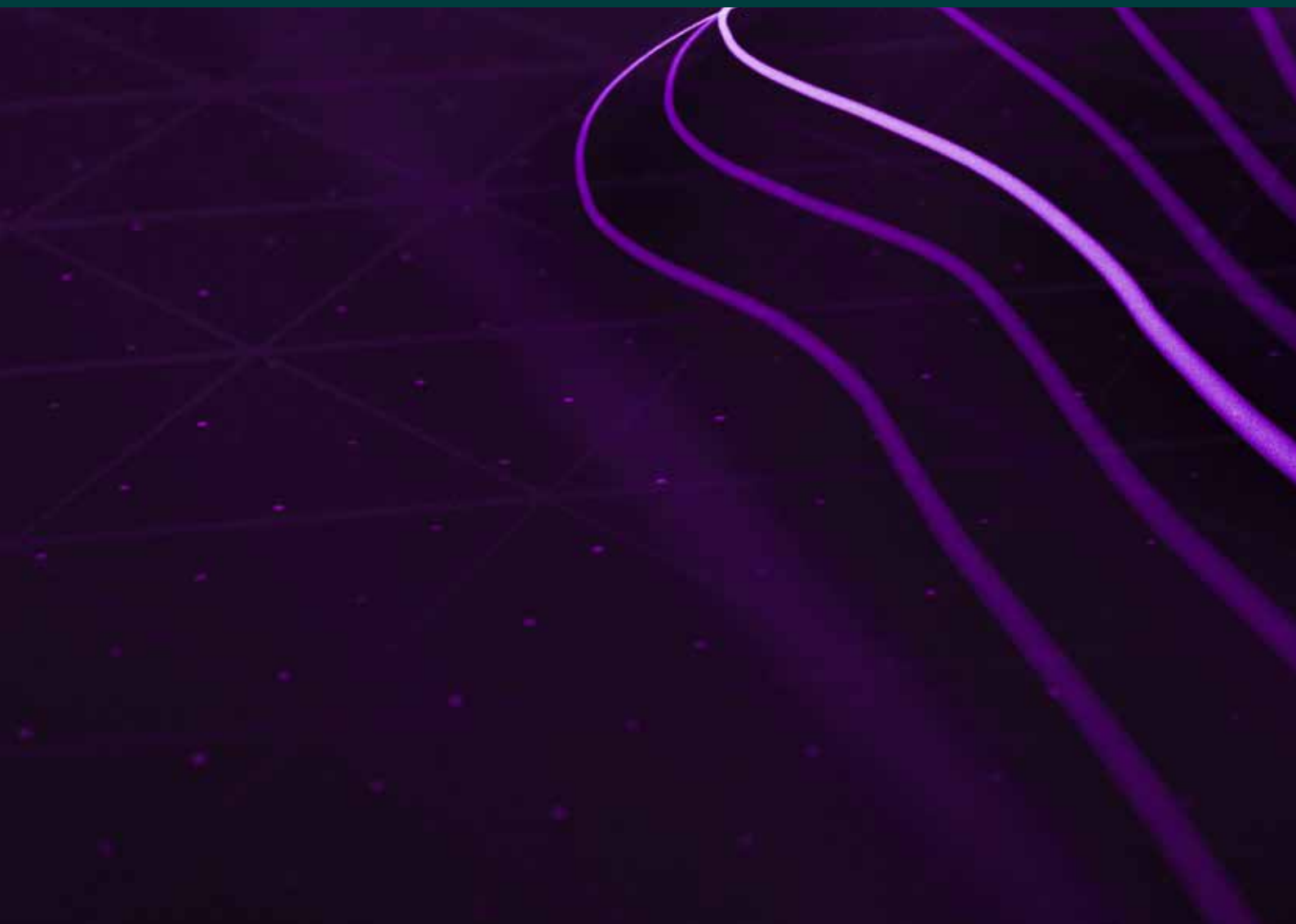
Business Ethics

- Business Integrity
- Data Ethics
- Security
- Gestione responsabile della catena di fornitura



Un approccio etico al business.

In Sisal crediamo in un approccio etico al business, inteso come l'insieme di comportamenti e di valori che orientano la condotta dell'individuo all'interno e nei confronti della comunità.

Per Sisal il concetto di Business Ethics viene declinato in tre pilastri:

1. **Business Integrity:** intesa come la modalità di agire da parte di Sisal e dei suoi dipendenti, nel rispetto delle leggi e dei regolamenti e ispirata a principi di **legalità, lealtà, correttezza, trasparenza e responsabilità**.
2. **Data Ethics:** intesa come l'adozione di pratiche eque e corrette in merito a modalità, tipologia e finalità di raccolta e trattamento dei dati personali, nonché nel rispetto della massima trasparenza verso i nostri clienti.
3. **Security:** intesa come il rispetto delle proprietà di **riservatezza, integrità e disponibilità delle infrastrutture e dei sistemi informatici**.

Business Ethics Week

Ogni anno in Sisal si svolge la **Business Ethics Week** (intitolata, nel 2022, "**We Are Aware**"), una settimana dedicata a iniziative di formazione e consapevolezza in ambito compliance. Le attività riguardano, in particolare, l'organizzazione di **iniziative di gamification**, **quiz a tema e webinar** diretti a tutta la popolazione aziendale. Nel 2022 la Business Ethics Week si è concentrata, in particolare, sugli ambiti privacy e data ethics, whistleblowing e codice etico, information security, HSE e relative certificazioni ISO, nonché anticorruzione e conflitto d'interesse. Il 98% dei rispondenti ad una survey sull'evento ha confermato di aver trovato l'iniziativa utile ed efficace, mentre l'89% ha riportato di essersi sentito coinvolto nel percorso della settimana. Il successo dell'iniziativa è stato confermato anche dal tasso di fruizione delle pillole inviate quotidianamente (pari al 58% della popolazione aziendale) e dall'elevato tasso di partecipazione ai webinar.

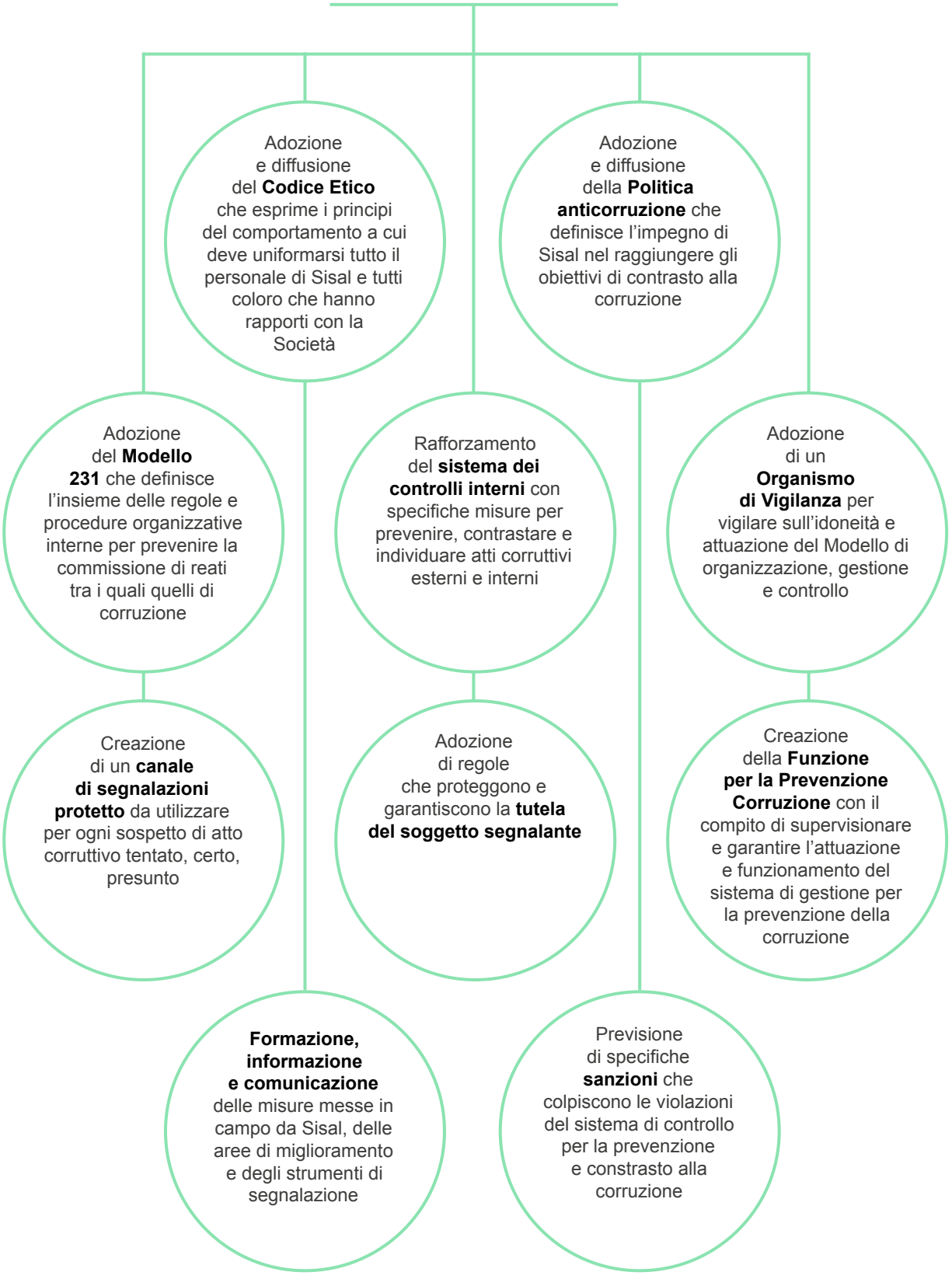
Business Integrity

Lotta alla corruzione

Il Gruppo Sisal, nel pieno rispetto delle leggi, dei regolamenti, nonché di tutte le prescrizioni previste da standard internazionali e linee guida, si impegna a prevenire e contrastare il verificarsi di illeciti nello svolgimento delle proprie attività, assumendo, tra i suoi valori primari, quello dell'etica aziendale, per mezzo della quale trasmettere messaggi di lealtà, correttezza, trasparenza, onestà e integrità.

In tale contesto la corruzione rappresenta un ostacolo intollerabile e abbiamo dunque la responsabilità di contribuire attivamente alla lotta alla corruzione e al conflitto di interesse. Sisal persegue questo obiettivo attraverso un sistema di regole, modelli, controlli e misure di formazione e comunicazione.

Modello e strumenti



Tutte le persone di Sisal sono responsabili del rispetto della normativa anticorruzione: tutti i dipendenti sono pertanto costantemente coinvolti in **iniziative di formazione e comunicazione**, inoltre tutti i documenti inerenti sono facilmente accessibili attraverso il sito internet e il portale intranet aziendale.

Sisal è inoltre la prima azienda nel settore del gaming in Italia ad avere ottenuto la **certificazione ISO 37001:2016 del Sistema di gestione per la prevenzione della corruzione**, finalizzato a mitigare il rischio connesso ad atti di corruzione attiva o passiva, tentata o commessa, pubblica o privata. La certificazione, assegnata da un ente terzo indipendente, identifica uno standard di gestione per aiutare le organizzazioni nella lotta contro la corruzione, istituendo una cultura di integrità, trasparenza e conformità. Nell'ambito del sistema di gestione per la prevenzione della corruzione, Sisal si avvale di **specifici strumenti** rafforzati e affinati (come le due diligence) o introdotti *ex novo* per soddisfare i requisiti previsti dagli standard normativi (come l'istituzione della Funzione di Conformità per la Prevenzione della Corruzione). Tutto questo attesta e rafforza il **sistema di controlli interni** affinché risulti idoneo a gestire e limitare il rischio di atti di "malagestione", che procurano un danno non solo economico ma, soprattutto, alla reputazionale della società. Le persone che svolgono attività sensibili ed esposte ai rischi rilevanti vengono infine identificate e coinvolte in attività di formazione specifiche.

Gestione del conflitto d'interessi

Con il termine "conflitto di interessi" si intende ogni situazione in cui si manifesta un conflitto tra le aspettative, gli interessi o i vantaggi di un singolo (per un dipendente) da un lato e le aspettative, gli interessi e i vantaggi di Sisal dall'altro, che può interferire, quindi, con la capacità del singolo di assumere decisioni e svolgere i propri compiti in modo imparziale ed efficace.

Sisal si è dotata di politiche e procedure atte a garantire la comunicazione, individuazione, gestione e monitoraggio dei conflitti di interesse, siano essi potenziali o effettivi.

In particolare, Sisal:

- è dotata di una Funzione di Conformità per la Prevenzione della Corruzione (FCPC), deputata, anche, alla gestione, censimento e monitoraggio dei conflitti di interesse, nonché alla comunicazione dei conflitti di interesse identificati come critici all'Amministratore Delegato;
- fornisce istruzioni a tutti coloro che intrattengono rapporti con la stessa (quali i membri del Consiglio di Amministrazione, del Collegio Sindacale e dell'Organismo di Vigilanza, i dipendenti di ogni grado, qualifica, livello, a tempo indeterminato o determinato, gli stagisti, i lavoratori interinali e assimilabili e i terzi in genere che intrattengano rapporti negoziali) per comunicare, seguendo le procedure aziendali definite, qualsiasi situazione che, anche solo potenzialmente, possa generare un conflitto di interessi, mitigare la situazione di un conflitto identificato e/o evidenziare la non completa efficacia dei presidi e delle misure di gestione istituiti da Sisal.

Rispetto dei diritti umani e non discriminazione

Sisal ha adottato una **Human Rights & Anti-Discrimination Policy** allineata con i maggiori accordi internazionali sul tema, quali la Dichiarazione Universale dei Diritti Umani, la Dichiarazione dell'Organizzazione Internazionale del Lavoro sui principi e i diritti fondamentali nel lavoro e i principi del Global Compact delle Nazioni Unite. La policy si applica a tutti i dipendenti di Sisal, qualunque sia il Paese in cui lavorano e lo statuto contrattuale adottato.

Promuoviamo i **principi di diversità, equità e inclusione e il diritto a condi-**

zioni di lavoro rispettose della persona e della sua dignità, garantendo:

- i diritti umani di base, un salario minimo ed equo, orari e condizioni di lavoro sostenibili, piena accessibilità sia dei luoghi che degli strumenti di lavoro, il contrasto al lavoro minorile (verificando l'età prima dell'assunzione) o forzato;
- l'integrità fisica e psicologica e l'individualità di ciascuno;
- il contrasto a tutte le forme di comportamento che si traducono in molestie o discriminazioni in relazione a sesso, età, disabilità, nazionalità, orientamento sessuale, etnia, religione, opinioni politiche e altre forme di diversità individuale;
- il diritto di espressione, di partecipazione a organizzazioni per la difesa e la promozione degli interessi di ciascuna persona, di rappresentazione da parte di sindacati o da altre forme elette in conformità alle legislazioni e alle prassi in vigore nei vari Paesi in cui operiamo.

Per questo abbiamo istituito canali dedicati per l'ascolto, dai meccanismi di segnalazione e reclamo, alle **survey periodiche** (survey sulla DE&I, NPE, Culture survey), ma siamo altresì consapevoli che l'assenza di segnalazioni non significhi assenza di potenziali problematiche e per questo agiamo proattivamente per cogliere in anticipo i bisogni specifici e le situazioni di rischio.

Segnalazione delle violazioni

Il management e **tutti i dipendenti Sisal sono incoraggiati e tenuti a segnalare** qualsiasi condotta, anche omissiva, che costituisca o possa costituire **una violazione o induzione ad una violazione di leggi e regolamenti**, nonché dei **valori e principi sanciti dal Codice Etico e di comportamento di Sisal, dal Modello 231 e dalle policy e procedure aziendali.**

Tutto il personale Sisal riceve formazione specifica e comunicazioni periodiche in merito a che cosa può essere segnalato e quali sono i canali che possono essere utilizzati per fare segnalazioni. Abbiamo inoltre messo a disposizione di dipendenti e soggetti esterni la **Piattaforma Speak Up!** per la ricezione e la gestione delle segnalazioni, disponibile in tutte le lingue parlate nel Gruppo[33], gestita da una terza parte in ottica di garanzia di indipendenza.

Inoltre, al fine di rafforzare la fiducia e la partecipazione al contrasto di condotte illecite, Sisal fornisce la **possibilità di segnalare** comportamenti legati a **frodi interne, scorretto trattamento dei dipendenti** (e.g. discriminazione, mobbing, molestie, ritorsioni), **salute e sicurezza sul luogo di lavoro, corruzione, conflitto di interessi, falsificazione di documenti, salvaguardia dei beni aziendali** (e.g. uso illecito di beni o informazioni aziendali), oppure **violazioni della privacy, sicurezza dei sistemi informativi**, integrità dell'organizzazione in materia fiscale, ecc[34].

I canali di segnalazione sono **sempre disponibili e gestiti da organi indipendenti**, quali l'**Organismo di Vigilanza** e il **Comitato Segnalazioni** (formato dall'Internal Audit Director e dal Chief Risk and Compliance Officer), che si occupano di ricevere e gestire le segnalazioni che vengono ricevute.

Indipendentemente dal canale di segnalazione utilizzato, è **sempre garantita la tutela e la riservatezza dell'identità del segnalante e del segnalato**, trattandone

[33] La piattaforma è disponibile al seguente link: https://sisal.integrityline.com/frontpage. Le segnalazioni possono essere inviate anche per posta all'indirizzo: "Servizio Segnalazioni" Via Ugo Bassi, 6 - 20159 Milano.
[34] Qualora la segnalazione risulti essere, per dolo o colpa grave, falsa, infondata e/o effettuata al solo scopo di danneggiare chi viene segnalato, ovvero volta a denunciare situazioni di natura esclusivamente personale ed estranee al perimetro delle previsioni di legge, la stessa non verrà presa in considerazione. Nei casi più gravi (e.g. dolo nella falsità della segnalazione), la condotta posta in essere potrà essere oggetto di procedimento disciplinare.

i dati in conformità alla legge e adottando ogni utile misura. **Sisal accetta segnalazioni anonime**.

Allo stesso tempo, Sisal vieta e sanziona atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

Nel 2022 Sisal ha ricevuto 47 segnalazioni, di cui 4 con rilevanza rispetto al Decreto Legislativo 231 (principalmente violazione Codice Etico e procedure aziendali – 2 concluse e 2 ancora in fase di analisi). Le segnalazioni firmate sono state 44 (su 3 caselle di segnalazioni) e 3 anonime sulla nuova piattaforma. Una sola segnalazione ha portato a provvedimenti disciplinari verso dipendenti di Sisal.

Contrasto al riciclaggio e al finanziamento del terrorismo

Per Sisal è una priorità assicurare l'efficacia e la tempestività delle attività di controllo e verifica dell'adeguatezza dei sistemi di prevenzione e contrasto al gioco illegale e del riciclaggio di denaro, nonché la prevenzione e la lotta al finanziamento al terrorismo. Per questo disponiamo di un articolato sistema di policy e procedure per tutto il Gruppo societario. La **Policy di gruppo** definisce la struttura e l'organizzazione della Funzione Anti-Money Laundering di Gruppo, con responsabilità, ruoli e funzioni, nonché le regole generali alle quali devono attenersi tutte le società, italiane e sussidiarie estere, per prevenire i fenomeni di riciclaggio e finanziamento del terrorismo. La Policy viene poi declinata nelle **singole procedure ed istruzioni operative**, distinte e specifiche per le singole entity, tenendo conto anche delle caratteristiche e dei requisiti nazionali.

In linea con il concetto di **risk-based approach** e al fine di adempiere agli obblighi normativi di riferimento, Sisal svolge l'**attività di adeguata verifica utilizzando appositi sistemi automatizzati, sviluppati internamente sulla base dello specifico know-how di settore, oltre a database forniti da provider esterni**. Tali sistemi consentono, tra le altre attività, di effettuare un attento **screening reputazionale** su giocatori e compagini societarie di gestione della rete dei negozi di gioco al fine di verificare - sia in fase di prima contrattualizzazione che nel continuo - il **mantenimento dei requisiti reputazionali previsti della normativa**.

Le attività di **transaction-monitoring e profilazione della clientela**, nonché la conservazione della documentazione, vengono realizzate mediante l'**utilizzo di sistemi sviluppati internamente e "customizzati" sulle peculiarità del mondo del gaming**. In particolare, lo **strumento di transaction-monitoring** consente di monitorare le operazioni di gioco al fine di identificare movimentazioni da attenzionare e, laddove necessario, attivare il processo di segnalazione di operazione sospetta da inviare alle Autorità competenti.

Parte imprescindibile del sistema di controllo interno **è quella di formazione. La formazione obbligatoria è rivolta a tutti i dipendenti** (nuovi e già esistenti) **e collaboratori, compreso il personale dei punti vendita**, al fine di accrescere la **consapevolezza dei rischi** di riciclaggio e finanziamento del terrorismo, la conoscenza di base della **normativa antiriciclaggio**, essendo peraltro informati sulle procedure interne e su come riconoscere e trattare potenziali transazioni o attività sospette.

Data Ethics

Nell'ambito della definizione delle finalità e delle modalità di trattamento dei dati personali effettuati, Sisal ha adottato una serie di principi di **Data Ethics** a supporto e garanzia di un processo decisionale ispirato ai massimi valori di etica nella conduzione del business. In particolare, Sisal valorizza e garantisce il rispetto di tali valori applicando i seguenti principi:

- **Accountability:** Sisal ha adottato un modello di governance volto a monitorare il presidio, il commitment e le responsabilità e rafforzare l'etica, la conformità e la sostenibilità dei propri prodotti e servizi, che sono sempre disegnati e implementati nel rispetto dei requisiti normativi applicabili in ottica di *privacy by design* al fine di garantire misure adeguate in termini di protezione dei dati personali.
- **Etica & Fairness:** Sisal adotta pratiche eque e corrette nei confronti dei clienti, il cui obiettivo è minimizzare le discriminazioni, i trattamenti penalizzanti o non imparziali.
- **Privacy:** Sisal tratta i dati personali dei clienti nel rispetto dei principi e delle normative in materia di privacy, garantendone la minimizzazione, la limitazione della conservazione, l'uso per finalità specifiche, determinate e trasparenti e il controllo in qualsiasi momento.
- **Qualità & accuratezza:** Sisal persegue un elevato livello di qualità dei dati in termini di accuratezza, esattezza e aggiornamento, adottando tutte le misure per consentirne la cancellazione o la tempestiva rettifica.
- **Trasparenza:** Sisal garantisce un elevato livello di trasparenza e chiarezza circa le modalità, la tipologia e le finalità della raccolta e del trattamento dei dati personali sui canali, prodotti e servizi erogati alla clientela.
- **Data sharing responsabile:** Sisal garantisce che siano implementate le misure tecniche e organizzative necessarie ad assicurare l'adeguatezza alla normativa e proteggere i dati personali trattati anche dalle terze parti che agiscono in nome e per conto di Sisal.

Alla luce dei principi di Data Ethics definiti, Sisal ha adottato specifici presidi privacy, organizzati in tre principali linee d'intervento:

Eminence & Strategy

Awareness e training: sono svolte almeno annualmente attività di formazione e awareness dedicate al personale dipendente e alle terze parti, il cui scopo è accrescere la sensibilità sulle tematiche inerenti alla protezione dei dati, attuare un modello di compliance diffusa e garantire il corretto governo, dal punto di vista Privacy e Data Ethics, dei processi aziendali.

Control framework: un continuo monitoraggio è attuato tramite controlli di secondo livello ai principi generali riferiti, in ambito Privacy & Data Ethics, a liceità, trasparenza, correttezza, minimizzazione dei dati, limitazione della conservazione, accountability del titolare.

Transparency: redazione di informative e pagine pubbliche dedicate a illustrare il commitment e la mission perseguita dal Gruppo Sisal su Privacy e Data Ethics e per gestire in maniera efficace le richieste di esercizio dei diritti da parte degli interessati.

Cookie management e cookie compliance: Sisal ha adottato un processo di implementazione e monitoraggio della conformità alle normative vigenti in materia di cookie sui siti web e app mobile di Sisal.

Privacy & Accountability

Modello di Governance: Sisal si è dotata di un modello di governance interno che costituisce un presidio capillare a garanzia della protezione dei dati personali in stretta connessione con l'attività di business, individuando i ruoli e le responsabilità dei soggetti coinvolti nel garantire la conformità dei trattamenti dei dati personali alla normativa applicabile, in primis al Regolamento (UE) 2016/679 (GDPR), e nel migliorare il commitment e la consapevolezza aziendale in questo ambito. È stato nominato, inoltre, il Responsabile della Protezione dei Dati Personali (DPO), con il compito di fornire consulenza al titolare del trattamento, anche in merito alla valutazione d'impatto sulla protezione dei dati, e verificare l'allineamento dei processi interni alla legislazione vigente sul trattamento dei dati personali.

Policy e procedure: per garantire il rispetto dei requisiti di privacy derivanti dalla normativa applicabile, Sisal ha predisposto e mantiene aggiornate policy e procedure in materia di Privacy & Data Ethics.

Registro dei trattamenti: gestione del processo di aggiornamento e monitoraggio del registro dei trattamenti al fine di garantire il tracciamento delle attività svolte da Sisal sui dati personali trattati.

Esercizio dei diritti degli interessati: Sisal ha definito un processo per la ricezione e il tempestivo riscontro delle richieste di esercizio dei diritti pervenute dagli interessati.

Privacy by design e by default: Sisal ha adottato una checklist per la valutazione dei presidi di privacy "by design" e "by default" nel caso di nuove iniziative, servizi o prodotti.

Data Protection Impact Analysis: Sisal ha adottato una metodologia di analisi del rischio e valutazione d'impatto sui trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati in linea con la metodologia aziendale adottata e con la definizione delle misure di sicurezza adeguate alla riduzione del rischio.

Responsible Data Sharing

Gestione contrattuale delle terze parti: gestione delle terze parti coinvolte nel trattamento dei dati personali, con predisposizione e negoziazione delle clausole di privacy nei contratti e degli accordi di data protection, nonché verifica delle garanzie prestate dalla terza parte.

Monitoraggio delle terze parti: monitoraggio continuo del livello di compliance privacy delle terze parti mediante esecuzione di audit periodici su stakeholder selezionati che trattano dati personali per conto di Sisal al fine di garantire il rispetto, da parte degli stessi, dei requisiti di privacy e security e quindi il corretto trattamento dei dati personali lungo tutta la filiera.

Formazione: organizzazione e gestione di training periodici dedicati alle terze parti, customizzati sui processi gestiti dalle stesse in nome e per conto di Sisal, così da garantire la conoscenza dei processi aziendali e delle procedure da seguire, nonché dei requisiti normativi applicabili.

Security

Per Sisal la protezione del patrimonio informativo aziendale e la gestione dei rischi ICT e di sicurezza sono obiettivi di primaria importanza.

Sisal identifica la **protezione del patrimonio informativo aziendale e la gestione dei rischi ICT e di sicurezza** (inclusi i rischi Cyber) come obiettivi di primaria importanza e si impegna per il loro perseguimento in un'ottica di miglioramento continuo.

In particolare, la **Cybersecurity** è un fattore abilitante per il perseguimento degli obiettivi aziendali. A fronte del trend crescente del numero e della gravità di attacchi informatici negli ultimi anni e con l'obiettivo di rafforzare continuamente i presidi di protezione e tutelare la sicurezza nell'ambito dei servizi offerti alla propria clientela, abbiamo definito una **strategia di cybersecurity** basata sui seguenti principi:

- garantire una **security governance centrale** volta a preservare riservatezza, integrità e disponibilità del patrimonio informativo aziendale;
- promuovere lo sviluppo e la continua evoluzione delle **soluzioni tecnologiche di sicurezza**, per assicurare a Sisal un vantaggio sostenibile, duraturo nel tempo e in linea con gli obiettivi e i valori aziendali;
- favorire la costituzione di un adeguato **modello organizzativo per la gestione della sicurezza delle informazioni** in linea con gli obiettivi di crescita aziendale e promuovere lo sviluppo delle competenze al fine di mantenere efficaci i presidi di protezione;
- garantire il **rispetto delle leggi, dei regolamenti e delle normative** applicabili con impatti sulla sicurezza delle informazioni, nonché degli accordi contrattuali specifici con i vari stakeholder;
- promuovere l'**innovazione nell'ambito della sicurezza** al fine di garantire un costante allineamento con l'evoluzione tecnologica e l'impiego di metodi, processi e soluzioni di nuova generazione;
- garantire la **sicurezza, la resilienza e la protezione dei dati** nell'ambito dei servizi offerti ai consumatori e clienti in ottica di aumentarne l'affidabilità;

- diffondere, all'interno di Sisal, **cultura e awareness** su tematiche di sicurezza delle informazioni e sui rischi cyber al fine di aumentare il grado di consapevolezza in relazione a comportamenti e linee guida cui attenersi per evitare il concretizzarsi di minacce;
- promuovere l'adozione di un *approccio risk-based* in relazione all'adozione di misure di sicurezza tramite impiego di un framework integrato nel modello complessivo di gestione dei rischi aziendali.

La strategia di cybersecurity di Sisal si basa sulle seguenti aree:

Security governance

Il presidio sulle tematiche di cybersecurity ha l'obiettivo di mantenere livelli di maturità adeguati al contesto di riferimento e allineati con l'evoluzione degli scenari di rischio. Il Chief Information Security Officer (CISO) assicura una visione strategica e il miglioramento costante dei processi volti a mitigare i rischi a cui siamo soggetti. A tale scopo, il CISO e la sua struttura operano in maniera sinergica con il Management, le funzioni di Business e Mercati, la funzione HR, l'Audit Interno e Risk Management, nonché l'area di Compliance. I principali ambiti di intervento sono relativi a:

- **Rafforzamento della struttura organizzativa di Security:** in linea con la crescita dell'organizzazione e con l'espansione del business in mercati internazionali, Sisal ha adeguato il dimensionamento della funzione di Security e inserito nuove figure professionali per rafforzare la gestione dei presidi di sicurezza.
- **Certificazioni di sicurezza:** Sisal ha implementato e mantiene nel tempo un Sistema di Gestione della Sicurezza delle Informazioni che recepisce gli indirizzi espressi dai principali standard e normative di settore, incluse le norme internazionali ISO27001 e WLA-SCS[35]. Nel corso del 2022, per migliorare ulteriormente i presidi atti a garantire la resilienza del business, abbiamo conseguito la certificazione ISO22301, relativa alla gestione della continuità operativa[36]. Inoltre, Sisal ha conseguito e mantiene nel tempo la certificazione ISS SGAD (Information Systems Security - Sistema di Gioco di Abilità a Distanza) – ovvero la certificazione della piattaforma di gioco richiesta dalla Direzione Centrale Gestione Tributi e Monopolio Giochi, Ufficio Gioco a distanza (Sisal Entertainment S.p.A.). La compliance dei sistemi di gestione viene verificata da parte di enti indipendenti attraverso audit e controlli periodici.
- **Security Framework:** al fine di definire i requisiti di sicurezza, declinarli nell'ambito dei processi e verificarne l'efficacia, Sisal ha sviluppato e mantiene nel tempo un framework di policy, procedure, linee guida, costantemente aggiornato. Il framework è corredato da controlli di primo, secondo e terzo livello e da opportuni indicatori per il monitoraggio continuo.
- **IT & Cyber Risk management:** le valutazioni del rischio ricoprono un ruolo fondamentale nella definizione degli obiettivi e nell'indirizzamento delle misure di protezione. A tal fine Sisal ha definito un modello di gestione dei rischi ICT e Cyber che prevede la valutazione e il monitoraggio dell'esposizione a tali rischi da parte dell'organizzazione e l'identificazione e attuazione delle relative azioni di mitigazione.

[35] Certificazione rilasciata dalla World Lottery Association, i cui controlli standard sono specifici per il settore del gioco e delle Lotterie internazionali. Il perimetro riguarda Sisal Lottery Italia S.p.A., Sisal Loterie Maroc, Sisal Sans.
[36] Il perimetro della certificazione ISO27001 è relativo a Sisal Lottery Italia S.p.A., Sisal Loterie Maroc, Sisal Sans. Il perimetro della certificazione ISO22301 è relativo a Sisal Lottery Italia S.p.A. e Sisal Entertainment S.p.A.

Cybersecurity culture

La diffusione all'interno dell'organizzazione di una adeguata cultura in merito ai rischi cyber e alle relative modalità di mitigazione è fondamentale per gli obiettivi strategici dell'azienda, da perseguire attraverso:

- **Security Awareness:** Sisal eroga continuativamente sessioni di awareness tramite diverse modalità di comunicazione e ne testa l'efficacia anche simulando scenari di attacco per verificare che l'organizzazione sia in grado di reagire adeguatamente.
- **Security Training:** le attività formative sono svolte a tutti i livelli gerarchici all'interno dell'organizzazione, inclusi i contractors, con focus differenziati in relazione ai ruoli. In particolare, nel 2022, sono state erogate sessioni di formazione specifiche sullo sviluppo sicuro del codice sorgente, dedicate ai team coinvolti nel ciclo di vita di sviluppo software, volte a evitare la presenza di vulnerabilità all'interno delle applicazioni e dei servizi erogati alla clientela.

Security enforcement

L'evoluzione tecnologica, la digitalizzazione dei servizi, l'adozione di servizi Cloud e l'evoluzione degli scenari di attacco cyber, sono alcuni degli elementi che Sisal ha considerato come driver per rafforzare la propria "security posture". Nel corso del 2022 sono state portate a termine iniziative afferenti ai seguenti ambiti:

- **Prevention:** Sisal ha effettuato investimenti per rafforzare le misure di sicurezza cyber tramite implementazione di soluzioni tecnologiche evolute. Particolare attenzione è posta al rafforzamento del sistema di controllo accessi e alle modalità di gestione delle identità, comprese quelle con accessi privilegiati, e alle misure di protezione dei dispositivi utilizzati dagli utenti per lo svolgimento delle proprie mansioni. Nell'ambito delle iniziative di prevention inoltre sono state migliorate le misure di protezione dei dati con tecniche di cifratura e anonimizzazione, e rafforzate le tecnologie per la gestione delle vulnerabilità, perseguendo un approccio basato sul rischio; inoltre, sono continuamente condotte attività di security test, sia innescate nei cicli di sviluppo software sia estemporanee sui sistemi critici, e audit periodici interni ed esterni condotti con frequenza almeno annuale. Infine, è stata ulteriormente migliorata la pratica di Cyber Threat Intelligence al fine di prevenire il più possibile eventuali attacchi cyber o eventi che possono condurre a impatti negativi sul brand Sisal.
- **Detection & Response:** gli investimenti in tecnologie di sicurezza sono stati impiegati anche con l'obiettivo di aumentare l'efficacia nelle fasi di identificazione e risposta a eventi e incidenti di sicurezza, rafforzando misure di protezione sia proattive che reattive. Particolare attenzione è costantemente rivolta ai servizi di gioco e, con l'obiettivo di rafforzare la capacità di identificazione tempestiva di tentativi di attacco o frode, sono state ampliate le funzionalità di monitoraggio e allarmistica di eventi o comportamenti anomali. Inoltre, sono state estese alcune funzionalità relative a soluzioni tecnologiche di sicurezza già presenti aumentando la copertura del perimetro sottoposto a monitoraggio e la capacità di rilevazione di eventi di sicurezza.
- **Resilience**: Vengono svolte periodicamente diverse attività di test per verificare che il sistema di gestione della continuità operativa sia efficace a fronte dei principali scenari di indisponibilità, anche attraverso *penetration test* gestiti con il supporto di terze parti.

Gestione responsabile della catena di fornitura

Le nostre sfide di sostenibilità devono essere condivise anche da tutti coloro che fanno parte della comunità di Sisal in senso più ampio, dai fornitori fino ai diversi punti vendita, per poter perseguire una sostenibilità di medio-lungo termine. Ci impegniamo quindi a **promuovere la nostra strategia di sostenibilità lungo tutta la filiera**.

I nostri fornitori

Siamo cresciuti e ci siamo rafforzati come azienda grazie alla costruzione di una rete di **partnership strategiche** con numerosi **fornitori**, rigorosamente selezionati in virtù delle migliori competenze specialistiche disponibili sul mercato, nonché sulla base dei nostri obiettivi e valori: **legalità, etica di impresa, lealtà, correttezza, trasparenza e meritocrazia**. Nello specifico, ci avvaliamo complessivamente di oltre **1.700 fornitori**[37].

[37] Il numero dei fornitori comprende il perimetro Italia e sue controllate estere.

Tipologie di forniture

Terminali di gioco, Materiali di gioco, Servizi logistici e di trasporto, Servizi di installazione e manutenzione HW, Servizi di Call Center, Media, Eventi, Marketing, Creatività e Ricerche di mercato, Servizi di comunicazione voce e Trasmissione dati, Hardware e software, Piattaforme di gioco, Servizi di consulenza e Servizi professionali, Appalti di ristrutturazione, Servizi alla persona e agli edifici-punti vendita, Food & beverage, Sisal Television, Servizi di Data Center.

Lo sviluppo internazionale degli ultimi anni ha portato all'**internazionalizzazione delle procedure di acquisto** volte all'ottenimento delle migliori condizioni contrattuali per l'approvvigionamento delle nostre filiali estere. In un'ottica di consolidamento e miglioramento continuo delle procedure, i team esteri dedicati agli acquisti sono affiancati costantemente dalla **funzione Procurement centrale**, al fine di supervisionare e supportare l'acquisizione dei prodotti e servizi.

Come avviene per il mercato italiano, la **funzione International Procurement** vigila su tutte le **attività negoziali** relative alla supply chain di ogni filiale estera. Queste comprendono: lo scouting di nuovi fornitori, il sourcing che include la preparazione della documentazione di gara, la valutazione delle offerte ricevute, la selezione e la contrattualizzazione del fornitore aggiudicatario ed infine la contrattualizzazione fino al caricamento dei contratti sulla piattaforma acquisti.

Il processo di valutazione e qualifica

Riserviamo una particolare attenzione al processo di **valutazione** e **qualifica** dei fornitori attraverso il nostro Sistema di Gestione Qualità, che richiede loro il rispetto dei requisiti richiesti dagli aggiornamenti normativi del settore del gioco e delle aspettative dei nostri stakeholder.

A tutti i nostri fornitori viene richiesta attraverso una specifica clausola l'**osservanza** delle norme e dei principi del **Codice Etico e di Comportamento**, tra cui **l'obbligo di operare in linea con i nostri standard etici** in materia di diritti dei lavoratori, di tutela dell'ambiente e di tutela della salute e sicurezza del personale e dei luoghi di lavoro. Disponiamo di sistemi di controllo per la **prevenzione della corruzione** secondo lo standard UNI ISO 37001:2016. Nei processi di acquisto teniamo conto, inoltre, delle caratteristiche che devono avere servizi, facility e strumenti per garantire la piena accessibilità, fruibilità o adoption a tutti, in linea con il nostro impegno per l'inclusione delle persone con disabilità[38].

La valutazione dei fornitori si basa sulla **conformità** a quanto previsto da contratti e ordini e sul **monitoraggio** degli scostamenti tra i **livelli di servizio concordati** e i livelli di servizio effettivamente erogati, nonché il rispetto dei tempi di consegna, della qualità, dei costi e delle altre specifiche contrattuali. Tali controlli ci consentono di condurre un'analisi globale del fornitore e di calcolare semestralmente l'**Indice di Vendor Rating (IVR)**, che indica la performance globale del fornitore, individuando opportunità di miglioramento.

[38] Per maggiori dettagli si rimanda alla policy sui diritti umani e sulla non discriminazione.