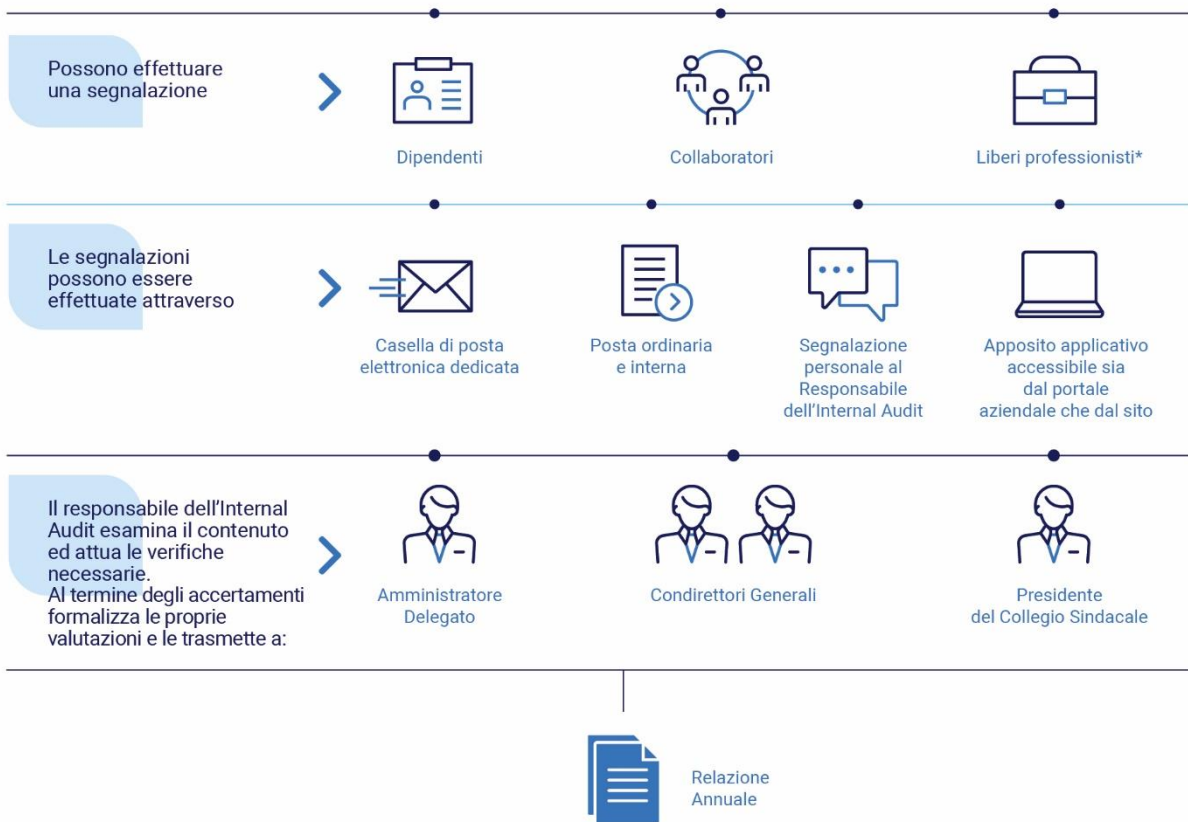
Banca Ifis, in qualità di Capogruppo, in coerenza con le disposizioni regolamentari e le best practice del settore, ha definito un sistema interno volto a permettere la segnalazione di atti, fatti e omissioni che possono costituire una violazione delle leggi e delle procedure interne disciplinanti l'attività 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 del Modello Organizzativo di Banca Ifis e adottata dalle società del Gruppo. 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.

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), 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 2022 non sono pervenute segnalazioni attraverso il sistema di segnalazione delle violazioni (Whistleblowing).



*Liberi professionisti che collaborano in modo prevalente e continuativo con il Gruppo

3.2 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 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 (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
- 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 dei log (Banca Ifis)
- Procedura Organizzativa per la gestione degli accessi logici
- Procedura Organizzativa per la gestione della Sicurezza Fisica delle risorse informative
- Politica di gruppo Sistemi pagamento via internet (Gruppo Banca Ifis)
- Procedura Organizzativa per il monitoraggio continuativo delle minacce e delle vulnerabilità di sicurezza
- Procedura Organizzativa per la Gestione dei log di Sicurezza delle informazioni
- Procedura Organizzativa Trattamento dei rifiuti 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)
- Procedura Organizzativa Gestione della sicurezza fisica (Gruppo 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.

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 2022, 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:

- predisporre 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 2022, a livello di Gruppo, analogamente all'esercizio precedente, **sono stati accolti 4 reclami** relativi a violazioni della privacy causati per la quasi totalità da errori operativi che, in ogni caso, non hanno comportato la divulgazione di dati sensibili.

Reclami documentati su violazioni della privacy e perdita di dati dei clienti		2022	2021	2020
Numero totale di reclami documentati ricevuti in merito a violazioni della privacy dei clienti	N.	4	4	4
<i>da terzi e documentati dall'organizzazione</i>	N.	4	4	4
<i>da parte di organismi di regolamentazione</i>	N.	0	0	0
Numero totale di eventi relativi a perdite e furti documentati dei dati dei clienti	N.	57 ²⁶	46	32

La crescita del numero di incidenti che hanno comportato la perdita, l'accesso o la divulgazione non autorizzata di dati personali è principalmente dovuta a un incremento delle attività di verifica del Gruppo su alcuni processi aziendali che hanno permesso di rilevare con maggiore accuratezza le violazioni dei dati personali. Gli incidenti rilevati nel 2022 riguardano soprattutto la perdita o il furto di dispositivi aziendali, l'errato invio di documentazione via posta ordinaria o via

²⁶ Il dato rappresenta il numero totale di incidenti occorsi nel 2022 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: 18 incidenti per Banca Ifis, 23 incidenti per Ifis Npl Servicing, 13 incidenti per Ifis Npl Investing, 1 incidente per Cap.Ital.Fin., 1 incidente per Farbanca, 1 incidente per Banca Credifarma.

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.

Al fine di mitigare l'esposizione a tali rischi, Gruppo Banca Ifis, nel corso del 2022, 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

Gruppo Banca Ifis, nel corso del 2022, ha attivato diverse campagne di sensibilizzazione sul tema della **cybersecurity** rivolte a tutti i dipendenti. In continuità con il periodo di riferimento precedente, è stata lanciata una **campagna di awareness** sui dipendenti del Gruppo attraverso l'iniziativa "**Ifis Cappuccino**" e altre pillole di sensibilizzazione, oltre alla 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 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 interessate della banca.

Sono state adottate, inoltre, misure di protezione stringenti, volte a ridurre ulteriormente il livello di rischio su specifici ambiti:

- in merito all'**infrastruttura e-mail del Gruppo**, attraverso l'introduzione di un sistema anti-phishing per l'individuazione di e-mail malevole in maniera più efficace;
- in merito alle **password aziendali**, attraverso una maggiore complessità delle stesse, con la contestuale introduzione progressiva della Multi Factor Authentication a tutta la popolazione aziendale.

Infine, nel corso del 2022 è stata effettuata un'altra campagna di simulazione di attacco di phishing volta alla sensibilizzazione dei dipendenti sul tema della sicurezza informatica.

La campagna rientra 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.**

3.3 Qualità e trasparenza di prodotti e servizi

[GRI 2-23]
[GRI 3-3]
[FS15]

Politiche e altra documentazione di riferimento

- Codice Etico di Gruppo
- Regolamento di Gruppo dei Comitati di Direzione (Banca Ifis, Ifis Npl Investing, Ifis Npl Servicing)
- Politica per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività, l'inserimento in nuovi mercati (Banca Ifis, Gruppo)
- Politica di Gruppo Gestione del ciclo passivo
- Politica di distribuzione (Cap.Ital.Fin.)
- 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 dei prodotti (Banca Ifis)
- Procedura Organizzativa Gestione RENDIMAX conto deposito (Banca Ifis)
- Procedura Organizzativa Gestione RENDIMAX conto corrente (Banca Ifis)
- Procedura Organizzativa Gestione Conto Corrente Ifis Impresa (Banca Ifis)
- Politica di Gruppo per la Gestione dei Rischi Operativi e di Reputazione

La qualità dei prodotti e servizi

La qualità del servizio e dei prodotti offerti ha un impatto importante sulla soddisfazione per il servizio ricevuto, sulla relazione con il cliente nonché sulla percezione di affidabilità e sicurezza nei confronti della Banca e degli operatori che agiscono per suo conto. Per tale ragione, la qualità e la trasparenza sono elementi strategici per il Gruppo, il quale si impegna a studiare, progettare e sperimentare prodotti e servizi sempre in linea con le esigenze di mercato e caratterizzati dai massimi livelli di qualità.

Attraverso una **politica per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività e l'inserimento in nuovi mercati**, Gruppo Banca Ifis definisce le regole per lo sviluppo e la distribuzione di nuovi prodotti, in coerenza con le strategie e gli obiettivi di business e aziendali.

In particolare, **in ambito leasing** nella fase che precede l'attivazione di un nuovo rapporto commerciale con un fornitore o un partner, e prima di acquistare un bene da concedere in leasing ai clienti, **sono attivate diverse verifiche**:

- **nel caso di potenziali partner/vendor convenzionati**, con i quali si mira a costruire un rapporto continuativo, l'attivazione dell'accordo commerciale è subordinata a un'istruttoria volta a verificare sia la qualità dei beni forniti sia il rispetto di criteri di affidabilità, credibilità e solidità dal punto di vista economico-finanziario e reputazionale. È inoltre previsto l'obbligo di sottoscrizione di un codice di comportamento al momento della definizione dell'accordo commerciale;
- **nel caso di fornitori occasionali** (ad esempio, proposti direttamente dal cliente ai fini dell'acquisto di un bene specifico) il controllo mira a verificare gli standard di qualità del bene, l'effettiva esistenza della società e il possesso delle principali credenziali, al fine di evitare frodi che coinvolgono il marchio e il cliente.

Livello di servizio di Gruppo Banca Ifis

Per Gruppo Banca Ifis l'impegno è quello di garantire ai propri clienti un elevato livello di servizio con velocità e tempestività di risposta distintive sul mercato. Di seguito si riportano i risultati ottenuti nel 2022 per i prodotti **leasing, factoring e mutui PMI**, i quali risultano sostanzialmente in linea con i risultati dell'esercizio 2021.

Tempi medi di **valutazione delle proposte di leasing** (in linea con il 2021):

- Auto e veicoli commerciali: 1,5 giorni
- Beni strumentali (industriali, IT e Office) e veicoli industriali di importo inferiore o uguale ad € 200.000: 4 giorni
- Beni strumentali e veicoli industriali di importo superiore ad € 200.000: 7 giorni

Tempi medi di **risposta alle richieste dei clienti leasing** (in linea con il 2021):

- Tempo di gestione delle richieste dei clienti: 2 giorni
- Abandon rate delle telefonate: 4%
- First Call Resolution: 95%
- Emissione dell'atto di vendita del bene al termine del contratto di leasing: 2 giorni

Tempi medi di **valutazione delle proposte di factoring**: 13,8 giorni

Tempi medi di **valutazione delle proposte di mutuo PMI**: 17,5 giorni

Ifis Npl Investing, anche per il tramite di Ifis Npl Servicing, promuove la continuità della relazione operatore-cliente per consolidare il livello di fiducia nel tempo e attua **diversi presidi** volti a garantire la qualità del servizio degli operatori della rete (società di recupero, agenti, call center interno), tra cui:

- **richiesta di credenziali e qualifiche:** gli agenti possono essere iscritti alle liste OAM (Organismo degli agenti e mediatori creditizi). Dal mese di settembre 2020, la società ha iniziato a inserire anche Agenti sotto la licenza di recupero 115 T.U.L.P.S., per i quali in fase di selezione vengono svolti numerosi controlli in tema di affidabilità del soggetto. Allo stesso modo anche le società di recupero vengono sottoposte, prima dell'attivazione del rapporto, a verifiche relative ad affidabilità, credibilità e solidità finanziaria;
- **incentivazione degli agenti e delle società di recupero:** sono previsti KPI specifici e SLA²⁷ contrattuali per verificare la qualità delle pratiche lavorate, con previsione e applicazione di penali (su SLA contrattuali) in caso di reiterata bassa qualità nel lavoro svolto.

²⁷ SLA: Service Level Agreement (accordo sul livello del servizio), cioè strumenti contrattuali attraverso i quali si definiscono le metriche di servizio che devono essere rispettate da un fornitore di servizi nei confronti dei propri clienti/utenti.

Modello di monitoraggio di agenti e dipendenti delle società recupero

Le strutture che gestisce le reti stragiudiziali e la struttura di monitoring ha definito un modello di monitoraggio degli agenti e delle società di recupero basato su differenti tipologie di KPI:

- **KPI qualitativi** quali, a titolo esemplificativo, reclami accolti, contestazioni e comportamenti anomali;
- **KPI quantitativi** quali, a titolo esemplificativo, le tempistiche di lavorazione, la qualità dei piani di rientro definiti in termini di numero e di importi, l'ammontare degli insoluti sui piani raccolti e le performance realizzate.

Il monitoraggio dei suddetti KPI è svolto **mensilmente** e, se del caso, è attivato un dialogo con agenti e società di recupero per avviare eventuali azioni correttive. I KPI vengono regolarmente condivisi.

Inoltre, in aggiunta alle consuete visite ispettive, presso le società di recupero, possono essere svolte **ispezioni ad hoc o questionari** volti a verificare, tra i vari aspetti, l'adeguatezza dei processi di recupero adottati rispetto alle best practice di settore. A partire dal 2021, sono iniziate attività ispettive (in modalità da remoto) anche nei confronti della rete di agenti da parte delle funzioni di controllo.

Annualmente, una volta elaborati gli esiti delle attività di controllo sopradescritte, viene svolta una **valutazione complessiva dei recuperatori** e in funzione dell'esito sono individuate le più opportune azioni da assumere per tutelare gli interessi di Gruppo Banca Ifis e dei suoi clienti.

In presenza di eventi rischiosi, le strutture interne informano le unità organizzative di controllo e, in particolare, la funzione Risk Management responsabile della gestione dei rischi operativi e reputazionali.

A verifica dell'efficacia dell'approccio di gestione adottato, le aree di business di competenza per ciascun prodotto o servizio ne verificano la conformità con i processi commerciali della Banca, al fine di garantire un'efficace copertura delle esigenze del cliente, e le funzioni di controllo possono prevedere ed effettuare verifiche secondo le modalità previste.

Nell'ambito della **definizione e introduzione di nuovi prodotti e servizi**, in particolare:

- la funzione **Compliance** garantisce il presidio del rischio di non conformità, ad esempio, valutando l'adeguatezza dei presidi rispetto alla normativa applicabile o verificando la conformità dei messaggi pubblicitari previsti e, in collaborazione con la funzione Human Resources, valuta l'adeguatezza della formazione al personale per sensibilizzarlo sui rischi insiti nel nuovo prodotto e sulle relative modalità di mitigazione;
- la funzione **Anti-Money Laundering** contribuisce alla valutazione del rischio che la nuova iniziativa può avere per la Banca con riferimento al potenziale coinvolgimento in fenomeni di riciclaggio e finanziamento del terrorismo determinato dall'offerta del nuovo prodotto.

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 2022 **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.

[GRI 2-27]

Nel corso del 2022 si sono registrati **2 episodi di non conformità a leggi e regolamenti**, uno dei quali ha comportato il pagamento di un'ammenda del valore di euro 9.157. Il secondo episodio non ha comportato sanzioni pecuniarie.

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, nonché 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 competenze 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, ecc.

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 predispose 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		2021 ²⁸	2020
Numero totale di reclami	N.	5.985	6.672
Accolti	N.	762	928
	%	12,7%	13,9%
Parzialmente accolti	N.	267	342
	%	4,5%	5,1%
Rigettati	N.	4.956	5.402
	%	82,8%	81,0%

²⁸ I dati riferiti all'anno 2022 verranno consolidati e approvati dal Consiglio di Amministrazione a marzo 2023 e successivamente pubblicati nel sito aziendale al seguente indirizzo: <https://www.bancaifis.it/reclami/resoconto/>.

3.4 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 della Banca
- Politica di gruppo per l'esternalizzazione di funzioni aziendali
- Procedura sulla gestione delle esternalizzazioni di funzioni aziendali

La catena di fornitura

[GRI 2-6]

Gruppo Banca Ifis regola 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 2022.

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 2022 il Gruppo si è servito di **4.524 fornitori** (4.946 nel 2020 e 4.625 nel 2021), 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		2022
Totale del valore distribuito ai fornitori	€	273.787.036
Totale del valore distribuito ai fornitori – Italia:	€	268.139.431,5
	%	98%
Italia - Nord-est	€	96.530.195,3
	%	36%
Italia - Nord-ovest	€	96.530.195,3
	%	36%
Italia - Centro	€	50.946.492
	%	19%
Italia - Sud e Isole	€	24.132.548,8
	%	9%
Totale del valore distribuito ai fornitori – Estero:	€	5.647.604,5
	%	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 esterni²⁹, attua diversi presidi in funzione dell'opera/prestazione concordata. Nello specifico, qualora di caso in caso venga 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;
- 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 2022-2023, 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.

²⁹ La presente metodologia viene adottata per tutti gli interventi che richiedono l'utilizzo di imprese appaltatrici, lavoratori autonomi, servizi e forniture.