3.

Ifis Integrity

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 Integrity rappresenta l'integrità del Gruppo, il nostro costante impegno per garantire la **qualità del credito** e 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 per la sostenibilità.

3.1 Integrità aziendale e lotta alla corruzione

Politiche e altra documentazione di riferimento

- Codice Etico
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001
- 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
- Procedura Organizzativa Adeguata verifica e profilatura della clientela per classi di rischio – nel continuo (Banca Ifis)
- Procedura Organizzativa per la Gestione dei crediti erariali (Banca Ifis)
- Procedura Organizzativa Gestione Rendimax Conto Corrente (Banca Ifis)
- Procedura Organizzativa Gestione Rendimax Conto Deposito (Banca Ifis)
- Procedura Organizzativa Gestione Conto Corrente Ifis Impresa (Banca Ifis)
- Procedura Organizzativa per la Gestione dei crediti erariali (Banca Ifis)
- Procedura Organizzativa Gestione Rendimax Conto Corrente (Banca Ifis)
- Procedura Organizzativa Gestione Rendimax Conto Deposito (Banca Ifis)
- Procedura Organizzativa Gestione Conto Corrente Ifis Impresa (Banca Ifis)
- Procedura Organizzativa Gestione e Concessione Finanza Strutturata
- Procedura Organizzativa Gestione e Concessione Special Situations
- Procedura Organizzativa Advisory
- Procedura Organizzativa Gestione della rete dei recuperatori stragiudiziali dei crediti distressed (Ifis Npl Servicing)
- Procedura Organizzativa Gestione della rete dei recuperatori stragiudiziali dei crediti distressed (Ifis Npl Servicing)
- Procedura Organizzativa di Adeguata Verifica e profilatura della Clientela NPL per classi di rischio (Ifis Npl Investing)
- Procedura organizzativa - Recupero del credito captive attraverso azioni giudiziali (ifis Npl Servicing)
- Procedura Organizzativa Gestione delle acquisizioni di portafogli di crediti (Ifis Npl Investing)
- Procedura Organizzativa Gestione dei pagamenti associati al recupero dei crediti distressed captive (Ifis Npl Servicing)
- Procedura Organizzativa Recupero del credito captive attraverso azioni stragiudiziali (Ifis Npl Servicing)
- Procedura Organizzativa Assegnazione delle pratiche NPL Captive ai bacini di recupero (Ifis Npl Servicing)
- Procedura Organizzativa - Adeguata verifica, profilatura della clientela e segnalazioni di operazioni sospette (Ifis Npl Servicing)
- Procedura Organizzativa Segnalazione di Operazioni Sospette (Banca Ifis)
- Manuale Antiriciclaggio Cap.Ital.Fin.
- Manuale Antiriciclaggio ed Antiterrorismo Credifarma
- Manuale Antiriciclaggio – Parte Procedurale Farbanca
- Manuale operativo Embargo e antiterrorismo: Controlli sui bonifici in entrata ed uscita (Banca Ifis)
- Manuale operativo Certificazione Posizioni in Liste Negative
- Politica di distribuzione (Cap.Ital.Fin)

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 del 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

le indicazioni, di promuovere la revisione periodica del Codice dei suoi meccanismi di attuazione e di riportare al Consiglio d'Amministrazione sull'attività svolta e sulle problematiche connesse all'attuazione del Codice Etico.

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 alla 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 di linee guida espresse nel Codice Etico.

A ottobre 2020 il Modello di Organizzazione, Gestione e Controllo della Capogruppo è stato aggiornato per dare particolare rilevanza all'intervento di riforma della Parte Speciale del Modello e procedere secondo le ordinarie direttrici che caratterizzano la strutturazione del documento quali: la rilevazione dei processi esistenti e la loro formalizzazione, la mappatura dei rischi inerenti, e la predisposizione o migliore esplicitazione dei relativi presidi.

Una parte dell'intervento è stata diretta ad un'individuazione delle aree di rischio, più dettagliata e concreta rispetto alla precedente versione del Modello, al fine di indirizzare l'agire di dirigenti, dipendenti e collaboratori della Banca e, di conseguenza, al fine di realizzare un Modello efficace ai sensi dell'art. 6 del D. lgs. 231/01.

I reati oggetto di maggiore e prioritaria attenzione nel contesto dell'aggiornamento del Modello Organizzativo della Banca sono stati, ad esempio: riciclaggio, reati societari, abusi di mercato, reati tributari.

L'integrità della condotta degli agenti del Gruppo

Oltre a stabilire regole di condotta per il proprio personale, il Gruppo Banca Ifis ritiene fondamentale assicurare l'integrità della condotta anche degli agenti dell'area Leasing e della società Cap.Ital.Fin. nonché degli agenti e delle società di recupero di Ifis Npl 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: la rete di agenti può avere al massimo tre mandati (per agenti in attività finanziaria e agenti iscritti all'OAM) e solo di attività non in concorrenza;
- l'adozione di un sistema di incentivazione le cui logiche scoraggiano comportamenti scorretti o insistenti da parte degli agenti;
- l'osservazione del "Codice di Condotta" redatto dal forum Unirec – Associazioni Consumatori.

Con riferimento alla rete distributiva di Cap.Ital.Fin., le Funzioni di Controllo svolgono verifiche periodiche in merito al rispetto della normativa di riferimento in materia di trasparenza e di antiriciclaggio. Sulla base delle evidenze che emergono dalle verifiche svolte, vengono quindi adottate iniziative specifiche (es. 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, un "Verbale di visita" che riepiloga quanto accaduto e gli accordi stabiliti, che deve essere sottoscritto dal cliente stesso così da tenere una traccia trasparente e oggettiva di quanto concordato;
- revisione trimestrale dei reclami non accolti per identificare eventuali problematiche emergenti o aspetti di crescente interesse per i clienti, al fine di definire azioni correttive;
- monitoraggio continuo dei canali social della 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.

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

- Corruzione per l'esercizio della funzione;
- Corruzione per un atto contrario ai doveri d'ufficio;
- Corruzione in atti giudiziari;
- Corruzione di persona incaricata di un pubblico servizio;
- Concussione, induzione indebita a dare o promettere utilità e corruzione;
- Corruzione tra privati;
- Istigazione alla corruzione tra privati;
- 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 di Banca Ifis specifica che le strutture di controllo per quanto riguarda la commissione dei reati potenziali relativi alla corruzione sono, oltre alle funzioni di controllo di secondo e terzo livello, l'Organismo di Vigilanza e il Collegio Sindacale.

[GRI 205-2]

Il Consiglio di Amministrazione, in sede di approvazione del Codice Etico del Gruppo, viene a conoscenza delle procedure anticorruzione adottate.[17] Tutti i dipendenti sono tenuti a conoscere e rispettare le regole in materia di contrasto alla corruzione, anche con riferimento alla tabella allegata al Modello che regola nel dettaglio le potenziali attività sensibili, le principali strutture e le tutele poste in atto in termini di politiche, regolamenti interni e strutture di controllo. Inoltre, tutti i dipendenti del Gruppo hanno accesso, attraverso la Intranet aziendale, alla normativa interna aziendale e in particolare il Codice Etico, 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, da luglio 2020 è stato pubblicato nella Intranet aziendale la nuova edizione del corso di formazione obbligatoria sulla "Responsabilità amministrativa degli Enti ed. 2020", a disposizione anche per il 2021. La tabella di seguito riportata 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		2021[18]	2020	2019
	N.	**543**	**691**	**476**
	%	**29,4%**	**40,0%**	**27,2%**
Dirigenti	N.	14	14	8
	%	15,7%	17,9%	10,8%
Quadri	N.	131	179	116
	%	24,0%	35,3%	22,7%
Impiegati	N.	398	498	352
	%	32,8%	43,6%	30,1%

I membri del Consiglio di Amministrazione della Capogruppo nell'ottobre 2020 hanno approvato l'aggiornamento del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 che contiene anche prescrizioni afferenti alla prevenzione del rischio di commissione dei reati corruzione e concussione mentre nell'agosto 2021 hanno approvato l'aggiornamento del Codice Etico.

Inoltre, nel corso del 2021 è stato avviato un percorso formativo rivolto agli organi di vertice del Gruppo Banca Ifis articolato in più incontri in aula virtuale, che ha visto il coinvolgimento sia di docenti esperti e professionalità di eccellenza, individuati attraverso Abiformazione ed il Politecnico di Milano, sia di responsabili interni con l'obiettivo di allineare i partecipanti circa le progettualità e gli indirizzi della Banca. I contenuti previsti nel piano si sono focalizzati sugli elementi di cambiamento strategico e organizzativo con cui il settore bancario si sta confrontando e sul presidio dei rischi di maggior rilievo; i moduli hanno approfondito il ruolo e le responsabilità degli Organi di vertice, il mercato nel quale opera il

[17] Il 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. Nello specifico, nel corso del 2021 è stato approvato l'aggiornamento del Codice Etico, integrato alla "Parte Generale" del MOG.

[18] 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
- Corsi di formazione con fornitori esterni

Gruppo, le principali sfide che l'evoluzione del contesto pone al settore bancario. Nello specifico, i temi trattati nel 2021 sono stati:

- Scenari del settore bancario anche a livello internazionale;
- Le dimensioni ESG tra Rischi e Opportunità;
- La disciplina delle operazioni con parti correlate;
- Il Fintech e l'innovazione dei modelli di business;
- Le novità regolamentari fondamentali e le prospettive 2021-2022;
- Il rischio strategico.

Per garantire l'integrità dei comportamenti delle reti esterne vengono attuati diversi presidi, tra cui 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.

In particolare, a seguito dell'aggiornamento 2020 del Modello e del Codice Etico, a gennaio 2021 si è proceduto alla comunicazione via mail della nuova documentazione agli agenti e fornitori di Banca Ifis. Nel corso dell'anno, con l'ulteriore aggiornamento del Codice Etico è stata prevista l'integrazione di una clausola contrattuale che richiamerà espressamente 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 violazione del rapporto contrattuale tra Banca Ifis e/o le Controllate e il destinatario e attribuisce a Banca Ifis e/o le Controllate anche il diritto di intimare la risoluzione o il recesso dal contratto per giusta causa qualora, ad insindacabile giudizio di Banca Ifis e delle Società, la violazione commessa sia tale da far venir meno il rapporto di fiducia ovvero venga arrecato un notevole pregiudizio per la Capogruppo e/o una delle sue Controllate. Resta ferma la facoltà della Capogruppo o delle sue Controllate di richiedere il risarcimento dei danni. Nei vari rapporti con i fornitori (sia già vigenti che nuovi) si stanno pertanto adeguando, ove possibile, i testi contrattuali a tali disposizioni.

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

[GRI 205-3]

Anche nel 2021, analogamente all'esercizio precedente, non sono stati registrati casi di corruzione o cause legali che abbiano riguardato dipendenti del Gruppo o operatori delle reti esterne.

La prevenzione al riciclaggio e finanziamento al terrorismo

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

- nel settore **Leasing** vengono esaminate le notizie negative di stampa tramite un processo automatizzato e integrato nella procedura dell'auto-delibera: se emergono riscontri la pratica viene bloccata e indirizzata verso la valutazione manuale, anche con il coinvolgimento dell'Antiriciclaggio. L'esito delle verifiche si traduce nell'assegnazione di un profilo di rischio in base al quale viene attivato un processo di approvazione a livelli diversi della gerarchia aziendale;
- nel **Credito Commerciale** 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 viene demandata all'appropriato livello gerarchico la decisione di procedere o meno con l'apertura/prosecuzione del rapporto;
- in **Capitalfin** viene effettuato uno screening per l'individuazione dei soggetti esposti politicamente o a rischio terrorismo. In caso di positività per le persone esposte politicamente, si procede con la verifica rafforzata e

autorizzazione dell'Alto dirigente[19] e l'innalzamento del profilo di rischio. 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. La società ha inoltre in uso 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 Credifarma vengono verificati i possibili soggetti esposti politicamente o a rischio terrorismo. In caso di riscontro positivo per le persone esposte politicamente si procede con approfondimenti volti alla valutazione dell'innalzamento del grado di rischio e all'autorizzazione dell'Alto dirigente. Sono in uso anche le liste sulle informazioni reputazionali negative, che sono sottoposte a verifica costante, come pure banche dati per il controllo dei documenti di identità. La società procede inoltre a identificare le intervenute variazioni societarie, in particolare riconducibili alla modifica della compagine e/o della denominazione sociale ed eventuali operazioni di finanza straordinaria effettuate;
- in Farbanca si applica lo screening delle liste per i soggetti esposti politicamente e per i terroristi. I gestori effettuano gli approfondimenti con il cliente e valutano in procedura Fastcheck, dando evidenza alla funzione AML degli esiti al fine della corretta gestione delle note anagrafiche. In caso di positività sulle persone esposte politicamente si attiva il processo di autorizzazione dell'Alto Dirigente per la prosecuzione dei rapporti e l'innalzamento del profilo di rischio. Tali controlli sulle liste sono effettuati nel continuo;
- nel settore Npl viene effettuata una prima verifica nel momento di acquisto del portafoglio crediti, e controlli successivi sulle singole controparti al momento della definizione dei piani di rientro.

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

L'Antiriciclaggio contribuisce alla definizione dei contenuti della formazione obbligatoria in materia di antiriciclaggio, in particolar modo per i dipendenti che hanno un contatto diretto con la clientela. Sia nel 2020 che nel 2021, la formazione in merito all'antiriciclaggio è stata svolta sia attraverso corsi in aula (in modalità virtuale) sia online tramite il corso e-learning "La disciplina antiriciclaggio ed. 2020" della durata di 4 ore, attivato sulla piattaforma Ifis Talent. Nel corso dell'anno è stato erogato un totale di 2.312,5 ore di formazione antiriciclaggio (circa 4.217 nel 2020 e 2.366 ore nel 2019). In particolare, il corso in e-learning è stato fruito da 332 dipendenti del Gruppo.

- per Banca Ifis sono state organizzate 12 sessioni formative in aula virtuale da due ore ciascuna su "La prevenzione del riciclaggio ai tempi dell'emergenza Covid-19", sia per gli addetti della funzione Antiriciclaggio, sia per i dipendenti delle funzioni commerciali, di valutazione e di gestione della Banca, per un totale di 341 dipendenti. La stessa classe è stata proposta ai responsabili di Business Unit e agli addetti delle funzioni di controllo (47 partecipanti), ai quali sono state dedicate 3 sessioni formative di due ore ciascuna;
- ulteriori sessioni formative sono state organizzate nella fase di On-boarding di 30 nuovi dipendenti tra apprendisti e nuovi sviluppatori commerciali e, per specifici argomenti operativi, per 21 addetti della gestione dei debitori e pagamenti e monetica;
- per Credifarma e Farbanca è stata organizzata una sessione formativa di due ore sulla "Prevenzione e gestione dei rischi di riciclaggio e di finanziamento del terrorismo" a 57 dipendenti.

Parimenti, la funzione Antiriciclaggio ha erogato specifiche sessioni formative di un'ora ciascuna in tema di "Collaborazione attiva e Segnalazione di Operazioni Sospette" a tutta la rete terza della Banca (agenti in attività finanziaria iscritti all'OAM che collocano il prodotto leasing) e di Ifis Npl Servicing (agenti in attività finanziaria iscritti all'OAM, società di recupero del credito, recuperatori ex art.115 TULPS); e ai nuovi agenti e recuperatori di Ifis Npl Investing.

[19] 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. Tale 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.

Gestione delle segnalazioni (Whistleblowing)

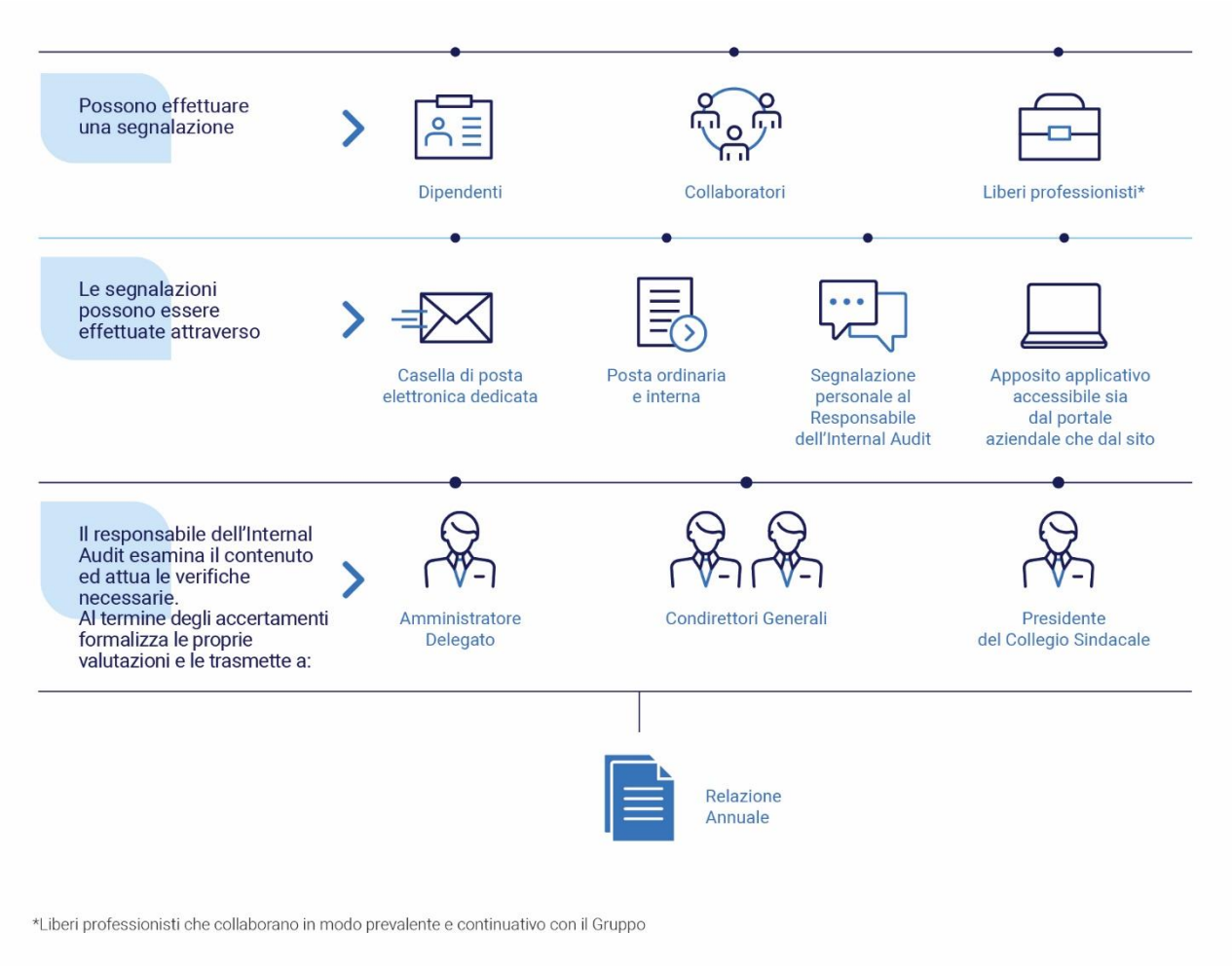
Banca Ifis, in qualità di Capogruppo, in coerenza con le disposizioni regolamentari e le best practices del settore, ha definito un sistema interno volto a permettere la segnalazione di atti, fatti e omissioni che possono costituire una violazione delle leggi e delle procedure interne disciplinanti l'attività svolta dalla Capogruppo e dalle Controllate, garantendo al contempo la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione. Il sistema di segnalazione è disciplinato dalla Politica di Gruppo per la gestione delle segnalazioni delle violazioni (Whistleblowing), parte integrante del Modello Organizzativo di Banca Ifis e adottata dalle società del Gruppo. Possono effettuare una segnalazione i dipendenti del Gruppo Banca Ifis, i collaboratori e i liberi professionisti regolarmente iscritti ad un albo che prestano la loro opera in modo prevalente e continuativo per il Gruppo.

La segnalazione può avere ad oggetto qualsiasi azione od omissione non conforme alle norme disciplinanti l'attività aziendale che arrechi o possa arrecare danno o pregiudizio al Gruppo Banca Ifis. Possono rientrare in questa casistica, ad esempio, azioni od omissioni, commesse o tentate, 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 dell'Internal Audit formalizza le proprie valutazioni e le trasmette all'Amministratore Delegato (o al il Presidente del Collegio Sindacale in caso di situazioni di potenziale incompatibilità), che valuteranno le necessarie azioni correttive. Internal Audit redige una relazione annuale sul corretto funzionamento del processo, contenente anche informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, che viene approvata dal Consiglio di Amministrazione e messa a disposizione del personale.

Nel 2021, sono state registrate 2 segnalazioni tramite il sistema di *Whistleblowing*.



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

3.2 Qualità del credito

Politiche e altra documentazione di riferimento

- Sistema delle deleghe di gruppo in materia di gestione del rischio di credito
- Sistema delle Deleghe di gruppo assunzione del credito
- Sistema delle deleghe di gruppo in materia di assunzione e gestione del rischio di credito (Cap.Ital.Fin.)
- Sistema delle deleghe di assunzione e gestione Ifis Finance IFN SA
- Sistema delle deleghe per l'assunzione e la gestione del rischio di credito IFIS FINANCE
- Politica di Gruppo per la gestione delle operazioni di maggior rilievo (OMR)
- Politica di Gruppo per la valutazione delle attività aziendali
- Politica di gestione del credito ordinario: BU PHARMA (Banca Ifis)
- Politica di gestione del credito ordinario: BU Farmacie (Banca Ifis)
- Politica di gestione del credito ordinario: Impresa Italia (Banca Ifis)
- Politica di gestione del recupero dei crediti distressed captive (Ifis Npl Servicing)
- Politica di impairment
- Politica di gestione dei portafogli di crediti acquistati a titolo definitivo e vantati verso gli enti della Pubblica Amministrazione (Banca Ifis)
- Politica di monitoraggio e recupero del credito ordinario (Banca Ifis)
- Politica di monitoraggio e recupero (Cap.Ital.Fin.)
- Politica di monitoraggio e recupero (Credifarma)
- Politica per la gestione del processo di verifica del corretto monitoraggio e dell'adeguatezza del processo di recupero (Banca Ifis)
- Manuale metodologico valutazione analitica del credito deteriorato (Banca Ifis)
- Procedura Organizzativa Gestione dei crediti erariali (Banca Ifis)
- Nota Operativa Processo di istruttoria Leasing (Banca Ifis)
- NO 111 – BU Leasing – Processo valutazione e settaggio Riscatti (Banca Ifis)
- NO 103 – BU Leasing – Valutazione qualità del credito soggettiva (Banca Ifis)
- Politica di monitoraggio e recupero del credito Leasing (Banca Ifis)
- Politica di gestione delle acquisizioni dei portafogli di crediti distressed e del relativo monitoraggio (Ifis Npl investing)
- Politica di distribuzione (Cap.Ital.Fin.)
- Politica di gestione del recupero dei crediti distressed captive (Ifis Npl Servicing)
- Procedura di Assegnazione delle pratiche Npl ai bacini di recupero (Ifis Npl Servicing)
- Procedura Organizzativa Recupero del credito attraverso azioni giudiziali (Ifis Npl Servicing)
- Procedura organizzativa di Recupero del credito attraverso azioni stragiudiziali (Ifis Npl Servicing)
- Procedura Organizzativa Gestione dei pagamenti associati al recupero dei crediti distressed (Ifis Npl Servicing)
- Procedura Organizzativa – Concessione e Gestione Finanza Strutturata (Banca Ifis)
- Procedura Organizzativa – concessione e Gestione Special Situations (Banca Ifis)
- Procedura Organizzativa Gestione della rete dei recuperatori stragiudiziali dei crediti distressed (Ifis Npl Servicing, Ifis Npl Investing)
- Politica attività di distribuzione assicurativa svolta dalla Banca (Banca Ifis)

La qualità del credito è strettamente connessa alla solidità patrimoniale, elemento chiave per la sostenibilità del modello di business del Gruppo ed una delle fondamenta della strategia del Gruppo.

Allo scopo di recepire gli impatti dell'emergenza sanitaria, sono state effettuate analisi ed implementate nuove logiche prudenziali, oltre alle misure istituzionali introdotte per il sostentamento temporaneo dell'economia nazionale. Per maggiori informazioni sugli impatti del Covid-19 sulla situazione finanziaria e la performance dell'impresa si prega di far riferimento al paragrafo "Rischi, incertezze e impatti dell'epidemia Covid-19", Parte A – Politiche contabili (A.1 – Parte generale, Sezione 5 – Altri aspetti) del documento "Relazioni e bilancio consolidato 2021".

La qualità del credito può avere impatti significativi sul valore del titolo azionario, sul livello del rating creditizio della Banca e del Gruppo, sul valore dei dividendi e sulla salvaguardia della solidità patrimoniale, rilevanti per azionisti, analisti finanziari, agenzie di rating, finanziatori e Autorità di Vigilanza, nonché sulla fiducia dei clienti nella capacità del Gruppo di fare fronte ai propri impegni, importante soprattutto per i risparmiatori retail del prodotto Rendimax.

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

- controlli automatici sia sulle persone fisiche sia su quelle giuridiche, al fine di verificare la presenza del potenziale cliente nelle "watch list" (terrorismo, embarghi, ecc.) e nelle liste di "Persone Politicamente Esposte", cui si aggiunge in relazione al livello di rischio un'analisi delle notizie di stampa effettuata dall'Antiriciclaggio;
- valutazione analitica, da parte dei team di Valutazione Operazioni e Valutazione Controparti, del cliente, dei clienti ceduti e del credito oggetto di cessione e sistema delle deleghe per l'assunzione del rischio di credito basato su importi e classi di rischio;
- continua interlocuzione con la rete territoriale, da cui possono provenire segnalazioni e riscontri sul potenziale cliente.

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

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

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

Le società del Gruppo operanti nel Settore Npl, la specificità delle quali è l'acquisizione e la gestione di crediti deteriorati, sono focalizzate sulla verifica della lavorabilità dei crediti e sul disegno di piani di rientro compatibili con la specifica situazione debitoria, attraverso diversi meccanismi di verifica lungo le fasi dell'acquisizione del credito:

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

L'identificazione dei Settori operativi è coerente con le modalità adottate dalla Direzione per l'assunzione di decisioni operative e si basa sulla reportistica interna, utilizzata ai fini dell'allocazione delle risorse ai diversi segmenti e dell'analisi delle relative performance.

L'informativa per Settore si articola, coerentemente con la struttura utilizzata dalla Direzione per l'analisi dei risultati del Gruppo, in:

- Settore Commercial & Corporate Banking, rappresenta l'offerta commerciale del Gruppo dedicata alle imprese e si sostanzia nelle Aree di Business Factoring, Leasing e Corporate Banking & Lending;

- Settore Npl, dedicato all'acquisizione pro-soluto e gestione di crediti di difficile esigibilità, di servicing e nella gestione dei crediti non performing secured;
- Settore Governance & Servizi e Non Core, che fornisce ai settori operativi nei core business del Gruppo le risorse finanziarie ed i servizi necessari per lo svolgimento delle rispettive attività. Il Settore comprende l'attività di tesoreria e il desk titoli di proprietà, l'attività di erogazione di finanziamenti contro cessione del quinto dello stipendio o pensione e alcuni portafogli di prestiti personali, oltre a taluni portafogli creditizi corporate posti in run-off in quanto ritenuti non strategici allo sviluppo del Gruppo.

Nel corso del 2020 sono state introdotte talune modifiche ai Settori operativi, al fine di dare piena attuazione al modello di business del Gruppo. Pertanto, i valori riportati nel presente documento risultano essere in linea con la nuova presentazione dei settori di attività.

Di seguito si riportano i valori del Gross e del Net NPE ratio del Settore Commercial & Corporate Banking. Il Gross Ratio risulta allineato al 2020 mentre il Net Ratio risulta in aumento rispetto al 31 dicembre 2020.

GROSS E NET NPE RATIO		2021	2020	2019
Gross	%	5,9%	5,9%	8,5%
Net	%	3,6%	2,7%	4,2%

Complessivamente i ratio calcolati sui crediti verso la clientela, al netto del Settore Npl e dei Titoli di stato compresi in tale voce, sono pari a:

- Gross Ratio: 6.4% (6.4% al 31.12.2020)
- Net Ratio: 3.9% (3.2% al 31.12.2020)

3.3 Data protection

Politiche e altra documentazione di riferimento

- Politica di Gruppo per la gestione della sicurezza informatica
- Politica di Gruppo per la valutazione e la gestione dei rischi informatici
- Procedura Organizzativa Gestione degli incidenti di sicurezza delle informazioni
- Procedura Organizzativa Gestione delle tematiche privacy attinenti ai diritti dell'interessato e al rapporto con il Garante (Cap.Ital.Fin., Ifis Rental Service, Ifis Npl Servicing, Ifis Npl Investing, Ifis Real Estate, Farbanca, Credifarma)
- 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 (Banca Ifis, Farbanca, Ifis Finance)
- Procedura Organizzativa Gestione dello sviluppo, dell'acquisizione e della manutenzione del software applicativo e dell'infrastruttura tecnologica
- Politica di gruppo per il monitoraggio e la misurazione delle performance (Banca Ifis, Ifis Finance)
- Procedura Organizzativa per la gestione dei log (Banca Ifis)
- Procedura Organizzativa per la gestione degli accessi logici (Banca Ifis)
- Politica di gruppo Sistemi pagamento via internet (Banca Ifis, Ifis Finance)

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

Il Gruppo Banca Ifis considera la protezione dei dati personali un principio inderogabile, fondamentale per rafforzare la fiducia e il senso di sicurezza dei clienti e per tutelare la reputazione del Gruppo. Il Gruppo è inoltre impegnato nella prevenzione e gestione tempestiva di incidenti di sicurezza informatica a tutela del patrimonio informativo della Banca, che comprende, tra gli altri, i dati di clienti, dipendenti, fornitori e ogni altro soggetto con cui Banca Ifis intrattiene rapporti. Nel corso del 2020 il Gruppo ha ulteriormente consolidato i presidi richiesti dal Regolamento europeo in materia di protezione dei dati personali (General Data Protection Regulation, GDPR).

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.

La sensibilizzazione dei dipendenti ed il programma sulla cybersecurity

Il Gruppo Banca Ifis, per sensibilizzare tutti i colleghi sul tema della cybersecurity, nel corso del 2021 ha effettuato molteplici comunicazioni volte ad allertare circa i rischi delle campagne in corso. In continuità con il periodo di riferimento precedente è stata lanciata una campagna di awareness sui dipendenti del Gruppo attraverso l'iniziativa "Ifis Talks – La tecnologia con gli occhi di un hacker: la Cyber Security riguarda tutti" per promuovere tra i dipendenti la conoscenza e la consapevolezza sulle più recenti minacce informatiche, fornendo informazioni aggiornate in materia di protezione cyber e per fornire utili suggerimenti per contrastarle. Tale iniziativa è stata attuata in occasione del mese dedicato al tema della sicurezza informatica nel quale Banca Ifis aderisce alla campagna ECSM (European Cybersecurity Month) dell'Unione Europea.

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 interno all'azienda. 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 della banca interessate.

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

- dell'infrastruttura e-mail della banca, attraverso l'introduzione di un sistema anti-phishing per l'individuazione di email malevole in maniera maggiormente efficace;
- delle password aziendali, attraverso una maggior complessità delle stesse, con la contestuale introduzione progressiva della Multi Factor Authentication a tutta la popolazione aziendale;

Infine, nel corso dell'anno 2021 è stata effettuata una 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 **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.**

Tra le attività di miglioramento del livello di sicurezza delle informazioni si citano:

- l'introduzione di misure di network security ad ulteriore protezione del perimetro tecnologico della banca;
- l'ampliamento del perimetro dei test di sicurezza, attività volta ad individuare eventuali vulnerabilità e porvi rimedio;
- l'effettuazione di attività di Red Teaming e cioè attività che si caratterizzano per la capacità di simulare un avversario reale che tenta di violare il perimetro tecnologico dei servizi esposti, delle applicazioni web, ecc. Ciò permette all'azienda di allenare i team preposti a rispondere agli attacchi informatici, individuando anche gli eventuali ambiti di miglioramento;
- la simulazione di campagne di ransomware mirate al fine di rafforzare la consapevolezza circa i rischi legati a questo tipo di minaccia.

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 informatica e quindi correttamente gestiti dalle strutture competenti.

Le segnalazioni e gli eventi che possono determinare incidenti di sicurezza possono provenire da diversi canali interni (altre unità organizzative) ed esterni (clienti, fornitori e canali istituzionali). L'Unità Organizzativa Information Security 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. Questo, insieme alle norme e procedure privacy, costituiscono il modello di gestione della privacy e l'insieme delle linee guida e delle regole che indicano come i dati personali sono protetti nel contesto aziendale.

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

- predispone e aggiorna la documentazione interna prevista dalla normativa in materia di privacy;
- monitora e controlla periodicamente l'osservanza della normativa e l'implementazione delle misure di sicurezza previste dalla legge;
- analizza le modalità di trattamento dei dati personali adottate dalla Banca e i rischi ad esse associati;

- valuta gli impatti in ambito privacy derivanti dal lancio di nuovi prodotti e servizi, dall'avvio di nuove attività, dall'ingresso in nuovi mercati e in tutti i casi in cui la Banca intenda realizzare internamente o acquistare un nuovo software;
- informa le unità organizzative della Banca, per gli ambiti di rispettiva competenza, in merito alle novità normative in tema privacy e fornisce supporto per garantirne l'adeguamento;
- supporta le Risorse Umane nello sviluppo di una adeguata cultura aziendale in ambito privacy 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 2021, a livello di Gruppo, analogamente all'esercizio precedente, sono stati accolti 4 reclami relativi a violazioni della privacy legati per la quasi totalità ad errori operativi/umani che, in ogni caso, non hanno comportato la divulgazione di dati sensibili.

Reclami documentati su violazioni della privacy e perdita di dati dei clienti		2021	2020	2019
Numero totale di reclami documentati ricevuti in merito a violazioni della privacy dei clienti	N.	4	4	4
da terzi e documentati dall'organizzazione	N.	4	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.	49[20]	32	10

La crescita del numero di incidenti che hanno comportato la perdita, l'accesso o la divulgazione non autorizzata di dati personali nel 2020 era principalmente dovuta ad un incremento dei pericoli e del rischio di attacchi informatici in relazione alle nuove modalità di lavoro da remoto. Al fine di mitigare l'esposizione a tali rischi, la Banca nel corso del 2020 ha avviato una campagna di sensibilizzazione interna sul tema della cybersecurity.

In seguito alle molteplici attività di awareness e sensibilizzazione messe in atto nel corso dell'anno, i dipendenti di Banca Ifis hanno sviluppato una maggior attenzione circa l'identificazione e la segnalazione di incidenti riguardanti i dati personali. Per questa ragione, nel 2021 si conferma, rispetto al periodo di riferimento precedente, il trend crescente del numero di incidenti, che non hanno comunque dato corso ad alcuna comunicazione verso l'Autorità Garante o verso gli interessati. Ad ulteriore giustificazione del trend crescente, si segnala che sono state effettuate attività di verifica su alcuni processi aziendali che hanno permesso di rilevare con maggior accuratezza le violazioni di dati personali. Gli incidenti rilevati nel 2021 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.

[20] Il dato rappresenta il numero totale di incidenti occorsi nel 2021 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: 19 incidenti per Banca Ifis, 24 incidenti per Ifis Npl Servicing, 4 incidenti per Ifis Npl Investing, 1 incidente per Cap.Ital.Fin., 1 incidente per Credifarma.