

Bilancio di Sostenibilità

2025



CYBEROO

Indice

LETTERA AGLI STAKEHOLDER	4
NOTA METODOLOGICA.....	7
1. IDENTITÀ E STRATEGIA.....	10
2. IL 2025 IN SINTESI - HIGHLIGHTS	54
3. GOVERNANCE.....	62
4. CAPITALE INFRASTRUTTURALE.....	69
5. CAPITALE RELAZIONALE	88
6. CAPITALE ECONOMICO - FINANZIARIO.....	126
7. CAPITALE UMANO.....	132
8. CAPITALE AMBIENTALE.....	147
9. GRI CONTENT INDEX.....	154

LETTERA AGLI STAKEHOLDER

CYBEROO INTENDE CONTINUARE A SVOLGERE IL PROPRIO RUOLO CON RESPONSABILITÀ, INVESTENDO IN RICERCA, INNOVAZIONE, QUALITÀ DEI SERVIZI, COMPETENZE E RELAZIONI DI FIDUCIA, NELLA CONSAPEVOLEZZA CHE LA SICUREZZA DIGITALE RAPPRESENTI UNA CONDIZIONE ABILITANTE PER LO SVILUPPO SOSTENIBILE DELLE ORGANIZZAZIONI E DEI TERRITORI.

Fabio Leonardi
CEO

A handwritten signature in white ink, appearing to read 'Fabio Leonardi', is positioned below the printed name and title.

Lettera agli stakeholder

Agli stakeholder,

il quarto Bilancio di Sostenibilità del Gruppo Cyberoo rappresenta un momento di rendicontazione e di responsabilità nei confronti di tutti gli stakeholder. In un contesto caratterizzato da crescente complessità tecnologica, evoluzione normativa e centralità della resilienza digitale, il Gruppo conferma il proprio impegno nel perseguire un modello di crescita solido, innovativo e sostenibile, capace di generare valore nel tempo e di contribuire alla sicurezza dell'ecosistema economico e sociale in cui opera.

Nel periodo di rendicontazione, Cyberoo ha consolidato il proprio percorso industriale, raggiungendo circa 28 milioni di euro di ricavi e contando 177 dipendenti al 31 marzo 2026. A tali risultati si affianca un utile di Gruppo pari a 2.570.755 euro, espressione della capacità dell'azienda di sostenere lo sviluppo del business, preservare la redditività e rafforzare progressivamente la propria posizione nel mercato della cybersecurity. Si tratta di risultati che assumono particolare rilevanza perché confermano la solidità del modello operativo e la coerenza delle scelte strategiche intraprese.

L'esercizio ha segnato un'ulteriore evoluzione del posizionamento del Gruppo, sempre più orientato a una gestione integrata del rischio cyber. In questa prospettiva si inserisce ORBIS, framework proprietario che riunisce threat management, governance dei processi, compliance normativa e security awareness in un unico modello operativo. La sua definizione rappresenta un passaggio strategico rilevante, perché consente di rispondere in modo organico alla crescente complessità della sicurezza informatica, superando approcci frammentati e offrendo alle imprese un presidio più completo, continuo e misurabile.

Innovazione e sostenibilità costituiscono direttrici strutturali del percorso di Cyberoo. La nascita di Keatrix, piattaforma proprietaria di Human Risk & Security TrAlning, testimonia la volontà del Gruppo di intervenire su una delle dimensioni più critiche della sicurezza informatica: il fattore umano. Con Keatrix, Cyberoo affianca alla protezione tecnologica lo sviluppo delle competenze delle persone: attraverso tecnologie avanzate e sistemi adattivi, la piattaforma supporta percorsi

di consapevolezza cyber personalizzati e continuativi, orientati alla misurabilità delle competenze, con strumenti che consentono alle organizzazioni di monitorare l'apprendimento e accompagnare l'evoluzione dei comportamenti. In questo modo Cyberoo intende contribuire allo sviluppo di comportamenti più consapevoli e alla riduzione del rischio operativo nelle organizzazioni clienti.

Il Bilancio evidenzia inoltre un percorso di sostenibilità più maturo e strutturato. L'aggiornamento dell'analisi di materialità ha individuato nove temi prioritari, che orientano il sistema di rendicontazione e le scelte del Gruppo: generazione e distribuzione di valore economico e finanziario, ricerca e innovazione tecnologica, privacy e sicurezza dei dati, qualità delle relazioni con i clienti, condizioni di lavoro e welfare aziendale, formazione e sviluppo delle competenze, salute e sicurezza sul lavoro, supporto alle comunità locali ed efficienza energetica. Tali temi riflettono le aspettative degli stakeholder e rafforzano il legame tra strategia, governance e impatti generati.

La centralità delle persone rappresenta un elemento qualificante di questo percorso. La crescita dell'organico, l'investimento nella formazione, le iniziative di welfare e il rafforzamento dei presidi in materia di salute e sicurezza confermano l'impegno del Gruppo nel costruire un contesto professionale fondato su competenze, responsabilità e collaborazione. Allo stesso tempo, il dialogo con clienti, partner, istituzioni, università, associazioni e comunità locali costituisce una leva essenziale per generare valore condiviso e diffondere una cultura della cybersecurity sempre più consapevole e accessibile.

La cybersecurity è oggi una componente essenziale della governance aziendale, della continuità operativa e della capacità delle imprese di affrontare scenari di rischio in costante evoluzione. Cyberoo intende continuare a svolgere il proprio ruolo con responsabilità, investendo in ricerca, innovazione, qualità dei servizi, competenze e relazioni di fiducia, nella consapevolezza che la sicurezza digitale rappresenti una condizione abilitante per lo sviluppo sostenibile delle organizzazioni e dei territori.

A nome del Gruppo Cyberoo, desidero rivolgere un ringraziamento a tutti gli stakeholder che accompagnano il nostro percorso: dipendenti, clienti, partner, investitori, istituzioni e comunità. Il loro contributo, la loro fiducia e il confronto continuo rappresentano un patrimonio fondamentale per proseguire nella

costruzione di un modello di crescita responsabile, orientato alla creazione di valore e alla tutela del futuro digitale.

Fabio Leonardi

CEO

Nota Metodologica

Il presente documento rappresenta il quarto Bilancio di sostenibilità del Gruppo Cyberoo (d'ora in poi anche "il Gruppo" o "Cyberoo"). Il documento contiene le informazioni relative ai temi economici, ambientali e sociali, utili ad assicurare la comprensione delle attività svolte da Cyberoo del suo andamento, dei suoi risultati e dell'impatto prodotto dalle stesse.

La redazione del presente Bilancio è, al momento, un esercizio di natura volontaria per il Gruppo e tiene conto dei principi generali degli Standard GRI (Global Reporting Initiative) — rilevanza, completezza, accuratezza, equilibrio, comparabilità, chiarezza, tempestività e affidabilità — compatibilmente con l'opzione di rendicontazione '*with reference*' adottata.

Gli indicatori di performance selezionati sono quelli previsti dagli standard di rendicontazione adottati, rappresentativi degli specifici ambiti di sostenibilità analizzati e coerenti con l'attività svolta da Cyberoo e gli impatti da essa prodotti. La selezione di tali indicatori è stata effettuata sulla base di un'analisi di rilevanza degli stessi, come descritto nel paragrafo "**Analisi di materialità**". Nelle diverse sezioni del Bilancio di sostenibilità, sono segnalate le informazioni quantitative per le quali è stato fatto ricorso a stime.

Il perimetro di rendicontazione dei dati e delle informazioni qualitative e quantitative si riferisce alle performance del Gruppo Cyberoo al 31 marzo 2026, che include la capogruppo Cyberoo S.p.A. e le società controllate Cyberoo51 S.r.l., Cyberoo Docetz S.r.l., Cyberoo PL Sp. z.o.o. (società di diritto polacco), Cyberoo UA LLC (società di diritto ucraino, controllata al 100% da Cyberoo51 S.r.l.), Cyberoo AL Sh.p.k. (società di diritto albanese) e Cyberoo Keatrix UA LLC (società di diritto ucraino), queste ultime due acquisite nel corso dell'esercizio a seguito della delibera del Consiglio di Amministrazione del 17 giugno 2025. Si segnala che, in data 22 luglio 2025, è stata perfezionata la fusione per incorporazione di MFD International S.r.l. nella capogruppo Cyberoo S.p.A. Cyberoo Capital S.r.l., società interamente controllata costituita nel dicembre 2025 e caratterizzata alla data di chiusura da poco più di tre mesi di operatività, non è inclusa nel perimetro di consolidamento dell'esercizio chiuso al 31 marzo 2026, in considerazione della

recente costituzione, del periodo di operatività limitato e della limitata significatività complessiva dei relativi dati nel contesto del Gruppo.

Il Bilancio di sostenibilità è redatto con cadenza annuale. Per il presente esercizio, il periodo di rendicontazione copre eccezionalmente 15 mesi, dal 1° gennaio 2025 al 31 marzo 2026. Tale estensione è conseguenza della modifica della data di chiusura dell'esercizio sociale del Gruppo, ora fissata al 31 marzo; coerentemente, il medesimo arco temporale di 15 mesi è adottato anche nel bilancio d'esercizio 2025. Al fine di permettere il confronto dei dati nel tempo e la valutazione dell'andamento delle attività di Cyberoo sono presentati, a fini comparativi, i dati relativi ai due esercizi precedenti. Si segnala che eventuali scostamenti dei dati rispetto agli esercizi precedenti possono derivare, almeno in parte, dalla maggiore ampiezza del periodo di rendicontazione (15 mesi anziché 12): tale differenza va pertanto tenuta in considerazione nella lettura e nel confronto con le annualità pregresse.

Il processo di redazione dell'informativa di sostenibilità ha visto il coinvolgimento dei responsabili delle diverse funzioni del Gruppo.

Il Bilancio di sostenibilità è stato approvato dal Consiglio di Amministrazione di Cyberoo S.p.A. in data 19/10/2026 e non è stato assoggettato a revisione da parte di un revisore indipendente.

Il Bilancio di sostenibilità è pubblicato nel sito istituzionale della Società al seguente indirizzo: www.cyberoo.com.

Per richiedere maggiori informazioni in merito è possibile rivolgersi all'indirizzo: sustainability@cyberoo.com.



Capitolo 1
**IDENTITÀ
E STRATEGIA**

1. Identità e strategia

Il Gruppo Cyberoo opera nel mercato dell'Information Technology con un'offerta articolata di servizi e soluzioni tecnologiche a supporto della sicurezza, della continuità operativa e dell'evoluzione digitale delle imprese. Il perimetro consolidato del Gruppo integra competenze specialistiche in ambito cybersecurity, managed services, digital transformation, data protection, sviluppo software e applicazioni basate su intelligenza artificiale, con l'obiettivo di accompagnare le organizzazioni nella gestione di ecosistemi IT sempre più complessi e interconnessi.

All'interno di questo perimetro, la cybersecurity rappresenta il principale ambito di specializzazione e il driver strategico più distintivo del Gruppo. Attraverso Cyberoo S.p.A. e le società controllate, il Gruppo affianca le imprese nella protezione degli asset informativi, nel monitoraggio continuativo delle minacce, nella governance dei processi di sicurezza, nella gestione della compliance e nello sviluppo della consapevolezza cyber delle persone.

Il posizionamento della Capogruppo trova oggi sintesi in ORBIS, framework proprietario che integra in un unico modello operativo le principali dimensioni del cyber risk management: threat management, governance dei processi, compliance normativa e regolatoria e security awareness. ORBIS rafforza il ruolo di Cyberoo come operatore specializzato nella gestione integrata del rischio cyber, senza esaurire il perimetro di attività del Gruppo, che continua a comprendere anche servizi gestiti, digital transformation, data protection e sviluppo di soluzioni tecnologiche.

In questa prospettiva, il Gruppo si propone come partner tecnologico per le imprese, in particolare del segmento mid-market, mettendo a disposizione un ecosistema di competenze complementari: da un lato, soluzioni e servizi avanzati di cybersecurity; dall'altro, capacità progettuali e operative a supporto della digitalizzazione, dell'efficienza dei processi, della gestione infrastrutturale e dell'innovazione applicativa.

La strategia del Gruppo è orientata alla creazione di valore attraverso innovazione, qualità dei servizi, sviluppo di tecnologie proprietarie e rafforzamento delle

competenze interne. L'obiettivo è supportare le imprese nella protezione e valorizzazione del patrimonio informativo, nella riduzione della complessità operativa e nella costruzione di modelli digitali più sicuri, resilienti e sostenibili.

I servizi offerti dal Gruppo si articolano in tre principali linee di business: Cyber Security & Device Security, Managed Services e Digital Transformation.

Le dimensioni

Il Gruppo Cyberoo ha realizzato ricavi per circa 28 milioni di euro e conta, nelle proprie sedi, un numero complessivo di 177 dipendenti (al 31 marzo 2026).

Ricavi per Industry (milioni di euro)	2023		2024		2025	
	Ricavi	%	Ricavi	%	Ricavi	%
Cyberoo S.p.A.	18,17	80,0%	20,98	80,33%	25,35	76,41
Cyberoo51 S.r.l.	2,64	11,6%	2,94	11,26%	5,51	16,60
Cyberoo Capital S.r.l.	-	-	-	-	0,56	1,68
Cyberoo Docetz S.r.l.	0,99	4,4%	1,21	4,63%	1,76	5,31
Cyberoo PL SP. ZO.O.	-	-	-	-	-	-
Totale*	22,70	100%	26,12	100%	33,18	100%

*Importo al lordo delle fatture Intercompany

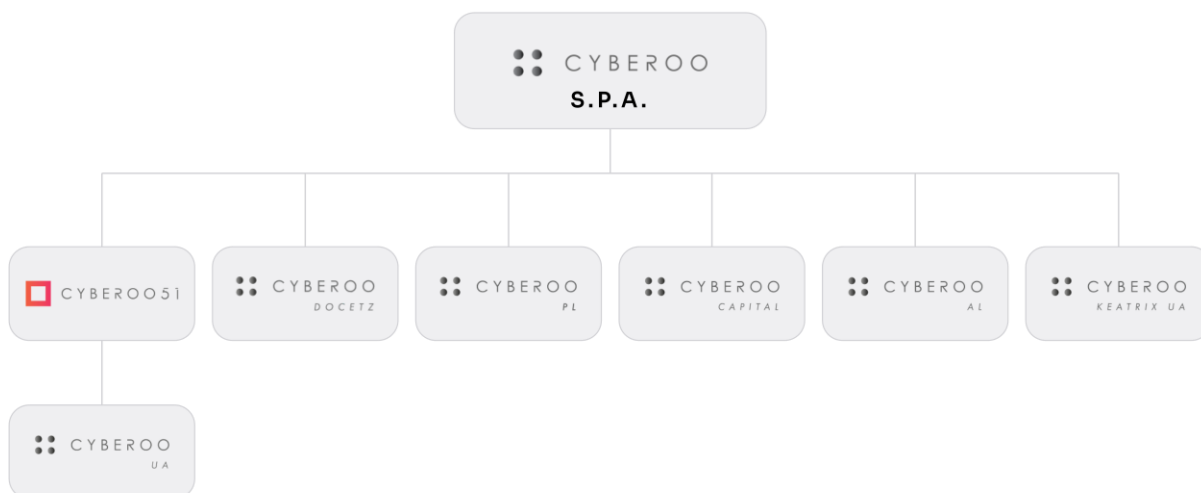
Ricavi per tipologia di servizio (milioni di euro)	2023		2024		2025	
	Ricavi	%	Ricavi	%	Ricavi	%
Cyber Security & Device Security	15,48	77,4%	17,97	78,7%	22,34	80,6%
Managed Services	4,37	21,8%	4,70	20,6%	5,17	18,6%
Digital Transformation	0,16	0,8%	0,16	0,7%	0,19	0,8%
Totale	20,01	100%	22,83	100%	27,71	100%

*Importo ricavi consolidati al netto delle intercompany

Il Gruppo

Il Gruppo, con headquarter a Reggio Emilia e sedi operative in Italia e all'estero, opera nel settore dell'Information Technology ed è costituito, al 31 marzo 2026, da sette entità legali: la capogruppo Cyberoo S.p.A. e le controllate Cyberoo51 S.r.l., Cyberoo Docetz S.r.l., Cyberoo Capital S.r.l., Cyberoo PL Sp. z.o.o., Cyberoo UA LLC, Cyberoo AL Sh.p.k. e Cyberoo Keatrix UA LLC.

La struttura del Gruppo al 31 marzo 2026 è di seguito rappresentata:



TUTTE LE PARTECIPAZIONI SONO AL 100% DEL CAPITALE SOCIALE

Cyberoo UA LLC è interamente detenuta da Cyberoo51 S.r.l.

Cyberoo S.p.A. detiene una partecipazione pari al 100% del capitale sociale di Cyberoo51 S.r.l. (CYBEROO51), Cyberoo Docetz S.r.l., Cyberoo Capital S.r.l., Cyberoo PL Sp. z.o.o. (società di diritto polacco), Cyberoo AL Sh.p.k. (società di diritto albanese) e Cyberoo Keatrix UA LLC (società di diritto ucraino). Le partecipazioni albanese e ucraina sono state acquisite dalla controllante Cyberoo Globl S.p.A. nel corso dell'esercizio 2025, a seguito della delibera del Consiglio di Amministrazione del 17 giugno 2025. Occorre precisare che Cyberoo51 S.r.l. detiene l'intero capitale della società Cyberoo UA LLC (società di diritto ucraino).

Le attività di **Cyberoo S.p.A.** sono organizzate secondo il modello ORBIS, framework proprietario che integra in un unico ecosistema le principali dimensioni della gestione del rischio informatico, rappresentate da threat management, governance dei processi, compliance normativa e regolatoria e security awareness.

Cyberoo Docetz S.r.l.

Cyberoo Docetz è la società del Gruppo specializzata nell'erogazione di servizi di Cyber Security Advisory e consulenza avanzata in ambito cybersecurity, con focus sulla governance dei processi aziendali rilevanti per la sicurezza informatica. Attraverso attività di risk assessment, incident response, vulnerability assessment e penetration testing, supporta le organizzazioni nell'identificazione e mitigazione delle vulnerabilità, nella gestione degli incidenti di sicurezza e nel rafforzamento

della postura di sicurezza aziendale. La società offre inoltre servizi di Virtual Chief Information Security Officer (vCISO), affiancando le imprese nella definizione delle strategie di sicurezza e nella governance dei processi di cybersecurity.

Cyberoo51 S.r.l.

Cyberoo51, costituita nel 2014, è attiva nello sviluppo di soluzioni digitali e servizi di digital transformation, data protection e applicazioni basate su intelligenza artificiale a supporto dei processi aziendali.

Le attività della società si articolano nelle seguenti principali aree operative:

Data Protection

Cyberoo51 offre servizi e soluzioni a supporto della gestione e protezione dei dati aziendali, con particolare riferimento alla progettazione di sistemi orientati alla governance e alla sicurezza delle informazioni.

Digital Transformation

La società supporta i processi di trasformazione digitale delle imprese attraverso la progettazione e l'implementazione di soluzioni applicative, basate su un mix di servizi proprietari e tecnologie di terze parti, finalizzati alla digitalizzazione e all'ottimizzazione dei processi aziendali. Nell'ambito di tali attività rientrano anche servizi di digital marketing, comprensivi della definizione di strategie di comunicazione digitale, del supporto alle attività di web design e della realizzazione di piattaforme e soluzioni a supporto dei canali di vendita online.

Solutions

Riguarda lo sviluppo di soluzioni software proprietarie e piattaforme digitali, incluse applicazioni web e mobile, sistemi CRM e HRM, a supporto delle esigenze operative e organizzative delle imprese clienti.

Intelligenza Artificiale

L'area Intelligenza Artificiale comprende l'integrazione di tecnologie di AI all'interno delle soluzioni e dei servizi sviluppati dalla società. Le attività sono finalizzate al supporto dell'automazione dei processi, all'analisi dei dati e al miglioramento dell'efficienza operativa, con un approccio orientato a sicurezza, responsabilità e corretto utilizzo delle informazioni.

Cyberoo51 detiene una partecipazione pari al 100% del capitale sociale di **Cyberoo UA LLC**, società con sede nella città di Ternopil in Ucraina che svolge, per le società appartenenti al Gruppo, servizi nei seguenti settori: *cyber security management; networking management; service desk; backup management; antivirus; antispam; cloud service; IT consulting*.

Cyberoo Capital S.r.l. è una società controllata da Cyberoo costituita come veicolo specializzato per l'offerta di contratti di locazione evolutiva delle soluzioni e dei servizi di cybersecurity sviluppati dalla Capogruppo. La società opera con l'obiettivo di favorire l'adozione di modelli di utilizzo flessibili in logica OPEX da parte della clientela e di supportare lo sviluppo dei ricavi ricorrenti del Gruppo. In tale contesto, Cyberoo Capital consente la strutturazione di contratti di noleggio evolutivo aventi ad oggetto le soluzioni di cybersecurity di Cyberoo, rispondendo alla domanda di mercato per modelli di fruizione più flessibili rispetto all'acquisto tradizionale. In particolare, la società facilita l'adozione delle soluzioni tecnologiche, supportando le negoziazioni dei rivenditori quando emergono vincoli finanziari, resistenze all'investimento iniziale o preferenze per modelli di spesa operativa. A tal fine, la società non acquista direttamente da Cyberoo, ma da distributori o rivenditori autorizzati esterni al perimetro di consolidamento, rendendo disponibili ai clienti le soluzioni oggetto degli accordi. L'operatività della società è supportata dal Gruppo anche attraverso forme di finanziamento e garanzie, nei limiti delle politiche di rischio e delle valutazioni economico-finanziarie applicabili.

Cyberoo PL z.o.o

Cyberoo PL z.o.o rappresenta il polo polacco per le attività commerciali effettuate nel territorio, parallelamente, essa gestisce il secondo livello dell'i-SOC Cyberoo insieme alle molteplici figure dei cybersecurity specialists.

Cyberoo AL Sh.p.k.

Cyberoo AL Sh.p.k. è la società di diritto albanese acquisita dal Gruppo nel corso dell'esercizio 2025, a seguito della delibera del Consiglio di Amministrazione del 17 giugno 2025. La società è specializzata nella erogazione di servizi VNOC e sviluppo software.

Cyberoo Keatrix UA LLC

Cyberoo Keatrix UA LLC è la società di diritto ucraino acquisita dal Gruppo nel corso dell'esercizio 2025, a seguito della delibera del Consiglio di Amministrazione del 17 giugno 2025. La società è dedicata allo sviluppo delle attività connesse alla piattaforma Keatrix e al rafforzamento delle competenze in ambito security awareness e human risk management.

Storia, evoluzione e crescita

2008–2016 | Le origini, l'evoluzione MSSP e l'avvio della Ricerca & Sviluppo

La storia di Cyberoo ha inizio nel 2008, quando l'azienda avvia la propria attività nel settore IT, concentrandosi inizialmente nella vendita di device. Nel dicembre 2011 il percorso evolutivo prosegue con l'avvio delle attività di Device Management, segnando un primo passo verso una gestione strutturata e continuativa delle infrastrutture dei clienti. Fin dai primi anni, il contatto diretto con le organizzazioni e l'esperienza maturata nell'affrontare minacce reali consentono a Cyberoo di sviluppare una profonda conoscenza dei rischi informatici e delle esigenze concrete di sicurezza del mercato.

Negli anni Cyberoo amplia costantemente la propria offerta di servizi ed entro il 2015 si afferma come Managed Security Service Provider (MSSP), specializzandosi nella fornitura di servizi di sicurezza informatica gestiti.

Tra il 2015 e il 2016, dall'esperienza sul campo nasce un percorso strutturato di ricerca e sviluppo in cybersecurity, con l'obiettivo di sviluppare soluzioni tecnologiche proprietarie e servizi avanzati, capaci di rispondere in maniera innovativa alle sfide del settore.

Nel 2016 Cyberoo conduce un'analisi di mercato per individuare le aree più strategiche in cui estendere le proprie attività di ricerca. Da questa valutazione emerge l'Ucraina, riconosciuta per il suo forte patrimonio di competenze in ambito cybersecurity e per l'elevata specializzazione tecnica. Questa scelta segna l'avvio di un modello di sviluppo che integra esperienza operativa, ricerca internazionale e innovazione tecnologica, ponendo le basi per la crescita e l'evoluzione di Cyberoo.

2019 | Nasce Cyberoo e inizia una nuova era

Il 2019 segna un momento di svolta nella storia dell'azienda con la nascita del brand Cyberoo, espressione di un'identità rinnovata e di una visione strategica sempre più focalizzata sulla cybersecurity avanzata. Il rebranding rappresenta non solo un cambio di nome, ma l'evoluzione del modello di business: da Managed Security Service Provider a vendor di soluzioni proprietarie di cybersecurity, sviluppate internamente e pensate per rispondere in modo strutturato alle nuove minacce digitali.

Nello stesso anno Cyberoo lancia le prime piattaforme proprietarie, tra cui Cypeer (CY), Cyber Security Intelligence (CSI) e la Titaan Suite, che segnano il passaggio verso un'offerta tecnologica distintiva e scalabile.

Parallelamente, l'azienda ridefinisce il proprio modello di Go-To-Market, avviando la creazione di un network distributivo strutturato basato su distributori e partner, con l'obiettivo di ampliare la presenza sul mercato e rendere le soluzioni Cyberoo accessibili a un numero crescente di aziende.

Il 7 ottobre 2019 Cyberoo viene quotata su Euronext Growth Milan, diventando la prima società di cyber security a quotarsi a Piazza Affari, un traguardo che rafforza la solidità dell'azienda e ne accelera il percorso di crescita e visibilità sul mercato.

A dicembre Cyberoo consolida il proprio impegno nella ricerca e nello sviluppo stringendo un accordo con l'Università di Ternopil "Ivan Puluj National Technical University" (Ucraina), finalizzato alla ricerca, allo sviluppo tecnologico e alla selezione di talenti altamente qualificati in ambito cybersecurity, rafforzando ulteriormente il proprio ecosistema di innovazione.

2020–2021 | Espansione dei servizi di consulenza cyber

Nel biennio 2020–2021, in un contesto profondamente segnato dalla pandemia e dall'accelerazione della digitalizzazione, Cyberoo, attraverso la propria controllata Cyberoo Docetz, amplia la propria offerta introducendo servizi di consulenza cyber ad alto valore, a supporto delle aziende nella gestione delle nuove e crescenti minacce informatiche.

In particolare, il servizio di Incident Response Team (IRT) registra una forte crescita: l'aumento esponenziale degli attacchi cyber nel periodo Covid porta numerose organizzazioni a rivolgersi a Cyberoo per affrontare incidenti di sicurezza, gestire

situazioni critiche e ripristinare rapidamente l'operatività. Cyberoo diventa così un punto di riferimento per la risposta agli incidenti, offrendo competenze specialistiche, supporto tempestivo e un approccio strutturato alla gestione delle crisi cyber.

Accanto all'Incident Response, l'azienda arricchisce il proprio portafoglio con servizi di consulenza strategica, come il vCISO, accompagnando le imprese nel rafforzamento della governance della sicurezza, nella definizione delle strategie di protezione e nel miglioramento complessivo della postura di sicurezza e della cyber resilience. Completano l'offerta i servizi di Vulnerability Assessment e Penetration Test (VA/PT) e di Risk Assessment, affiancando le imprese nella valutazione delle vulnerabilità, nell'analisi del rischio cyber e nella definizione di priorità di intervento.

2022 | Cypeer Sonic e l'evoluzione dell'Automatic Remediation

Nel 2022 Cyberoo compie un passo decisivo nell'evoluzione del proprio servizio di Threat Management con il lancio di Cypeer Sonic, una soluzione progettata per abilitare funzionalità avanzate di Automatic Remediation. L'obiettivo è superare i limiti dei modelli tradizionali di risposta, riducendo in modo significativo i tempi di reazione e l'impatto operativo degli attacchi informatici.

Grazie all'integrazione di intelligenza artificiale e machine learning, Cypeer Sonic consente di automatizzare specifiche azioni di risposta agli eventi critici, intervenendo in modo rapido, controllato e coerente con le policy di sicurezza definite. L'Automatic Remediation diventa così un elemento centrale del modello Cyberoo, permettendo di contenere le minacce in tempo reale e di limitarne l'impatto sull'operatività aziendale.

L'automazione non sostituisce l'intervento umano, ma lo potenzia: la sinergia tra i sistemi intelligenti e gli analisti dell'I-SOC, già consolidata in ambito detection, si estende ai servizi di response, combinando velocità di esecuzione e capacità decisionale e rendendo la risposta agli attacchi più efficace e scalabile.

Con Cypeer Sonic, Cyberoo introduce un approccio alla cybersecurity sempre più orientato alla resilienza operativa, in cui l'Automatic Remediation rappresenta un passo concreto verso una gestione del rischio cyber proattiva e continua.

2023 | Crescita e presenza internazionale

Nel 2023 Cyberoo rafforza la propria presenza internazionale avviando una nuova sede in Polonia, pensata come hub operativo e commerciale per il mercato europeo. La sede ospita un SOC operativo 24/7, e un team commerciale dedicato che opera a sostegno della rete distributiva, replicando il modello di Go-To-Market già consolidato in Italia.

Questo approccio consente a Cyberoo di combinare prossimità al cliente, capacità operative avanzate e sviluppo di un ecosistema di partner strutturato, garantendo coerenza nell'erogazione dei servizi in lingua, scalabilità del modello e continuità nella relazione con il mercato.

Nel giugno 2023 Cyberoo ottiene l'accreditamento come CERT di Trusted Introducer, entrando a far parte di una rete internazionale di Computer Emergency Response Team. Essere CERT significa disporre delle competenze, dei processi e dell'operatività necessari per prevenire, gestire e rispondere in modo strutturato agli incidenti di sicurezza informatica. Il riconoscimento certifica l'affidabilità del SOC di Cyberoo, la capacità di operare in modalità continuativa h24 e l'esperienza nella gestione di eventi cyber critici, rafforzando ulteriormente il ruolo dell'azienda come partner di riferimento per la sicurezza delle infrastrutture digitali.

2024 | Espansione in Spagna e Portogallo e innovazione tecnologica

Nel 2024 Cyberoo prosegue il proprio percorso di crescita internazionale con l'apertura delle attività commerciali in Spagna e Portogallo, rafforzando la presenza nei principali mercati europei attraverso un modello basato su distributori e partner locali, in continuità con il Go-To-Market già consolidato.

Parallelamente, Cyberoo consolida la propria evoluzione tecnologica arricchendo l'ecosistema Cypeer e introducendo Keera, una soluzione progettata per supportare in modo concreto ed efficace Cyberoo nelle attività di remediation presso le aziende, rendendo gli interventi più rapidi, strutturati ed efficaci. Keera aiuta a tradurre le attività di detection in azioni correttive guidate e controllate, contribuendo a ridurre i tempi di risposta e l'impatto operativo degli incidenti.

Con Keera, Cyberoo compie un ulteriore passo verso una cybersecurity orientata alla resilienza operativa, in cui la remediation diventa parte integrante e strutturata della gestione del rischio cyber.

A supporto del posizionamento strategico e culturale del brand, Cyberoo lancia la campagna-manifesto “Above The Rest”, un progetto di comunicazione multicanale volto a diffondere la cultura della cybersecurity attraverso spot e podcast narrati da Federico Buffa.

2025 | Nasce la nuova piattaforma Keatrix

Nel 2025 Cyberoo annuncia Keatrix, la nuova piattaforma proprietaria di Human Risk & Security TrAlning, progettata per affrontare uno dei principali fattori di rischio cyber: il comportamento umano. Basata su intelligenza artificiale adattiva ed elementi di edutainment, Keatrix consente di costruire percorsi formativi dinamici e personalizzati, calibrati sulle esigenze dei singoli utenti e sul livello di maturità cyber delle organizzazioni.

La piattaforma è pensata per rafforzare in modo concreto la postura di sicurezza delle persone, aumentando consapevolezza, competenze e capacità di risposta ai rischi digitali. Keatrix certifica in modo nominativo le competenze acquisite, offrendo alle aziende uno strumento misurabile e tracciabile per la gestione del rischio umano. A partire dal 1° dicembre 2025, Keatrix entra ufficialmente in distribuzione commerciale in Italia e all'estero, ampliando l'ecosistema di soluzioni Cyberoo e integrandosi in una visione di cybersecurity sempre più orientata alla resilienza, in cui tecnologia, processi e persone evolvono insieme.

2026 | Nasce ORBIS, il modello integrato per la gestione del rischio cyber

Nel 2026 Cyberoo consolida il proprio posizionamento strategico con la definizione di ORBIS, il framework proprietario che integra in un unico ecosistema le principali dimensioni del cyber risk management.

Il modello supera l'approccio frammentato alla sicurezza informatica, riunendo in una visione organica threat management, governance dei processi, compliance normativa e security awareness, attraverso l'integrazione della Cyber Security Suite, Cyberoo Docetz, Titaan Neemesi e Keatrix.

ORBIS rappresenta l'evoluzione dell'approccio Cyberoo alla cybersecurity: un modello end-to-end che accompagna le organizzazioni lungo l'intero ciclo del rischio cyber, dalla prevenzione alla rilevazione, dalla risposta agli incidenti fino alla gestione della compliance e del fattore umano, riducendo la complessità e rafforzando la resilienza digitale delle aziende.

Business Timeline



Mission e Valori

WE ARE



Euronext Growth Milan · CERT Trusted Introducer · ISO/IEC 27001:2022
Cybersecurity Made in Europe

Vision & Mission

Cyberoo vuole essere “*il faro made in Italy che illumina le zone oscure e poco chiare del cyberspazio*”, **una guida che accompagna aziende, persone ed enti nel percorso di conoscenza, formazione e difesa necessario per vivere e operare in sicurezza nell’ecosistema digitale.** Un faro che rappresenta anche un polo di ricerca e sviluppo per le tecnologie più avanzate di Intelligenza Artificiale applicate alla cybersecurity.

Il posizionamento competitivo di Cyberoo si fonda su **ORBIS**, un framework proprietario che integra in un unico ecosistema le principali dimensioni del **cyber risk management**, superando l’approccio frammentato tipico del mercato, caratterizzato dall’adozione di soluzioni eterogenee spesso non integrate tra loro,

con conseguenti complessità operative e limitazioni nella governance complessiva del rischio.

Le **quattro torri di vedetta di Cyberoo** rappresentano le quattro aree operative che compongono il modello ORBIS e che, integrate tra loro, consentono di presidiare l'intero ciclo di gestione del rischio cyber:

- **Threat Management**, attraverso la Cyber Security Suite, per il monitoraggio continuo, la rilevazione e la risposta alle minacce informatiche;
- **Governance dei processi**, tramite Cyberoo Docetz, per la strutturazione, il controllo e il miglioramento dei processi di sicurezza aziendale;
- **Compliance normativa e regolatoria**, attraverso Titaan Neemesi, per la gestione degli adempimenti e degli obblighi richiesti dalle normative vigenti;
- **Security Awareness**, mediante Keatrix, per sviluppare consapevolezza e comportamenti sicuri nelle persone.



Le quattro aree operative del modello ORBIS, integrate in un unico ecosistema

L'integrazione di queste quattro dimensioni all'interno di un unico modello operativo rappresenta un elemento distintivo del posizionamento di Cyberoo rispetto a un mercato spesso basato su strumenti specialistici separati, che richiedono elevati livelli di coordinamento da parte delle aziende.

Attraverso ORBIS, Cyberoo accompagna le organizzazioni lungo l'intero ciclo del rischio cyber: dalla prevenzione alla rilevazione, dalla risposta agli incidenti fino alla compliance e alla gestione del fattore umano, riducendo la complessità operativa e supportando una maggiore efficacia nei processi decisionali.

Grazie alla combinazione di tecnologie proprietarie, Intelligenza Artificiale, Machine Learning, sistemi adattivi e competenza specialistica, Cyberoo offre un modello evolutivo e integrato di cybersecurity, pensato per aiutare le aziende del segmento mid-market europeo a rafforzare la propria resilienza digitale e affrontare il rischio cyber in modo strutturato, continuo e consapevole.

Valori

Cyberoo è da sempre impegnata a sviluppare e favorire una cultura fondata sulla collaborazione, che contribuisce all'eccellenza dei servizi professionali forniti e alla creazione di un ambiente di lavoro partecipativo.

In questo contesto, i valori a cui il Gruppo si ispira – e dai quali derivano i propri modelli di condotta – per competere efficacemente e lealmente sul mercato, accrescere il valore e sviluppare le competenze e la crescita professionale delle persone sono:



Innovazione

Promuovere un ambiente che stimoli l'esplorazione e l'identificazione continua di nuove opportunità per progettare, sviluppare e promuovere soluzioni creative, tempestive ed efficaci.

Efficienza

Focalizzarsi sulla produttività e sul miglioramento continuo attraverso soluzioni innovative che incrementino il valore e le performance delle aziende clienti, affrontare rapidamente le sfide di un mercato in evoluzione, garantendo sempre un'elevata qualità del servizio offerto.

Persone

Le persone sono il fattore chiave per il conseguimento degli obiettivi e dei piani aziendali. Per questo motivo Cyberoo tutela il capitale umano, con la promozione del potenziale di ogni singola risorsa e l'incentivazione di competenze individuali e professionali.

Onestà

I dipendenti e i collaboratori di Cyberoo operano con responsabilità, onestà e trasparenza, astenendosi dal perseguire l'utile personale in violazione delle leggi vigenti. Il Gruppo si impegna a garantire l'integrità nella condotta del business, la migliore qualità di servizio e la massima trasparenza su tempi e aspettative.

Mercato di riferimento

Il Gruppo Cyberoo opera nel mercato della cybersecurity con un posizionamento focalizzato sulle imprese mid-market europee, segmento caratterizzato da crescente complessità del rischio cyber, aumento dell'esposizione a minacce evolute, incremento degli obblighi normativi e limitata disponibilità di strutture interne specializzate per la gestione integrata della sicurezza informatica e della compliance.

Il posizionamento competitivo del Gruppo è fondato sul modello ORBIS, un framework proprietario che integra in un unico ecosistema le principali dimensioni del cyber risk management, superando l'approccio frammentato tipico del mercato, nel quale le imprese adottano soluzioni eterogenee non sempre integrate

tra loro, con conseguenti inefficienze operative e limitazioni nella governance complessiva del rischio.

In particolare, ORBIS combina quattro aree operative tra loro integrate: (i) il threat management, attraverso la Cyber Security Suite, focalizzata su attività di monitoraggio, rilevazione e risposta alle minacce; (ii) la governance dei processi, tramite Cyberoo Docetz, orientata alla strutturazione e al controllo dei processi di sicurezza; (iii) la compliance normativa e regolatoria, attraverso Titaan Neemesi, dedicata alla gestione degli adempimenti e degli obblighi regolamentari; (iv) la security awareness e il fattore umano, mediante Keatrix, finalizzata alla formazione e alla sensibilizzazione degli utenti aziendali.

L'integrazione di tali componenti all'interno di un unico modello operativo rappresenta un elemento distintivo del posizionamento del Gruppo rispetto all'offerta di mercato, generalmente basata su soluzioni specialistiche (quali servizi gestiti, piattaforme tecnologiche o servizi consulenziali) che richiedono elevati livelli di coordinamento da parte del cliente.

Il modello Cyberoo consente invece di ricondurre tali ambiti a un ecosistema proprietario e integrato, in grado di coprire in modo continuativo l'intero ciclo di gestione del rischio cyber, dalla prevenzione alla rilevazione, dalla risposta agli incidenti fino alla compliance e alla gestione del fattore umano, riducendo la complessità operativa e supportando una maggiore efficacia nei processi decisionali delle imprese clienti.

In tale contesto competitivo, il Gruppo si posiziona come operatore specializzato nella gestione integrata del rischio cyber per il segmento mid-market europeo, caratterizzato da esigenze crescenti di strutturazione della sicurezza e da limitate economie di scala per l'adozione e l'integrazione di soluzioni eterogenee, favorendo l'adozione di piattaforme e modelli end-to-end come quello proposto da Cyberoo.

Il mercato della cybersecurity

Il mercato della cybersecurity si trova oggi in una fase di espansione sostenuta, ma soprattutto di profonda trasformazione strutturale. La crescita della spesa globale e l'accelerazione della digitalizzazione non rappresentano soltanto un aumento della domanda di soluzioni di sicurezza, ma riflettono un cambiamento qualitativo nel modo in cui le organizzazioni interpretano e gestiscono il rischio cyber. La

sicurezza informatica non è più un ambito tecnico circoscritto alla protezione dei sistemi, ma una componente centrale della governance aziendale, sempre più intrecciata con continuità operativa, compliance normativa e gestione strategica del rischio.

A livello europeo, il mercato della cybersecurity ha raggiunto nel 2025 una valutazione stimata di circa 81,81 miliardi di dollari e si prevede possa crescere fino a 165,73 miliardi di dollari entro il 2034, con un CAGR dell'8,16% (IMARC Group, 2026). Questa traiettoria di crescita è sostenuta da tre fattori principali: l'aumento della superficie di attacco legata alla digitalizzazione dei processi, la crescente sofisticazione delle minacce e l'intensificazione del quadro normativo europeo in materia di sicurezza e resilienza digitale.

In Italia, la dinamica è ancora più evidente sul piano relativo. Secondo l'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, nel 2025 la spesa in cybersecurity ha raggiunto i 2,78 miliardi di euro, con un incremento del 12% rispetto all'anno precedente. Tuttavia, questa crescita degli investimenti non si traduce automaticamente in una corrispondente riduzione del rischio. Al contrario, i dati evidenziano una persistente vulnerabilità sistemica: nello stesso periodo, circa il 34% delle grandi imprese italiane ha subito attacchi cyber con impatti economici e operativi significativi, mentre solo il 28% dichiara di aver adottato un approccio realmente orientato alla cyber-resilienza.

Questa apparente contraddizione segnala un punto chiave: il mercato sta crescendo rapidamente, ma la maturità di governo del rischio cresce a un ritmo inferiore. In altre parole, le imprese stanno investendo di più, ma non sempre in modo coordinato, efficace e integrato.

Il principale elemento di trasformazione del mercato non riguarda soltanto l'aumento della domanda, ma la natura stessa del problema da risolvere. La cybersecurity contemporanea non è più riconducibile a un modello lineare di difesa perimetrale o di gestione reattiva degli incidenti. Le organizzazioni operano oggi all'interno di ecosistemi digitali complessi, caratterizzati da interdipendenze tra sistemi, fornitori, processi e persone.

In questo contesto, il rischio cyber assume una natura sistemica: non nasce da un singolo evento isolato, ma dalla combinazione dinamica tra minacce esterne, vulnerabilità interne, esposizione dei processi e capacità organizzativa di risposta. Ogni nuova applicazione cloud, ogni integrazione con un fornitore terzo, ogni

identità digitale abilitata e ogni processo digitalizzato contribuisce a modificare la superficie di attacco complessiva dell'organizzazione.

Questo spiega perché la logica tradizionale basata sull'accumulo di strumenti di sicurezza non sia più sufficiente. L'aumento del numero di soluzioni non determina necessariamente un aumento proporzionale della sicurezza. Al contrario, la frammentazione degli strumenti può introdurre nuove complessità operative, generare sovrapposizione di responsabilità e rallentare i tempi di risposta.

Secondo una ricerca dell'IBM Institute for Business Value, le organizzazioni utilizzano mediamente decine di soluzioni di sicurezza provenienti da numerosi vendor differenti, con un impatto diretto sulla capacità di identificazione, correlazione e gestione degli incidenti. In molti casi, la complessità dello stack tecnologico diventa essa stessa un fattore di rischio, riducendo la visibilità complessiva e aumentando il tempo necessario per rilevare e contenere un attacco.

L'evoluzione del mercato della cybersecurity negli ultimi anni è stata fortemente influenzata dalla diffusione dei modelli Managed Detection and Response (MDR), che hanno introdotto un approccio più operativo e continuativo alla gestione delle minacce. L'MDR ha rappresentato un passaggio importante perché ha spostato il focus dalla sola implementazione tecnologica alla capacità di rilevazione e risposta continua agli eventi di sicurezza.

Tuttavia, la progressiva maturazione di questa categoria ha portato a una crescente eterogeneità delle offerte. Sotto l'etichetta MDR convivono oggi modelli molto diversi tra loro: servizi focalizzati sulla gestione di endpoint (Managed EDR), centri operativi di sicurezza erogati in outsourcing (SOC as a Service), piattaforme XDR con capacità di correlazione avanzata e servizi di monitoring continuo.

Secondo Gartner (2025), questa evoluzione riflette una fase di espansione del mercato, ma comporta anche una crescente difficoltà per le organizzazioni nel distinguere tra strumenti, servizi e reali capacità operative. Il risultato è un mercato più ampio ma meno immediatamente leggibile, in cui la moltiplicazione delle offerte non sempre corrisponde a una maggiore chiarezza sui risultati attesi.

A questo fenomeno si aggiunge un ulteriore elemento critico: la difficoltà crescente delle organizzazioni nel valutare e selezionare fornitori e soluzioni. Il fenomeno del "choice overload" evidenzia come un numero eccessivo di alternative possa rallentare i processi decisionali invece di facilitarli. Secondo il

report Cybersecurity Trust Reality 2026, il 95% delle organizzazioni dichiara di non avere piena fiducia nei vendor cyber e oltre il 60% segnala difficoltà anche nella valutazione dei fornitori già attivi. Questa condizione contribuisce a rafforzare un paradosso centrale del mercato: l'aumento dell'offerta non si traduce automaticamente in una maggiore capacità di governo del rischio.

Il panorama competitivo della cybersecurity può essere interpretato come un ecosistema composto da quattro grandi domini funzionali:

- Threat Management, focalizzato sulla rilevazione e risposta alle minacce;
- Governance e compliance, focalizzata su controllo, normative e accountability;
- Resilienza dei processi, focalizzata sulla continuità operativa;
- People Security, focalizzata sul comportamento umano e sulla riduzione del rischio legato all'errore.

Ciascuno di questi domini rappresenta un mercato necessario, con competenze specifiche e valore autonomo. Tuttavia, nessuno di essi è sufficiente, se considerato isolatamente, a governare l'intero rischio cyber.

Il punto critico del mercato contemporaneo non è quindi la mancanza di soluzioni, ma la mancanza di integrazione tra esse. Le organizzazioni si trovano spesso in una condizione in cui dispongono di tecnologie avanzate, ma prive di una regia unica capace di collegare minacce, processi, persone e obblighi normativi in un modello coerente di decisione.

La trasformazione del mercato è particolarmente evidente nel segmento mid-market europeo, che rappresenta una fascia sempre più esposta. Le imprese di medie dimensioni presentano oggi superfici di attacco comparabili a quelle delle grandi organizzazioni, ma senza disporre delle stesse risorse interne in termini di competenze, processi e strutture dedicate.

La crescente adozione di cloud, l'integrazione con fornitori esterni e la digitalizzazione dei processi industriali hanno ampliato in modo significativo il perimetro del rischio. In questo contesto, anche attività ordinarie come l'onboarding di un dipendente, l'attivazione di un nuovo fornitore o la migrazione di un sistema applicativo diventano punti potenziali di esposizione.

Il rischio cyber non è quindi più un evento eccezionale, ma una condizione strutturale dell'operatività aziendale. Questo sposta la cybersecurity da funzione tecnica a funzione di governo del rischio aziendale.

La direzione evolutiva del mercato indica un progressivo superamento della logica basata sulla somma di strumenti e vendor verticali. Il problema principale non è più soltanto rilevare e rispondere alle minacce, ma costruire un modello capace di integrare detection, governance, compliance, processi e fattore umano in una visione unitaria.

In questo scenario, la cybersecurity sta evolvendo da insieme di tecnologie specialistiche a disciplina di governo del rischio sistemico. La crescente complessità normativa europea (NIS2, DORA, GDPR, AI Act, Cyber Resilience Act) rafforza ulteriormente questa direzione, imponendo alle organizzazioni non solo di proteggere i sistemi, ma di dimostrare la capacità di governarli in modo coerente, tracciabile e responsabile.

Il GDPR (General Data Protection Regulation) costituisce il pilastro della normativa europea in materia di protezione dei dati personali. Introdotto nel 2018, impone alle organizzazioni obblighi stringenti in termini di accountability, sicurezza dei trattamenti, gestione dei data breach e dimostrabilità delle misure adottate. Il suo impatto va oltre la compliance formale, poiché richiede alle imprese di strutturare processi di gestione del rischio sui dati e di garantire tracciabilità delle decisioni in caso di incidenti.

La direttiva NIS2 (Network and Information Security Directive 2) estende in modo significativo il perimetro della sicurezza informatica a livello europeo, imponendo requisiti più severi in materia di gestione del rischio, continuità operativa, supply chain security e responsabilità del management. La normativa introduce inoltre obblighi di notifica degli incidenti più stringenti e rafforza il principio di accountability del vertice aziendale, rendendo la cybersecurity una responsabilità esplicita della governance e non più esclusivamente dell'IT.

Il regolamento DORA (Digital Operational Resilience Act), rivolto in particolare al settore finanziario, stabilisce un quadro armonizzato per la resilienza operativa digitale. Il suo obiettivo è garantire che banche, assicurazioni e operatori finanziari siano in grado di resistere, rispondere e recuperare da incidenti ICT. DORA introduce requisiti avanzati di gestione del rischio ICT, test di resilienza, monitoraggio dei fornitori terzi e standardizzazione dei processi di incident reporting, rafforzando il legame tra cybersecurity e continuità del business.

L'AI Act, prima normativa organica al mondo sull'intelligenza artificiale, introduce un sistema di classificazione del rischio per i sistemi AI, imponendo obblighi

differenziati in base al livello di rischio (inaccettabile, alto, limitato e minimo). Per la cybersecurity, il suo impatto è rilevante perché regola l'uso di sistemi AI anche in ambito di sicurezza, governance dei dati e automazione decisionale, imponendo requisiti di trasparenza, controllo umano e gestione del rischio algoritmico.

Il Cyber Resilience Act (CRA) completa il quadro normativo introducendo requisiti di sicurezza obbligatori per prodotti hardware e software immessi sul mercato europeo. L'obiettivo è garantire che la sicurezza sia integrata "by design" lungo tutto il ciclo di vita del prodotto digitale, dalla progettazione alla manutenzione, riducendo la superficie di vulnerabilità dell'ecosistema digitale europeo e rafforzando la responsabilità dei produttori.

Nel loro insieme, queste normative non rappresentano vincoli isolati, ma un framework coerente di trasformazione del mercato europeo della cybersecurity. Esse convergono verso un principio comune: la sicurezza non è più solo una funzione tecnica, ma una capacità organizzativa dimostrabile, governata e continua, che integra tecnologia, processi, persone e responsabilità decisionali.

Il mercato, quindi, non sta semplicemente crescendo: sta cambiando natura. Da mercato di strumenti a mercato di integrazione. Da mercato di prodotti a mercato di sistemi. Da mercato di difesa a mercato di governance del rischio.

Nel complesso, il mercato della cybersecurity si trova in una fase di transizione strutturale. La crescita della spesa e l'evoluzione tecnologica non sono sufficienti, da sole, a garantire una riduzione del rischio. Al contrario, la crescente frammentazione degli strumenti e la complessità degli ecosistemi digitali stanno rendendo sempre più evidente la necessità di modelli integrati di gestione del rischio.

La sfida principale per le organizzazioni non è quindi l'accesso alla tecnologia, ma la capacità di trasformarla in una funzione coerente di governo del rischio aziendale. In questo scenario, il valore competitivo non risiede più nella singola soluzione, ma nella capacità di integrare minacce, processi, compliance e persone all'interno di un unico modello decisionale.

La regolamentazione di settore

Nel mercato in cui opera, Cyberoo si trova oggi a confrontarsi con il più recente quadro normativo europeo e nazionale in materia di sicurezza informatica. A livello

europeo il riferimento principale è la Direttiva NIS2 (UE 2022/2555), che innalza il livello comune di cybersicurezza nell'Unione ampliando i settori e i soggetti obbligati; in Italia la Direttiva è stata recepita con il D.Lgs. 4 settembre 2024, n. 138, la cui attuazione procede attraverso un regime di adempimenti scaglionati nel corso del 2025 e del 2026.

Per Cyberoo ciò si traduce nella conferma di adozione di un rigoroso sistema di gestione del rischio, che va dall'introduzione di policy interne volte a garantire la prevenzione e il tempestivo rilevamento degli incidenti, fino alla formalizzazione di un modello di governance. Parallelamente, il Gruppo ha adeguato le procedure di notifica per segnalare eventuali incidenti, oltre a rafforzare i controlli sulla supply chain.

A livello nazionale, il quadro si è ulteriormente rafforzato con la Legge 28 giugno 2024, n. 90 ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"), in vigore dal 17 luglio 2024, che ha introdotto obblighi più stringenti di notifica degli incidenti all'Agenzia per la Cybersicurezza Nazionale (ACN), requisiti di cybersicurezza negli appalti pubblici, criteri di premialità per le tecnologie sviluppate in ambito italiano, europeo e NATO e un inasprimento dei reati informatici, con impatti anche sul catalogo dei reati-presupposto di cui al D.Lgs. 231/2001.

Dal 17 gennaio 2025, inoltre, è divenuto pienamente applicabile il Regolamento UE 2022/2554, noto come Digital Operational Resilience Act (DORA) che, pur essendo rivolto principalmente a istituzioni finanziarie e ai loro provider ICT dedicati, impone a Cyberoo – in quanto fornitore di servizi di sicurezza a banche, assicurazioni e intermediari – l'adozione di un solido framework di resilienza operativa digitale.

L'insieme di queste disposizioni normative richiede a Cyberoo un continuo e proattivo aggiornamento delle proprie procedure interne, un rafforzamento degli investimenti in ricerca e sviluppo – soprattutto nelle aree di threat intelligence e dei Security Operations Center – e un costante miglioramento delle competenze del personale tecnico, in un'ottica di servizio sempre più avanzato e capillare a tutela della sicurezza e della resilienza digitale dei clienti.

Normativa in materia di privacy

In data 24 maggio 2016 è entrato in vigore il nuovo Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, in materia di protezione dei dati delle persone fisiche, volto a definire un quadro normativo comune in materia di tutela dei dati personali per tutti gli Stati membri dell'Unione Europea. Esso è direttamente applicabile in tutti i Paesi dell'Unione Europea a partire dal 25 maggio 2018.

In particolare, il GDPR ha introdotto significative modifiche ai processi da adottare per garantire la protezione dei dati personali (tra cui dotarsi di una nuova figura del data protection officer, implementare un efficace modello organizzativo in materia privacy, sottostare a obblighi di comunicazione in caso di particolari violazioni dei dati) aumentando il livello di tutela delle persone fisiche e inasprendo, tra l'altro, le sanzioni applicabili al titolare e all'eventuale responsabile del trattamento dei dati, in caso di violazioni delle previsioni del GDPR. Con riferimento alle violazioni dei dati personali (c.d. data breach), si segnala che il GDPR impone che il titolare del trattamento debba comunicare tali eventuali violazioni all'Autorità nazionale di protezione dei dati.

Intelligenza Artificiale

Considerata la centralità, soprattutto prospettica, dell'intelligenza artificiale per il business del Gruppo Cyberoo, si segnala che il quadro normativo europeo in materia si è ormai consolidato con l'entrata in vigore, il 1° agosto 2024, del Regolamento (UE) 2024/1689 (c.d. "AI Act"), primo quadro giuridico organico al mondo sull'intelligenza artificiale. Il Regolamento adotta un approccio basato sul rischio, articolando i sistemi di IA in quattro livelli (inaccettabile, alto, limitato, minimo), e prevede un'applicazione scaglionata nel tempo: dal 2 febbraio 2025 sono operativi i divieti sulle pratiche a rischio inaccettabile e gli obblighi di alfabetizzazione in materia di IA; dal 2 agosto 2025 gli obblighi per i modelli per finalità generali (GPAI); con applicazione progressiva delle restanti disposizioni, incluse quelle relative ai sistemi ad alto rischio, negli anni successivi. Il Regolamento stabilisce inoltre regole di trasparenza armonizzate per i sistemi che interagiscono con le persone fisiche e per quelli utilizzati per generare o manipolare immagini, audio, video o contenuti.

Strategia e sostenibilità

Il ruolo di Cyberoo e le linee strategiche di sviluppo

L'impronta Cyberoo ha il suo cardine nella cultura dell'innovazione che permea ogni aspetto del processo di management.

Le finalità di Cyberoo sono coerenti con i principi di un modello di sviluppo sostenibile, rispetto al quale il settore IT viene riconosciuto come strategico secondo tre direttrici:

- Trasformazione digitale quale motore di sviluppo.
- Innovazione che punti su ricerca e sviluppo applicate e favorisca le idee, la condivisione della conoscenza, a sostegno delle filiere produttive.
- Sviluppo sostenibile e inclusivo, dove l'innovazione è al servizio delle persone, delle comunità e dei territori, nel rispetto della sostenibilità ambientale.

Obiettivi di sviluppo sostenibile

Cyberoo persegue da sempre un modello di sviluppo industriale che fa propri i principi di sostenibilità, trasparenza e qualità, assumendo impegni concreti e adottando specifici assetti gestionali e organizzativi, con **l'obiettivo di creare valore condiviso per tutti i propri stakeholder e nel rispetto dell'ambiente.**



In particolare, Cyberoo fonda il proprio approccio strategico in coerenza con il percorso di sostenibilità intrapreso, che prevede una progressiva integrazione degli obiettivi di sviluppo sostenibile (SDGs – Sustainable Development

Goals), parte dell'Agenda 2030 delle Nazioni Unite.

L'attuale contesto ed i megatrend in atto richiedono alle imprese un impegno nel perseguimento di obiettivi economici che possano generare degli impatti positivi, anche in termini ambientali e sociali. L'attuazione di una politica di sviluppo sostenibile da parte delle imprese, quale parte del core business di Gruppo, è infatti una leva per il raggiungimento degli SDGs, alla quale si affiancano progetti ed iniziative specifiche.

In questo contesto, Cyberoo ha effettuato una prima analisi di coerenza del proprio modello di business ed obiettivi strategici rispetto agli SDGs, consentendole di

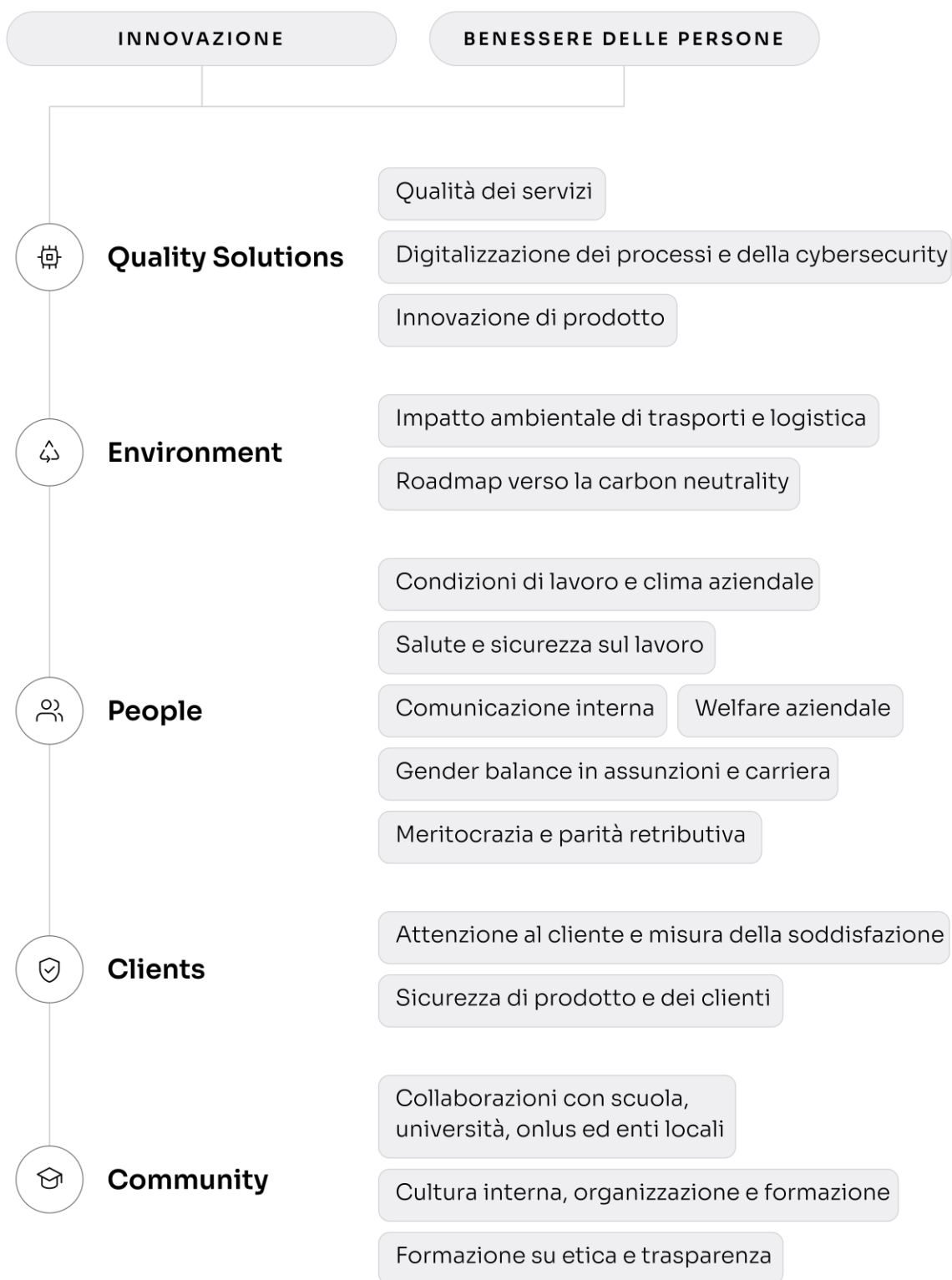
evidenziare alcuni SDGs ritenuti prioritari, rispetto ai quali le attività di business del Gruppo sono in grado di dare un contributo significativo.

I driver del Piano industriale e l'impegno di Cyberoo rispetto agli Obiettivi di sviluppo sostenibile trovano la loro integrazione nelle attività, nei progetti e nelle azioni di gruppo, secondo lo schema di seguito rappresentato.

I driver della strategia di Cyberoo

L'innovazione per Cyberoo è da sempre il cuore pulsante attorno al quale ruotano idee, progetti, servizi, design e processi di sviluppo. L'innovazione è alimentata dalla ricerca che favorisce lo sviluppo delle idee e la condivisione della conoscenza, a sostegno dei diversi settori di mercato. Ma l'innovazione, dove è al servizio delle persone, delle imprese, delle comunità e dei territori, nel rispetto della sostenibilità ambientale, produce anche lo sviluppo sostenibile e inclusivo.

Partendo proprio dal connubio **INNOVAZIONE** unita al **BENESSERE DELLE PERSONE**, Cyberoo ha individuato sei linee di azione, alla base anche delle politiche e dei sistemi di gestione che regolano i processi e l'operatività della Società coerenti con lo sviluppo sostenibile.



Innovation & Wellbeing

Linee di azione	Obiettivi	SDGs
Quality Solutions (Innovation & Digital Transformation)	<ul style="list-style-type: none"> Sviluppare progetti per il controllo e l'ottimizzazione della qualità dei servizi Promuovere la digitalizzazione dei processi e della cybersecurity Sviluppare l'innovazione dei prodotti 	   
Environment	<ul style="list-style-type: none"> Migliorare l'impatto ambientale dei trasporti e della logistica Roadmap verso la carbon neutrality 	  
People	<ul style="list-style-type: none"> Migliorare le condizioni di lavoro e il clima aziendale Potenziare la salute e sicurezza sul lavoro Migliorare la comunicazione interna verso i dipendenti Sviluppare il sistema di welfare aziendale Assicurare il gender balance nei percorsi di carriera e assunzioni Valorizzare la meritocrazia e assicurare la parità nei percorsi retributivi e di carriera 	   
Clients	<ul style="list-style-type: none"> Sviluppare iniziative per migliorare l'attenzione verso i clienti e la misurazione della loro soddisfazione Incrementare la sicurezza di prodotto e dei clienti 	  
Community	<ul style="list-style-type: none"> Sviluppare collaborazioni e partnership con il mondo scuola, università, onlus ed enti locali Sviluppare la cultura delle risorse interne attraverso iniziative di organizzazione e formazione Sviluppare la formazione su etica e trasparenza 	   

Analisi di materialità

Il ruolo degli stakeholder

Gli stakeholder sono i soggetti (individui o gruppi) espressione di interessi, aspettative e valutazioni diversi nei confronti di un'impresa, con i quali essa intrattiene relazioni costanti nello svolgimento della propria attività. Il coinvolgimento ed il confronto con gli stakeholder (*stakeholder engagement*) consente non soltanto di comprenderne le esigenze, aspettative e valutazioni, ma anche di definire una migliore strategia e obiettivi di business, valutando il cambiamento, i rischi e le opportunità.

Il sistema di relazioni di Cyberoo con i propri stakeholder prevede strumenti e canali di dialogo differenziati per le diverse categorie di stakeholder, coerenti con il livello di interdipendenza e influenza sull'organizzazione.

Categoria Stakeholder	Attività di engagement (Progetti – Iniziative – Relazioni)
Banche e finanziatori	Assemblea azionisti – Sito internet – Incontri ed eventi periodici
Dipendenti	Dialogo costante con Direzione Risorse umane – Incontri informali / istituzionali – Incontri di formazione – Iniziative di welfare aziendale – Intranet aziendale – Newsletter interna / Piano di comunicazione dedicato; Performance Management – Questionario di materialità
Fornitori & Partner	Incontri commerciali – Definizione e condivisione di standard – Partnership su progetti (prodotti e innovazione)
Clienti	Interazione tramite incontri commerciali / workshop e presentazioni – Incontri progettuali – Social network – Sito web e Altri canali di comunicazione dedicati – Newsletter informative
Pubblica Amministrazione	Enti pubblici nazionali e locali / Autorità nazionali / locali – Enti di controllo e regolatori: incontri / invio e scambio comunicazioni per adempimenti o richieste specifiche
Comunità e territorio – Istituzioni ed Associazioni locali	Incontri con rappresentanti comunità locali – Collaborazione a progetti di open innovazione – formazione e di responsabilità sociale
Media	Interviste – Conferenze stampa – Sito web istituzionale – Comunicati stampa

I temi materiali

Nell'ambito della rendicontazione di natura ESG, l'**analisi di materialità** è volta a identificare gli aspetti ambientali, sociali, economici e di governance considerati rilevanti e significativi per il business del Gruppo Cyberoo e per i suoi stakeholder.

Tali tematiche vengono definite “materiali” in quanto risultano associate agli impatti (positivi o negativi, effettivi o potenziali, di breve o lungo periodo) più significativi che le attività aziendali sono (o potrebbero essere) in grado di generare sull'economia, l'ambiente e le persone, compresi gli impatti sui loro diritti umani.

In occasione del presente Bilancio di Sostenibilità, Cyberoo ha condotto un aggiornamento dell'analisi di materialità, superando il processo adottato nei precedenti esercizi — basato sull'analisi originaria del 2022 — e svolgendo un nuovo percorso strutturato, coerente con i requisiti del GRI 3: Material Topics (2021) e con l'approccio della materialità di impatto (impact materiality). L'aggiornamento è stato motivato dall'evoluzione significativa del contesto di riferimento, tra cui la crescita dimensionale e l'internazionalizzazione del Gruppo, il rafforzamento del quadro normativo europeo in materia di cybersecurity e intelligenza artificiale (NIS2, DORA, AI Act), e la crescente rilevanza dei temi ESG per gli stakeholder del settore.

Il processo si è articolato nelle seguenti fasi:

1. Identificazione dei temi potenzialmente rilevanti (Analisi di Benchmark)

La prima fase ha previsto un'analisi di benchmark condotta su un campione di 29 aziende competitor nel segmento dei servizi di Managed Detection and Response (MDR), selezionate sulla base di criteri quali il settore, la dimensione e la territorialità. Di queste, 16 hanno pubblicato almeno un report di sostenibilità (a livello di gruppo o stand-alone). I temi ESG più frequentemente rendicontati sono stati identificati e classificati in sei categorie: Governance, Economics, Human Resources, Supply Chain & Clients, Products & Infrastructure ed Environment.

I temi così individuati sono stati confrontati con le liste di temi rilevanti per il settore rese disponibili da SASB (Sustainability Accounting Standards Board) e

S&P (Standard & Poor's). Per determinare i temi potenzialmente materiali per Cyberoo sono state applicate soglie di frequenza: i temi presenti nel 50% o più delle aziende analizzate sono stati classificati automaticamente come potenzialmente materiali; quelli presenti in una quota compresa tra il 30% e il 50% sono stati inclusi solo se risultavano in almeno una delle liste SASB o S&P. Questa fase ha portato all'identificazione di 15 temi potenzialmente materiali per Cyberoo, rispetto ai 26 del processo originario del 2022, a conferma di un affinamento del perimetro di analisi e di una maggiore focalizzazione sui temi effettivamente rilevanti per il settore di riferimento.

2. Identificazione e valutazione degli impatti (Questionario di Materialità)

Per la valutazione e prioritizzazione dei 15 temi potenzialmente materiali è stato somministrato un questionario mediante Google Form ai referenti interni del Gruppo, con il quale è stato chiesto di attribuire un punteggio agli impatti — positivi e negativi, effettivi e potenziali — che le attività aziendali generano o potrebbero generare sull'economia, l'ambiente e le persone, compresi gli eventuali impatti sui diritti umani.

In particolare, la valutazione del livello di rilevanza degli impatti ESG connessi a ciascun tema ha tenuto conto dei seguenti elementi:

- **scala:** entità (in senso positivo o negativo, a seconda dei casi) dell'impatto generato direttamente o indirettamente dalle attività aziendali;
- **portata:** diffusione dell'impatto in termini geografici (es: livello locale, nazionale, ecc.), considerando il numero di stakeholder coinvolti, ecc.;
- **carattere di rimediabilità:** misura in cui è possibile mitigare o porre rimedio all'impatto una volta che esso si è verificato (da considerare solo per gli impatti negativi);
- **probabilità:** probabilità con cui tale impatto potrebbe verificarsi nel breve, medio e lungo periodo (da considerare solo per gli impatti potenziali).

I risultati sono stati analizzati calcolando, per ciascun impatto, il prodotto tra entità e probabilità media (rilevanza) e definendo una soglia di rilevanza distinta per gli impatti positivi e negativi (pari alla media dello score massimo complessivo). I temi

i cui impatti hanno superato la soglia di rilevanza sono stati classificati come materiali.

3. Validazione dei temi materiali

Al termine del processo di valutazione, i risultati sono stati presentati al management e validati, confermando come materiali i 9 temi che hanno ottenuto una valutazione superiore alla soglia di rilevanza.

I 9 temi materiali risultanti, in ordine di priorità sulla base dello score complessivo degli impatti, sono i seguenti:

AMBITO	TEMA MATERIALE
Economics	Generazione e distribuzione di valore economico e finanziario
Products & Infrastructure	Ricerca & Sviluppo e innovazione
Products & Infrastructure	Privacy e sicurezza dei dati e delle informazioni
Supply Chain & Clients	Soddisfazione e gestione delle relazioni con i clienti
Human Resources	Condizioni di lavoro, clima interno e welfare aziendale
Human Resources	Formazione e sviluppo delle competenze
Supply Chain & Clients	Supporto/impatto sulla comunità e sul territorio locale
Environment	Efficienza Energetica
Human Resources	Salute e Sicurezza sul lavoro

Rispetto all'esercizio precedente, l'aggiornamento dell'analisi ha comportato alcune variazioni significative nella lista dei temi materiali. Tra le principali novità si segnalano l'ingresso di "Condizioni di lavoro, clima interno e welfare aziendale", "Salute e sicurezza sul lavoro" e "Supporto/impatto sulla comunità e sul territorio locale", temi la cui rilevanza è cresciuta in coerenza con l'espansione dell'organico e il radicamento territoriale del Gruppo. Al contempo, temi quali "Anticorruzione e compliance", "Gestione dei rifiuti" e "Lotta al cambiamento climatico e gestione delle emissioni" non hanno superato la soglia di materialità nel nuovo processo, pur restando monitorati dall'organizzazione. Si segnala inoltre che tra i 15 temi potenzialmente materiali identificati nella fase di benchmark è stato incluso per la prima volta il tema "Etica dell'intelligenza artificiale", a testimonianza della crescente attenzione del settore ai rischi e alle opportunità connessi all'utilizzo di

modelli di AI e machine learning nell'erogazione dei servizi di cybersecurity. Tale tema, pur non avendo superato la soglia di materialità nell'attuale processo di valutazione quantitativa, è stato valutato dal top management del Gruppo come strategicamente rilevante per Cyberoo, anche alla luce dell'entrata in vigore del Regolamento (UE) 2024/1689 (AI Act) e del ruolo centrale che le tecnologie di intelligenza artificiale rivestono nell'offerta di servizi del Gruppo.

I principali presidi che caratterizzano la gestione del tema nel settore della cybersecurity, e che costituiscono il quadro di riferimento verso cui il Gruppo orienta il proprio percorso, riguardano l'adozione di principi di Responsible AI nello sviluppo e nell'erogazione dei servizi. Tra questi assumono particolare rilievo la supervisione umana sui modelli di intelligenza artificiale impiegati nelle attività di detection, correlazione e risposta alle minacce, il rispetto delle disposizioni in materia di protezione dei dati personali (Regolamento (UE) 2016/679 — GDPR) nell'utilizzo di dati nei processi di AI e il progressivo adeguamento ai requisiti introdotti dal Regolamento (UE) 2024/1689 (AI Act). Il Gruppo monitora costantemente l'evoluzione del quadro normativo e delle migliori pratiche di settore, orientando le proprie scelte in coerenza con i principi di sicurezza, trasparenza e responsabilità che caratterizzano l'offerta di servizi di cybersecurity.

Nella tabella successiva viene data evidenza, per ciascun tema materiale identificato, delle ragioni di rilevanza del tema (impatti generati sull'economia, ambiente e persone), dei KPI relativi che sono stati rendicontati e dei processi di monitoraggio adottati.

Tema materiale	Impatti e rilevanza del tema	KPI/GRI Standards	Attività che genera l'impatto	Impegni, politiche e strumenti di monitoraggio
Capitale economico-finanziario				
Generazione e distribuzione di valore economico e finanziario	Possibilità di incidere positivamente o negativamente su: <ul style="list-style-type: none"> gestione delle risorse finanziarie a beneficio della società e dell'ecosistema economico in cui opera 	GRI 201-1 GRI 203-1	Sviluppo e rafforzamento delle relazioni con gli stakeholder e relativa distribuzione della ricchezza generata	Piano Industriale di Gruppo Stakeholder Engagement Adozione di misure in grado

Tema materiale	Impatti e rilevanza del tema	KPI/GRI Standards	Attività che genera l'impatto	Impegni, politiche e strumenti di monitoraggio
	<ul style="list-style-type: none"> • mantenimento delle relazioni con i principali stakeholder con cui l'Organizzazione interagisce • capacità di retention e attraction e sulla stabilità occupazionale delle risorse umane 			di garantire la continuità operativa, la stabilità finanziaria e la redditività del business
Capitale Infrastrutturale e Produttivo				
Ricerca e innovazione tecnologica	Possibilità di incidere positivamente o negativamente su: <ul style="list-style-type: none"> • gestione delle risorse finanziarie a beneficio della società e dell'ecosistema economico in cui opera. • disponibilità nei mercati di prodotti e servizi in grado di soddisfare i bisogni della clientela. 	GRI 3-3	Attività di analisi delle richieste di mercato e di R&S	
Privacy e sicurezza dei dati e delle informazioni	<ul style="list-style-type: none"> • Impatto positivo: il rafforzamento dei controlli di sicurezza (cifatura, segregazione degli accessi, incident response) aumenta la fiducia dei clienti e riduce probabilità e impatti degli incidenti, proteggendo dati e continuità operativa. Impatto negativo: data breach o gestione non corretta di log, eventi e dati personali può determinare danni agli interessati, sanzioni (es. GDPR) e impatti reputazionali significativi. 	GRI 418-1	Erogazione dei servizi MDR e gestione dei dati dei clienti; Gestione dell'infrastruttura IT e dei data center	ISO/IEC 27001:2022 (certificazione DNV); Registrazione al portale ACN ex D.Lgs. 138/2024; DPO nominato ai sensi del GDPR Procedure di incident response e data breach notification
Capitale Umano e Relazionale				
Formazione e sviluppo delle competenze	Possibilità di incidere positivamente o negativamente su:	GRI 404-1	Sviluppo di piani di formazione obbligatoria e specializzata per	Impegno per la formazione e

Tema materiale	Impatti e rilevanza del tema	KPI/GRI Standards	Attività che genera l'impatto	Impegni, politiche e strumenti di monitoraggio
	<ul style="list-style-type: none"> opportunità di ciascun collaboratore di intraprendere un percorso di crescita professionale e di realizzare pienamente il proprio potenziale disponibilità di percorsi finalizzati al rafforzamento e sviluppo delle competenze e delle skill professionali 		la crescita professionale dei dipendenti	addestramento del personale
Condizioni di lavoro, clima interno e welfare aziendale	<p>Impatto positivo: misure di welfare e benessere (flessibilità, benefit, supporto alla genitorialità) migliorano il clima interno, riducendo stress e assenteismo e rafforzando l'attrattività come datore di lavoro. Impatto negativo: carichi di lavoro elevati, scarsa prevedibilità o pressione legata a scadenze e incident response possono aumentare stress e rischio di burnout, con effetti su salute mentale, turnover e qualità del servizio.</p>	GRI 401-1 GRI 401-2 GRI 401-3	Gestione delle risorse umane e politiche di welfare; Organizzazione del lavoro e gestione dei carichi	Piano welfare aziendale; Monitoraggio del turnover e delle cessazioni; Dialogo costante con la Direzione Risorse Umane
Soddisfazione e gestione delle relazioni con i clienti	<p>Possibilità di contribuire positivamente o negativamente a:</p> <ul style="list-style-type: none"> realizzazione e soddisfacimento dei bisogni della clientela in termini di offerta dei prodotti e qualità dei servizi 	GRI 418-1	Attività di customer satisfaction Attività di analisi delle richieste del mercato	Gestione della customer satisfaction
Salute e sicurezza sul lavoro	<ul style="list-style-type: none"> Impatto positivo: programmi di formazione periodica su salute e sicurezza, procedure operative e near-miss reporting riducono infortuni e incidenti, migliorando prevenzione e cultura della sicurezza. Impatto negativo: attività prolungate al videoterminale e posture non corrette possono generare rischi ergonomici e disturbi muscolo-scheletrici, con 	GRI 403-9 GRI 403-10	Gestione della sicurezza nei luoghi di lavoro; Valutazione dei rischi e sorveglianza sanitaria	DVR (Documento di Valutazione dei Rischi); Formazione obbligatoria in materia di salute e sicurezza;

Tema materiale	Impatti e rilevanza del tema	KPI/GRI Standards	Attività che genera l'impatto	Impegni, politiche e strumenti di monitoraggio
	conseguenti assenze e calo di performance.			
Supporto/impatto sulla comunità e sul territorio locale	<ul style="list-style-type: none"> Impatto positivo: iniziative di sensibilizzazione cyber (formazione a scuole e PMI, campagne di awareness) e partnership con università e ITS accrescono le competenze digitali nel territorio e la resilienza delle comunità. Impatto negativo: incidenti cyber sui clienti possono generare impatti indiretti sul territorio, con interruzioni operative a livello locale e perdita di fiducia. 	GRI 413-1 GRI 203-1	Sviluppo di partnership con università, ITS e associazioni locali; Attività di formazione e sensibilizzazione cyber sul territorio	Collaborazione con Università Cattolica del Sacro Cuore. Accordo con Università di Ternopil. Rinnovo partnership con FAI. Programmi di security awareness per il territorio (Keatrix)
Capitale Ambientale				
Efficienza energetica	Possibilità di incidere positivamente o negativamente su: <ul style="list-style-type: none"> costi energetici attraverso azioni e progetti di efficientamento energetico tutela delle comunità locali e del territorio rispetto all'esposizione a eventi atmosferici estremi (es: alluvioni, allagamenti, uragani, desertificazione, ecc.) 	GRI 302-1	Monitoraggio dei consumi di energia in ottica di efficientamento energetico	Sottoscrizione contratto per l'acquisto di energia proveniente da sole fonti rinnovabili con certificato di origine

Il modello di business

Il Gruppo Cyberoo ha adottato un **business model** caratterizzato da risorse con forti competenze commerciali che presidiano in modo trasversale lo sviluppo del portafoglio clienti, integrate e coadiuvate da business solution specifiche per ogni area di competenza in grado di soddisfare le esigenze della propria clientela.

Oltre a una conoscenza approfondita delle necessità dei clienti, il modello di business del Gruppo si basa su un'elevata **specializzazione tecnica**, avvalendosi di partnership consolidate e di professionisti altamente qualificati e specializzati per il settore di riferimento, che richiede una marcata e specifica professionalità nonché capacità di integrazione di soluzioni tecnologiche complesse.

Analisi e individuazione delle esigenze del cliente

L'attività del Gruppo si articola inizialmente mediante un'accurata analisi delle esigenze del cliente e dei processi aziendali che conducono all'identificazione delle possibili implementazioni di soluzioni a servizio della gestione dei sistemi informativi. In tale fase, il team di specialisti del Gruppo procede a raccogliere informazioni sulle necessità di business dei clienti analizzando sia i fabbisogni espliciti che latenti, indipendentemente dalla tecnologia che verrà utilizzata: riveste, infatti, particolare importanza l'analisi degli aspetti organizzativi ai fini dell'individuazione delle lacune tecnologiche.

Comparazione delle soluzioni applicabili

In tale fase, vengono analizzate le principali soluzioni applicabili ai fabbisogni del cliente. In particolare, si procede all'analisi delle soluzioni personalizzate grazie all'apporto delle capacità professionali altamente specifiche delle risorse interne ed esterne a Cyberoo.

Progettazione delle soluzioni

Completate le attività di analisi, il Gruppo si occupa di progettare internamente le soluzioni tecnologiche da offrire al cliente, a supporto dell'implementazione dei processi organizzativi e operativi e al fine di garantire altresì una sicurezza integrale del perimetro aziendale.

All'esito dell'individuazione delle soluzioni e dei servizi tecnologici da offrire al cliente, si procede a elaborare l'offerta economica che dovrà essere sottoposta all'approvazione del cliente stesso. In particolare, il Gruppo, tenendo conto delle esigenze e caratteristiche del cliente, predispone una soluzione tecnologica strutturata attraverso la combinazione di software e/o hardware prodotti e

distribuiti dai propri partner e/o soluzioni tecnologiche sviluppate internamente dal Gruppo e concesse in licenza ai clienti. Al fine di proporre al cliente finale un'offerta adeguata alle sue esigenze, il Gruppo individua e seleziona le singole applicazioni, integrando le stesse in un'**unica soluzione tecnologica customizzata alle esigenze del modello di business del cliente**.

Installazione della soluzione

Una volta individuata la soluzione, il Gruppo svolge le **attività necessarie per l'attivazione e l'installazione della stessa sui sistemi del cliente**, il quale viene assistito e affiancato da risorse specializzate del Gruppo.

Erogazione dei servizi di gestione della soluzione

Il Gruppo offre, infine, al proprio cliente servizi di gestione della soluzione prescelta che comprendono: il **servizio di monitoraggio costante dei possibili malfunzionamenti, manutenzione ordinaria della soluzione, risoluzione di possibili errori procedurali**, nonché **implementazione di aggiornamenti**.

Le caratteristiche distintive di Cyberoo

Cyberoo si contraddistingue nel mercato di riferimento per una marcata "anima tech" che si riflette non solo nell'expertise tecnologica, ma soprattutto nelle proprie risorse umane, con l'obiettivo di realizzare per le imprese clienti una strategia globale in grado di proteggerle dagli attacchi esterni, monitorare e gestire le informazioni dell'ecosistema IT.

In particolare, il successo di Cyberoo può essere sinteticamente riassunto in determinati *fattori critici di successo* di seguito riportati:

- **Settore in forte crescita:** il Gruppo opera in un settore in continua crescita, contraddistinto da un ampio spettro di opportunità di sviluppo.
- **Personale dotato di competenze professionali specifiche e management con elevato know-how:** il Gruppo nasce dall'aggregazione di figure imprenditoriali con esperienza pluriennale nel settore dell'Information Technology con competenze distintive nella gestione di progetti e soluzioni

IT complesse per clienti appartenenti a settori strategici per l'economia italiana. Cyberoo offre un portafoglio completo di soluzioni a valore aggiunto per la clientela grazie all'apporto di figure professionali specializzate e dotate di elevate competenze nel settore di riferimento. Grazie a ciò, ha la capacità di sviluppare ed offrire tempestivamente alla propria clientela soluzioni personalizzabili e servizi integrati a supporto delle principali piattaforme infrastrutturali.

- **Comprovata capacità di M&A:** nel perseguimento della strategia di crescita intrapresa fin dalla sua fondazione dal management per il tramite di operazioni di merger & acquisition, il Gruppo ha maturato una considerevole esperienza nelle attività di selezione di società e aziende target e nell'integrazione delle stesse all'interno del Gruppo. Tale capacità ha trovato ulteriore conferma nel corso del 2025, con la fusione per incorporazione della controllata MFD International S.r.l. in Cyberoo S.p.A. — finalizzata a semplificare la struttura societaria del Gruppo — e con l'acquisizione di due partecipazioni estere, in Albania e in Ucraina, e di un ramo d'azienda dalla controllante Cyberoo Globl S.p.A.
- **Capacità di offrire soluzioni tecnologiche innovative:** il Gruppo, grazie a un costante investimento nella ricerca e nello sviluppo, è fortemente orientato all'innovazione di servizi e all'offerta di soluzioni proprietarie sviluppate in house ed è in grado di mantenere un'elevata competitività a livello tecnologico.
- **Modello di distribuzione TIER II:** Cyberoo adotta questo modello di distribuzione, basato su una rete indiretta di distributori e partner a valore, che consente una penetrazione capillare del mercato grazie a relazioni consolidate con i clienti finali. Questa scelta strategica permette di massimizzare l'efficienza commerciale, ridurre i costi di acquisizione, aumentare la fidelizzazione e garantire una crescita scalabile, valorizzando le competenze e la presenza locale dei partner. Sedoc Digital Group, azionista di riferimento e tra i principali partner commerciali, dal 1° luglio 2024 acquisisce le soluzioni Cyberoo tramite il sistema distributivo nazionale e non più attraverso il canale diretto. Coerentemente con questo percorso di razionalizzazione dei rapporti con parti correlate, nel corso dell'esercizio l'esposizione creditizia verso Sedoc Digital Group si è ridotta in misura

significativa, passando da 11,53 milioni di euro al 31 dicembre 2024 a 2,56 milioni di euro al 31 marzo 2026 (circa -78%), in anticipo rispetto alla traiettoria di rientro comunicata al mercato. La riduzione è stata conseguita attraverso i piani di rientro definiti tra le parti e ulteriori operazioni volte a diminuire la concentrazione del rischio di credito e a migliorare la qualità del capitale circolante.

Le linee di prodotti e servizi

Si riporta di seguito una sintesi delle principali aree di attività e delle soluzioni e servizi sviluppati dal Gruppo Cyberoo.

Le attività di **Cyberoo S.p.A.** sono organizzate secondo il modello ORBIS, framework proprietario che integra in un unico ecosistema le principali dimensioni della gestione del rischio informatico, rappresentate da threat management, governance dei processi, compliance normativa e regolatoria e security awareness.

Cyber Security Suite (Threat Management)

La Cyber Security Suite è un servizio evoluto di Threat Management, finalizzato alla protezione degli ambienti IT aziendali attraverso un presidio continuativo di sicurezza informatica.

Il servizio integra i sistemi di sicurezza già presenti presso il cliente con una piattaforma di raccolta e correlazione degli eventi, consentendo il monitoraggio continuo dell'infrastruttura IT e l'identificazione di anomalie e potenziali minacce. Le informazioni raccolte vengono analizzate e correlate al fine di supportare le attività di rilevazione e gestione degli eventi di sicurezza.

Il servizio è erogato attraverso un I-SOC (Intelligence Security Operations Center) attivo 24/7, che svolge attività di analisi, verifica e gestione degli allarmi, contribuendo alla riduzione dei falsi positivi e alla definizione delle azioni di risposta agli incidenti.

La Cyber Security Suite si articola nei servizi Cypeer e Cyber Security Intelligence (CSI). Cypeer consente la raccolta, aggregazione e correlazione degli eventi provenienti dall'infrastruttura IT del cliente, fornendo una visione integrata della postura di sicurezza interna. CSI è il servizio di Cyber Threat Intelligence basato su

fonti OSINT, deep e dark web, finalizzato all'identificazione di minacce esterne e alla rilevazione di eventuali esposizioni dell'azienda sul web.

Titaan Neemesi

Titaan Neemesi è la soluzione del Gruppo dedicata alla gestione della compliance GDPR e alla sicurezza dell'infrastruttura IT. La piattaforma consente la raccolta e la correlazione dei log e degli eventi provenienti dai principali componenti dell'ambiente IT, inclusi servizi, applicazioni, server, infrastruttura e directory services, all'interno di un unico centro di controllo.

La soluzione garantisce l'inalterabilità dei dati e dei log raccolti grazie all'utilizzo di tecnologie blockchain e si basa sui principi di Privacy by Design e Privacy by Default. Titaan Neemesi supporta inoltre il monitoraggio degli eventi relativi ad Active Directory e l'identificazione di anomalie e criticità operative, contribuendo al rafforzamento della sicurezza e della governance dell'infrastruttura IT.

Keatrix

È la piattaforma proprietaria di Human Risk & Security Awareness sviluppata da Cyberoo per supportare le organizzazioni nella gestione del rischio cyber associato al fattore umano attraverso percorsi strutturati di formazione, sensibilizzazione e misurazione dei comportamenti degli utenti. La soluzione nasce dalla considerazione che una quota rilevante degli incidenti di sicurezza informatica è riconducibile a errori umani, comportamenti non consapevoli o insufficiente conoscenza delle principali minacce digitali. La piattaforma adotta un approccio orientato al cambiamento comportamentale, superando i tradizionali modelli di formazione basati sulla sola trasmissione di contenuti informativi. Keatrix combina metodologie derivate dalle neuroscienze cognitive, tecnologie di apprendimento adattivo basate sull'intelligenza artificiale e contenuti di edutainment, con l'obiettivo di migliorare l'efficacia dell'apprendimento e favorire l'adozione di comportamenti sicuri nel tempo. L'intelligenza artificiale consente di personalizzare i percorsi formativi in funzione delle caratteristiche, dei comportamenti e del livello di apprendimento del singolo utente, mentre le tecniche di adaptive learning, spacing e interleaving supportano il consolidamento delle conoscenze e la loro applicazione in contesti operativi reali. La piattaforma integra, inoltre, strumenti di verifica e misurazione dell'efficacia formativa,

permettendo alle organizzazioni di monitorare l'evoluzione del livello di consapevolezza e del rischio umano all'interno dell'azienda. Attraverso Keatrix, Cyberoo intende contribuire al rafforzamento della cultura della cybersecurity nelle organizzazioni, trasformando la formazione in un processo continuo di riduzione del rischio e di incremento della resilienza aziendale rispetto alle minacce informatiche.

Cyberoo Docetz S.r.l.

Cyberoo Docetz S.r.l. offre attività di consulenza avanzata in ambito cybersecurity attraverso diverse business unit specializzate:

- **Incident Response Team (IRT):** preposto alla gestione tempestiva degli incidenti di sicurezza, il team valuta l'impatto degli incidenti, definisce e attua processi di mitigazione, contenimento e ripristino, adottando misure preventive per ridurre il rischio di future violazioni.
- **Risk Assessment:** identificazione e valutazione di rischi e vulnerabilità con definizione e monitoraggio di misure di mitigazione per aumentare la resilienza aziendale.
- **Cyber Security Advisory & vCISO:** consulenza e supporto operativo nella definizione di politiche, procedure e tecnologie di sicurezza; il vCISO coordina sicurezza, risposta agli incidenti e conformità normativa secondo le best practice del settore
- **Vulnerability Assessment & Penetration Test:** analisi delle vulnerabilità dei sistemi e simulazione di attacchi reali per testarne la resilienza, con raccomandazioni operative per rafforzare la sicurezza.
- **Compliance & NIS2:** supporto alle aziende nell'adeguamento a normative e standard di sicurezza, inclusa la certificazione ISO 27001 e la conformità alla direttiva NIS2, per garantire protezione dei dati e delle risorse aziendali.

Cyberoo51, ha lo scopo di portare il valore e l'integrazione della tecnologia digitale in tutte le aree di un'azienda, cambiando radicalmente il modo in cui esse operano, apportando valore ai clienti e supportandone il cambiamento culturale.

I servizi di digital transformation, data protection e Intelligenza Artificiale comprendono le seguenti soluzioni:

- CRM (Customer Relationship Management) è un software manageriale, strategico ed operativo, che pone il cliente al centro della propria azienda e che porta straordinari benefici al proprio business. In particolare, CRM consente di creare un'efficace pianificazione, gestione e monitoraggio di tutte le attività legate ai clienti. Su ogni modulo è possibile impostare dei processi automatizzati per aumentarne l'efficienza, soprattutto se la mole di dati inseriti viene aggiornata frequentemente. Tale software permette altresì di personalizzare le relazioni con i propri contatti, creare comunicazioni ed attività mirate e sviluppare, conseguentemente, l'offerta che meglio soddisfa le particolari esigenze di ciascun interlocutore in tempi rapidi.
- HRM (Human Resources Management) è un software ideato al fine di supportare l'attività quotidiana di ciascun dipendente e dell'intera azienda, garantendo risultati immediati ed elevate prestazioni in termini di ottimizzazione. L'applicativo è in grado di gestire in maniera efficiente le presenze in azienda, le entrate/uscite dei dipendenti, le richieste ferie e/o permessi, i processi di rimborso spese. Inoltre, il software può includere al suo interno dei moduli per l'assegnazione dei compiti di progetto, con conseguente misurazione della performance individuale per dipendente e reportistica sulle performance di lavoro. HRM aiuta altresì gli ospiti a connettersi alla rete wi-fi aziendale in modo autonomo e consente di creare una sezione dove scambiare documenti fra colleghi.
- PMS (Product Management System) è una soluzione che consente alle aziende di organizzare puntualmente i dati dei propri prodotti, accentrando in un unico sistema per renderli disponibili e fruibili. Le funzionalità di integrazione con gestionali e software aziendali rendono il PMS uno strumento con un'interfaccia strutturata, che automatizza i processi di gestione, ricerca, estrapolazione, raccolta e pubblicazione su più canali aziendali (website, B2B, B2C) dei dati relativi ai diversi prodotti e servizi commercializzati.
- C51 CheckIn è una soluzione ideata per gestire l'accesso e l'accoglienza dei visitatori in reception in modo organizzato e automatizzato, tutelando le esigenze di sicurezza. Allo stesso tempo tale soluzione migliora l'immagine

aziendale, contribuendo a garantire l'idea di un'azienda all'avanguardia. Tale applicativo consente quindi di controllare i flussi di accesso nelle varie sedi del Gruppo con modalità innovative (tramite app). Inoltre, mediante tale soluzione, l'ospite ha altresì la possibilità di visionare l'informativa sulla privacy aziendale, al fine di tutelare la sua sicurezza e la sua permanenza in azienda.

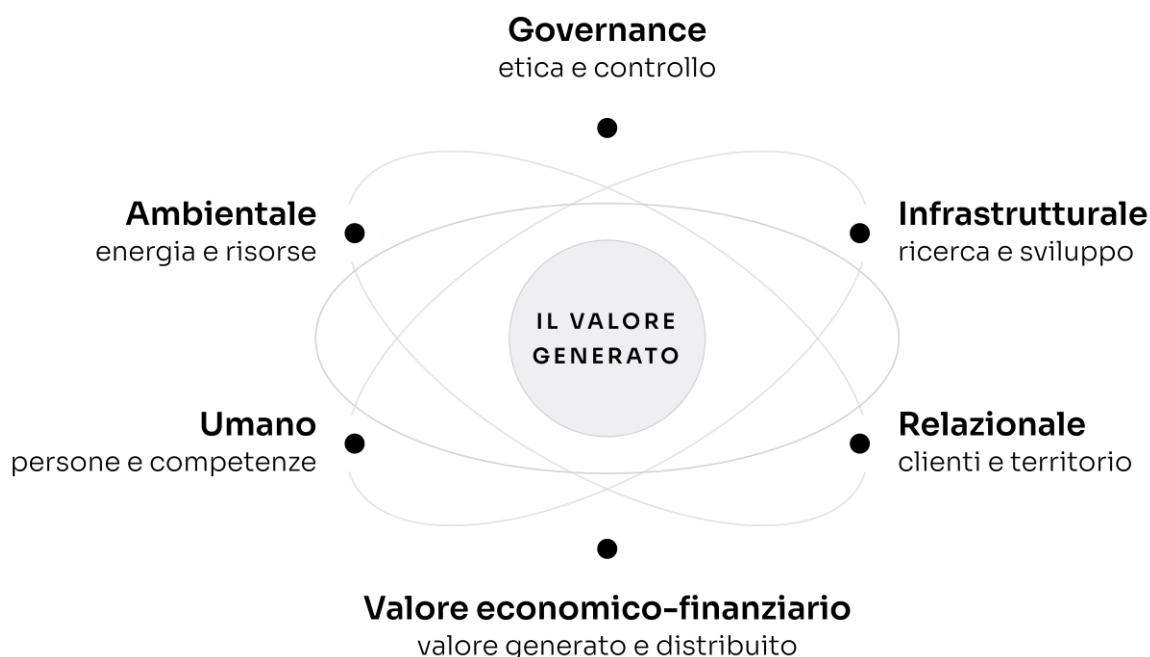
- C51 Events è l'applicativo pensato per migliorare e ottimizzare la gestione di eventi in presenza. Disponibile sia per mobile che versione web, aiuta a concentrare tutte le attività necessarie per l'organizzazione in un unico spazio e a rendere perfetto l'evento.
- C51 Commerce è la piattaforma proprietaria per siti e-commerce di Cyberoo51 in grado di adattarsi alle specifiche esigenze di ognuno dei suoi clienti, integrando i loro processi aziendali e creando per ognuno un design unico e completamente personalizzato. Consente di gestire i portali di vendita online, sia B2B che B2C, con un sistema multiplatforma e multilingua che guida l'utente nel suo processo di acquisto.
- Digital marketing: comprende tutte le attività di marketing di un'azienda volte a sviluppare la propria rete commerciale, analizzare i trend di mercato, prevederne l'andamento e creare offerte nel profilo del cliente target, con lo scopo di commercializzare beni o servizi, aumentare clienti e rafforzare il proprio brand (ad esempio: SEO, social media marketing, web advertising, web marketing, web design, e-commerce).
- App mobile: comprende la progettazione, lo sviluppo, la realizzazione e la manutenzione di applicazioni mobile per dispositivi iOS e Android, utili per la comunicazione interna ed esterna alle aziende, consentendo l'interazione tra gli utenti in qualsiasi luogo e momento in modo semplice.
- AMY: un sistema integrato basato sull'Intelligenza Artificiale (IA) progettato per assistere, migliorare ed evolvere il lavoro quotidiano dei dipendenti in ogni settore d'impiego.



Capitolo 2
IL 2025
IN SINTESI

2. Il 2025 in sintesi - Highlights

Il presente capitolo offre una rappresentazione sintetica dei principali temi affrontati dal Gruppo Cyberoo nell'esercizio 2025 e dei risultati più significativi raggiunti nel corso del periodo di rendicontazione (1° gennaio 2025 – 31 marzo 2026). Attraverso una serie di schede tematiche organizzate per capitali, sono richiamati i temi materiali rendicontati, gli Obiettivi di Sviluppo Sostenibile (SDGs) delle Nazioni Unite ai quali le attività del Gruppo contribuiscono, e i risultati chiave conseguiti in ambito economico-finanziario, ambientale, sociale e di governance. Le informazioni riportate rappresentano una sintesi di quanto approfondito nei singoli capitoli del Bilancio, ai quali si rimanda per un'analisi puntuale delle politiche adottate, degli indicatori di performance e dei processi di gestione presidiati dal Gruppo.



TEMI MATERIALI RENDICONTATI

Privacy e sicurezza dei dati e delle informazioni

GOVERNANCE

Etica, controllo e conformità

Quello che non è successo

0 **Episodi di corruzione**
accertati nel triennio 2023-2025

0 **Azioni legali**
per pratiche anticoncorrenziali,
antitrust o monopolio

0 **Data breach**
e denunce comprovate
sulla privacy dei clienti

Quello che è stato fatto

01 **Modello 231/2001**
Codice Etico e nomina
dell'Organismo di Vigilanza

02 **Direttiva NIS2**
Registrazione al portale ACN

03 **Made in Europe**
Marchio europeo rilasciato da ECSO

04 **AI Act**
Avvio dell'adeguamento al
Regolamento UE 2024/1689

SDGs SUPPORTATI

SDG 9 Imprese, innovazione e infrastrutture · SDG 16 Pace, giustizia e istituzioni solide
SDG 17 Partnership per gli obiettivi

TEMI MATERIALI RENDICONTATI

Ricerca & Sviluppo e innovazione



Le piattaforme nate nel 2025

- 
Keatrix
Human Risk & Security
Training su AI adattiva
- 
AMY
Assistente AI proprietario
basato su LLM e tecnologia RAG
- 
CyberBoar
Piattaforma modulare GRC
per governance, compliance
e supply chain security

ISO/IEC 27001:2022

rinnovata nel 2025

SDGs SUPPORTATI

SDG 8 Lavoro dignitoso e crescita economica

SDG 9 Imprese, innovazione e infrastrutture

TEMI MATERIALI RENDICONTATI

Privacy e sicurezza dei dati e delle informazioni
Soddisfazione e gestione delle relazioni con i clienti
Supporto e impatto sulla comunità e sul territorio locale

CAPITALE RELAZIONALE

La rete delle relazioni nel 2025



Sostegno sociale e donazioni

Rinnovo triennale con il FAI, Progetto Itaca (salute mentale) e SanPro Special (sport paraolimpico)

SDGs SUPPORTATI

SDG 4 Istruzione di qualità · SDG 9 Imprese, innovazione e infrastrutture
SDG 17 Partnership per gli obiettivi

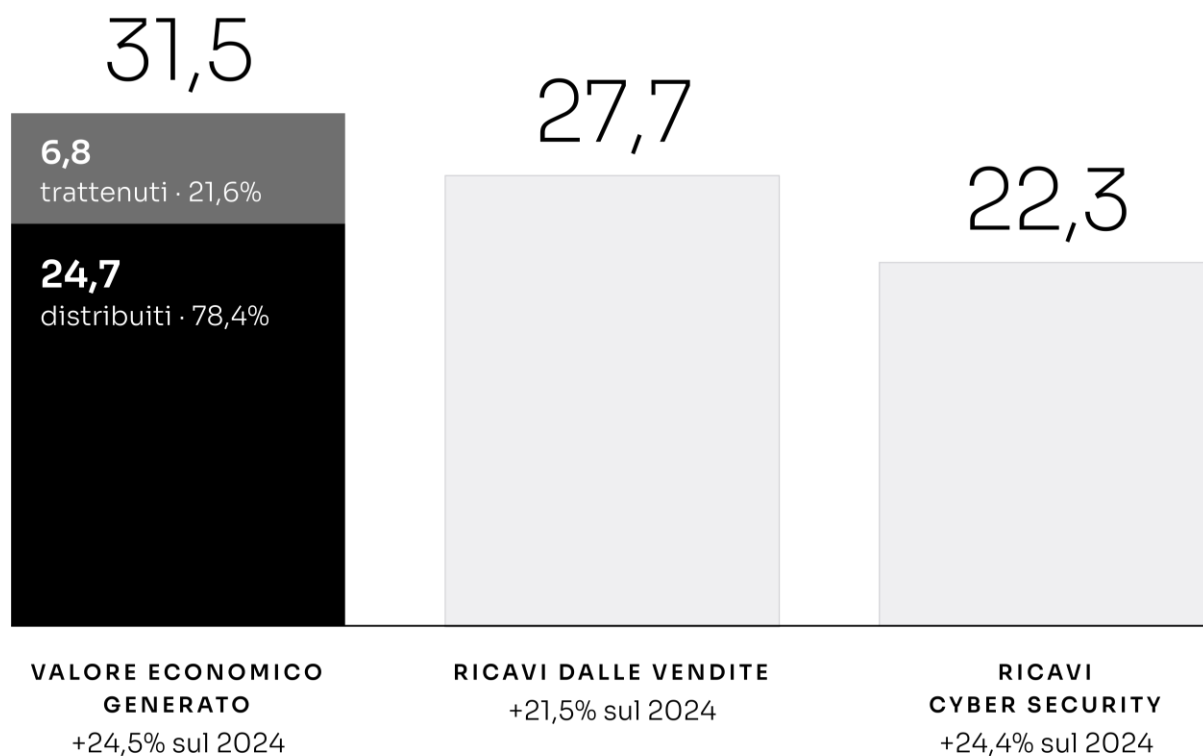
TEMI MATERIALI RENDICONTATI

Generazione e distribuzione di valore economico e finanziario

CAPITALE ECONOMICO E FINANZIARIO

Il valore generato nel 2025

milioni di euro



Le due colonne di destra sono voci comprese nel valore generato.

0 **CONTENZIOSI TRIBUTARI**
significativi nell'esercizio

SDGs SUPPORTATI

SDG 8 Lavoro dignitoso e crescita economica
SDG 9 Imprese, innovazione e infrastrutture

TEMI MATERIALI RENDICONTATI

Condizioni di lavoro, clima interno e welfare aziendale

Formazione e sviluppo delle competenze · Salute e sicurezza sul lavoro

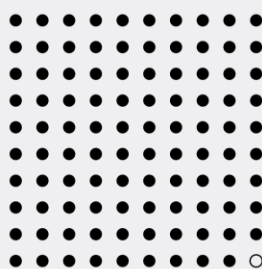
CAPITALE UMANO

Persone, competenze e sicurezza

177

DIPENDENTI DI GRUPPO

+17% sul 2024



99% A TEMPO
INDETERMINATO

100%

DEI DIPENDENTI
ITALIANI COPERTI
DA CCNL

1.671

ORE DI FORMAZIONE

erogate nel 2025

0

INFORTUNI E MALATTIE

nel triennio 2023-2025

SDGs SUPPORTATI

SDG 3 Salute e benessere · SDG 4 Istruzione di qualità · SDG 5 Parità di genere

SDG 8 Lavoro dignitoso e crescita economica

TEMI MATERIALI RENDICONTATI

Efficienza energetica

CAPITALE AMBIENTALE

Energia, risorse e impatto

^
123

GIGAJoule AUTOPRODOTTI

da fonti rinnovabili, +20,5% sul 2024

∨
4,28

TONNELLATE DI RIFIUTI

prodotte, -39,5% sul 2024



**RIFIUTI NON
PERICOLOSI**

sul totale
prodotto nel 2025

Energia rinnovabile

Fornitura da sole fonti rinnovabili
con certificato di origine.

Data center certificati

Server presso terze parti
con ISO 14001 e ISO 50001.

SDGs SUPPORTATI

SDG 7 Energia pulita e accessibile · SDG 12 Consumo e produzione responsabili
SDG 13 Lotta al cambiamento climatico



Capitolo 3

GOVERNANCE

3. Governance

La gestione responsabile d'impresa

Cyberoo crede fermamente che la definizione di specifiche procedure che regolano la gestione dell'impresa orientate alla creazione di valore condiviso sia fondamentale per perseguire la crescita sostenibile della società.

Grazie alla spinta dei vertici del Gruppo nell'adottare strategie sempre più orientate alla sostenibilità, Cyberoo tramite il presente Bilancio di Sostenibilità ha l'obiettivo di implementare l'attività di comunicazione esterna al fine di incentivare una trasparente, puntuale e accurata informazione agli *stakeholder* relativamente agli sviluppi strategici e operativi.

Cyberoo è determinata ad assicurare la massima correttezza nella conduzione dei propri affari e delle relative attività aziendali, anche a tutela della propria immagine e reputazione: per questo motivo nel corso del 2025 ha adottato Modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001.

La governance

Cyberoo adotta il sistema di governo tradizionale costituito dai seguenti organi sociali:

- l'Assemblea degli Azionisti (competente a deliberare in ordine alle materie previste dalla legge e dallo Statuto sociale);
- il Consiglio di Amministrazione (a cui è affidata la gestione della Società);
- il Collegio Sindacale (organo di vigilanza sull'osservanza della legge e dello statuto e sul rispetto dei principi di corretta amministrazione).

A tali organi si affianca la revisione legale dei conti, affidata ad una società di revisione esterna.

All'approvazione del bilancio al 31 dicembre 2024, in occasione dell'assemblea del 28 aprile 2025, sono state rinnovate le cariche dell'intero Consiglio di Amministrazione, del Collegio Sindacale¹ e della Società di Revisione. Nella

¹ È stato nominato Luciano Volta come Sindaco supplente al posto di Mariangela Rossetti.

medesima seduta, in sede straordinaria, l'Assemblea ha modificato l'art. 29 dello statuto sociale, fissando la chiusura dell'esercizio sociale al 31 marzo di ciascun anno in luogo del 31 dicembre. L'incarico di revisione legale dei conti per gli esercizi 2025-2027 è stato conferito a BDO Italia S.p.A.

Il Consiglio ha designato Massimo Bonifati nella carica di Presidente. Il Consiglio di Amministrazione rimarrà in carica sino all'approvazione del bilancio al 31 marzo 2028.

Consiglio di Amministrazione	Massimo Bonifati	Fabio Leonardi	Davide Cignatta	Veronica Leonardi	Riccardo Pietro Leonardi	Renzo Bartoli	Alessandro Viotto
Funzione	Presidente	Consigliere	Consigliere	Consigliere	Consigliere	Consigliere indipendente	Consigliere indipendente
Esecutivo / Non esecutivo	Non esecutivo	Esecutivo	Esecutivo	Esecutivo	Non esecutivo	Non esecutivo	Non esecutivo
Altre posizioni rivestite nel Gruppo Cyberoo e/o esternamente	-	C.E.O Cyberoo S.p.A.	Sales Director	C.M.O. Cyberoo S.p.A.	-	-	-

Il Consiglio di Amministrazione è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società, con la facoltà di compiere tutti gli atti che ritenga opportuni per il raggiungimento dell'oggetto sociale, esclusi quelli che la legge riserva all'Assemblea.

Nel 2024 la società ha rinominato il Responsabile della Protezione dei Dati (RPD o DPO) ai sensi dell'art. 37 del Regolamento UE 2016/679 (GDPR).

Con riferimento alla composizione degli organi di amministrazione delle società ricomprese nel perimetro di rendicontazione ESG, si segnala che, oltre a Cyberoo S.p.A., anche le ulteriori tre società appartenenti al medesimo perimetro presentano la stessa composizione dell'organo amministrativo, costituita da Massimo Bonifati, Davide Cignatta, Veronica Leonardi e Fabio Leonardi, quest'ultimo in qualità di Legale Rappresentante. Tale configurazione evidenzia l'omogeneità della struttura di governance delle società incluse nel perimetro oggetto di rendicontazione per il periodo 1° gennaio 2025 – 31 marzo 2026.

Composizione degli organi amministrativi delle società considerate – Diversità (genere – classi di età)					
Donne		Uomini		Totale	
Nr	%	Nr	%	Nr	%
4	21%	15	79%	19	100%
Minori di 30 anni		Tra 30 e 50 anni		Maggiori di 50 anni	
Nr	%	Nr	%	Nr	%
-	-	10	53%	9	47%

Il Collegio Sindacale, nominato dall'assemblea del 28 aprile 2025, rimarrà in carica per tre esercizi, sino all'approvazione del bilancio chiuso al 31 marzo 2028, ed è composto da 3 membri effettivi e 2 supplenti.

Collegio Sindacale	Gianluca Settepani	Rita Sciaraffa	Alberto Ventura	Luciano Volta	Claudia Peri
Funzione	Presidente	Sindaco effettivo	Sindaco effettivo	Sindaco supplente	Sindaco supplente
Esecutivo / Non esecutivo	Non esecutivo	Non esecutivo	Non esecutivo	Non esecutivo	Non esecutivo
Altre posizioni rivestite nel Gruppo Cyberoo e/o esternamente	-	-	-	-	-

Collegio Sindacale – Diversità (genere – classi di età)					
Donne		Uomini		Totale	
Nr	%	Nr	%	Nr	%
2	40%	3	60%	5	100%
Minori di 30 anni		Tra 30 e 50 anni		Maggiori di 50 anni	
Nr	%	Nr	%	Nr	%
-	-	4	80%	1	20%

Assetto organizzativo

L'assetto organizzativo esprime il sistema di funzioni, poteri, deleghe, processi decisionali e procedure aziendali e fornisce una chiara individuazione dei compiti e delle responsabilità di ciascuno rispetto alle attività aziendali.

La struttura organizzativa del Gruppo Cyberoo è fortemente improntata a fornire una governance della Società, oltre che a definire i principi dell'organizzazione aziendale, della gestione dei processi e delle risorse.

I sistemi di gestione

Cyberoo ha istituito un Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni (SGI), inteso come sistema per garantire e migliorare la qualità dei processi aziendali, in conformità ai requisiti della norma **ISO/IEC 27001:2022**.

In coerenza con la natura del business, la Società ha identificato nella sicurezza delle informazioni l'asse portante del proprio sistema di gestione integrato, presidiando attraverso il SGI tanto la protezione del patrimonio informativo quanto il miglioramento continuo dei processi operativi.

Il SGI si fonda sulla gestione e il governo dei processi primari di business - progettazione, realizzazione ed erogazione di servizi di cybersecurity, cyber security awareness, managed detection and response (MDR) e monitoraggio infrastrutture fisiche e virtuali attraverso strumenti di intelligenza artificiale, di correlazione avanzata degli eventi e tecnologie di machine learning - e costituisce l'insieme di responsabilità, procedure, strutture e risorse predisposte per realizzare la Politica per la Sicurezza delle Informazioni, garantendo la riservatezza, integrità e disponibilità delle informazioni.

A presidio della gestione dei processi, il Gruppo ha:

- identificato e documentato i processi operativi, stabilendone sequenze e interazioni;
- definito per ogni processo gli elementi in ingresso, gli elementi in uscita, le responsabilità e i documenti di riferimento;
- individuato i punti di controllo interni;
- individuato le interfacce e i requisiti di sicurezza dei fornitori esterni (contenuti in appositi documenti contrattuali o attraverso audit eseguiti da Cyberoo).

Le policy e le procedure di sicurezza delle informazioni definite nel SGI costituiscono il riferimento operativo anche per le attività svolte dalle società controllate del Gruppo, nell'ambito della direzione e coordinamento esercitata dalla capogruppo.

Certificazioni e riconoscimenti

- La certificazione ISO/IEC 27001:2022 è stata rinnovata il 20 ottobre 2025 (certificato DNV n. 10000375538, valido fino al 23 dicembre 2026, Dichiarazione di Applicabilità v.5 del 17 ottobre 2025). Il campo di applicazione è stato ampliato rispetto al precedente ciclo, includendo esplicitamente i servizi di cyber security awareness e di MDR, oltre al monitoraggio di infrastrutture sia fisiche che virtuali.
- Nel 2025 la Società ha ottenuto il marchio "Cybersecurity Made in Europe" rilasciato da ECSO (European Cyber Security Organisation), che attesta l'origine europea, la qualità e la conformità normativa dei servizi offerti, coerentemente con le politiche ENISA e con il Regolamento GDPR.

Conformità normativa

In ottemperanza al D.Lgs. 138/2024 (recepimento della Direttiva NIS2), Cyberoo ha completato la registrazione sul portale dell'Agenzia per la Cybersicurezza Nazionale (ACN) e la designazione del referente CSIRT, come previsto dalla Determinazione ACN 379887/2025. L'adeguamento alle misure di sicurezza di base e agli obblighi di notifica degli incidenti è in corso secondo le tempistiche previste dalla normativa.

Sviluppi futuri

Tra gli obiettivi di evoluzione del SGI, Cyberoo prevede di integrare il proprio sistema con le linee guida ISO/IEC 27035 per la gestione degli incidenti di sicurezza delle informazioni. Con riferimento al Regolamento (UE) 2024/1689 (AI Act), la Società ha avviato un percorso di adeguamento normativo, in considerazione del ruolo che le tecnologie di intelligenza artificiale e machine learning rivestono nell'erogazione dei propri servizi di cybersecurity. L'obiettivo è assicurare la piena conformità ai requisiti del Regolamento entro le scadenze previste per i sistemi applicabili.

Compliance normativa

Nel corso del 2025 non si sono verificati eventi che hanno dato origine a sanzioni e/o contenziosi per non conformità a leggi, normative in materia ambientale, sociale ed economica.

Analogamente, alla data di redazione del presente Bilancio di sostenibilità, nessuna contestazione e/o denuncia da parte esterna o da enti regolatori è ad oggi pervenuta alla Società per non conformità a leggi e normative in materia sociale, economica e fiscale, né le sono state comminate sanzioni per violazioni delle normative nelle attività di marketing e per comportamenti anti-competitivi. Tali risultati riflettono l'efficacia dei presidi adottati dal Gruppo.

Gestione dei rischi

Cyberoo adotta un approccio strutturato alla gestione dei rischi, integrato nei propri presidi di governance, nel Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni e nel Modello 231. Tale approccio si basa sull'identificazione dei processi aziendali rilevanti, sulla mappatura delle attività sensibili e dei punti di controllo, sulla definizione di procedure e responsabilità e sul monitoraggio dei rischi operativi, di compliance, informatici e connessi alla supply chain.

Il monitoraggio è supportato, da un lato, dai presidi del SGI - che prevedono la documentazione dei processi, l'individuazione di input, output, responsabilità e interfacce con i fornitori esterni - e, dall'altro, dal Modello 231, che contempla analisi dei rischi-reato, flussi informativi verso l'Organismo di Vigilanza, verifiche periodiche e azioni correttive. In ambito cybersecurity, il presidio è ulteriormente rafforzato da policy interne orientate alla prevenzione e al rilevamento tempestivo degli incidenti, nonché da procedure di notifica e controlli sui fornitori.

In prospettiva, Cyberoo è impegnata nel continuo aggiornamento dei propri processi di risk management per recepire l'evoluzione normativa e organizzativa, anche in relazione agli adempimenti connessi a NIS2, DORA e al quadro europeo sull'intelligenza artificiale.



Capitolo 4

CAPITALE INFRASTRUTTURALE

4. Capitale infrastrutturale

Innovazione e digitalizzazione

Cyberoo, attenta all'evoluzione tecnologica e in ottica di miglioramento continuo, sta procedendo con un massiccio lavoro di ottimizzazione delle soluzioni e dei processi interni: partendo dall'analisi dei punti di forza e debolezza di ogni entità aziendale, sono stati disegnati nuovamente i flussi operativi delle varie business unit secondo modello BPM², consentendo così di avere ben chiaro il risultato di ogni fase.

Nel 2025 il Gruppo Cyberoo ha consolidato il percorso di evoluzione organizzativa avviato negli anni precedenti, trasformando il lavoro di revisione dei flussi interni in un modello operativo più strutturato, misurabile e orientato alla scalabilità. L'attività si è concentrata sulla standardizzazione dei processi chiave, sul rafforzamento della governance interfunzionale e su una più chiara attribuzione di ruoli, responsabilità e punti di controllo, con l'obiettivo di rendere l'operatività sempre più fluida, integrata e coerente con la crescita del Gruppo. Parallelamente, è proseguita l'adozione di metodologie di miglioramento continuo e di strumenti di monitoraggio a supporto delle decisioni, favorendo una progressiva riduzione delle inefficienze interne, una maggiore rapidità di esecuzione e un ulteriore innalzamento della qualità dei servizi erogati a clienti e partner. In questo contesto, il 2025 ha rappresentato per Cyberoo un anno di messa a terra e consolidamento, in cui innovazione di processo, cultura organizzativa ed eccellenza operativa hanno agito in modo sempre più sinergico.

I progetti

Cyber Security Suite

La Cyber Security Suite è composta da CSI (Cyber Security Intelligence) e Cypeer.

La Soluzione CSI è composta dalla sinergia di diversi servizi volti a identificare nel web (clear, dark e deep) tutti i segnali che possano far supporre che vi è un'attività

² BPM: Business Process Modeling

propedeutica alla violazione della cyber-sicurezza delle realtà monitorate o che vi è stato un attacco e quali servizi/informazioni sono stati colpiti. CSI sfrutta l'accesso a informazioni pubbliche analizzandole mediante complessi algoritmi di navigazione e di estrapolazione semantica del contenuto di informazioni presenti nel web, nel dark e deep web per ottenere una serie di informazioni relative alla sicurezza dall'azienda cliente.

Di seguito vengono descritti sinteticamente i diversi servizi che compongono la soluzione e le funzionalità operative ad essi associati che sono disponibili al termine delle attività implementative della soluzione.

1. Servizio CSI di Data Breach

Il servizio di Data Breach si pone l'obiettivo di mostrare al cliente una visione completa dello stato di compromissione delle credenziali relative alla propria realtà. Per effettuare questa attività vengono utilizzate conoscenze e servizi che effettuano la raccolta di tutte le credenziali apparse pubblicamente online. Tale raccolta include anche le credenziali non rilasciate pubblicamente, ma vendute o diffuse nei Black Market online dagli autori della compromissione.

2. Servizio CSI di Domini Malevoli

Gli agenti malevoli che effettuano attacchi a utenti e società, con lo scopo di trarre del profitto con attività illecite, devono preparare l'ambiente necessario affinché il loro attacco vada a buon fine. Questo ambiente deve necessariamente attestarsi pubblicamente in Internet, poiché questa tipologia di attacco viene effettuata completamente da remoto.

Il fattore comune di molteplici tipologie di attacco, ad esempio attacchi come Phishing, Spear Phishing, CEO Fraud, IT Fraud, Malware campaign ecc., consistono nella registrazione di domini web afferenti all'obiettivo dell'attacco. Se l'obiettivo dell'attacco è una società o un'azienda, gli attaccanti con l'intenzione di perpetrare un attacco come quelli di cui sopra, effettueranno molto probabilmente delle registrazioni di dominio con nomi simili a quelli utilizzati legittimamente dalla società. Il servizio si propone di analizzare tutti i domini recentemente registrati a livello mondiale al fine di identificare quelli che potrebbero essere stati registrati per effettuare, di lì a breve, attività malevole ai danni dei Clienti. Questo servizio effettua un'analisi dei domini registrati nelle ultime 24 ore su un ampio insieme di

Top-Level Domain (gTLD e ccTLD, es. .com, .org, .net, .it, .eu). Il servizio effettua un'analisi della somiglianza dei domini registrati con i domini dei Clienti sotto monitoraggio. Se la somiglianza supera una certa soglia, viene inviata una notifica a MSS che si opererà per analizzare il dominio sospetto e, se le analisi avranno dato riscontro positivo, attuare le procedure necessarie per implementare attività mitigative prima dell'accadimento dell'attacco.

3. Servizio CSI di Early Warning

Ogni giorno vengono identificate da parte di ricercatori e società di ricerca nuove vulnerabilità e problematiche che possono impattare sulla postura di sicurezza cyber di qualunque ente, società o azienda. Mantenersi aggiornati sugli ultimi ritrovamenti in materia di cybersecurity non è semplice e, in particolar modo, risulta ancor più ostico scremare tutte le informazioni con lo scopo di identificare solo quelle realmente utili per la propria realtà aziendale. Il servizio sviluppato si pone l'obiettivo di fornire al Cliente evidenza delle ultime notizie in ambito cybersecurity focalizzandosi specificatamente sulla realtà del Cliente. Tale specificità viene concordata con il Cliente stesso nel momento dell'attivazione del servizio e può integrare diverse aree di competenza. L'attività viene eseguita in modo automatico facendo uso di funzionalità atte alla raccolta, categorizzazione e visualizzazione delle informazioni.

4. Servizio CSI di Deep Analysis

Molte informazioni di forte interesse per l'area di cybersecurity non vengono rese pubblicamente disponibili dato il loro valore di mercato in questo ambito. Informazioni come gravi vulnerabilità di sistemi molto diffusi, informazioni trafugate illegittimamente contenenti dati personali come username e password o le modalità per l'accesso non autorizzato a sistemi privati non vengono rese pubbliche, ma esistono, e possono essere recuperate sotto certe condizioni.

I vantaggi che offre la piattaforma ai propri clienti sono:

- up to date nuove minacce: l'I-SOC di Cyberoo è costantemente attivo sull'analisi del deep e dark web allo scopo di scovare informazioni rilevanti per la sicurezza e per rimanere aggiornati sulle più recenti tecniche di hacking;

- **root cause analysis:** circoscrive il problema, basandosi sulla correlazione di una o più metriche. Monitora i valori presupposti di quelle metriche, e i valori attuali. Individua chi e come sta causando un mal funzionamento;
- **eliminazione dei falsi positivi:** grazie al lavoro di intelligence e correlazione effettuato dai Cyber security specialist, il cliente viene allertato solo in caso certo di minaccia, eliminando il tempo perso nell'analisi di falsi positivi;
- **competitività verso ogni business:** pur avendo una tecnologia all'avanguardia, il nostro modello di mercato ci permette di essere accessibile anche alle realtà più piccole.

Le principali attività R&S svolte nell'ambito del progetto sono riconducibili alle seguenti:

1. analisi dei requisiti/modello e flussi (con Key Users);
2. progettazione dell'architettura e algoritmi;
3. implementazione del codice del programma prototipo (con sviluppo sperimentale);
4. test e prove su versione prototipale Alfa e Beta (con Key Users).

5. Servizio CSI di OSINT Social

All'interno della Cyber Security Suite, la componente CSI è stata potenziata con l'introduzione di **nuovi moduli di raccolta e analisi OSINT** orientati alla profilazione e tracciabilità di soggetti e asset digitali.

Tra i nuovi strumenti integrati:

- **profilazione cross-platform:** moduli che raccolgono e aggregano automaticamente le tracce digitali associate a un determinato username o dominio, identificando la presenza su social network, piattaforme professionali, repository di codice e marketplace. Questa funzionalità consente una ricostruzione approfondita della footprint digitale del soggetto analizzato.
- **crawling mirato per info-leak e metadati:** attraverso motori ad hoc, il sistema è in grado di recuperare informazioni pubblicamente accessibili (ma non indicizzate nei motori tradizionali) come indirizzi e-mail, IP correlati, nomi utente e contenuti testuali associabili a potenziali violazioni.

- **moduli di enrichment automatico:** i dati raccolti vengono incrociati con fonti OSINT e pubblici registri per arricchire le evidenze e attribuire contesto, con l'obiettivo di supportare analisi più accurate e azioni tempestive.

L'integrazione di questi moduli rafforza ulteriormente la capacità investigativa della piattaforma CSI, rendendola uno strumento completo per l'intelligence proattiva e la risposta alle minacce emergenti.

Cypeer rappresenta la soluzione MDR (Managed Detection and Response). Ad oggi Cypeer è l'unica soluzione MDR Italiana riconosciuta da Gartner ed inserita nella Gartner Market Guide. La Soluzione Cypeer è in grado di raccogliere e normalizzare tutte le informazioni relative a diverse fonti dato, con lo scopo di identificare minacce o attacchi già presenti impattanti sulla postura cyber di sicurezza del Cliente. Tra le principali caratteristiche, che distinguono inoltre la Soluzione tra quelle di mercato, vi è una approfondita gestione delle informazioni e la capacità di correlazione orizzontale tale per cui il sistema è in grado di elevare le potenzialità e le capacità identificative delle singole soluzioni che rappresentano per Cypeer le fonti dato, nonché fungere da osservatore super partes in grado di correlare eventi relativi a diverse entità. La Soluzione Cypeer permette di automatizzare un'attività di per sé complessa e che richiede una capacità di identificazione e reazione specifica per ogni evento. Tramite questa Soluzione il team di Cybersecurity è in grado di fornire al Cliente una visibilità approfondita e gestita di quelle che sono le minacce che potrebbero tramutarsi in impatti per le proprietà di sicurezza di dati e servizi afferenti al Cliente stesso.

Inoltre, la Soluzione prevede un portale di *Case Handling*, il quale, permette al Cliente di avere piena trasparenza delle attività in carico ai vari livelli di SOC che gestiscono la Soluzione. Tramite il portale si palesa la capacità di correlazione degli allarmi basata sulle entità degli stessi. Tali allarmi, vengono quindi raccolti in Case e dai SOC analizzati.

Infine, la Soluzione mette a disposizione una tecnologia di automatic remediation agnostica che è in grado, sulla base di condizioni definite, di eseguire autonomamente attività volte a mitigare o bloccare gli attacchi in corso direttamente sui sistemi coinvolti del cliente.

Per lo sviluppo del progetto sono stati adottati algoritmi e modalità tali per cui risulta possibile alla Intelligenza del sistema identificare automaticamente minacce non altrimenti identificabili, tramite l'implementazione di metodologie proprietarie. L'architettura, le logiche e le modalità di funzionamento delle soluzioni sono state completamente ideate durante il processo di definizione del progetto e implementazione.

La soluzione è stata completamente sviluppata in "Cloud" garantendo elevati livelli di affidabilità sfruttando sistemi di ridondanza e controllo delle informazioni in essa gestite. Inoltre, tali informazioni sono secretate e disponibili solo agli utenti/sistemi autorizzati alla gestione di queste. Ogni accesso alle informazioni è dovutamente registrato e i log sono mantenuti secondo gli standard di sicurezza in materia. Obiettivo principale del progetto è stato quello di implementare una soluzione che potesse portare su un cliente, di qualunque dimensione e competenze strutturali in ambito IT, un prodotto completamente gestito in h24 dagli specialisti Cyberoo (esternalizzando quindi la competenza).

FlowShield

Nell'ambito dell'evoluzione di Cypeer, Cyberoo ha definito FlowShield, un motore di correlazione orizzontale e risk scoring spiegabile pensato per trasformare gli alert in situazioni di rischio gestibili, riducendo il rumore operativo e aumentando il segnale utile per il SOC. La soluzione analizza il contesto relativo a entità quali host, utenti, subnet e siti, così da comprendere se un nuovo alert si inserisca in uno scenario già degradato e debba quindi essere prioritizzato diversamente. Questo approccio consente di migliorare il triage, aumentare la capacità di individuazione delle minacce e supportare un ulteriore miglioramento degli indicatori di efficacia operativa, come MTTD e MTTR.

FlowShield introduce un modello dichiarativo per la definizione delle logiche di correlazione, attraverso template configurabili che permettono di gestire finestre temporali, entità, pesi, categorie, sequenze, decadimento del rischio, soglie di escalation e logiche di deduplicazione. Il motore è compatibile con lo standard ECS, si integra con l'architettura esistente di Cypeer con un approccio di refactor soft e garantisce elevata tracciabilità del processo decisionale, grazie alla possibilità di motivare il punteggio attribuito in base a categorie, sequenze, tassonomie MITRE e fonti coinvolte. In questo modo, oltre a rafforzare la qualità

dell'analisi, la piattaforma consolida la propria aderenza ai requisiti di audit e compliance, con particolare riferimento a NIS2, DORA e AI Act.

Dal punto di vista applicativo, FlowShield abilita la creazione di "Situation", ossia viste aggregate che collegano alert correlati alla stessa entità o allo stesso scenario, offrendo agli analisti SOC, ai threat hunter e agli incident responder una visione più completa e contestualizzata dell'incidente. Il progetto rappresenta quindi una direttrice strategica di sviluppo per Cypeer, perché rafforza il posizionamento della piattaforma MDR in termini di scalabilità, explainability e capacità evolutiva, predisponendo inoltre l'integrazione futura con modelli AI controllati e con un layer unificato di ModelOps.

Cypeer

Cypeer rappresenta la Soluzione MDR (Managed Detection and Response). Ad oggi Cypeer è l'unica Soluzione MDR Italiana riconosciuta da Gartner ed inserita nella Gartner Market Guide. La Soluzione Cypeer è in grado di raccogliere e normalizzare tutte le informazioni relative a diverse fonti dato, con lo scopo di identificare minacce o attacchi già presenti impattanti sulla postura cyber di sicurezza del Cliente. Tra le principali caratteristiche, che distinguono inoltre la Soluzione tra quelle di mercato, vi è una approfondita gestione delle informazioni e la capacità di correlazione orizzontale tale per cui il sistema è in grado di elevare le potenzialità e le capacità identificative delle singole soluzioni che rappresentano per Cypeer le fonti dato, nonché fungere da osservatore super partes in grado di correlare eventi relativi a diverse entità. La Soluzione Cypeer permette di automatizzare un'attività di per sé complessa e che richiede una capacità di identificazione e reazione specifica per ogni evento. Tramite questa Soluzione il team di Cybersecurity è in grado di fornire al Cliente una visibilità approfondita e gestita di quelle che sono le minacce che potrebbero tramutarsi in impatti per le proprietà di sicurezza di dati e servizi afferenti al Cliente stesso.

Inoltre, la Soluzione prevede un portale di *Case Handling*, il quale, permette al Cliente di avere piena trasparenza delle attività in carico ai vari livelli di SOC che gestiscono la Soluzione. Tramite il portale si palesa la capacità di correlazione degli allarmi basata sulle entità degli stessi. Tali allarmi, vengono quindi raccolti in Case e dai SOC analizzati.

Infine, la Soluzione mette a disposizione una tecnologia di automatic remediation agnostica che è in grado, sulla base di condizioni definite, di eseguire autonomamente attività volte a mitigare o bloccare gli attacchi in corso direttamente sui sistemi coinvolti del cliente.

Per lo sviluppo del progetto sono stati adottati algoritmi e modalità tali per cui risulta possibile alla Intelligenza del sistema identificare automaticamente minacce non altrimenti identificabili, tramite l'implementazione di metodologie proprietarie. L'architettura, le logiche e le modalità di funzionamento delle soluzioni sono state completamente ideate durante il processo di definizione del progetto e implementazione.

La soluzione è stata completamente sviluppata in "Cloud" garantendo elevati livelli di affidabilità sfruttando sistemi di ridondanza e controllo delle informazioni in essa gestite. Inoltre, tali informazioni sono secretate e disponibili solo agli utenti/sistemi autorizzati alla gestione di queste. Ogni accesso alle informazioni è dovutamente registrato e i log sono mantenuti secondo gli standard di sicurezza in materia. Obiettivo principale del progetto è stato quello di implementare una soluzione che potesse portare su un cliente, di qualunque dimensione e competenze strutturali in ambito IT, un prodotto completamente gestito in h24 dagli specialisti Cyberoo (externalizzando quindi la competenza).

CyberBoar

CyberBoar è il progetto sviluppato per offrire alle aziende una piattaforma integrata, modulare e intuitiva a supporto della governance della cybersecurity, della gestione del rischio e della conformità normativa. L'iniziativa nasce dall'esperienza operativa maturata da Cyberoo Docetz nell'affiancamento alle imprese sui temi di cyber security, compliance, incident response e supervisione strategica, e risponde a un'esigenza concreta del mercato: superare l'utilizzo di strumenti frammentati, poco integrati o eccessivamente complessi, mettendo a disposizione un ambiente unico per la gestione strutturata della postura di sicurezza.

La piattaforma è stata progettata secondo una logica a moduli integrabili, così da garantire elevata flessibilità e permettere alle aziende di attivare solo i servizi coerenti con i propri obiettivi. L'architettura di CyberBoar si articola in quattro

componenti principali: Security Manager, dedicato alla governance della sicurezza informatica e alla gestione di processi, documentazione, BIA, BCP e DRP; Supply Chain Watcher, focalizzato sulla valutazione del rischio connesso ai fornitori IT e sull'automazione delle campagne di assessment; Cyber Posture Evaluator, sviluppato per supportare in modo evoluto le attività di analisi condotte dal team vCISO; SAM Assistant, pensato per rafforzare le attività di risk assessment svolte dai SAM sui clienti dei servizi Cyberoo.

Tra gli elementi distintivi del progetto rientrano l'alto livello di configurabilità, l'integrazione tra moduli e con i servizi consulenziali del Gruppo, la reportistica avanzata con KPI personalizzabili, la storicizzazione delle informazioni, il supporto multilingua e un impianto di sicurezza basato su gestione granulare degli accessi, MFA, separazione logica e fisica dei dati, crittografia e sistemi evoluti di backup e ripristino. CyberBoar rappresenta quindi una direttrice di innovazione rilevante per il Gruppo, in quanto consente di unire in un'unica piattaforma gli aspetti di governance, assessment, supporto consulenziale e conformità, con particolare attenzione ai requisiti introdotti dalla direttiva NIS2 e ai processi di miglioramento continuo della postura cyber delle organizzazioni clienti.

Keatrix

Keatrix è la Human Risk & Security TrAlning Platform sviluppata da Cyberoo per innovare il settore della cyber security awareness attraverso un approccio formativo evoluto, personalizzato e ad alto coinvolgimento. Il progetto è stato definito a partire da un'analisi strutturata dei principali competitor internazionali dell'e-learning in ambito cyber, condotta secondo il modello Quality Matters, con l'obiettivo di identificare le aree di differenziazione e costruire una piattaforma coerente con gli standard qualitativi e con l'identità Cyberoo.

I principali caratteri innovativi di Keatrix si fondano su tre pilastri distintivi. Il primo è l'adaptive learning, che attraverso un motore proprietario di intelligenza artificiale consente di costruire percorsi formativi personalizzati in base al livello iniziale, alle modalità di apprendimento e al tempo disponibile di ciascun utente, con l'obiettivo di incidere concretamente sui comportamenti quotidiani rilevanti ai fini della cyber security. Il secondo è l'utilizzo delle tecniche di interleaving and spacing, che migliorano la memorizzazione e la capacità di applicazione dei concetti nel lungo periodo. Il terzo è l'edutainment, che combina apprendimento e

intrattenimento attraverso avatar digitali, video animati, contenuti audio-grafici e format cinematografici, così da aumentare attenzione, engagement ed efficacia didattica. A questi elementi si aggiunge il modello di certificazione ad personam, che valorizza il percorso individuale dell'utente e ne rende tracciabile la crescita anche in contesti organizzativi differenti.

La piattaforma, erogata in cloud, prevede un ambiente dedicato agli utenti finali e uno rivolto agli amministratori, con particolare attenzione all'esperienza d'uso, alla compatibilità multi-device e alla semplicità di navigazione. I contenuti sono organizzati in modo modulare secondo una struttura che comprende generazione della conoscenza, esemplificazione, rielaborazione attiva e testing, e sono localizzati in quattro lingue — italiano, inglese, spagnolo e polacco — con la prospettiva di ulteriori estensioni. Keatrix adotta inoltre un modello licensing pensato per il canale distributivo Cyberoo, con modalità transazionali e MSSP, e abilita percorsi dedicati sia alla security awareness diffusa sia ai contenuti NIS2 e alle campagne di phishing e smishing. Nel complesso, il progetto rappresenta un'evoluzione significativa dell'offerta Cyberoo nell'ambito della formazione cyber, coniugando intelligenza artificiale, personalizzazione, multicanalità e una forte distintività metodologica e comunicativa.

Titaan

Al momento sul mercato esistono sistemi di monitoraggio che si basano su un paradigma detto "Supervised". I software tradizionali, come Nagios, si affidano a regole e soglie/ threshold. La conseguenza è che questi sistemi non sono in grado di discernere tra picchi di carico abituali (si pensi agli aggiornamenti) e quelli realmente anomali. Il progetto mira allora a sviluppare un sistema di monitoraggio totalmente innovativo basato su logica "unsupervised".

La piattaforma Titaan è un innovativo servizio di monitoraggio in real time dell'infrastruttura informatica di un'azienda, dei suoi servizi e delle sue applicazioni che permetta di garantire la Business continuity all'interno delle infrastrutture aziendali con un approccio "unsupervised" che permette di superare le limitazioni dei tradizionali sistemi "supervised". I principali contenuti innovativi derivano dall'utilizzo delle tecnologie di Machine Learning e Intelligenza Artificiale, scelte perché sono le uniche in grado di operare in maniera proattiva e di generare previsioni analizzando in tempo reale elevati volumi di dati (big data), garantendo

così un vantaggio competitivo rispetto alla concorrenza. In aggiunta, per ogni macchina sotto monitoraggio, si genera un modello di comportamento tailor-made della macchina, che consente di identificare tutte quelle stranezze che i normali software non sono in grado di riconoscere. Titaan, in maniera disruptive, identifica le anomalie prima che diventino un problema e circoscrive la causa prima che il Team del cliente debba effettuare un'analisi.

A complemento delle funzionalità predittive e real time di Titaan, è stato sviluppato un **modulo avanzato di monitoraggio eventi conforme alla direttiva NIS2**. Il modulo consente un controllo capillare su eventi di sicurezza, processi di sistema e accessi, offrendo visibilità dettagliata sulle attività a livello endpoint, server e infrastruttura di rete.

Questa integrazione rappresenta un'evoluzione nella capacità della piattaforma di anticipare minacce e supportare attività di forensic analysis, garantendo tracciabilità completa degli eventi significativi all'interno dell'ambiente monitorato. Il modulo adotta una struttura di regole dinamiche e un motore di correlazione che consente l'identificazione automatica di pattern sospetti o anomali, minimizzando il tasso di falsi positivi e ottimizzando le attività di response.

La piattaforma permette di ottenere i seguenti vantaggi rispetto alla concorrenza:

- eliminazione dei falsi positivi: Titaan non utilizza regole o soglie preimpostate, bensì sfrutta le più avanzate tecnologie dell'Intelligenza Artificiale con il risultato di riuscire a intercettare le anomalie certe, che non siano falsi positivi. Ciò riduce significativamente la mole di notifiche giornaliere che i sistemi tradizionali inviano ai responsabili IT e per le quali è stato stimato che, per la maggior parte, si tratta di falsi positivi. Indirizzando il dipartimento IT direttamente verso le reali anomalie dei propri sistemi;
- proattività: Titaan individua l'inizio del degrado dei sistemi con uno scarto di pochi secondi;
- visibilità integrata in un'unica dashboard: Titaan riunisce tutti i log e dati di monitoraggio in un unico pannello, per cui i tecnici IT non dovranno continuamente cambiare da un'interfaccia all'altra per avere una visione a 360° sulla propria infrastruttura;

- competitività: pur sfruttando tecnologie avanzate nel campo dell'Intelligenza Artificiale, il sistema permette di essere accessibile anche alle realtà medio-piccole;
- monitoraggio in tempo reale;
- monitoraggio predittivo: Titaan effettua previsioni fino a due mesi permettendo il giusto dimensionamento dei sistemi business critical.

AMY

Tra i nuovi progetti in ambito intelligenza artificiale, Cyberoo ha sviluppato AMY, una piattaforma integrata progettata per assistere, migliorare ed evolvere il lavoro quotidiano delle persone in azienda. La soluzione nasce per supportare diversi contesti d'uso, dall'onboarding interno alla ricerca documentale, dalla redazione e revisione dei contenuti all'assistenza tecnica, fino alla comunicazione multilingue, all'analisi dei dati e al customer care. L'obiettivo è rendere più rapide, precise e accessibili attività che oggi richiedono tempi di ricerca, coordinamento o gestione elevati, aumentando l'efficienza operativa e la produttività complessiva.

AMY adotta un'architettura cognitiva avanzata che combina Large Language Models e tecnologie di Natural Language Processing per comprendere il contesto, identificare entità, categorizzare le richieste e fornire risposte pertinenti in linguaggio naturale, sia scritto sia parlato. La piattaforma può essere alimentata con documenti aziendali e contenuti digitali del cliente, anche tramite tecnologia RAG, così da costruire una knowledge base contestualizzata e valorizzare il patrimonio informativo interno. A questo si affiancano funzionalità evolute quali image vision, ricerca web con citazione delle fonti e un pannello di controllo amministrativo che consente di configurare chatbot, modelli, prompt, documenti accessibili, utenti, gruppi e parametri operativi, offrendo piena governabilità della soluzione.

Dal punto di vista tecnologico, AMY si caratterizza inoltre per un'architettura a micro-servizi serverless gestita su Amazon AWS, compatibilità con i principali modelli linguistici commerciali e open source e strumenti di analisi delle conversazioni e del sentiment utili anche ai fini della business intelligence. Coerentemente con il posizionamento di Cyberoo sui temi della data protection, la soluzione è stata progettata con particolare attenzione alla riservatezza del dato: le informazioni trattate restano di proprietà del cliente, non vengono utilizzate per

il riaddestramento dei modelli e sono gestite secondo criteri di sicurezza e conformità alle direttive europee in materia di privacy.

C51 Commerce

C51 Commerce è la piattaforma proprietaria sviluppata da Cyberoo51 per la realizzazione di ecosistemi e-commerce B2B e B2C altamente personalizzabili, pensati per adattarsi ai processi commerciali, logistici e organizzativi delle aziende clienti. La soluzione nasce dall'esperienza maturata nella progettazione di portali per la vendita online e si distingue per la capacità di coniugare personalizzazione grafica, integrazione applicativa e autonomia gestionale, mettendo a disposizione un'infrastruttura in grado di valorizzare la brand identity del cliente e, al contempo, supportarne in modo strutturato l'operatività digitale.

Dal punto di vista tecnologico, C51 Commerce si basa su uno stack moderno e scalabile, sviluppato in ambiente Python e Django, con architettura cloud, database relazionale e componenti dedicati alla gestione dei task e delle notifiche. La piattaforma è progettata per garantire sicurezza, stabilità, manutenibilità e capacità evolutiva, anche attraverso logiche di scalabilità elastica su infrastruttura AWS. Un elemento qualificante del progetto è la piena integrazione con i sistemi gestionali del cliente tramite API, così da sincronizzare in modo continuo e strutturato dati relativi a catalogo, categorie, giacenze, ordini, tracking e anagrafiche, assicurando coerenza tra canale digitale e processi aziendali di back office.

La soluzione integra, inoltre, un pannello di controllo centralizzato per la gestione di prodotti, contenuti, clienti, ordini, promozioni, spedizioni, pagamenti e parametri SEO, favorendo una gestione autonoma e semplificata del portale. A ciò si affiancano attività dedicate all'ottimizzazione della user experience e della user interface, alla strategia SEO multilingua, all'analisi delle performance digitali tramite strumenti avanzati di analytics e alla gestione degli aspetti di compliance, inclusi cookie management e sicurezza delle comunicazioni web. C51 Commerce rappresenta quindi una direttrice di innovazione rilevante per Cyberoo51, in quanto consolida un'offerta proprietaria capace di unire sviluppo software, integrazione con i processi aziendali, valorizzazione commerciale e governo del dato in un'unica piattaforma digitale evoluta.

Il valore delle partnership

Cyberoo vende i suoi servizi sul mercato in via indiretta, costruendo e consolidando un importante network di partner a valore aggiunto in Italia e all'estero, che permette di presidiare in modo capillare tutto il territorio italiano e internazionale.

Tale modello di business adottato consente un rapporto *win-win* che permette:

- ai partner, grazie a Gruppo Cyberoo, di riuscire a fornire dei servizi evoluti di cyber security che diversamente farebbero fatica a proporre ai clienti;
- al Gruppo Cyberoo di raggiungere velocemente il cliente finale tramite un rapporto già consolidato tra il partner e l'end-user.

Ad oggi Cyberoo può contare su tre contratti di distribuzione nazionale e oltre cento contratti di partnership a valore aggiunto che permettono di coprire l'intero territorio italiano.

Di seguito, vengono elencati alcuni dei principali partner con cui il Gruppo Cyberoo collabora nella sua attività:

NPO Torino S.r.l.	Euro Informatica S.p.A.
Zerouno Informatica S.p.A.	Cyber-Bee-R1 S.p.A.
Magnetic Media Network S.p.A.	WindTre S.p.A.
NPO Sistemi S.r.l.	Retelit Digital Service S.p.A.
Ergon S.r.l.	Eurosystem S.p.A.
Vidata S.r.l.	Reti S.p.A.

Inoltre, nel corso del 2025 Cyberoo ha ampliato le sue operazioni internazionali con altre sei partnership in Polonia sotto riportate.

- STORIO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ SP.K
- LEVELITE PROSTA SPÓŁKA AKCYJNA
- ADVATECH SP. Z O.O.
- CLOCKWISE Sp. z o. o. Sp. K.
- NFLO SP. Z O.O.

Il Gruppo ha la possibilità di supportare i clienti e i partner con maggior facilità, avendo asset e personale in loco. I clienti ricevono un supporto diretto e da un servizio 24/7 svolto da personale che parla la loro lingua.

I partner sono inoltre agevolati dalla costruzione di un network e sono in condizione, insieme a Cyberoo, di supportare un maggior numero di aziende nel paese.

Cyberoo Black Club – Il Partner Program

Dal 2020, Cyberoo ha istituito il “**Cyberoo Black Club**”, un programma di Partnership con alcuni dei più rilevanti brand del settore IT, in Italia e all'estero: è fondamentale per Cyberoo supportare i partner nella buona riuscita delle loro attività commerciali e di rapporto con il cliente e, per questo motivo, mette a disposizione tutte le sue competenze tecniche per la formazione delle risorse del partner e nella realizzazione di attività di marketing congiunte per dare sostegno al brand, alla proposizione di valore e alla generazione di lead sul canale.

Il Black Club è un programma con tre livelli di partnership, definito in base a due valori che devono risultare contemporaneamente soddisfatti, ovvero (i) quantità di fatturato nell'anno precedente e (ii) numero di persone certificate sales, presales e tecniche:

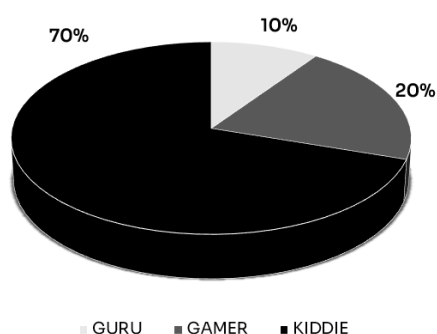
- **KIDDIE:** il livello è quello di iscrizione iniziale e offre ai partner l'accesso a una varietà di risorse, materiali, strumenti e vantaggi di marketing;
- **GAMER:** il livello fornisce ai partner maggiori vantaggi, oltre all'accesso a risorse aggiuntive progettate per aiutarli a sviluppare piani aziendali incentrati sulla crescita e abilità tecnologiche sempre più avanzate;
- **GURU:** il livello è pensato per i partner che hanno una relazione strategica con Cyberoo. I partner che raggiungono questo livello hanno investito fortemente nel portfolio di Cyberoo e hanno contribuito maggiormente alla buona riuscita del Go to Market. Ricevono quindi il massimo livello di benefici.

Nel 2025 Cyberoo ha confermato il Cyberoo Black Club, il programma di partnership dedicato al canale, quale strumento a supporto dello sviluppo commerciale e del rafforzamento della propria Go to Market Strategy. Il programma, valido per l'intero anno 2025, ha confermato la struttura su tre livelli di

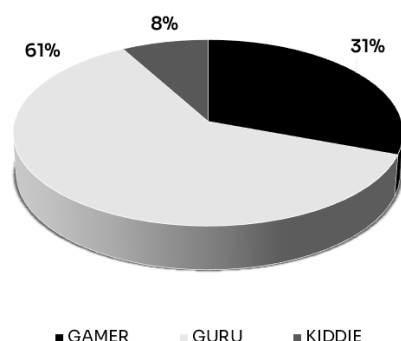
partnership – KIDDIE, GAMER e GURU – definiti sulla base di requisiti oggettivi, tra cui il fatturato annuale, il livello di formazione delle risorse commerciali, presales e tecniche, nonché, per i livelli più avanzati, la capacità di sviluppare nuovi clienti e iniziative di co-marketing. In funzione del livello raggiunto, i partner possono accedere a benefici di natura economica, tecnica, commerciale, di marketing e di relazione, inclusi percorsi di formazione, strumenti di supporto alla vendita e alla prevendita, fondi marketing, rebate, opportunità commerciali dedicate e il presidio di figure di riferimento dedicate. Attraverso il Black Club, Cyberoo intende consolidare un ecosistema di partnership qualificato, favorendo la crescita delle competenze, la generazione di valore condiviso e una maggiore efficacia nel supporto ai clienti finali.

PARTNER ITALIA

Partner certificati

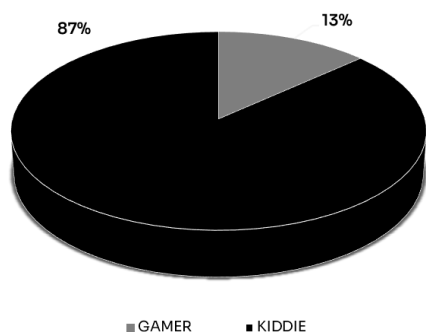


% fatturato Cyberoo per tipologia di certificazione

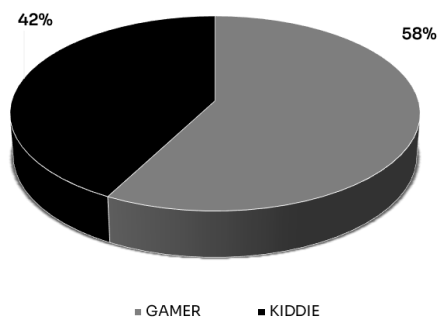


PARTNER POLONIA

Partner certificati



% fatturato Cyberoo per tipologia di certificazione



Cyberoo Black Academy

A fianco del Black Club, Cyberoo ha avviato Black Academy, un'iniziativa dedicata in modo specifico ai partner che operano sulla piattaforma Keatrix. Più che un tradizionale programma di canale, Black Academy si configura come uno strumento di specializzazione della partnership, rivolto ai soggetti che accompagnano clienti e organizzazioni nei percorsi di crescita della consapevolezza cyber. La nascita di questo programma riflette la crescente centralità della Human Risk & Security Awareness nei percorsi di protezione delle organizzazioni e valorizza il ruolo di Keatrix come soluzione distintiva dell'offerta Cyberoo: una piattaforma progettata per innovare la formazione cyber grazie a contenuti personalizzati, approcci adattivi all'apprendimento e un elevato livello di coinvolgimento dell'utente. In questo contesto, Black Academy è stata concepita come un percorso di qualificazione progressiva riservato al canale Keatrix, capace di premiare nel tempo competenze, risultati e capacità di presidio del mercato, mettendo a disposizione strumenti di enablement, supporto specialistico e meccanismi di valorizzazione coerenti con il posizionamento della piattaforma. L'iniziativa, rafforza così la strategia di Cyberoo non solo sul piano commerciale, ma anche nella costruzione di una rete partner preparata a promuovere una cultura della sicurezza più consapevole, misurabile e continuativa.

Premi e riconoscimenti

L'impegno di Cyberoo nello sviluppo di tecnologie innovative, nella crescita sostenibile e nel rafforzamento della propria competitività a livello nazionale e internazionale ha trovato conferma attraverso numerosi premi e riconoscimenti ottenuti nel periodo di rendicontazione. A livello internazionale, Cyberoo ha rafforzato il proprio posizionamento nel settore della cybersecurity grazie alla menzione come Sample Vendor in due report di Gartner® – Emerging Tech Impact Radar: 2025 ed Emerging Tech Impact Radar: Digital Identity and Edge Security – dedicati alle tecnologie emergenti e alle soluzioni di Advanced Behavioral Detection Analytics. La Società è stata inoltre citata da Gartner come Client Success per il percorso di rafforzamento del proprio posizionamento sul mercato, l'innovazione tecnologica e l'evoluzione della propria offerta, a testimonianza della capacità di anticipare le esigenze di un settore in continua trasformazione.

A conferma del valore delle proprie soluzioni sviluppate in Europa, Cyberoo ha inoltre ottenuto il marchio Cybersecurity Made in Europe, rilasciato dall'European Cyber Security Organisation (ECSO), certificazione che valorizza l'origine europea delle tecnologie, il rispetto degli standard comunitari e il contributo del Gruppo al rafforzamento della sovranità digitale europea.

Il percorso di crescita del Gruppo è stato riconosciuto anche in ambito economico e imprenditoriale attraverso l'inserimento tra i Campioni della Crescita 2026, classifica realizzata dalla Repubblica Affari & Finanza e Istituto Tedesco Qualità e Finanza (ITQF) che individua le imprese italiane con le migliori performance di crescita sulla base di criteri oggettivi relativi all'incremento del fatturato registrato negli ultimi esercizi. La Società è stata inoltre selezionata per l'iniziativa editoriale La Storia Italiana del Sole 24 Ore, dedicata alle eccellenze imprenditoriali che contribuiscono allo sviluppo e alla competitività del Paese.

La solidità del modello di business e le performance economico-finanziarie sono state ulteriormente valorizzate dal riconoscimento Industria Felix, assegnato alle imprese che si distinguono per affidabilità gestionale, solidità finanziaria e performance economiche, sulla base di un'analisi oggettiva dei dati di bilancio. Il premio valorizza le realtà imprenditoriali capaci di coniugare crescita, sostenibilità economica e capacità di creare valore nel lungo periodo.

Il posizionamento di Cyberoo nel panorama europeo della cybersecurity è stato ulteriormente valorizzato attraverso la partecipazione allo studio realizzato da ANSSI – Agence nationale de la sécurité des systèmes d'information, l'autorità francese per la sicurezza informatica, in collaborazione con Wavestone, società europea di consulenza specializzata in trasformazione digitale e cybersecurity. Lo studio, dedicato all'evoluzione dell'utilizzo dell'Intelligenza Artificiale nei processi di rilevazione e risposta agli incidenti informatici, ha analizzato lo stato dell'arte delle tecnologie AI applicate al mercato della Detection & Response, con particolare attenzione alle soluzioni sviluppate dai vendor europei. Cyberoo è stata inclusa tra le realtà analizzate nell'ambito della ricerca, contribuendo al confronto attraverso il proprio know-how tecnologico e l'esperienza maturata nell'ambito dei Security Operation Center (SOC) e dei servizi di monitoraggio e risposta agli incidenti.



Capitolo 5

CAPITALE RELAZIONALE

5. Capitale relazionale

La relazione con i clienti

Nel corso degli anni, Cyberoo ha consolidato una rete stabile di relazioni con le principali aziende che propongono soluzioni e attività specialistiche nell'ambito della cybersecurity, sia a livello nazionale che internazionale. Tali aziende svolgono un ruolo chiave nella diffusione delle soluzioni Cyberoo, contribuendo allo sviluppo del business attraverso la loro capacità di presidiare il mercato finale.

Il presidio del partner rappresenta un elemento centrale del modello operativo del Gruppo Cyberoo, che si impegna costantemente per accrescere il valore generato dalla relazione con ciascun cliente.

La capacità di rispondere in modo efficace alle esigenze dei clienti rappresenta un fattore chiave per lo sviluppo sostenibile di Cyberoo ed è determinante per mantenere e rafforzare la fiducia nel rapporto.

Dall'altro lato, i partner scelgono Cyberoo perché garantisce il raggiungimento di tre obiettivi fondamentali:

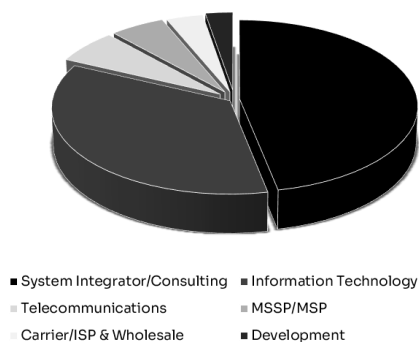
- **Valore:** ampliare il proprio portafoglio di offerta con servizi cybersecurity ad alto valore aggiunto, erogati in modalità H24 tramite un I-SOC altamente specializzato;
- **Fidelizzazione:** l'erogazione di servizi *always on* consente ai partner di seguire il cliente finale in modo proattivo e continuativo, aumentando il grado di fidelizzazione;
- **Ricavi ricorrenti:** i servizi proposti generano benefici economici attraverso ricavi ricorrenti, contribuendo a rafforzare la solidità degli economics aziendali.

La base partner di Cyberoo è costituita da aziende con profili eterogenei, accomunate dalla capacità di interagire con i clienti finali in funzione della loro propensione a indirizzare l'adozione tecnologica, a offrire consulenza o a fornire direttamente servizi. Nei grafici seguenti sono riportati:

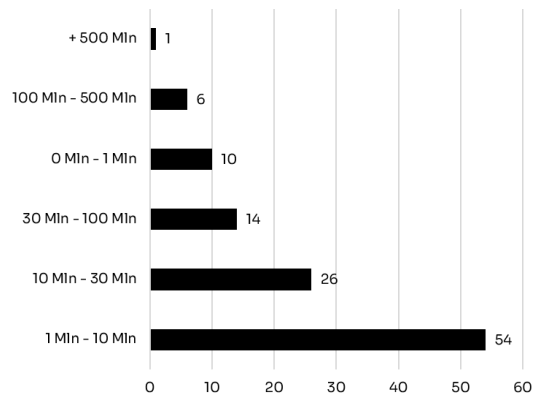
- i partner suddivisi per tipologia di business sviluppato;
- La concentrazione del fatturato per tipologia di partner.

PARTNER ITALIA

Tipologia di business del partner

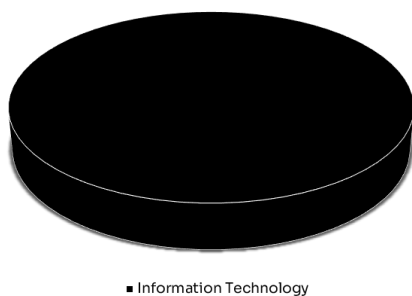


Fatturato del partner

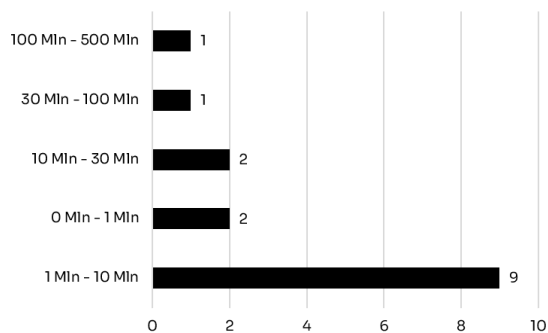


PARTNER POLONIA

Tipologia di business del partner

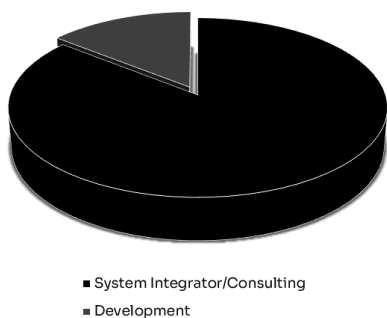


Fatturato del partner

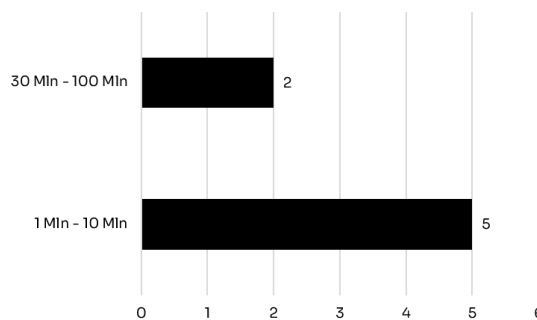


PARTNER SPAGNA

Tipologia di business del partner



Fatturato del partner



Cyberoo stipula con essi **contratti di partnership di durata annuale o pluriennale.**

La gestione delle relazioni con i clienti

I partner possono contare su una struttura composta da risorse altamente qualificate e interamente dedicate allo sviluppo del business. Cyberoo mette a disposizione figure professionali specializzate, ciascuna con un ruolo specifico all'interno del processo di gestione della relazione con partner e clienti finali:

- **Area Manager:** individua nuovi partner sul territorio e collabora con i partner attivi nella definizione di account plan, iniziative formative e attività di marketing. È responsabile delle vendite nella propria area geografica, della gestione delle risorse commerciali di area, dell'organizzazione del lavoro del team e della presentazione del forecast settimanale.
- **Territory Manager:** approfondisce le caratteristiche dei clienti, le tecnologie utilizzate, i fornitori attivi e le relative scadenze. Rappresenta il principale punto di riferimento del partner per la gestione delle offerte ed è responsabile delle vendite nel territorio assegnato, del coordinamento dei Key Account Manager locali e dello sviluppo della propria attività commerciale.
- **Key Account Manager (KAM):** sviluppa e mantiene le relazioni con gli end user al fine di generare nuove opportunità commerciali, successivamente assegnate al partner più idoneo. Conosce in modo approfondito le esigenze dei clienti in relazione alle tecnologie e ai servizi di cyber security proposti.
- **Inside Sales:** effettua il primo contatto con prospect di origine commerciale o marketing, supportando e potenziando l'attività dei Key Account Manager nello sviluppo di nuove opportunità.
- **Business Development Manager (BDM):** svolge un ruolo tecnico di pre-sales, affiancando le figure commerciali di Cyberoo e dei partner nelle fasi di approfondimento delle soluzioni, nelle demo e nelle presentazioni tecniche. Supporta inoltre i partner nelle attività formative relative ai servizi offerti.
- **Deal Manager:** gestisce il processo di deal registration sul portale dedicato, verificando e approvando le opportunità registrate dai partner al fine di garantire l'esclusività commerciale delle trattative. A seguito dell'approvazione, coordina l'avvio delle attività di demo e di predisposizione delle offerte insieme ai BDM e alle figure commerciali coinvolte.

Il modello organizzativo adottato da Cyberoo si basa su una forte integrazione tra le diverse funzioni commerciali e tecniche. Area Manager, Territory Manager, Key Account Manager, Business Development Manager e Deal Manager collaborano costantemente nella definizione delle strategie territoriali, nello sviluppo dei partner, nella presentazione delle soluzioni e nel monitoraggio delle opportunità commerciali attraverso il forecast settimanale.

Questa struttura è pienamente operativa nel mercato italiano, dove tutte le figure sopra descritte sono presenti e integrate nei processi di vendita e di gestione della relazione con partner e clienti finali.

Nei mercati esteri, come la Polonia, il modello è attualmente più snello e si concentra principalmente sulle figure di Key Account Manager e Business Development Manager, che svolgono un ruolo centrale nello sviluppo del business locale e nel supporto ai partner. L'obiettivo del Gruppo è estendere progressivamente il modello integrato di supporto commerciale e tecnico, mantenendo in tutti i Paesi elevati standard di vicinanza ai partner, qualità del servizio e attenzione alle esigenze dei clienti finali.

La struttura dei partner

Cyberoo sviluppa il proprio modello di partnership attraverso programmi dedicati alla crescita e alla valorizzazione dei partner, con l'obiettivo di favorire la diffusione delle competenze in ambito cyber security, supportare lo sviluppo commerciale e garantire ai clienti finali un elevato livello di qualità nell'erogazione dei servizi.

Il **Black Club** rappresenta il programma di partnership dedicato ai partner che collaborano con Cyberoo nella commercializzazione dell'intero portafoglio di soluzioni e servizi di cyber security. Attraverso questo programma, i partner possono accedere a strumenti, supporto commerciale e tecnico, iniziative formative e opportunità di sviluppo finalizzate a rafforzare la propria competenza sulle soluzioni Cyberoo e a migliorare la capacità di supportare i clienti.

La **Black Academy** è un percorso dedicato alla formazione e alla crescita delle competenze dei partner, con un focus specifico sul servizio Keatrix. La Black Academy ha l'obiettivo di fornire ai partner le conoscenze necessarie per presentare, proporre e valorizzare efficacemente la soluzione presso i clienti finali.

Il modello di partnership è basato su un principio di crescita condivisa: all'aumentare del livello di collaborazione, del commitment e della conoscenza delle soluzioni Cyberoo, i partner possono accedere a maggiori opportunità di supporto e a strumenti dedicati per sviluppare il proprio business e contribuire alla diffusione di un approccio evoluto alla sicurezza informatica.

Processo di on-boarding dei partner

Il reclutamento dei partner avviene sia su base territoriale sia in funzione del modello di sviluppo del business definito per una determinata tipologia di cliente. Una volta identificata l'azienda, condiviso il modello di business e ottenuta la manifestazione di interesse a diventare partner Cyberoo, si avvia il processo strutturato di **“on-boarding del partner”**, articolato nelle seguenti fasi:

- firma del contratto di partnership e adesione al Cyberoo Black Club o Cyberoo Black Academy;
- formazione iniziale del personale del partner (Sales, Presales, Tecnici);
- condivisione dello Starter Kit commerciale e tecnico;
- definizione del piano commerciale;
- pianificazione e supporto allo sviluppo del business, attraverso incontri e gestione delle trattative).

Formazione e certificazione

Per garantire ai partner una piena comprensione e autonomia nella proposizione delle soluzioni Cyberoo, il Gruppo ha sviluppato un programma strutturato di formazione e certificazione rivolto alle diverse figure coinvolte nel processo commerciale e tecnico, tra cui Sales, Pre-sales e Management.

I percorsi formativi, gratuiti e organizzati periodicamente, hanno l'obiettivo di trasferire competenze specifiche sulle soluzioni Cyberoo, sui principali temi della cybersecurity e sull'evoluzione delle minacce informatiche, favorendo una maggiore capacità del canale di supportare i clienti e di valorizzare le soluzioni offerte.

La formazione dedicata ai partner si articola in percorsi differenziati in funzione delle caratteristiche delle soluzioni del portafoglio Cyberoo:

- **Cyber Security Suite**, attraverso percorsi formativi dedicati ai diversi ruoli coinvolti: Basic, finalizzato alla conoscenza generale della soluzione e dei suoi principali elementi distintivi; Sales, orientato allo sviluppo delle competenze commerciali necessarie alla corretta presentazione del servizio; Pre-sales, dedicato all'approfondimento degli aspetti tecnici e al supporto nelle fasi di analisi e presentazione della soluzione al cliente;
- **Compliance**, con percorsi dedicati alle soluzioni Titaan Neemesi e Cyberoo Services, finalizzati a sviluppare le competenze necessarie per comprendere il valore delle soluzioni, il loro posizionamento e le modalità di supporto al cliente nell'ambito della gestione della compliance e della sicurezza informatica;
- **Keatrix**, attraverso percorsi di formazione Sales e Management, progettati per accompagnare i partner nella conoscenza della soluzione, nella sua valorizzazione commerciale e nella gestione delle opportunità di sviluppo del business.

Attraverso questi programmi di formazione continua, Cyberoo contribuisce alla crescita delle competenze del proprio ecosistema di partner, rafforzando la qualità del supporto offerto al mercato e promuovendo una maggiore diffusione della cultura della cybersecurity.

Organizzazione tecnica

Research & Development

Il reparto Research & Development (R&D) rappresenta il centro di innovazione tecnologica di Cyberoo e svolge un ruolo fondamentale nello sviluppo e nell'evoluzione continua delle soluzioni offerte. Il team è composto da professionisti con competenze multidisciplinari, tra cui sviluppatori, specialisti di Data Science, DevOps, Cyber Architect, esperti di Intelligenza Artificiale e specialisti dei Red Team e Blue Team. La combinazione di queste competenze consente a Cyberoo di progettare, migliorare e adattare costantemente le proprie soluzioni, mantenendo un approccio orientato all'innovazione e alla capacità di risposta rispetto all'evoluzione delle minacce informatiche. Il reparto collabora strettamente con i team di vCISO e Incident Response, condividendo conoscenze ed evidenze operative per comprendere le tecniche, le tattiche e le procedure

utilizzate dal cyber crime e tradurle in evoluzioni tecnologiche e miglioramenti dei servizi. Un ulteriore ambito di collaborazione strategica è rappresentato dal confronto con le funzioni legali e normative, con l'obiettivo di assicurare che le soluzioni sviluppate siano costantemente allineate ai requisiti regolatori applicabili e alle esigenze emergenti del mercato.

Project Manager

Il team Project Management è composto da specialisti che accompagnano il cliente lungo tutte le fasi di implementazione delle soluzioni Cyberoo, garantendo un percorso strutturato e coordinato tra cliente, partner e team interni. I Project Manager avviano il processo attraverso un'attività iniziale di analisi e studio dell'integrazione, finalizzata alla conoscenza del perimetro tecnologico del cliente e alla definizione delle modalità di implementazione più appropriate. A seguito di questa fase, il Project Manager coordina la pianificazione delle attività operative coinvolgendo le diverse funzioni aziendali e gli stakeholder interessati, fino alla corretta installazione e configurazione delle soluzioni. Il processo si conclude con la sottoscrizione del documento di collaudo, che certifica il completamento delle attività previste e la corretta attivazione dei servizi.

Security Advisor Manager

A seguito dell'attivazione delle soluzioni Cyberoo, ai clienti viene affiancata una figura altamente specializzata: il Security Advisor Manager (SAM), con il compito di accompagnare il cliente durante l'erogazione dei servizi e supportarne il progressivo miglioramento della postura di sicurezza.

Attraverso incontri periodici di Service Review, generalmente organizzati con cadenza trimestrale e con il coinvolgimento del partner quando possibile, il Security Advisor Manager analizza il livello di servizio erogato, raccoglie esigenze evolutive e supporta il cliente nell'ottimizzazione dei processi di sicurezza.

Durante questi incontri vengono approfonditi:

- lo stato dei servizi attivi;
- le principali segnalazioni ricevute e le opportunità di miglioramento;
- eventuali criticità operative e le relative azioni correttive.

Un elemento centrale delle Service Review è rappresentato dal Risk Assessment, un documento finalizzato a fornire una fotografia aggiornata del livello di rischio del cliente, considerando infrastrutture, networking e aspetti legati alla sicurezza informatica. L'analisi viene svolta da specialisti Cyberoo che valutano gli elementi emersi, identificano eventuali aree di miglioramento e forniscono indicazioni operative per rafforzare il livello di protezione complessivo. Questo approccio consente a Cyberoo di offrire un servizio personalizzato e orientato al miglioramento continuo, supportando i clienti nell'evoluzione della propria strategia di cybersecurity.

Team Deploy

Il Team Deploy supporta il cliente nelle fasi di installazione e configurazione dei servizi Cyberoo, garantendo un corretto avvio operativo delle soluzioni. Il team si occupa della configurazione degli ambienti necessari al funzionamento dei servizi, sia in presenza di infrastrutture fisiche sia virtuali, e fornisce il supporto tecnico necessario per integrare le tecnologie già presenti presso il cliente con le piattaforme Cyberoo. Tra le attività del team rientrano inoltre la valutazione delle nuove integrazioni tecnologiche, le attività di test e configurazione e l'abilitazione delle funzionalità di remediation, siano esse manuali o automatiche, previste dai servizi di Cyber Security. Attraverso un approccio strutturato e collaborativo, il Team Deploy contribuisce a garantire una corretta implementazione delle soluzioni e una piena efficacia operativa dei servizi erogati.

Qualità, sicurezza ed affidabilità del servizio

Il monitoraggio costante dei servizi erogati ai clienti consente al Gruppo Cyberoo di perseguire un duplice obiettivo: da un lato, garantire **costantemente un'elevata qualità di erogazione del servizio al cliente**; dall'altro, **ottimizzare i processi interni** aziendale in un'ottica di miglioramento continuo.

Con una particolare attenzione alla qualità e alla soddisfazione del cliente, la Direzione aziendale di Cyberoo, sensibile a questa particolare tematica, ha istituito una struttura dedicata: il **Quality and Customer Relationship Department**, responsabile delle seguenti attività:

- analizzare e comprendere le aspettative e i bisogni di business dei clienti;

- garantire la qualità dei processi/servizi erogati e il raggiungimento degli obiettivi prefissati sin dalla fase progettuale;
- coordinare le interazioni tra tutti gli stakeholder coinvolti, supervisionandone l'operatività;
- elaborare piani di *problem management* e iniziative di *service improvement*;
- organizzare riunioni periodiche con i clienti per la verifica dello stato del servizio, sulla base di KPI e stati di avanzamento del servizio condivisi con il cliente finale;
- redigere report sulle performance di servizio, secondo modalità e frequenza concordate;
- registrare e analizzare i dati relativi ai feedback ricevuti su prodotti e servizi;
- condividere, ove necessario, evoluzioni dei servizi attivi attraverso progetti ad hoc (tempi e attività);
- rafforzare la fidelizzazione dei clienti e dei partner, stimolando al contempo la generazione di nuove opportunità commerciali.

Privacy dei clienti e perdita di dati dei clienti

Nel corso del 2025, Cyberoo ha proseguito il presidio dei temi di data protection e cybersecurity attraverso un approccio integrato, che coniuga misure organizzative, procedurali e tecnologiche volte a garantire la riservatezza, l'integrità e la disponibilità delle informazioni trattate, sia nei processi interni sia nell'erogazione dei servizi ai clienti. Alla data di redazione del presente Bilancio non risultano pervenute contestazioni o reclami da parte dei clienti in materia di privacy, né violazioni accertate della normativa sulla protezione dei dati personali con riferimento ai trattamenti svolti dal Gruppo in qualità di Titolare o di Responsabile del trattamento.

Nel medesimo periodo, per quanto rilevato dai presidi interni di controllo e monitoraggio, non si sono verificati eventi di divulgazione, furto, perdita o accesso non autorizzato a dati dei clienti tali da configurare data breach o incidenti significativi di sicurezza delle informazioni. Il presidio di tali rischi si fonda su procedure interne, attività di monitoraggio, misure di prevenzione e risposta agli incidenti e su un costante rafforzamento delle competenze del personale sui temi della sicurezza e della protezione dei dati.

Coerentemente con il proprio modello di business B2B, Cyberoo tratta prevalentemente dati riferibili a organizzazioni e interlocutori professionali, limitando il trattamento dei dati personali a quanto necessario per finalità contrattuali, commerciali, di assistenza e di marketing, nel rispetto dei principi di minimizzazione, liceità, correttezza e trasparenza. A supporto della qualità del servizio e della sicurezza dei clienti, il Gruppo mette inoltre a disposizione servizi e soluzioni dedicati al monitoraggio delle infrastrutture, alla cybersecurity intelligence, al vulnerability assessment e all'incident response, in un'ottica di prevenzione, rilevazione tempestiva e gestione degli eventi di sicurezza.

Attività di marketing

Il Gruppo Cyberoo opera in ambito B2B e, nell'ambito delle attività di marketing, tratta prevalentemente dati relativi a soggetti giuridici. Le informazioni utilizzate riguardano principalmente le caratteristiche delle aziende, quali numero di dipendenti, fatturato, settore di appartenenza e tecnologie adottate. Con riferimento ai dati delle persone fisiche, il trattamento è limitato a informazioni professionali essenziali, quali l'indirizzo e-mail aziendale e il numero di telefono aziendale. Non vengono trattati dati personali di natura sensibile, quali preferenze individuali, abitudini personali, dati relativi alla salute o informazioni relative a orientamento politico, religioso o sessuale.

Le attività di comunicazione e marketing sono rivolte esclusivamente a clienti già acquisiti oppure a potenziali clienti che hanno manifestato un interesse volontario nei confronti del Gruppo, ad esempio mediante iscrizione a newsletter, partecipazione a eventi o webinar, oppure download di contenuti o applicazioni proprietarie. Le modalità di trattamento dei dati sono chiaramente descritte e rese disponibili sul sito web aziendale. Il Gruppo svolge inoltre attività di telemarketing attraverso l'utilizzo di database forniti da operatori specializzati, i quali garantiscono la conformità alla normativa vigente in materia di protezione dei dati personali.

Nel corso del triennio 2023-2025 non si sono verificati casi di non conformità con le normative vigenti e con i codici di autoregolamentazione in materia di comunicazioni di marketing, incluse la pubblicità, la promozione e la sponsorizzazione.

Presenza digitale e diffusione dei contenuti

Nel corso del 2025 Cyberoo ha continuato a rafforzare la propria presenza digitale, consolidando il lavoro editoriale sviluppato sui diversi canali online e aumentando la capacità del brand di raggiungere stakeholder, clienti e interlocutori interessati ai temi della cybersecurity.

Il sito istituzionale *cyberoo.com* ha registrato 87.161 visite e oltre 3 milioni di impression su Google, evidenziando una crescente visibilità del brand nei percorsi di ricerca online e una maggiore riconoscibilità dei contenuti aziendali.

Particolarmente significativa è stata la performance dei due blog aziendali, strumenti dedicati alla diffusione di contenuti informativi, divulgativi e specialistici sui temi della sicurezza informatica. I risultati evidenziano una crescita rilevante rispetto al 2024, considerando che il confronto avviene tra un periodo di rendicontazione esteso a 15 mesi e un periodo precedente di 12 mesi.

Il blog dedicato ai temi di awareness ha raggiunto 22.770 visite, registrando un incremento del 61,6% rispetto alle 14.091 visite del 2024. Ancora più rilevante la crescita del blog tecnico, che ha totalizzato 14.629 visite, con un incremento del 341,7% rispetto alle 3.312 visite dell'anno precedente. Questi risultati confermano il crescente interesse verso contenuti specialistici e di approfondimento e il ruolo dei canali editoriali aziendali nella diffusione di una maggiore consapevolezza sui rischi cyber.

Anche i canali social hanno contribuito al consolidamento della presenza digitale di Cyberoo. La pagina LinkedIn ha raggiunto 17 mila follower e generato circa 1 milione di impression, confermandosi un canale strategico per la comunicazione verso il pubblico professionale, la valorizzazione delle competenze aziendali e il rafforzamento della brand awareness.

Il canale Instagram, avviato nel 2024 con l'obiettivo di ampliare le attività di employer branding e proporre contenuti di awareness attraverso formati più immediati e visuali, ha raggiunto 600 follower e quasi 700 mila visualizzazioni video complessive, evidenziando una progressiva crescita nella capacità di coinvolgere gli utenti attraverso linguaggi digitali innovativi.

La strategia digitale di Cyberoo rappresenta un elemento di supporto al posizionamento del brand e alla diffusione della cultura della cybersecurity,

favorendo un dialogo continuativo con clienti, partner, talenti e stakeholder attraverso contenuti accessibili e di valore.

Network360

Nel corso del 2025 Cyberoo ha collaborato con Nextwork360, partner strategico per le attività di comunicazione e marketing digitale, con l'obiettivo di valorizzare il proprio posizionamento sul mercato, rafforzare la brand reputation e supportare le attività di generazione della domanda attraverso un approccio integrato tra contenuti, canali digitali e strumenti tecnologici.

La collaborazione ha previsto l'integrazione di attività di ottimizzazione SEO e azioni mirate sui canali esterni del network Nextwork360 (attività outbound), con l'obiettivo di aumentare la visibilità dell'azienda, valorizzarne competenze ed expertise nel settore della cybersecurity e creare nuove opportunità di relazione con il mercato.

Le principali aree di intervento hanno riguardato:

- **Content Strategy Human First**

Attraverso un approccio editoriale orientato alla valorizzazione delle competenze aziendali e alla produzione di contenuti di qualità, sono stati realizzati: 4 articoli dedicati a tematiche strategiche per il settore cybersecurity, pubblicati sulle testate editoriali del network Nextwork360; 2 video interviste curate dalle redazioni Nextwork360; una nuova vlog series composta da 6 appuntamenti, finalizzata a raccontare competenze e punti di vista dell'azienda attraverso un formato multimediale.

- **SEO & AIO Optimization**

Sono state sviluppate attività di ottimizzazione tecnica e semantica dei contenuti digitali, in linea con l'evoluzione dei motori di ricerca e dei nuovi strumenti basati sull'intelligenza artificiale, con l'obiettivo di migliorare la presenza organica del brand e la reperibilità delle informazioni relative all'offerta Cyberoo.

- **Technology & Process Optimization**

La collaborazione ha incluso attività di configurazione e integrazione degli strumenti tecnologici a supporto dei processi di marketing digitale, tra cui HubSpot e Microsoft Dynamics 365, con l'obiettivo di migliorare la gestione

dei flussi, la tracciabilità delle attività e l'efficacia delle iniziative di marketing automation.

- **Marketing Automation Strategy e monitoraggio continuo**

È stata definita e gestita una strategia di Marketing Automation “Always On”, attraverso: aggiornamenti periodici e sviluppo di workflow dedicati alle attività di nurturing e re-engagement; attività di gestione ed evoluzione del blog aziendale in HubSpot, con interventi di riallineamento editoriale e stilistico; monitoraggio delle performance tramite KPI, reporting, SAL di progetto e attività di consulenza operativa finalizzate a garantire coerenza strategica e miglioramento continuo.

La collaborazione con Nextwork360 prosegue anche nel 2026 attraverso i canali editoriali e digitali del network, confermandosi un elemento di supporto alla strategia di comunicazione di Cyberoo e contribuendo al consolidamento del posizionamento del brand, alla valorizzazione delle competenze aziendali e alla diffusione della cultura della cybersecurity presso gli stakeholder di riferimento.

Attività	Output	Dettaglio
Ottimizzazione SEO dei contenuti	<ul style="list-style-type: none"> Audit del sito Mappatura pagine per redirect Ottimizzazioni SEO 	Assessment sito, e consegna roadmap interventi. Ottimizzazione in ottica SEO dei contenuti per migliorare il posizionamento sui motori di ricerca
Creazione contenuti da promuovere sul Network Digital360	<ul style="list-style-type: none"> 3 contenuti originali/anno 	Contenuti sulle tematiche concordate (interviste, use case, news, scenari e trend di settore, ecc.) pubblicati sul Network Digital360 e relative riprese social e di NL di testata.
Contenuti asset Cyberoo corredati di riprese social	<ul style="list-style-type: none"> 2 Pillar page 15 articoli da Blog + 30 post social 5 articoli passati con rich media 4 Vlog + pillole video per LinkedIn 1 White paper Deep & Dark web 1 Review del White paper «Security as a service: il nuovo approccio alla sicurezza informatica che rivoluziona il mercato» 	Contenuti e riprese social sulle tematiche concordate (interviste, use case, news, scenari e trend di settore, ecc.) pubblicati su asset Cyberoo.
Marketing Automation Technology	<ul style="list-style-type: none"> Licenza Hubspot Marketing (+ 6.000 Marketing contact included) Implementazione workflow e supporto marketing automation 	<ul style="list-style-type: none"> Licenza Hubspot PRO Workflow di benvenuto Workflow di marketing automation Workflow nurturing Sales Workflow pagine web Workflow content curation Workflow preparazione evento Workflow follow up evento

Marketing Arena

Nel corso del 2025 Cyberoo ha collaborato con Marketing Arena, partner digitale a supporto della definizione e implementazione di una strategia di digital marketing finalizzata ad aumentare la brand awareness e a favorire una maggiore consapevolezza degli utenti rispetto ai temi della cybersecurity.

La collaborazione ha previsto lo sviluppo di campagne di digital advertising su diversi canali online, con l'obiettivo di promuovere i contenuti digitali dell'azienda, rafforzare il presidio dei temi legati alla sicurezza informatica e raggiungere target qualificati attraverso i principali ecosistemi digitali, tra cui Google, LinkedIn e Meta.

- Le attività di advertising sviluppate nel 2025 si sono articolate in diverse campagne con obiettivi specifici: Campagna Lead Generation su LinkedIn, finalizzata alla raccolta di contatti qualificati attraverso contenuti e iniziative mirate rivolte al pubblico professionale;
- Campagna Google Search, supportata da una nuova strategia di keyword targeting, volta a intercettare le ricerche degli utenti interessati ai temi della cybersecurity e ai servizi offerti da Cyberoo;
- Campagna Google Display, con focus sulla diffusione di contenuti informativi quali whitepaper e articoli del Cyber Blog, per aumentare la conoscenza del brand e favorire l'engagement degli utenti;
- Campagne Performance Max (PMax), organizzate per aree tematiche legate alla Security Awareness (Keatrix) e ai temi della cybersecurity a più ampio spettro;
- Campagne Meta, a supporto del canale Instagram.

Tra i contenuti che hanno registrato le migliori performance nell'ambito delle attività di advertising si evidenzia l'Osservatorio Cyberoo, progetto editoriale dedicato all'analisi dei principali trend di attacco informatico e all'evoluzione delle strategie di difesa. L'iniziativa rappresenta uno strumento di divulgazione e sensibilizzazione sui temi della cybersecurity, contribuendo a rafforzare il ruolo di Cyberoo come interlocutore qualificato nel settore e a diffondere maggiore consapevolezza sui rischi cyber presso aziende e stakeholder. La seconda edizione dell'Osservatorio Cyberoo, pubblicata nel 2026, ha analizzato i principali trend e pattern di attacco emersi nel 2025, traducendo le evidenze raccolte in indicazioni operative per rafforzare la capacità di prevenzione e risposta agli incidenti informatici. Il report si basa sulle informazioni raccolte dal team I-SOC e dall'Incident Response Team attraverso il monitoraggio continuo degli eventi di sicurezza e delle minacce emergenti.

La collaborazione con Marketing Arena proseguirà anche nel periodo successivo, attraverso ulteriori investimenti in advertising online e attività mirate sui diversi canali digitali, con l'obiettivo di consolidare la presenza del brand, ampliare la diffusione dei contenuti e rafforzare il dialogo con gli stakeholder di riferimento.

VENTISETTE Digital Communication

Nel corso degli anni Cyberoo ha intrapreso un percorso di evoluzione della propria identità digitale e della comunicazione istituzionale in collaborazione con VENTISETTE Digital Communication SB, partner creativo e digitale a supporto delle attività di sviluppo del sito web, della progettazione grafica dei documenti corporate e della valorizzazione del brand.

Il progetto di evoluzione del sito web, avviato negli anni precedenti, ha avuto l'obiettivo di rafforzare la presenza digitale di Cyberoo attraverso un'esperienza utente distintiva, caratterizzata da una comunicazione chiara, una user experience innovativa e una rappresentazione coerente dei valori aziendali. Il sito continua a rappresentare un elemento centrale della strategia di comunicazione del Gruppo, grazie a un aggiornamento costante dei contenuti e delle funzionalità in linea con l'evoluzione del posizionamento aziendale.

Nel corso del 2025 la collaborazione con VENTISETTE Digital Communication SB è proseguita attraverso attività di aggiornamento e ottimizzazione del sito web corporate, oltre alla progettazione grafica dei principali documenti di comunicazione istituzionale, tra cui Bilanci Consolidati, Bilanci di Sostenibilità e documentazione societaria.

La collaborazione prosegue anche nel 2026 con l'obiettivo di garantire continuità nell'evoluzione degli strumenti digitali e della comunicazione visiva di Cyberoo, mantenendo coerenza tra identità del brand, posizionamento sul mercato e modalità di relazione con gli stakeholder.

L'etica delle relazioni commerciali

In coerenza con i principi contenuti nel Codice Etico, nel Modello di organizzazione, gestione e controllo adottato ai sensi del D.Lgs. 231/2001 e nelle procedure aziendali applicabili, Cyberoo impronta le proprie relazioni commerciali al rispetto

della normativa vigente e ai principi di integrità, correttezza, professionalità, trasparenza, lealtà e reciproca collaborazione.

Nella fase di presentazione e negoziazione delle proprie soluzioni, Cyberoo si impegna a fornire ai clienti, ai distributori e ai partner informazioni veritiere, comprensibili e coerenti con le caratteristiche effettive dei servizi, specificandone il perimetro, i prerequisiti tecnici, la modalità di erogazione, i livelli di servizio applicabili, i corrispettivi e le rispettive professionalità. Tale approccio è finalizzato a consentire agli interlocutori commerciali di assumere decisioni informate e consapevoli, evitando rappresentazioni ambigue o suscettibili di generare aspettative non coerenti con quanto effettivamente contrattualizzato.

Gli impegni assunti sono disciplinati nelle offerte, negli ordini, nei contratti, nelle condizioni generali, negli accordi sul trattamento dei dati, negli EULA e negli eventuali SLA applicabili. Il Gruppo opera affinché tali impegni siano rispettati secondo il perimetro, le tempistiche e le responsabilità concordate, fermo restando il coinvolgimento e la cooperazione richiesti al cliente, al partner e agli altri soggetti della filiera.

Nell'ambito delle relazioni commerciali sono vietati comportamenti corruttivi, la concessione o l'accettazione di utilità non adeguatamente giustificate dal rapporto professionale, nonché ogni condotta idonea a compromettere l'indipendenza e l'imparzialità delle decisioni. Cyberoo tutela, inoltre, la riservatezza delle informazioni acquisite nel corso delle trattative e dei rapporti contrattuali, il corretto trattamento dei dati personali e il rispetto dei diritti di proprietà intellettuale e dei segreti commerciali.

Cyberoo promuove una concorrenza libera e leale e non ammette l'acquisizione, l'utilizzo o la divulgazione illecita di informazioni riservate appartenenti a clienti, partner, concorrenti o altri soggetti del mercato.

Il processo commerciale e la qualità del servizio

Il processo commerciale del Gruppo Cyberoo si sviluppa attraverso fasi strutturate, finalizzate a comprendere le esigenze del cliente, definire con chiarezza il perimetro della fornitura e assicurare continuità tra la fase commerciale e quella di erogazione del servizio.

- La fase iniziale prevede l'analisi delle esigenze di sicurezza e del contesto tecnologico del cliente, svolta con il coinvolgimento delle funzioni commerciali e tecniche competenti e, nel modello di vendita indiretta, del partner di riferimento. Sulla base delle informazioni raccolte vengono individuate le soluzioni ritenute maggiormente coerenti con il perimetro e gli obiettivi rappresentati dal cliente.
- la proposta commerciale descrive le caratteristiche dei servizi modalità di attivazione ed erogazione, gli eventuali prerequisiti tecnici, i corrispettivi, la durata, i livelli di servizio e le responsabilità delle parti. Le soluzioni possono essere configurate o integrate, ove tecnicamente applicabile, in funzione delle caratteristiche dell'ambiente del cliente, senza modificare il perimetro e le funzionalità proprie del servizio contrattualizzato.
- Successivamente alla formalizzazione dell'accordo, le attività di onboarding, implementazione e attivazione sono coordinate dalle funzioni aziendali competenti, secondo le modalità previste per ciascun servizio. L'erogazione viene monitorata rispetto agli impegni contrattuali, ai livelli di servizio e agli indicatori operativi applicabili.
- Durante il rapporto, Cyberoo mantiene un confronto con il cliente e con il partner attraverso i canali di assistenza, le Service Review e gli ulteriori momenti di verifica previsti. Le segnalazioni e i feedback raccolti sono analizzati al fine di individuare eventuali azioni correttive, interventi di service improvement ed evoluzioni del servizio compatibili con il perimetro contrattuale e tecnico.

Il canale di distribuzione

Cyberoo opera attraverso un modello di vendita indiretta di tipo TIER II, basato sulla collaborazione con una rete di distributori e partner qualificati, supportata da una struttura commerciale interna dedicata. La concreta configurazione del canale può variare in funzione del Paese, della tipologia di soluzione, delle caratteristiche dell'opportunità e degli specifici accordi commerciali applicabili.

Il modello prevede una catena di valore composta da quattro principali attori: Cyberoo, distributori, partner e clienti finali, ciascuno con un ruolo specifico all'interno del processo commerciale e operativo.

Cyberoo presidia lo sviluppo tecnologico delle soluzioni, ne definisce il quadro contrattuale e le condizioni di utilizzo ed erogazione, fornisce il supporto tecnico di propria competenza e monitora la qualità dei servizi direttamente erogati.

I distributori rappresentano un elemento strategico del modello di canale e operano a supporto dello sviluppo commerciale dell'ecosistema Cyberoo nei diversi Paesi. Il loro ruolo comprende l'identificazione e il coinvolgimento di nuovi partner, la gestione dei flussi amministrativi e finanziari tra Cyberoo e il canale, nonché il supporto operativo alla rete dei rivenditori.

I partner, principalmente System Integrator e operatori specializzati, rappresentano il punto di contatto commerciale con il cliente finale. Grazie alla relazione consolidata con le organizzazioni clienti, i partner sono in grado di proporre le soluzioni Cyberoo integrandole all'interno delle proprie offerte e accompagnando il cliente nel percorso di adozione dei servizi di cybersecurity.

Il cliente finale mantiene quindi una relazione commerciale principalmente con il partner di riferimento, che gestisce la trattativa, la definizione delle condizioni economiche e gli aspetti contrattuali. Cyberoo interviene direttamente nei casi in cui generi un'opportunità commerciale, affidandone successivamente la gestione al partner più idoneo secondo criteri condivisi, oppure quando viene coinvolta dal partner per opportunità strategiche o caratterizzate da particolare complessità.

Il modello TIER II consente a Cyberoo di ampliare la propria presenza sul mercato attraverso un ecosistema strutturato, valorizzando le competenze dei partner e garantendo al contempo elevati standard qualitativi, grazie al presidio diretto delle componenti tecnologiche, progettuali e di supporto.

La collaborazione con distributori e partner permette inoltre di creare valore condiviso: i partner possono arricchire la propria proposta commerciale con soluzioni avanzate di cybersecurity, mentre Cyberoo può raggiungere un numero crescente di clienti attraverso relazioni commerciali consolidate e di fiducia e una rete qualificata di operatori sul territorio.

Fidelizzazione e misurazione della qualità

Cyberoo mira a costruire rapporti duraturi con partner e clienti, fondati sulla continuità del servizio, sull'affidabilità operativa, sulla trasparenza delle comunicazioni e sulla capacità di gestire tempestivamente eventuali criticità.

La qualità del servizio e la solidità delle relazioni commerciali sono valutate, in funzione dei processi e dei servizi applicabili, attraverso l'analisi dei rinnovi contrattuali, della continuità dei rapporti, del rispetto dei livelli di servizio, dell'andamento dei ticket e delle segnalazioni, degli esiti delle Service Review, dei feedback ricevuti e delle azioni correttive o di miglioramento intraprese.

Cyberoo mantiene un'attenzione costante verso la soddisfazione del cliente grazie anche al ruolo strategico del Security Advisor Manager (SAM), figura che non si limita al monitoraggio della qualità del servizio ma agisce anche come punto di contatto privilegiato per il cliente nel post-vendita. Il SAM supporta la gestione operativa delle attività, raccoglie feedback in modo strutturato e promuove un miglioramento continuo delle soluzioni e del rapporto con il cliente.

Le informazioni raccolte vengono utilizzate per monitorare l'efficacia dei processi, individuare eventuali criticità ricorrenti e orientare le iniziative di service improvement, nel rispetto del perimetro contrattuale e delle caratteristiche tecniche delle soluzioni erogate.

La concentrazione dei ricavi su una clientela di riferimento dimostra l'efficacia delle relazioni instaurate e la qualità dei servizi forniti. Cyberoo si impegna a soddisfare le esigenze dei propri clienti attraverso soluzioni innovative e personalizzate, il che ha permesso al Gruppo di consolidare la propria posizione come leader nel settore della cybersecurity.

La gestione della supply chain

I fornitori

Il parco fornitori del gruppo Cyberoo è costituito da un ristretto numero di aziende con cui si è stabilito e consolidato nel tempo un rapporto di stretta collaborazione.

Le diverse esigenze commerciali di offrire alla clientela soluzioni al passo con l'innovazione tecnologica richiedono di selezionare eventuali nuovi fornitori, seppur la politica aziendale incoraggi, ove possibile, a mantenere contatti continuativi con i fornitori qualificati.

Tutte le volte che si rende necessario scegliere, valutare e approvare un Fornitore (sia di prodotti che servizi) che possa avere influenza sulla qualità e sicurezza delle

informazioni dei prodotti e servizi forniti da Cyberoo, il Gruppo applica una procedura standardizzata, di seguito sintetizzata:

- i prodotti e i servizi affidati ai fornitori devono essere conformi ai requisiti stabiliti in sede di accordo con Gruppo Cyberoo;
- i prodotti e i servizi approvvigionati esternamente devono essere tenuti sotto controllo secondo modalità definite internamente in base alla tipologia di fornitura, tenendo in considerazione l'impatto potenziale sulla capacità di soddisfare con regolarità il cliente;
- la scelta di selezione dei Fornitori devono avvenire seguendo criteri di affidabilità, che consentano di ottenere la massima soddisfazione dei requisiti di qualità e sicurezza delle informazioni del prodotto o servizio acquistato;
- l'affidabilità dei Fornitori deve essere periodicamente controllata;
- i dati di acquisto devono essere gestiti in forma controllata;
- le modalità di comunicazione identificate con i fornitori esterni devono rispondere a requisiti stabiliti.

La selezione e gestione della catena di fornitura

Per i fornitori con cui si intende intraprendere una collaborazione continuativa, una volta superata con esiti positivi l'attività di valutazione iniziale, vengono completate le informazioni commerciali e tecniche relative al fornitore e, per Cyberoo S.p.A., viene compilato il record fornitore sul file *M APS QVF Qualifica e Valutazione Fornitore*, riportando i dati e l'esito delle prime forniture come da Procedura Approvvigionamenti.

Se un fornitore è ritenuto strategico, viene inserito all'interno dei "fornitori in osservazione" per poi essere promosso a fornitore qualificato in occasione di forniture ricorrenti.

Per tutte le altre aziende del gruppo, l'esito positivo corrisponde con la codifica a gestionale, corredata di tutti i documenti integrativi (sla, visure, certificazioni richieste).

Per Cyberoo, come da normativa ISO 27001, l'approvazione formale dei potenziali fornitori viene effettuata a cura dell'Ufficio Acquisti, sulla base dei dati raccolti e assegnando un voto (da 0 a 3) ai seguenti criteri di valutazione:

- qualità del prodotto/ servizio;
- referenze e professionalità;
- rispetto degli impegni;
- collaborazione e disponibilità;
- sistema gestione qualità;
- sistema di gestione di sicurezza delle informazioni (nel caso in cui non fosse stata conseguita alcuna certificazione in tale ambito, Cyberoo si assicura che i fornitori di servizi, considerati i fornitori più critici, gestiscano in maniera congrua le informazioni, allegando a tutti i contratti con gli stessi una documentazione specifica);
- prezzi e condizioni economiche.

I criteri di valutazione dei fornitori sono i seguenti:

0 = Insufficiente	Si sono riscontrate non conformità/ inconvenienti e scarsa reattività ai problemi
1 = Sufficiente	Si sono riscontrate episodiche non conformità/ inconvenienti con reattività positiva del fornitore
2 = Buono	Non si sono riscontrate non conformità/ inconvenienti significativi
3 = Ottimo	Prestazione eccellente.

Per quanto riguarda la domanda sul Sistema Gestione Sicurezza delle Informazioni del fornitore, particolare rilevanza è data ai fornitori di servizi che gestiscono informazioni sensibili.

Nel gestionale sono indicati esplicitamente i fornitori in possesso della certificazione ISO 27001 e quindi ritenuti idonei in automatico. Per gli altri fornitori di servizi, Cyberoo ha inviato un modulo di autocertificazione delle misure tecniche e organizzative per misurarne la sicurezza. Per i fornitori occasionali (fornitori utilizzati per momentanea indisponibilità dei fornitori abituali o per soddisfare una richiesta di servizio nuovo occasionale inoltrata da parte del cliente), invece, non è richiesta l'attività formalizzata di selezione e valutazione.

Analogamente, per i fornitori con i quali c'è uno stretto rapporto di partnership, non si richiede una formale selezione e valutazione, bensì vengono assoggettati a definizione di specifiche di fornitura (es. capitolati di servizio, condivisione delle procedure operative) e controllo delle forniture, con eventuale rilevazione / registrazione di non conformità.

Per essere qualificato, il fornitore deve ottenere la valutazione almeno “sufficiente” per il criterio “qualità prodotto/ servizio e la valutazione media pesata maggiore o uguale a 55%.

I Fornitori che hanno superato positivamente la fase di valutazione iniziale vengono qualificati: l'evidenza di tale qualifica risulta dalla data di qualifica inserita nel M APS QVF.

Le schede di Valutazione ed eventuali certificati o documenti tecnici inviati dai Fornitori sono conservati a cura dell'Ufficio Acquisti, quali riferimenti documentati delle caratteristiche del Fornitore e della sua valutazione.

Tutte le informazioni contenute nell'archivio fornitori sono considerate riservate e non possono essere divulgate senza l'autorizzazione del responsabile.

La filiera sostenibile

Le società del Gruppo Cyberoo gestiscono i fornitori con lealtà, correttezza e professionalità incoraggiando rapporti continuativi e solidi.

Il gruppo Cyberoo ha intrapreso in percorso di sostenibilità aziendale ESG (Environmental, Social and Corporate Governance) in base al quale si richiede una presa di coscienza a tutta la filiera di fornitura.

Il miglioramento degli impatti ambientali, sociali e di governance di Cyberoo richiede consapevolezza e trasparenza delle attività presenti e future per ampliare l'impatto del percorso che è stato intrapreso internamente: Cyberoo considera essenziale misurare gli impatti del proprio ecosistema e stabilire un dialogo collaborativo con i partner, riconoscendo che ognuno è indispensabile per l'altro, in un processo di apprendimento reciproco e di co-evoluzione.

Ad ogni fornitore ritenuto strategico per volume, numero di ordini, impatto e brand Cyberoo ha intenzione di sottoporre il Form Etico che permetterà di conoscere il livello di maturità in merito alle tematiche ESG.

Le macrocategorie trattate sono riassumibili in: **sostenibilità ambientale, etica, rispetto dei diritti e gestione dei fornitori.**

NUMERO FORNITORI	2023		2024		2025	
	n.	% sul totale	n.	% sul totale	n.	% sul totale
Numero di fornitori LOCALI ³	188	28%	194	26%	270	26%
Numero di fornitori situati in ITALIA	418	64%	473	65%	654	62%
Numero di fornitori situati in EUROPA	27	4%	38	5%	81	8%
Numero di fornitori situati in AMERICA	11	2%	15	2%	23	2%
Numero di fornitori situati in ASIA	1	0%	1	0%	3	0%
Numero di fornitori situati nel RESTO DEL MONDO	12	2%	11	2%	17	2%
TOTALE FORNITORI	657	100%	732	100%	1.048	100%

Nonostante si cerchi di dare preferenza ai fornitori locali, sia per prodotti che servizi, la scelta dei fornitori è anche condizionata dalla specificità di brand, caratteristiche e qualità alla base di quanto ordinato.

A parità di condizioni aziendali si è deciso di orientarsi su fornitori i più locali possibile.

Nel triennio si osserva una crescita esponenziale del budget complessivo speso in fornitori, che passa da 6,1 milioni di euro nel 2023 a 17,5 milioni di euro nel 2025 (+186%).

L'incidenza dei fornitori locali mostra un trend positivo o comunque costante ad almeno il 26% rimanendo stabile nonostante l'aumento dei budget spesi in Italia ed Europa, a dimostrazione di un crescente impegno verso il sostegno all'economia del territorio.

I fornitori italiani si confermano il principale canale di approvvigionamento, rappresentando costantemente oltre l'80% della spesa totale. I numeri del 2025 vedono aggregati tutte le realtà del gruppo Cyberoo.

La spesa verso fornitori europei è più che raddoppiata negli ultimi anni anche se rimane contenuta (dal 4% al 8%). Gli acquisti da fornitori extraeuropei (America, Asia, resto del mondo) sono sempre più contenuti.

³ Per fornitori locali si intende i fornitori provenienti dall'Emilia Romagna.

Budget speso in fornitori	2023		2024		2025	
	€	% sul totale	€	% sul totale	€	% sul totale
Budget speso in fornitori LOCALI	1.107.000	18%	1.751.000	21%	1.838.767	10%
Budget speso in fornitori situati in ITALIA	4.192.000	69%	5.565.000	65%	15.127.679	86%
Budget speso in fornitori situati in EUROPA	171.000	3%	366.073	4%	408.265	2%
Budget speso in fornitori situati in AMERICA	64.000	1%	115.257	1%	129.535	1%
Budget speso in fornitori situati in ASIA	100	0%	110	0%	2.856	0%
Budget speso in fornitori situati nel RESTO DEL MONDO	570.000	9%	734.000	9%	71.476	0%
TOTALE FORNITORI	6.104.100	100%	8.531.440	100%	17.578.582	100%

Il monitoraggio della filiera di produzione

Tutti i fornitori del Gruppo sono sottoposti a riesami periodici delle prestazioni, per valutare se i prodotti o servizi forniti hanno rispettato i requisiti di qualità e sicurezza delle informazioni attesi, ponderati e rapportati al volume delle forniture effettuate.

Per Cyberoo S.p.A., le valutazioni periodiche avvengono con frequenza commisurata agli eventuali problemi che si sono presentati nel periodo, seppur indicativamente a intervalli non superiori a 12 mesi (a inizio anno, per l'anno solare precedente, in occasione del Riesame Sistema Qualità e sicurezza delle informazioni da parte della Direzione).

In assenza di prestazioni, il fornitore viene comunque preso in considerazione almeno una volta all'anno per verificare la necessità di mantenerlo tra i fornitori approvati.

Per mantenere lo stato di Fornitore qualificato, il fornitore deve conservare nel tempo la valutazione almeno "sufficiente" per il criterio "qualità prodotto/servizio" e la valutazione media pesata maggiore o uguale al 55%.

Il fornitore in precedenza "qualificato", che nelle successive verifiche di prestazione risultasse "scarso" per due volte consecutive, non verrà più considerato fornitore approvato ed evidenziato in quanto tale nell'anagrafica dei

fornitori. In caso di valutazione scarsa viene normalmente attivato un reclamo formale al fornitore con la richiesta di normalizzare la situazione.

L'Ufficio Acquisti, in occasione del monitoraggio, si occupa di verificare se i fornitori approvati sono stati interpellati nell'arco del periodo: qualora non gli fosse richiesto alcun servizio di fornitura per tre anni, non verrà più considerato approvato e, in caso di successiva necessità di utilizzo, si provvederà a ripetere l'iter di qualificazione.

Gli acquisti possono rispondere sia a esigenze di vendite transazionali, di canoni di servizio, sia di riapprovvigionamento interno.

Tabella aggregata delle sole controllate estere

Budget speso in fornitori ⁴	2024		2025	
	€	% sul totale	€	% sul totale
Budget speso in fornitori LOCALI	1.050.342	99,58%	1.253.440	99,99%
Budget speso in fornitori situati in ITALIA	-	0%	-	0%
Budget speso in fornitori situati in EUROPA	4.432	0,42%	60	0,0048%
Budget speso in fornitori situati in AMERICA	-	0%	-	0%
Budget speso in fornitori situati in ASIA	-	0%	-	0%
Budget speso in fornitori situati nel RESTO DEL MONDO	-	0%	-	0%
TOTALE FORNITORI	1.054.774	100%	1.253.500	100%

A livello di gruppo la precedente tabella mostra l'evidenza delle controllate estere di Ucraina, Polonia e Albania che, come si evince, sono quasi esclusivamente consolidate sul territorio (il locale è inteso come nazionale) con numeri crescenti.

⁴ A seguito dell'ampliamento del perimetro di rendicontazione a tutte le società del Gruppo, intervenuto per la prima volta nel presente esercizio, i dati disaggregati relativi al budget speso in fornitori non sono risultati interamente disponibili per l'esercizio 2023. Cyberoo si impegna a garantire la comparabilità dei dati su base triennale nei futuri Bilanci di Sostenibilità.

Le relazioni con il territorio

Cyberoo riconosce l'importanza di sviluppare relazioni solide e sostenibili con il territorio in cui opera, impegnandosi a contribuire attivamente alla crescita sociale, culturale ed economica delle comunità locali e internazionali. La politica di relazioni territoriali del Gruppo si fonda su una costante collaborazione con attori locali, istituzioni e associazioni e realtà accademiche, con l'obiettivo di promuovere iniziative che generino valore condiviso e benessere per la collettività. Nel 2025, Cyberoo ha rafforzato il proprio impegno attraverso diverse attività di stakeholder engagement, inclusi incontri dedicati con gli investitori per la presentazione dei risultati legati alla sostenibilità. Sono stati attivati comitati d'impresa e per la sicurezza e la salute sul lavoro, che hanno favorito un dialogo costruttivo con le comunità locali. Complessivamente, le attività che hanno previsto il coinvolgimento diretto del territorio sono aumentate del 90% rispetto al 2024.

ATTIVITÀ CHE PREVEDONO IL COINVOLGIMENTO DELLE COMUNITÀ LOCALI, VALUTAZIONI D'IMPATTO E PROGRAMMI DI SVILUPPO ⁵	2023		2024		2025	
	n.	% sul totale	n.	% sul totale	n.	% sul totale
Incontri organizzati (conferenze, workshop, focus group, ecc..) per divulgare i risultati delle valutazioni d'impatto ambientale e sociale	2	11%	12	40%	26	45,6%
Programmi di sviluppo comunitario locali	-	0%	-	0%	4	7%
Attività di stakeholder engagement	15	78%	16	53%	23	40,4%
Comitati di consultazione aperti alla comunità locale e processi che includono categorie vulnerabili	-	0%	-	0%	2	3,5%
Comitati di impresa, comitati per la sicurezza e la salute sul lavoro	2	11%	2	7%	2	3,5%
TOTALE ATTIVITÀ	19	100%	30	100%	57	100%

Nel 2025, Cyberoo ha consolidato il proprio impegno nel campo della sostenibilità sociale e culturale attraverso iniziative che hanno coinvolto attivamente il territorio e le comunità di riferimento. Le attività si sono sviluppate in ambiti strategici come la valorizzazione del patrimonio culturale, la promozione della formazione digitale

⁵ È importante sottolineare che nella tabella non sono incluse tutte le iniziative a carattere gratuito realizzate in collaborazione con i partner commerciali sul territorio, finalizzate esclusivamente alla divulgazione e sensibilizzazione delle aziende del territorio.

e il contrasto alle disuguaglianze, in particolare quelle legate al divario di genere. In collaborazione con organizzazioni no-profit e istituzioni culturali, Cyberoo ha contribuito alla realizzazione di eventi pubblici, percorsi formativi e campagne di sensibilizzazione, favorendo la diffusione della cultura della protezione – sia materiale che digitale – e l’accesso consapevole alle tecnologie.

Parallelamente, sono proseguite e si sono rafforzate le collaborazioni con enti professionali e accademici, finalizzate allo sviluppo di progetti di formazione. Queste sinergie hanno permesso l’attivazione di corsi, webinar, tirocini e iniziative congiunte, generando nuove opportunità di crescita e contribuendo allo sviluppo delle competenze nel settore della cybersecurity.

Attraverso tali attività, Cyberoo conferma la propria volontà di generare valore condiviso, promuovendo uno sviluppo sostenibile e inclusivo, e rafforzando il legame con le comunità e i territori in cui opera.

Collaborazioni con Università, scuola ed enti di ricerca

Nel corso del periodo di rendicontazione, il Gruppo ha rafforzato il proprio impegno nella collaborazione con il mondo accademico e della ricerca, con l’obiettivo di contribuire alla formazione e sviluppo di competenze specialistiche, favorire l’orientamento professionale degli studenti e sostenere la diffusione della cultura della cybersecurity.

Università di Modena e Reggio Emilia (UNIMORE) – Dipartimento di Ingegneria Informatica

Il Gruppo ha collaborato con il Dipartimento di Ingegneria Informatica dell’Università degli Studi di Modena e Reggio Emilia – “Enzo Ferrari” di Modena, nell’ambito del corso di sicurezza informatica, attività seminariali e formative rivolte agli studenti della laurea magistrale. L’iniziativa ha rappresentato un momento di confronto tra mondo accademico e realtà aziendale sui temi della cybersecurity, con particolare attenzione alle implicazioni operative della normativa europea e al ruolo dei Security Operations Center (SOC).

UNIMORE – Career Day “MoreJobs” 2026

A inizio 2026 il Gruppo ha partecipato al Career Day UNIMORE “MoreJobs”, uno dei principali eventi di incontro tra aziende, studenti e laureati del territorio.

L'iniziativa ha registrato la partecipazione di oltre 50 candidati interessati, principalmente provenienti da Ingegneria Informatica con specializzazione in cybersecurity, oltre che da altri percorsi accademici, tra cui giurisprudenza, marketing ed economia. La partecipazione ha confermato il posizionamento del Gruppo come realtà di riferimento nel settore della sicurezza informatica e la capacità di attrarre giovani talenti qualificati, rafforzando ulteriormente il legame con il sistema universitario e il territorio.

Università degli Studi di Torino – Master di I livello in Cybersecurity

Il Gruppo ha collaborato con l'Università degli Studi di Torino nell'ambito del Master di I livello in Cybersecurity, contribuendo al corso "Sicurezza delle infrastrutture ICT: Malware". L'attività ha avuto l'obiettivo di fornire agli studenti una visione operativa delle minacce malware e delle principali tecniche di difesa adottate in contesti aziendali complessi, con particolare riferimento alle infrastrutture ICT critiche e ai processi di detection e response.

Università Cattolica del Sacro Cuore

Il Gruppo ha consolidato la collaborazione con l'Università Cattolica del Sacro Cuore, Campus di Cremona e Piacenza, attraverso la partecipazione a iniziative accademiche e di orientamento, nonché attività di recruiting rivolte agli studenti.

La collaborazione, avviata nel 2021 anche nell'ambito del Comitato di Indirizzo del corso di laurea in "Innovazione e Imprenditorialità Digitale", ha favorito nel tempo il dialogo tra formazione accademica e mondo aziendale, contribuendo allo sviluppo di competenze digitali e di cybersecurity e all'attivazione di percorsi di stage e inserimento professionale.

Il Gruppo ha inoltre partecipato a iniziative di orientamento e selezione, tra cui Stage Day (speed interviews) e Career Day, che hanno permesso l'incontro con studenti e neolaureati provenienti da diversi percorsi formativi e l'avvio di esperienze di inserimento in azienda (3 assunzioni nel 2025 tramite stage day e career days universitari).

Politecnico di Milano – Osservatorio Cybersecurity & Data Protection

Il Gruppo ha avviato una collaborazione con il Politecnico di Milano – Dipartimento di Ingegneria Gestionale, nell'ambito del contratto di ricerca "Osservatorio

Cybersecurity & Data Protection 2025”, promosso dagli Osservatori Digital Innovation.

L’iniziativa ha permesso al Gruppo di contribuire attivamente alle attività di ricerca dell’Osservatorio e di partecipare a un ecosistema strutturato di confronto tra imprese, istituzioni e mondo accademico sui temi della cybersecurity e della protezione dei dati.

In particolare, la collaborazione ha consentito di:

- contribuire alle attività di ricerca e alle survey dell’Osservatorio;
- partecipare a workshop, incontri e momenti di confronto con altri attori del settore;
- intervenire in eventi e convegni dedicati alla diffusione dei risultati della ricerca;
- accedere ai report e ai contenuti di approfondimento prodotti dall’Osservatorio;
- condividere esperienze e casi aziendali a supporto delle attività di analisi e divulgazione.

La partecipazione all’Osservatorio rappresenta per il Gruppo un elemento rilevante di posizionamento nel dibattito scientifico e industriale sulla cybersecurity, oltre che un’opportunità di confronto continuo sulle evoluzioni normative, tecnologiche e organizzative del settore. Abbiamo partecipato anche evento istituzionale nel 2026 su sovranità digitale presso Palazzo Montecitorio, con focus su cloud, governance dei dati e AI.

Attività di formazione e sensibilizzazione in ambito sindacale

Il Gruppo ha proseguito le attività di divulgazione e formazione sui temi della cybersecurity anche verso stakeholder non accademici, contribuendo alla diffusione della cultura della sicurezza digitale in ambito lavorativo e sindacale. Nel 2025 il Gruppo ha partecipato a un’iniziativa formativa nell’ambito del programma “Green Rooms” promosso dalla FIM-CISL. Le Green Rooms sono spazi di confronto e approfondimento dedicati a rappresentanti sindacali e lavoratori, finalizzati allo sviluppo di competenze su temi legati all’innovazione, alla transizione digitale e alla sostenibilità del lavoro. L’intervento ha avuto l’obiettivo di sensibilizzare i partecipanti sui rischi cyber e sul ruolo della cybersecurity nella tutela dei

lavoratori, dei dati e della continuità operativa delle organizzazioni, favorendo una maggiore consapevolezza nella gestione dei temi digitali all'interno delle relazioni industriali. La collaborazione con il sindacato CISL si inserisce in un percorso già avviato negli anni precedenti, che ha incluso iniziative formative rivolte ai rappresentanti sindacali sui temi della sicurezza informatica, della protezione dei dati e della resilienza digitale, con l'obiettivo di promuovere una cultura della sicurezza sempre più diffusa e trasversale nei contesti aziendali.

Adesione a iniziative esterne, partnership e membership

Nel corso del 2025 e all'inizio del 2026 il Gruppo ha proseguito il proprio impegno nella partecipazione a iniziative istituzionali, associative e di sistema, con l'obiettivo di rafforzare il posizionamento nel dibattito nazionale sulla cybersecurity, favorire il confronto con imprese e istituzioni e contribuire alla diffusione della cultura della sicurezza digitale.

Sistema Confindustria – RetIndustria Servizi e associazioni territoriali

Il Gruppo prosegue la collaborazione con RetIndustria Servizi, società del sistema Confindustria dedicata alla promozione di convenzioni e servizi per le imprese associate, con l'obiettivo di diffondere la cultura della cybersecurity e supportare la protezione delle PMI italiane.

Nel 2025 le attività si sono concretizzate in iniziative di comunicazione e webinar rivolti al network associativo, oltre alla partecipazione a eventi di sistema come il FARETE di Bologna, appuntamento annuale di networking industriale promosso da Confindustria Emilia Area Centro.

Il Gruppo ha inoltre partecipato a iniziative promosse da Confindustria Abruzzo Medio Adriatico nell'ambito dei programmi dedicati all'innovazione e alla trasformazione digitale delle imprese, nonché a cicli di webinar formativi organizzati per gli associati di Unione Industriale Pisana, con focus sulla gestione del rischio cyber e sulla resilienza digitale.

Parallelamente, il Gruppo conferma la propria adesione a Unindustria Reggio Emilia e a Confindustria Piacenza, contribuendo a iniziative di sistema e momenti di approfondimento sui temi della sicurezza informatica. A inizio 2026 il Gruppo ha inoltre aderito a Confindustria Emilia Area Centro, rafforzando ulteriormente la propria presenza all'interno del sistema associativo territoriale.

Clusit – Associazione Italiana per la Sicurezza Informatica

Il Gruppo è membro del Clusit, principale associazione italiana nel campo della sicurezza informatica, che promuove la cultura della cybersecurity e contribuisce all'evoluzione normativa e tecnica del settore. Nel corso del periodo di riferimento, la partecipazione al network ha consentito il contributo a iniziative di divulgazione e confronto scientifico sui temi della sicurezza delle infrastrutture digitali, anche attraverso la partecipazione a momenti di approfondimento e agli eventi collegati alle ricerche dell'associazione, tra cui i Security Summit di Milano e Napoli, che rappresentano occasioni di networking, formazione e confronto tra operatori del settore e mondo istituzionale. A inizio 2026, il Gruppo ha preso parte a ulteriori iniziative di rilievo istituzionale, tra cui l'evento "Sovranità digitale" presso Palazzo Montecitorio, dedicato al ruolo di cloud, dati e infrastrutture nella costruzione di un ecosistema digitale sicuro e autonomo, con approfondimenti su governance, intelligenza artificiale e protezione delle informazioni.

FAI – Fondo per l'Ambiente Italiano ETS

Il Gruppo ha consolidato la collaborazione con la Fondazione FAI – Fondo per l'Ambiente Italiano ETS, organizzazione non profit impegnata nella tutela, valorizzazione e gestione del patrimonio culturale, paesaggistico e storico italiano. La partnership, avviata nel 2022 e rinnovata nel tempo, si fonda su una visione condivisa di protezione e valorizzazione del patrimonio, sia fisico sia digitale, e sulla promozione della sostenibilità. Nel 2025 il Gruppo ha partecipato al Convegno nazionale del FAI, momento istituzionale di confronto sui temi della tutela del patrimonio culturale e del ruolo dei diversi attori nella sua valorizzazione. Il Gruppo ha inoltre preso parte a ulteriori iniziative a supporto del FAI e alla conferenza stampa regionale delle Giornate FAI di Primavera in Emilia-Romagna, iniziativa nazionale che ogni anno apre ai pubblici beni culturali normalmente non accessibili, promuovendone la conoscenza e la valorizzazione.

Comunicazione interna ed esterna

Comunicazione interna

Il Gruppo dedica particolare attenzione alla comunicazione interna con l'obiettivo di garantire flussi informativi strutturati, tempestivi e coerenti, favorendo la diffusione di conoscenze, valori aziendali e obiettivi strategici all'interno

dell'organizzazione. La comunicazione interna non si limita alla condivisione di informazioni operative, ma contribuisce allo sviluppo di un ambiente di lavoro collaborativo e trasparente, in cui ciascun collaboratore è consapevole del proprio ruolo e del proprio contributo agli obiettivi del Gruppo. In questo contesto, il rafforzamento del senso di appartenenza e la promozione di una cultura aziendale condivisa rappresentano elementi centrali.

Il Gruppo promuove inoltre strumenti e canali digitali finalizzati a migliorare l'efficienza e la qualità della comunicazione. Accanto agli strumenti tradizionali come la posta elettronica, è utilizzata la piattaforma intranet aziendale basata su Microsoft SharePoint, che consente la gestione centralizzata dei documenti, la condivisione in cloud e la collaborazione su contenuti in modalità strutturata e aggiornata in tempo reale. Questo strumento consente una riduzione del numero di e-mail, la possibilità di scambiare file in cloud e lavorare in modalità wiki su documenti condivisi, ottimizzando così il flusso di lavoro. A supporto di una comunicazione ancora più efficace, ordinata e facilmente fruibile, è stata inoltre introdotta la modalità di Outlook Newsletter interna. Si tratta di un sistema di comunicazione periodica strutturata, veicolata tramite Microsoft Outlook, che consente di aggregare in un unico flusso le principali informazioni aziendali, aggiornamenti organizzativi e comunicazioni di rilievo. Tale strumento permette di ridurre la frammentazione delle informazioni, migliorare la tracciabilità dei messaggi e garantire una maggiore coerenza nella diffusione dei contenuti all'interno del Gruppo.

Comunicazione agli investitori finanziari

Il Gruppo gestisce attivamente la comunicazione con gli investitori finanziari e il mercato attraverso un modello strutturato di Investor Relations, finalizzato a garantire trasparenza, continuità informativa e corretto posizionamento della Società presso stakeholder finanziari e istituzionali. La comunicazione esterna a supporto delle attività di media relations è curata in collaborazione con Reputation Value, agenzia di consulenza di Milano specializzata in comunicazione e ufficio stampa, e a partire da inizio 2026 con CDR Communication, società di Milano specializzata in comunicazione finanziaria e relazione con i media. Tali partnership consentono la diffusione coordinata e continuativa di informazioni relative a risultati economico-finanziari, eventi societari, iniziative strategiche e innovazioni,

attraverso comunicati stampa, interviste e attività di media relations, contribuendo a rafforzare la visibilità del Gruppo presso un pubblico qualificato di stakeholder e potenziali investitori.

Sul fronte Investor Relations, il Gruppo mantiene un dialogo costante con investitori, analisti e intermediari finanziari, inclusi istituti bancari e soggetti incaricati della gestione degli adempimenti societari e dei rapporti con i sistemi di mercato, tra cui Monte Titoli. La Società assicura la gestione strutturata dei principali flussi informativi verso il mercato e organizza periodicamente conference call in occasione della pubblicazione dei risultati finanziari annuali e semestrali, finalizzate alla condivisione dei dati economico-finanziari e al confronto diretto con la comunità finanziaria. Nel corso del 2025 e all'inizio del 2026 il Gruppo ha inoltre partecipato a iniziative e incontri dedicati al confronto con investitori istituzionali, contribuendo al rafforzamento della propria visibilità sui mercati e alla consolidazione delle relazioni con la comunità finanziaria:

23 gennaio 2025	Italian Day in Frankfurt
18 febbraio 2025	EnVent Winter Conference Milano
28 marzo 2025	Presentazione dei dati di bilancio FY2024
2 aprile 2025	Roadshow Alantra Milano
9 aprile 2025	Mid&Small London
12 giugno 2025	Kt&Partners Annual Investors Summit Day
1° luglio 2025	Mid&Small Virtual
3 luglio 2025	Roadshow Alantra Madrid
26 settembre 2025	Presentazione dei dati di bilancio H12025
10 ottobre 2025	Roadshow Alantra Virtual
28 ottobre 2025	Roadshow Alantra Milano
12 novembre 2025	Roadshow Alantra Parigi
2 dicembre 2025	Mid&Small Milano
18 marzo 2026	Mid&Small Parigi

Questi eventi hanno rappresentato un'importante opportunità per Cyberoo di confrontarsi con investitori e analisti, promuovendo ulteriormente la propria crescita e consolidando la propria presenza sul mercato.

Eventi PR, attività istituzionali ed eventi con partner – Italia ed estero

Nel corso del 2025 e all'inizio del 2026, il Gruppo ha proseguito e rafforzato il proprio impegno nella diffusione della cultura della cybersecurity e dell'innovazione tecnologica, attraverso la partecipazione e l'organizzazione di eventi PR, iniziative istituzionali e momenti di confronto con partner strategici, sia in Italia che all'estero. Le attività hanno coinvolto stakeholder istituzionali, imprese, studenti e operatori del settore, contribuendo al consolidamento del posizionamento del Gruppo come attore di riferimento nel panorama della cybersecurity. Gli interventi hanno incluso speech, workshop e sessioni di approfondimento su temi chiave quali intelligenza artificiale, rischio cyber, normative europee (tra cui NIS2), sicurezza delle infrastrutture digitali e rischio reputazionale, security awareness. La collaborazione con partner strategici ha rappresentato un elemento centrale delle attività del periodo, favorendo la diffusione di competenze e best practice e supportando al contempo iniziative di sviluppo commerciale. Nel complesso, sono stati realizzati 57 eventi, a testimonianza della solidità dell'ecosistema relazionale del Gruppo. A livello internazionale, il Gruppo ha inoltre proseguito il percorso di espansione delle proprie attività di comunicazione e presenza di mercato, con iniziative realizzate sia in Polonia che in Spagna, contribuendo al rafforzamento della rete relazionale e al consolidamento della presenza nei mercati esteri.

Tra i principali appuntamenti del periodo si segnalano:

- **Assonext – Academy di Borsa per società associate**

Il Gruppo ha partecipato al webinar dell'Academy di Borsa di Assonext, iniziativa dedicata alle società quotate e agli emittenti per l'approfondimento dei temi legati alla sostenibilità e all'evoluzione del quadro normativo.

Nel corso dell'intervento, il Gruppo ha condiviso la propria esperienza nel primo processo di rendicontazione ESG volontaria, con focus su

organizzazione interna, raccolta dati, principali criticità operative e benefici del reporting in termini di trasparenza e dialogo con gli stakeholder.

- **Cyber Crime Conference – Roma, 16-17 aprile 2025**

il Gruppo ha partecipato alla tredicesima edizione della Cyber Crime Conference, uno dei principali appuntamenti nazionali dedicati alla cybersecurity, organizzato da ICT Security Magazine presso l'Auditorium della Tecnica di Roma. Nel corso dell'evento, il Gruppo ha presentato i risultati dell'Osservatorio Cyberoo 2025 attraverso lo speech “Cybersecurity nel 2025: sfide e cambiamenti, l'Europa leader di sicurezza”. L'intervento ha approfondito l'evoluzione del panorama geopolitico e delle minacce informatiche, evidenziando il ruolo strategico delle aziende europee di cybersecurity nel garantire protezione e compliance alle imprese e la necessità di adottare un approccio alla sicurezza sempre più proattivo, integrato e orientato all'innovazione.

- **HackInBo – Bologna, 7 giugno 2025**

il Gruppo ha rinnovato la propria partecipazione a HackInBo 2025, una delle principali conferenze italiane dedicate alla sicurezza informatica e punto di riferimento per professionisti, aziende e appassionati del settore. Nel corso dell'evento, il Gruppo ha contribuito al dibattito sui principali trend della cybersecurity attraverso interventi basati sui dati dell'Osservatorio Cyberoo, approfondendo l'evoluzione del panorama delle minacce informatiche, con particolare attenzione ai rischi emergenti legati all'utilizzo dell'intelligenza artificiale, agli attacchi di nuova generazione, al fenomeno del cybercrime nel Dark Web e all'importanza di adottare modelli di difesa proattivi e integrati. La partecipazione ha rappresentato un'importante occasione di confronto con la community cyber e ha contribuito a rafforzare il posizionamento del Gruppo quale attore attivo nella diffusione della cultura della sicurezza digitale.

- **Farete – Bologna, 3-4 settembre 2025**

in qualità di partner di RetIndustria, il Gruppo ha partecipato a FARETE 2025, l'evento annuale di networking promosso da Confindustria Emilia Area Centro e dedicato all'incontro tra imprese, istituzioni e stakeholder del territorio. La partecipazione ha consentito di presentare le soluzioni e le competenze del Gruppo in ambito cybersecurity, favorendo il confronto con

il tessuto imprenditoriale e il consolidamento delle relazioni con aziende e partner, contribuendo alla diffusione della cultura della sicurezza digitale nel sistema produttivo italiano.

- **Milano Digital Week – Milano, 3 ottobre 2025**

il Gruppo ha partecipato alla Milano Digital Week, iniziativa dedicata ai temi dell'innovazione e della trasformazione digitale, con un intervento incentrato sull'evoluzione della security awareness e sul ruolo del fattore umano nella cybersecurity. Nel corso dell'evento è stato approfondito il tema della formazione quale elemento strategico per la gestione del rischio cyber, evidenziando l'importanza di sviluppare comportamenti consapevoli e una cultura della sicurezza diffusa all'interno delle organizzazioni. L'iniziativa ha inoltre rappresentato l'occasione per presentare Keatrix, la piattaforma sviluppata dal Gruppo per la formazione e la sensibilizzazione in ambito cybersecurity, basata su metodologie didattiche innovative e intelligenza artificiale adattiva, con l'obiettivo di favorire un cambiamento comportamentale duraturo e rafforzare la resilienza delle organizzazioni.

- **Semafor – Polonia, 10 marzo 2025**

il Gruppo ha partecipato a SEMAFOR Conference, uno dei principali appuntamenti in Polonia dedicati alla cybersecurity, all'IT audit e alla cybersecurity. L'evento ha riunito professionisti della sicurezza, responsabili IT e figure coinvolte nei processi di compliance, favorendo il confronto su evoluzione delle minacce cyber, gestione degli incidenti, protezione dei dati e adeguamento ai nuovi requisiti normativi.

- **AT Summit – Polonia, 18 novembre 2025**

il Gruppo ha preso parte all'Advanced Threat Summit (AT Summit), conferenza di riferimento in Polonia dedicata all'evoluzione delle minacce informatiche e alle strategie di difesa. L'evento ha rappresentato un'occasione di confronto con esperti e operatori del settore sui temi della gestione del rischio cyber, della protezione delle infrastrutture digitali e dell'integrazione della cybersecurity nelle strategie aziendali.

- **Women in IT – Polonia, 20 maggio 2025:**

il Gruppo ha partecipato all'iniziativa Women in IT, dedicata alla promozione della diversità e dell'inclusione nel settore tecnologico. L'evento ha approfondito il ruolo delle competenze femminili nell'innovazione digitale,

attraverso momenti di confronto, networking e sensibilizzazione sul superamento del divario di genere nei percorsi professionali in ambito IT e cybersecurity.

Iniziative di solidarietà e supporto alla comunità

Nel corso del 2025 il Gruppo ha confermato il proprio impegno in iniziative di responsabilità sociale a sostegno della comunità, attraverso contributi economici destinati a progetti con impatto sociale e inclusivo.

Progetto Itaca – Donazione a sostegno della salute mentale

Il Gruppo ha effettuato una donazione a favore di Progetto Itaca, fondazione attiva a livello nazionale nella promozione di programmi di informazione, prevenzione, supporto e riabilitazione in ambito salute mentale. L'iniziativa sostiene attività rivolte a persone con disturbi della salute mentale e alle loro famiglie, contribuendo alla diffusione della cultura dell'inclusione, alla riduzione dello stigma e al rafforzamento dei percorsi di supporto e reinserimento sociale.

SanPro Special – Sostegno allo sport inclusivo

Il Gruppo ha inoltre sostenuto SanPro Special, squadra di atleti paralimpici della ASD San Prospero Correggio, Sassuolo FS, impegnata in attività sportive dedicate a giovani adulti, con l'obiettivo di promuovere l'inclusione sociale attraverso lo sport. Il contributo è stato destinato al supporto delle attività sportive, tra cui l'acquisto di attrezzature, l'organizzazione degli allenamenti e la partecipazione a competizioni, favorendo lo sviluppo di competenze motorie, relazionali ed emotive e rafforzando il senso di appartenenza e collaborazione.



Capitolo 6

CAPITALE
ECONOMICO
FINANZIARIO

6. Capitale economico – finanziario

Andamento della gestione

Il bilancio consolidato del Gruppo Cyberoo, relativo all'esercizio 2025 e della durata eccezionale di 15 mesi, si è chiuso con un utile netto pari a 2.570.755 euro, rispetto ai 4.376.867 euro realizzati nell'esercizio 2024. I ricavi delle vendite e delle prestazioni hanno raggiunto i 27,7 milioni di euro, in crescita rispetto ai 22,8 milioni di euro del 2024. Si segnala che il confronto con l'esercizio precedente non è omogeneo in ragione della differente durata dei due periodi e va pertanto letto tenendo conto di tale circostanza.

Sul fronte dei principali indicatori economici, l'EBITDA dell'esercizio 2025 si è attestato a 8,56 milioni di euro (pari al 27,4% sul valore della produzione), mentre l'EBIT è stato pari a 4,32 milioni di euro (13,8% sul valore della produzione). La contrazione dei margini rispetto all'esercizio precedente (EBITDA margin 42,6% e EBIT margin 28,3% nel 2024) riflette la fase di investimento strategico in cui il Gruppo si trova: la significativa crescita dell'organico (+28% in Italia, con l'avvio delle sedi estere), il rafforzamento della struttura operativa e commerciale, gli investimenti nello sviluppo e nell'evoluzione dell'offerta di servizi e soluzioni di cybersecurity — tra cui la Cyber Security Suite, Keatrix e i progetti di intelligenza artificiale e ricerca e sviluppo — e l'aumento degli oneri finanziari connessi all'espansione hanno inciso sulla redditività dell'esercizio, in coerenza con la strategia di crescita dimensionale e di internazionalizzazione perseguita dal Gruppo.

Di seguito le principali direttrici di investimento e le iniziative effettuati per rafforzare il posizionamento e accelerare la crescita:

- Evoluzione dell'offerta di cybersecurity: sviluppo del modello strategico e operativo per integrare threat management, governance dei processi, compliance e people security, con il rafforzamento delle capacità di monitoraggio, risposta agli incidenti, supporto ai percorsi NIS2 e miglioramento continuo della postura di sicurezza dei clienti. In tale ambito sono previsti, già a partire dal mese di luglio, nuovi annunci di piattaforma

finalizzati ad ampliare ulteriormente il supporto operativo e consulenziale alle aziende.

- vCISO e NIS2: sviluppo delle attività consulenziali a supporto dei clienti nei percorsi di adeguamento normativo, governance del rischio cyber e miglioramento della postura di sicurezza.
- Keatrix: sviluppo della piattaforma proprietaria Human Risk & Security TrAlning basata su intelligenza artificiale adattiva, edutainment e personalizzazione dei percorsi formativi.
- Intelligenza artificiale e R&D: prosecuzione degli investimenti in tecnologie proprietarie e nuovi progetti innovativi in ambito cybersecurity.
- Canale distributivo e internazionalizzazione: sviluppo di nuovi accordi distributivi e rafforzamento delle direttrici commerciali in Italia, Polonia e Spagna.
- Cyberoo Capital: avvio di un'iniziativa dedicata a modelli di locazione evolutiva delle soluzioni di cybersecurity, finalizzata ad ampliare le modalità di accesso ai servizi del Gruppo da parte della clientela.
- Governance e razionalizzazione societaria: semplificazione della struttura del Gruppo e rafforzamento dei presidi organizzativi.

Il valore economico generato e distribuito

Il prospetto che evidenzia il valore generato e distribuito viene elaborato sulla base del Conto Economico consolidato, con l'obiettivo di dare evidenza del valore economico direttamente generato dal Gruppo Cyberoo e della sua distribuzione tra le principali categorie di stakeholder.

Il **Valore Economico generato** comprende i ricavi delle vendite e delle prestazioni, gli incrementi per lavori interni, gli altri ricavi e proventi e i proventi finanziari. Nel 2025 il Valore Economico generato è stato pari a 31,50 milioni di euro, in crescita rispetto ai 25,27 milioni di euro del 2024, riflettendo l'incremento dei ricavi nell'esercizio esteso a 15 mesi. Il **Valore Economico distribuito**, pari a 24,68 milioni di euro (78,4% del valore generato), rappresenta la ricchezza trasferita dal Gruppo ai propri stakeholder e si compone di: costi operativi per 13,29 milioni di euro (principalmente acquisti di materie, servizi e godimento di beni di terzi), remunerazione dei dipendenti per 9,37 milioni di euro, remunerazione della Pubblica Amministrazione per 1,25 milioni di euro (imposte correnti),

remunerazione dei finanziatori per 0,76 milioni di euro (interessi e oneri finanziari) e investimenti nella collettività per 10 mila euro.

Il **Valore Economico trattenuto**, pari a 6,81 milioni di euro, è dato dalla differenza tra il valore generato e quello distribuito e comprende gli ammortamenti, le svalutazioni e le rettifiche di valore (4,24 milioni di euro) e il risultato d'esercizio destinato a riserve (2,57 milioni di euro). Rispetto ai 7,63 milioni di euro trattenuti nel 2024, la riduzione riflette il minor utile dell'esercizio, parzialmente compensato dai maggiori ammortamenti legati agli investimenti in immobilizzazioni immateriali effettuati nel periodo.

VALORE AGGIUNTO	2023 ⁶	2024	2025
Ricavi	21.746.026	24.567.052	30.746.011
Altri proventi	271.209	444.141	480.100
Proventi finanziari	95.252	255.810	270.220
Totale valore economico generato	22.112.487	25.267.003	31.496.331
Costi operativi	7.107.418	8.690.517	13.292.970
Remunerazione del personale	5.596.319	6.570.914	9.373.701
Remunerazione dei finanziatori	489.446	484.680	757.587
Remunerazione degli investitori	-	-	-
Remunerazione della Pubblica Amministrazione	1.716.523	1.857.864	1.249.354
Liberalità esterne	35.250	35.000	10.000
Totale valore economico distribuito	14.944.956	17.638.975	24.683.612
Valore economico trattenuto	7.167.531	7.628.028	6.812.719

Gli investimenti

L'attività di ricerca e sviluppo, finalizzata allo studio e alla progettazione di nuovi prodotti, rappresenta un elemento fondamentale del modello industriale del Gruppo nonché la principale leva strategica.

⁶ Si segnala che è stato effettuato un restatement rispetto al valore dei ricavi e dei costi operativi 2023.

Il Gruppo Cyberoo tramite le società Cyberoo S.p.A. e Cyberoo51 S.r.l. realizza attività precompetitive a carattere innovativo, indirizzando i propri sforzi su progetti ritenuti particolarmente innovativi quali attività di studio, analisi, ricerca e sviluppo di soluzioni non esistenti sul mercato della cyber security.

I progetti si pongono l'obiettivo di fornire alle società un servizio basato su specifici algoritmi di intelligenza artificiale che permettano di avere una visione quanto più completa delle cyber minacce relative a una specifica azienda, degli attacchi potenziali in termini di confidenzialità, integrità e disponibilità dei dati e dei servizi.

Approccio fiscale

Il Gruppo Cyberoo considera la gestione responsabile della fiscalità un elemento integrante del proprio sistema di governance e un fattore essenziale per la creazione di valore sostenibile nel lungo periodo. L'approccio fiscale del Gruppo è improntato ai principi di legalità, correttezza, trasparenza e responsabilità e si fonda sul pieno rispetto delle normative tributarie vigenti nei Paesi in cui opera.

La capogruppo ha sede fiscale in Italia e assolve i propri obblighi tributari in conformità alla normativa nazionale. Nell'ambito delle attività svolte con le società controllate estere, il Gruppo garantisce il rispetto delle disposizioni fiscali applicabili nei diversi ordinamenti, assicurando che le operazioni infragruppo siano condotte secondo criteri di trasparenza, coerenza economica e conformità alla normativa vigente.

Il Gruppo adotta un approccio prudente nella gestione delle tematiche fiscali, evitando pratiche di pianificazione fiscale aggressiva o strutture finalizzate al conseguimento di vantaggi fiscali non coerenti con la sostanza economica delle operazioni. Eventuali aspetti caratterizzati da particolare complessità interpretativa sono affrontati attraverso un'analisi puntuale della normativa e, ove necessario, con il supporto di qualificati consulenti esterni, al fine di individuare le soluzioni maggiormente conformi al quadro legislativo e regolamentare.

La governance fiscale è presidiata dalla Direzione Amministrazione, Finanza e Controllo, che assicura il corretto adempimento degli obblighi tributari, monitora l'evoluzione della normativa e presidia i principali rischi fiscali connessi alle attività del Gruppo. Gli impatti fiscali sono considerati nell'ambito dei processi di

pianificazione strategica e operativa, contribuendo alle valutazioni economiche e alla gestione complessiva dei rischi aziendali.

Il Gruppo promuove un rapporto improntato alla collaborazione e alla trasparenza nei confronti delle Autorità fiscali, assicurando la completezza, l'accuratezza e la tempestività degli adempimenti e delle informazioni fornite. Le informazioni di natura fiscale sono rappresentate in modo chiaro e conforme alla normativa vigente nel bilancio d'esercizio e nella relativa Nota integrativa, a beneficio di tutti gli stakeholder.

Pur operando anche attraverso società controllate estere, il Gruppo mantiene la propria residenza fiscale in Italia e non adotta strutture societarie o operazioni finalizzate a trasferire artificialmente la base imponibile verso giurisdizioni caratterizzate da regimi fiscali privilegiati. L'approccio del Gruppo è orientato a garantire che le imposte siano corrisposte nei Paesi in cui viene effettivamente generato il valore economico, in coerenza con le normative applicabili e con i principi di trasparenza e responsabilità fiscale.

Nel corso dell'esercizio di riferimento, il Gruppo non è stato interessato da contenziosi tributari significativi né da contestazioni fiscali tali da produrre effetti rilevanti sulla situazione economico-finanziaria, patrimoniale o reputazionale del Gruppo. Tale risultato conferma l'attenzione costante riservata alla compliance fiscale e al presidio dei rischi tributari, nonché l'impegno del Gruppo a mantenere un rapporto improntato alla trasparenza e alla collaborazione con le Autorità competenti.



Capitolo 7
CAPITALE
UMANO

7. Capitale umano

Le politiche del personale

Il Gruppo Cyberoo considera le persone come una risorsa strategica per l'azienda: con il suo operato intende valorizzare il lavoro e le esperienze dei suoi dipendenti, garantendo condizioni di lavoro ottimali, il rispetto dei diritti umani e la trasparenza nel processo di selezione del personale. Per il Gruppo è fondamentale che ogni dipendente contribuisca alla creazione di valore dell'organizzazione in un ambiente che promuova il benessere, il merito e lo sviluppo delle competenze in linea con i principi dell'azienda. La gestione del personale è ispirata a principi di correttezza ed imparzialità, evitando favoritismi o discriminazioni, nel rispetto della professionalità e delle competenze del lavoratore. Al contempo, nel perseguimento degli obiettivi della Società, il lavoratore deve operare nella consapevolezza che l'etica rappresenta un interesse di primario rilievo per il Gruppo Cyberoo e che, pertanto, deve sempre conformarsi, nelle sue azioni, al rispetto del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 adottato, al Codice Etico e ai protocolli aziendali. È proprio l'Etica il primo valore che il Gruppo persegue, con l'obiettivo di instaurare e mantenere tra i dipendenti un clima di reciproco rispetto e tutelare la dignità, l'onore e la reputazione di ciascuno. La crescita delle persone è un altro dei valori aziendali cardine, dalla fase di recruiting e per tutta la durata della permanenza aziendale, grazie all'organizzazione di iniziative di formazione interaziendale mirate a rafforzare il legame tra Cyberoo e i dipendenti.

I processi di selezione

La politica di selezione adottata da Cyberoo nella selezione di persone altamente specializzate su tutto il territorio italiano ha come obiettivo quello di mantenere alti i livelli di competenza e trasversalità, favorendo l'integrazione tra figure tecniche, commerciali e di staff con il duplice scopo di creare occupazione e di valorizzare e sviluppare professionisti sempre più verticali nel settore della cybersecurity.

Anche per il 2025 rimane alta l'attenzione sia nei riguardi delle risorse nel territorio emiliano locale, circa il 70% del totale della forza lavoro, ma anche delle risorse provenienti da altre Regioni, circa il 30%, per tutti i ruoli e livelli presenti in azienda.

Al fine di agevolare l'integrazione di quest'ultimi e al fine di favorire la loro presenza in azienda, Cyberoo si mobilita sempre per organizzare riunioni periodiche presso la propria sede, sostenendo o rimborsando sia il costo di trasferta che di alloggio.

La selezione è svolta nel pieno rispetto delle pari opportunità e senza discriminazione alcuna, evitando favoritismi, clientelismo e agevolazioni, ispirando la propria scelta esclusivamente a criteri di professionalità e competenza. Il processo di selezione è, infatti, attento e strutturato e prevede una valutazione delle candidature sulla base di requisiti oggettivi, tramite colloqui tecnici e commerciali per valutarne le competenze e quanto altro necessario per fornire un giudizio obiettivo e colloqui attitudinali volti ad approfondire le motivazioni e i valori della persona. Tale flusso di selezione è condiviso con tutti i responsabili di Area in modo da garantirne l'ingaggio e una maggiore uniformità di valutazione.

Poiché le persone sono il fattore chiave per il raggiungimento degli obiettivi di Cyberoo, il processo di selezione riveste un ruolo fondamentale, in quanto destinato a individuare candidati in possesso delle skill, della professionalità, serietà e preparazione tecnica, corrispondenti ai profili effettivamente necessari alle esigenze della Società e che, al contempo, condividano i principi etici e i valori di onestà e lealtà cui Società si ispira.

Ogni persona coinvolta nel processo di selezione si attiene alle seguenti regole di comportamento:

- imparzialità nel trattamento dei candidati che partecipano all'iter di selezione;
- riservatezza sulle informazioni acquisite durante la selezione;
- indipendenza e astensione dal coinvolgimento in azioni che possano generare un conflitto di interessi e divieto di dar seguito a qualsiasi pressione indebita proveniente da soggetti interni o esterni.

Il candidato neoassunto viene accompagnato durante l'inserimento in azienda tramite un processo di *on-boarding* differenziato a seconda del profilo professionale. Il processo di selezione di figure junior prevede il coinvolgimento di enti di formazione, di Università e di scuole superiori locali attraverso la stipula di convenzioni al fine di ospitare giovani talenti in stage e coinvolgerli in progetti già in essere o "ad hoc". L'iniziativa dell'azienda di offrirsi come ente ospitante rappresenta un'occasione per i giovani studenti di mettere in pratica le

conoscenze apprese all'interno di un'organizzazione aziendale e di confrontarsi con un ambiente di lavoro complesso e dinamico; per Cyberoo è invece un'opportunità per sviluppare mini-progetti, per addestrare giovani manager – in qualità di tutor – nella gestione di risorse, per conoscere, formare e valutare potenziali collaboratori futuri.

I dipendenti

Il numero di dipendenti è in costante aumento: al 31 marzo 2026 l'organico in Italia ha raggiunto le 134 unità, in crescita di circa il 28% rispetto alle 105 del 2024, mentre a livello di Gruppo il personale in forza è pari a 177 unità cresciuto del 17% rispetto ai 151 dipendenti dell'anno precedente. Questo trend conferma la solidità e l'evoluzione dell'Azienda, che continua a rafforzare la propria struttura organizzativa sia in termini quantitativi sia qualitativi; l'incremento a livello di Gruppo riflette anche il progressivo consolidamento del personale delle società estere.

Numero dipendenti ⁷	2023 ⁸			2024			2025		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
	35	97	132	36	115	151	43	134	177

Le forme di impiego

Numero dipendenti per tipologia di contratto / per genere	2023			2024			2025		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
Contratto a tempo indeterminato	35	97	132	36	114	150	42	133	175
Contratto a tempo determinato	-	-	-	-	1	1	1	1	2
Totale	35	97	132	36	115	151	43	134	177

⁷ Con riferimento al GRI 2-7, i dati relativi alla classificazione del personale nelle categorie "Altro" e "Non rivelato" sono pari a zero e, pertanto, non state inserite le colonne relative a queste due categorie in tutte le tabelle del presente capitolo.

⁸ Al fine di garantire la comparabilità intertemporale delle informazioni, i dati quantitativi relativi alle risorse umane del 2023 differiscono da quelli pubblicati nel precedente Bilancio di Sostenibilità a seguito di un restatement. La variazione è riconducibile al mutamento del perimetro di rendicontazione, ora allineato per la prima volta al perimetro di consolidamento dell'intero Gruppo.

Numero dipendenti per tipologia di contratto / per genere	2023			2024			2025		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
Stagisti e tirocinanti	1	-	1	-	1	1	5	-	5
Lavoratori Autonomi	21	57	78	19	58	77	25	51	76
CO.CO.CO	4	12	16	4	12	16	4	12	16
Totale	26	69	95	23	71	94	34	63	97

Il personale dipendente di Cyberoo è assunto esclusivamente con regolare contratto di lavoro, in conformità alle leggi e alle normative vigenti al Contratto Collettivo Nazionale del terziario, distribuzione e servizi.

Nel 2025, quasi il 100% dei dipendenti è assunto tramite contratto a tempo indeterminato (ad eccezione di due soli dipendenti con contratto a tempo determinato), a dimostrazione della stabilità e valorizzazione del capitale umano all'interno di Cyberoo. Inoltre, nel triennio 2023–2025 si registra un aumento del numero e della percentuale di Senior Manager assunti dalla comunità locale, passati da 2 su 4 nel 2023 a 7 su 7 nel 2025, in linea con una crescente presenza di figure locali nelle sedi operative significative.

Senior manager assunti dalla comunità locale	2023	2024	2025
N. Senior manager presso le sedi operative significative assunti dalla comunità locale ⁹	2	7	7
N. totale di Senior manager	4	7	7
% di Senior manager presso le sedi operative significative assunti dalla comunità locale	50%	100%	100%

Il Contratto Collettivo Nazionale di Lavoro applicato dal Gruppo alle società italiane è il CCNL Terziario, Distribuzione e Servizi. Nella tabella seguente è riportata la percentuale di dipendenti coperti da contrattazione collettiva:

⁹ Per comunità locale si fa riferimento alle Unità Locali della Regione Emilia-Romagna (Reggio Emilia e Piacenza). Mentre per Senior manager si fa riferimento alla categoria al Livello Quadro.

Dipendenti coperti da CCNL	2023	2024	2025
N. totale di dipendenti coperti da CCNL	94	105	134
N. totale di dipendenti	132	151	177
Percentuale di dipendenti coperti da CCNL	71%	70%	76%

Si precisa che il personale delle sedi estere (Polonia, Albania, Ucraina) è inquadrato secondo le rispettive normative locali in materia di lavoro e non è coperto dal CCNL italiano.

Diversità

La componente maschile continua a essere preponderante in Azienda, riflettendo una tendenza comune nel settore IT: in Italia, infatti, la percentuale media di donne nel comparto della cybersecurity si attesta attorno al 15%. Cyberoo, con una presenza femminile del 24% nel 2025, mantiene una posizione più favorevole rispetto alla media del mercato, confermando l'attenzione al tema della diversità e dell'inclusione.

La totalità delle dipendenti donne ricopre ruoli impiegatizi, con un progressivo incremento del numero di profili femminili in ingresso: 43 donne su un totale di 177 dipendenti a livello di gruppo al 31 marzo 2026. La composizione dell'organico vede inoltre una netta predominanza della categoria degli impiegati, che rappresentano il 96% della forza lavoro aziendale, mentre i quadri si attestano al 4%.

Dipendenti per categoria/ genere	2023			2024			2025		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
Dirigenti	-	-	-	-	-	-	-	-	-
Quadri ¹⁰	-	4	4	-	7	7	-	7	7
Impiegati	35	93	128	36	108	144	43	127	170
Operai	-	-	-	-	-	-	-	-	-
Totale	35	97	132	36	115	151	43	134	177

¹⁰ La percentuale di Senior manager (quadri) presso le sedi operative dell'Azienda che sono stati assunti dalla comunità locale è pari al 100%.

Di seguito si riportano le percentuali di dipendenti divise per categoria e genere, rapportati al totale dei dipendenti nel triennio 2023-2025.

Dipendenti per categoria/ Genere %	2023			2024			2025		
	Donne	Uomini	Totale	Donne	Uomini	Totale	Donne	Uomini	Totale
Dirigenti	-	-	-	-	-	-	-	-	-
Quadri	-	3%	3%	-	5%	5%	-	4%	4%
Impiegati	27%	70%	97%	24%	71%	95%	24%	72%	96%
Operai	-	-	-	-	-	-	-	-	-
Totale	27%	73%	100%	24%	76%	100%	24%	76%	100%

Anche nel 2025 la distribuzione per fasce d'età¹¹ conferma la prevalenza di dipendenti nella fascia tra i 30 e i 50 anni, pari al 60% del totale aziendale, seguita dal 27% di under 30 e dal 13% di over 50. In particolare, i quadri si collocano quasi esclusivamente nelle fasce più esperte (dai 30 anni in su), mentre la categoria impiegatizia abbraccia tutte le fasce d'età.

Dipendenti per figura professionale e per fascia di età	2025			
	< 30 anni	30-50 anni	> 50 anni	Totale
Dirigenti	-	-	-	-
Quadri	-	2	5	7
Impiegati	48	104	18	170
Operai	-	-	-	-
Totale	48	106	23	177

Il Gruppo Cyberoo è molto sensibile al tema della *diversity* e ha cercato nel corso degli anni di creare opportunità di orientamento e formazione che coinvolgano il più possibile le donne come gli uomini, ad avvicinarsi al settore partecipando a giornate di formazione nelle scuole, eventi in Università, piuttosto che stage formativi. Inoltre, nel corso del triennio di riferimento non si sono verificati episodi di discriminazione all'interno di Cyberoo. Il rispetto delle pari opportunità e la

¹¹ A seguito dell'allargamento del perimetro di reportistica a tutte le società del Gruppo, avvenuto per la prima volta in questo esercizio, i dati disaggregati relativi alla distribuzione anagrafica del personale non sono risultati interamente disponibili. Cyberoo ha già avviato un processo di implementazione dei propri sistemi di data collection e si impegna a fornire tale spaccato informativo nei futuri Bilanci di Sostenibilità

prevenzione di ogni forma di discriminazione sono principi sanciti dal Codice Etico e presidiati attentamente in tutte le sedi del Gruppo.

Turnover

Nel triennio 2023–2025 la popolazione aziendale è cresciuta in modo costante, in linea con la fase di assestamento organizzativo avvenuta durante gli anni precedenti.

Nel corso di questi anni, il Gruppo ha privilegiato l'assunzione di personale già qualificato e con elevata esperienza nelle aree core del business, con una prevalenza di profili appartenenti alla fascia d'età tra i 30 e i 50 anni.

Le percentuali di turnover sono state calcolate, in linea con i requisiti del GRI Standard, sulla base del totale dei dipendenti alla fine del periodo di rendicontazione prestabilito, confrontando i tassi di turnover positivo (assunzioni) con quelli di turnover negativo (cessazioni).

Nel 2025 si è registrato un turnover positivo pari al 30%, a fronte di un turnover negativo del 21%, confermando una dinamica aziendale complessivamente ancora orientata alla crescita, seppur in un contesto meno espansivo rispetto agli anni precedenti. Cyberoo ha comunque continuato a investire nell'inserimento di nuove risorse, mantenendo la capacità di attrarre professionalità coerenti con le esigenze strategiche, soprattutto nelle fasce d'età intermedie e in profili specializzati.

Assunzioni ¹²	2025		
	Donne	Uomini	Totale
Fino a 29 anni	13	12	25
Da 30 a 50 anni	6	17	23
Oltre 50 anni	1	4	5
Totale	20	33	53

¹² A seguito dell'allargamento del perimetro di reportistica a tutte le società del Gruppo, avvenuto per la prima volta in questo esercizio, i dati disaggregati relativi alla distribuzione anagrafica di nuovi assunti e cessati non sono risultati interamente disponibili. Cyberoo ha già avviato un processo di implementazione dei propri sistemi di data collection e si impegna a fornire tale spaccato informativo nei futuri Bilanci di Sostenibilità

Cessazioni	2025		
	Donne	Uomini	Totale
Fino a 29 anni	5	9	14
Da 30 a 50 anni	8	12	20
Oltre 50 anni	-	4	4
Totale	13	25	38

Tasso di turnover	2025		
	Donne	Uomini	Totale
Turnover negativo - cessazioni	30%	19%	21%
Turnover positivo - assunzioni	47%	25%	30%

L'incremento dell'organico comprende 11 ingressi mediante trasferimento da Cyberoo Global S.p.A., rappresentati separatamente dalle assunzioni ordinarie nella riconciliazione del personale. Nel periodo di rendicontazione, n. 11 persone sono state trasferite dalla società del Gruppo Cyberoo Global S.p.A. a Cyberoo S.p.A. Considerata la natura di tali movimentazioni, riconducibili a trasferimenti di personale all'interno del Gruppo, le stesse non sono state considerate come nuove assunzioni né come cessazioni ai fini del calcolo degli indicatori di turnover di Cyberoo S.p.A., in quanto non rappresentative di un effettivo ingresso o uscita dal perimetro occupazionale del Gruppo.

I congedi parentali

Congedi parentali	2023			2024			2025		
	Donna	Uomo	Totale	Donna	Uomo	Totale	Donna	Uomo	Totale
Dipendenti che hanno avuto diritto al congedo parentale	4	4	8	7	2	9	3	3	6
Dipendenti che hanno usufruito del congedo parentale	4	4	8	7	2	9	3	3	6
Dipendenti che sono tornati al lavoro durante il periodo di rendicontazione dopo aver usufruito del congedo parentale	1	4	5	4	2	6	3	3	6

Dipendenti che sarebbero dovuti tornare al lavoro durante il periodo di rendicontazione dopo aver usufruito del congedo parentale	1	4	5	4	2	6	3	3	6
Dipendenti che sono tornati al lavoro dopo aver usufruito del congedo parentale e che sono ancora dipendenti dell'organizzazione nei 12 mesi successivi al rientro	1	3	4	4	2	6	2	3	5

Nel 2024 e 2025, quasi tutti i dipendenti che hanno usufruito del congedo parentale sono rientrati nei tempi previsti e risultano ancora in forza dopo 12 mesi, segnalando una buona continuità nel reinserimento post-congedo.

Formazione e competenze

Il Gruppo considera la formazione e lo sviluppo delle competenze una leva strategica per la crescita dell'organizzazione e delle persone che ne fanno parte. Nel triennio di riferimento sono stati strutturati percorsi formativi su più livelli e moduli, articolati sia in ambito trasversale — con focus su collaborazione, comunicazione efficace e sviluppo manageriale — sia in ambito tecnico-specialistico, con particolare attenzione alle normative di settore e alle competenze in materia di sicurezza sul lavoro e primo soccorso.

Nel 2024 le attività formative hanno registrato una significativa contrazione (272 ore totali, rispetto alle 1.228 del 2023), a seguito di un avvicinamento nella gestione dell'Ufficio Risorse Umane che ha temporaneamente rallentato la pianificazione e l'erogazione dei corsi. Nonostante questa fase di transizione, sono stati attivati interventi formativi mirati su tematiche strategiche e di stretta attualità per il settore, tra cui:

- corsi sulle nuove normative europee in ambito cybersecurity (Direttiva NIS2 e Regolamento DORA), destinati al personale con responsabilità in materia di compliance e sicurezza;
- un master in contrattualistica di impresa per il Legal Specialist;
- percorsi tecnici dedicati ai Product Manager;

- momenti formativi per l'Ufficio Risorse Umane, con focus su strumenti e metodi per una più efficace ricerca e selezione del personale.

Nel 2025 il Gruppo ha dato seguito all'impegno assunto, strutturando un piano formativo articolato che ha consentito di riportare le ore erogate a 1.671 (media di 9,4 ore per dipendente), con un significativo recupero rispetto alla contrazione del 2024. Il piano ha previsto, da un lato, il proseguimento dei corsi in materia di sicurezza sul lavoro e primo soccorso e, dall'altro, l'attivazione di percorsi mirati su competenze trasversali e tecnico-specialistiche, tra cui:

- Corsi di inglese, destinato ai professionisti che interagiscono frequentemente con clienti o fornitori internazionali;
- Corso di Public Speaking, rivolto alle figure che, per ruolo professionale, devono affrontare platee di varie dimensioni;
- Corso di Leadership per Capi Intermedi, progettato per i manager responsabili della gestione e del mentoring di altre risorse;
- Corso di Excel avanzato, pensato per i professionisti che necessitano di elaborare e presentare dati attraverso grafici e tabelle personalizzate;
- Corso sulle Skill di Vendita, dedicato ai professionisti dell'area commerciale;
- Corso per DPO (Data Protection Officer), destinato ai professionisti che presidiano la privacy interna ed esterna, inclusa quella dei clienti;
- Corso di Problem Solving, aperto a diverse categorie professionali per rafforzare la capacità di gestione e risoluzione di problematiche operative.

Il Gruppo ha inoltre avviato l'adozione di modalità di apprendimento flessibili, anche tramite soluzioni e-learning, per garantire maggiore accessibilità e continuità nei percorsi di sviluppo professionale.

Nelle tabelle seguenti sono riportate le ore di formazione erogate e le ore medie di formazione per dipendente, suddivise per genere e categoria professionale:

Ore di formazione	2023			2024			2025		
	Donna	Uomo	Totale	Donna	Uomo	Totale	Donna	Uomo	Totale
Dirigenti	-	-	-	-	-	-	-	-	-
Quadri	-	60	60,00	-	10	10,00	-	104	104,00
Impiegati	146	1022	1.168,00	-	262	262,00	350	1217	1.567,00
Operai	-	-	-	-	-	-	-	-	-
Totale	146,00	1.082,00	1.228,00	-	272,00	272,00	350,00	1.321,00	1.671,00

ORE MEDIE DI FORMAZIONE	2023	2024	2025
Numero totale di ore di formazione fornite ai dipendenti	1.228,00	272,00	1.671,00
Numero totale di dipendenti	132,00	151,00	177,00
Media ore di formazione per dipendente	9,303030303	1,801324503	9,440677966
Numero totale di ore di formazione fornite ai dipendenti donne	146,00	-	350,00
Numero totale di dipendenti donne	35,00	36,00	43,00
Media ore di formazione per dipendente donna	4,171428571	0	8,139534884
Numero totale di ore di formazione fornite ai dipendenti uomini	1.082,00	272,00	1.321,00
Numero totale di dipendenti uomini	97,00	115,00	134,00
Media ore di formazione per dipendente uomo	11,15463918	2,365217391	9,858208955
Numero totale di ore di formazione fornite ai Quadri	60,00	10,00	104,00
Numero totale di Quadri	4,00	7,00	7,00
Media ore di formazione per Quadro	15	1,428571429	14,85714286
Numero totale di ore di formazione fornite agli Impiegati	1.168,00	262,00	1.567,00
Numero totale di Impiegati	128,00	144,00	170,00
Media ore di formazione per Impiegato	9,125	1,819444444	9,217647059

Welfare aziendale

Cyberoo, nel porre al centro delle strategie di crescita e sviluppo aziendale le proprie risorse umane, ha rinnovato l'attenzione nei loro confronti attraverso iniziative legate al welfare aziendale: l'iscrizione al Fondo Est (Ente Assistenza

Sanitaria Integrativa del Commercio, del turismo e dei Servizi e settori Affini). Tale fondo ha l'obiettivo di supportare i bisogni e le necessità dei lavoratori, fornendo prestazioni di assistenza sanitaria integrative a quelle del Sistema Sanitario Nazionale (SSN). Hanno diritto alle prestazioni di assistenza sanitaria garantite da Fondo Est tutti i lavoratori dipendenti a tempo indeterminato e gli apprendisti ed è consentita l'iscrizione di lavoratori dipendenti con contratto a tempo determinato di durata superiore a tre mesi.

Tra le altre misure, è prevista l'adozione dello *smart working* semplificato che ha accelerato il processo di flessibilità del lavoro, attualmente regolamentato da accordi che variano in base alla funzione lavorativa del dipendente.

Al 31 marzo 2026 quasi la totalità dei dipendenti del Gruppo è coperta da assicurazione per invalidità e disabilità, ad eccezione dei lavoratori a tempo determinato, per i quali questa copertura non è prevista. È intenzione del Gruppo consolidare questo modus operandi e continuare a investire nel benessere dei dipendenti.

Salute e sicurezza sul lavoro

Nel rispetto della persona quale elemento indispensabile al raggiungimento degli obiettivi dell'Azienda, Cyberoo si impegna affinché la propria attività, i propri impianti e servizi siano compatibili con l'obiettivo della miglior prevenzione e protezione della sicurezza e della salute dei lavoratori, nell'ottica di minimizzare i rischi derivanti dall'attività lavorativa normale, da situazioni particolari o di emergenza.

La Società si impegna a diffondere e consolidare una cultura della sicurezza, sviluppando la consapevolezza dei rischi e il rispetto della normativa vigente in materia di prevenzione e protezione, e promuovendo comportamenti responsabili da parte di tutti; inoltre, opera per preservare e migliorare, soprattutto con azioni preventive, le condizioni di lavoro, la salute e la sicurezza dei dipendenti.

Cyberoo si impegna pertanto a:

- eliminare/ridurre al minimo i rischi in relazione alle conoscenze acquisite in base al progresso tecnico, privilegiando gli interventi alla fonte;
- adottare, per l'esercizio dell'attività produttiva, attrezzature, macchinari e impianti rispondenti ai requisiti essenziali di sicurezza;

- sostituire, per quanto riguarda i prodotti utilizzati, ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;
- limitare al minimo il numero dei lavoratori che sono, o che possono essere, esposti ai rischi;
- garantire idonea informazione, formazione, sensibilizzazione e addestramento in materia di sicurezza e di salute a tutti i lavoratori.

Al fine della prevenzione, la Società assicura il rispetto delle leggi e delle normative di settore: per questo motivo viene redatto il Documento di Valutazione dei Rischi (DVR), dove sono stati individuati gli specifici fattori di rischio potenziale relativi a tali ambiti di riferimento operativi e il Documento di Valutazione dei Rischi Interferenti (DUVRI), dove sono stati valutati i “rischi interferenti” in relazione agli appalti. Viene inoltre periodicamente redatto e aggiornato un documento che contiene il piano di lavoro e gli interventi di miglioramento (Piano di miglioramento). Nel corso dell'esercizio 2025 sono stati erogati i corsi obbligatori in materia di sicurezza sul lavoro, addetti antincendio e primo soccorso.

Come previsto dal D.Lgs 81/08, è istituito un servizio di sorveglianza sanitaria (medico competente) con lo scopo di controllare lo stato di salute dei dipendenti e di esprimere il giudizio di idoneità alla mansione specifica cui il dipendente è assegnato.

Inoltre, il Gruppo Cyberoo ha nominato come Responsabile del Servizio di Prevenzione e Protezione (RSPP) una persona esterna. Tale figura, coordinando il servizio di prevenzione e protezione, si reca in azienda con regolare frequenza e si occupa della gestione della sicurezza negli ambienti lavorativi e dei rapporti con i diversi enti e organismi di controllo e certificazione e si coordina con le rappresentanze dei lavoratori per la sicurezza e gli Amministratori.

Gli infortuni

Nel corso del 2024, 2025 e fino al 31/03/2026, non sono stati registrati infortuni.

Infortuni sul lavoro ¹³	2023	2024	2025
Mortali	-	-	-
Incidenti gravi	-	-	-
Altri Incidenti ¹⁴	-	-	-
Totale Incidenti registrati	-	-	-
Di cui: Incidenti in itinere	-	-	-
Giorni assenza per infortuni	-	-	-
Totale ore lavorate	157.638	176.826	267.225
Tasso di decessi risultanti da infortuni sul lavoro	-	-	-
Tasso di infortuni sul lavoro con gravi conseguenze (ad esclusione dei decessi)	-	-	-
Tasso di infortuni sul lavoro registrabili	-	-	-

¹³ Il tasso di infortuni sul lavoro registrabili è stato calcolato come di seguito: numero di infortuni sul lavoro su ore lavorate per 1.000.000.

¹⁴ Incidente inferiore a un mese.



Capitolo 8

CAPITALE AMBIENTALE

8. Capitale ambientale

Cyberoo, considerando la tutela dell'ambiente essenziale per uno sviluppo sostenibile, si propone di contemperare le esigenze di sviluppo economico e di creazione di valore con il rispetto e la salvaguardia ambientale.

Obiettivo primario della Società è quindi quello di sviluppare le attività di business nell'ottica di un miglioramento delle performance e nel rispetto dell'ambiente.

Responsabilità ambientale

Pur operando nel settore dei servizi che per sua natura non presenta generalmente aree di rischio specifiche rispetto alla sfera ambientale, il Gruppo Cyberoo non si limita ad agire passivamente ma promuove, nelle proprie attività quotidiane, comportamenti virtuosi in merito all'utilizzo razionale delle risorse e alla riduzione dei consumi. Coerentemente con la natura digitale del proprio business, gli impatti ambientali diretti del Gruppo sono contenuti e concentrati in due ambiti: i consumi di carburante della flotta aziendale e i consumi elettrici delle sedi. L'infrastruttura tecnologica più energivora — i server — è invece ospitata presso data center di terze parti certificati ISO 14001:2015 e ISO 50001:2018, standard di riferimento per la gestione ambientale ed energetica di tali strutture: il relativo impatto è pertanto presidiato da operatori specializzati.

Il management, consapevole del proprio ruolo e dei propri obblighi nei confronti dell'ambiente in cui opera, ha intrapreso un percorso di miglioramento delle proprie prestazioni nell'ottica di sviluppare soluzioni di valore e sostenibili nel rispetto delle normative e capaci di soddisfare le richieste e le aspettative dei propri stakeholder.

Gli obiettivi principali della **Politica ambientale** di Cyberoo vengono di seguito sintetizzati:

- rispettare leggi, norme e regolamenti vigenti relativi al settore e ad altre eventuali prescrizioni sottoscritte dalla Società;
- coinvolgere il personale, garantendo un elevato livello di professionalità, anche nelle tematiche di sostenibilità ambientale;
- scegliere partner e fornitori che dichiarano di agire nell'ottica di un miglioramento continuo delle loro prestazioni ambientali;

- efficacia, efficienza e affidabilità, impiegando tutte le risorse necessarie al fine di garantire il rispetto dei principi di diligenza e correttezza;
- operare riducendo la produzione di rifiuti, prevenendo l'inquinamento e provvedendo allo smaltimento di rifiuti in conformità alla normativa in vigore;
- rinnovare sistematicamente il proprio parco automezzi, consentendo di mantenere basso l'impatto ambientale dei veicoli impiegati;
- divulgare la cultura ambientale tra i propri dipendenti, clienti e fornitori;
- gestire in maniera sostenibile le risorse naturali e l'energia all'interno delle sedi aziendali, riducendo gli sprechi e presidiando il monitoraggio e il controllo degli aspetti ambientali.

Consumi energetici¹⁵

Il Gruppo Cyberoo crede fermamente nello sviluppo sostenibile e di conseguenza non possono essere ignorati i consumi energetici derivanti dalle soluzioni tecnologiche.

Questo si traduce nel saper scegliere con attenzione fornitori capaci di garantire non solo sostenibilità economica ma anche quella ambientale.

I consumi energetici (e le relative emissioni) di Cyberoo sono relativi a:

- Energia elettrica, prelevata dalla rete e utilizzata per l'infrastruttura tecnologica (server¹⁶);
- Gas per il riscaldamento della sede centrale;
- Diesel, benzina e GPL per l'alimentazione delle auto aziendali. Relativamente a quest'ultima voce, il Gruppo ha avviato un'attività di monitoraggio continuativo per raccogliere dati quantitativi a supporto delle proprie politiche di mobilità sostenibile. Inoltre, è stata installata una colonnina di ricarica elettrica in una delle sedi del Gruppo.

Nelle successive tabelle sono riportati i consumi energetici relativi al triennio 2023 - 2025.

¹⁵ I dati relativi all'esercizio 2025 si riferiscono a un periodo di 15 mesi (1° gennaio 2025 - 31 marzo 2026) e non sono pertanto pienamente comparabili con quelli degli esercizi precedenti, di durata pari a 12 mesi

¹⁶ I server sono localizzati in centri terzi. Si specifica che essi sono certificati ISO 14001:2015 e ISO 50001:2018

I dati relativi ai consumi energetici e idrici si riferiscono al perimetro italiano del Gruppo. Le sedi estere operano infatti in spazi di coworking i cui contratti includono le utenze nel canone di locazione; per tali sedi il Gruppo non dispone, pertanto, di una misurazione autonoma dei relativi consumi.

Nell'esercizio 2025, della durata eccezionale di 15 mesi, il Gruppo Cyberoo ha registrato un **consumo energetico complessivo pari a 3.363 GJ**, in aumento rispetto al 2024 (+23%).

La lettura del dato richiede due chiavi interpretative. La prima è la maggiore ampiezza del periodo di rendicontazione (15 mesi anziché 12): al netto di questo effetto, i consumi si mantengono sostanzialmente allineati al trend degli esercizi precedenti. La seconda è la composizione del mix energetico: la quota largamente prevalente (oltre il 90%) è rappresentata dai carburanti della flotta aziendale, il cui incremento riflette l'intensificarsi dell'attività commerciale e del percorso di espansione, anche internazionale, del Gruppo. L'energia elettrica acquistata, destinata alle sedi e all'infrastruttura d'ufficio, cresce invece in coerenza con l'ampliamento dell'organico e degli spazi di lavoro.

In questo quadro assume rilievo l'autoproduzione da fonte rinnovabile: nel 2025 circa 102 GJ del fabbisogno elettrico sono stati coperti da energia autoprodotta e autoconsumata, cui si aggiungono circa 21 GJ ceduti alla rete. Insieme all'installazione di una colonna di ricarica elettrica presso una delle sedi e alla politica di progressivo rinnovo del parco automezzi, tale iniziativa segna l'avvio concreto di un percorso di transizione energetica e di mobilità sostenibile, destinato a incidere in misura crescente negli esercizi futuri.

Energia consumata (GJoule) ¹⁷	2023	2024	2025
Energia elettrica			
Energia elettrica acquistata	229	167	228
<i>Di cui da fonti non rinnovabili</i>	229	167	228

¹⁷ I fattori di conversione impiegati per trasformare i consumi energetici in GJ sono stati derivati dal documento UK Government GHG Conversion Factors for Company Reporting (versione 2024), pubblicato dal Department for Energy Security and Net Zero del Regno Unito (in precedenza veniva invece sviluppato dal c.f. DEFRA). Tale documento, è riconosciuto per la regolarità degli aggiornamenti, l'elevata qualità dei dati e l'ampia copertura delle fonti di energia, motivo per cui è ampiamente adottato anche al di fuori del Regno Unito per ricavare i consumi di energia e le emissioni di ambito 1.

<i>Di cui da fonti rinnovabili</i>	-	-	-
Carburanti			
GPL	-	-	-
Diesel	2.377	2.397	2.900
Benzina	96	88	133
Totale	2.702	2.652	3.261

Energia elettrica Autoprodotta (GJoule)	2023	2024	2025
Totale energia elettrica autoprodotta			
<i>Di cui tot. Energia consumata</i>	-	84	102
<i>Di cui tot. Energia venduta</i>	-	18	21
Totale energia elettrica autoprodotta	-	102	123

Emissioni

Nell'esercizio 2025 le emissioni dirette di gas serra (Scope 1) sono state pari a 218 tCO₂e, mentre quelle indirette da consumi elettrici (Scope 2) si sono attestate a 19 tCO₂e secondo l'approccio location-based e a 31 tCO₂e secondo l'approccio market-based. In continuità con il profilo dei consumi, le emissioni sono determinate in via preponderante dalla flotta aziendale (Scope 1), mentre la crescita dello Scope 2 riflette i maggiori consumi elettrici delle sedi. Si segnala che l'energia elettrica autoprodotta da fonte rinnovabile non genera emissioni e che lo Scope 2 è calcolato sulla sola energia acquistata. Anche in questo caso l'andamento rispetto agli esercizi precedenti risente in modo rilevante della maggiore durata del periodo di rendicontazione.

Emissioni GHG Scope 1 (tCO₂e) – Scope 1¹⁸	2023	2024	2025
Emissioni dirette			
GPL	-	-	-
Gasolio	168	169	209
Benzina	6	6	9

¹⁸ I fattori di emissione impiegati per il calcolo delle tCO₂e Scope 1 sono tratti dal documento UK Government GHG Conversion Factors for Company Reporting (versione 2024), pubblicato dal Department for Energy Security and Net Zero del Regno Unito (in precedenza veniva invece sviluppato dal c.f. DEFRA). Tale documento, è riconosciuto per la regolarità degli aggiornamenti, l'elevata qualità dei dati e l'ampia copertura delle fonti di energia, motivo per cui è ampiamente adottato anche al di fuori del Regno Unito per ricavare i consumi di energia e le emissioni di ambito 1.

Emissioni complessive – Totale Scope 1	174	175	218
Emissioni GHG Scope 2 (tCO₂e) – Location Based¹⁹			
Emissioni indirette			
Energia elettrica acquistata	19	12	19
Emissioni Complessive – Totale Scope 2	19	12	19
Totale emissioni Scope 1 + Scope 2	193	187	237
Emissioni GHG Scope 2 (tCO₂e) – Market Based²⁰			
Emissioni indirette			
Energia elettrica acquistata	29	23	31
Emissioni Complessive – Totale Scope 2	29	23	31
Totale emissioni Scope 1 + Scope 2	203	198	249

Utilizzo responsabile delle risorse naturali

Acqua

Per le società del Gruppo Cyberoo l'acqua non rappresenta una risorsa critica, non essendo impiegata a fini industriali. La gestione dell'approvvigionamento idrico e dello smaltimento è affidata, per la quasi totalità, alla capogruppo, che adotta specifiche politiche di gestione dei reflui. Le società si impegnano a monitorare costantemente i propri consumi, così da individuare tempestivamente eventuali perdite e ridurre al minimo il proprio impatto.

I prelievi avvengono dalla rete dell'acquedotto pubblico e riguardano prevalentemente usi di tipo sanitario, in quantità modeste. Come per i consumi energetici, anche i dati idrici si riferiscono al perimetro italiano del Gruppo.

Acqua consumata (in MegaLitri)	2023	2024	2025
Risorse idriche di terze parti - fornitori idrici <i>Di cui: Acqua dolce (≤1.000 mg/l di solidi disciolti totali)</i>	0,279	0,164	0,264
Totale (in ML)	0,279	0,164	0,264

¹⁹ La fonte dei fattori di emissione utilizzati per il calcolo delle emissioni di GHG indirette Location Based per il 2023 è *Terna Confronti internazionali 2019*. La fonte dei fattori di emissione utilizzati per il calcolo 2024 e 2025 è *Ispra 2024*.

²⁰ La fonte dei fattori di emissione utilizzati per il calcolo delle emissioni di GHG indirette Market Based per il 2023 è l'*European Residual Mixes "AIB"* ultimo aggiornamento (31.05.2021). La fonte dei fattori di emissione utilizzati per il calcolo 2024 e 2025 è l'*European Residual Mixes "AIB"* (2023) ultimo aggiornamento al 2024.

Nell'esercizio 2025 (15 mesi) il consumo idrico è stato pari a circa 0,264 ML, in aumento rispetto ai 0,164 ML del 2024. L'incremento è riconducibile in prevalenza alla maggiore durata del periodo di rendicontazione e alla crescita dell'organico; i prelievi restano comunque limitati e destinati a usi prevalentemente sanitari. Il consumo idrico non costituisce un impatto ambientale rilevante per il Gruppo, data la natura terziaria dell'attività.

Rifiuti

Le società del Gruppo Cyberoo adottano tutte le misure necessarie per lo smaltimento dei dispositivi tecnologici, che rappresentano comunque una quota minima. Per i rifiuti assimilabili a quelli civili è attiva la raccolta differenziata. Lo smaltimento dei rifiuti è gestito, a livello di Gruppo, direttamente da Sedoc Digital Group; i relativi quantitativi sono pertanto rendicontati in forma semplificata nella tabella seguente.

Rifiuti prodotti (in t) ²¹	2023	2024	2025 ²²
Rifiuti non pericolosi	16,60	5,53	3,86
Rifiuti pericolosi	3,70	1,54	0,42
Totale rifiuti prodotti	20,30	7,07	4,28

Al 31 marzo 2026 i rifiuti prodotti dal Gruppo Cyberoo sono stati pari a 4,28 tonnellate, di cui circa il 90% non pericolosi (3,86 tonnellate). Il dato è particolarmente positivo se si considera che, pur a fronte di un periodo di rendicontazione più lungo (15 mesi), i volumi risultano in ulteriore diminuzione rispetto alle 7,07 tonnellate del 2024. Il trend pluriennale in costante calo (da 20,30 t nel 2023 a 4,28 t nel 2025) conferma l'efficacia del progressivo affinamento nella gestione e nello smaltimento dei rifiuti.

²¹ I dati relativi ai rifiuti prodotti sono stati rettificati in quanto è stata utilizzata una differente metodologia di calcolo. I dati relativi al triennio fanno riferimento alla capogruppo Sedoc.

²² Nel 2025 il Gruppo non ha effettuato smaltimenti di rifiuti. Le uniche operazioni sui rifiuti nel gruppo sono state effettuate dalla capogruppo Sedoc, che ha gestito esclusivamente rifiuti destinati al recupero (codice R13).



Capitolo 9

GRI CONTENT INDEX

9. GRI Content Index

Ove non diversamente indicato, sono stati utilizzati i GRI Standards pubblicati nel 2021.

Statement of use		Gruppo Cyberoo ha redatto la presente informativa non finanziaria con riferimento agli Standard GRI per il periodo 1° gennaio 2025 - 31 marzo 2026 secondo l’opzione “with reference”.			
GRI 1		GRI 1: Foundation 2021			
GRI Sector Standard(s) applicabile		N/A			
GRI SUSTAINABILITY REPORTING STANDARD		RIFERIMENTO CAPITOLO / PARAGRAFO		PAG.	NOTE APPLICAZIONE STANDARD / OMISSIONI
GENERAL DISCLOSURES					
GRI 2: General Disclosures 2021	2-1	Dettagli organizzativi	1. Identità e strategia/Il Gruppo	9	
	2-2	Entità incluse nella rendicontazione di sostenibilità dell'organizzazione	Nota Metodologica	6	
	2-3	Periodo di rendicontazione, frequenza e punto di contatto	Nota Metodologica	6	
	2-4	Revisione delle informazioni	Nota Metodologica	6	
	2-5	Assurance esterna	Nota Metodologica	6	Il presente Bilancio di Sostenibilità non è stato oggetto di revisione da parte di un ente terzo
	2-6	Attività, catena del valore e altri rapporti di business	1. Identità e strategia/Il modello di business	39	

	2-7	Dipendenti	6. Capitale umano/I Dipendenti	115	
	2-8	Lavoratori non dipendenti	6. Capitale umano/I Dipendenti	116	
	2-9	Struttura e composizione della governance	2. Governance/La Governance	55	
	2-10	Nomina e selezione del massimo organo di governo	2. Governance/La Governance	55	
	2-11	Presidente del massimo organo di governo	2. Governance/La Governance	55	
	2-14	Ruolo del massimo organo di governo nella rendicontazione di sostenibilità	Nota Metodologica	6	
	2-16	Comunicazione delle criticità	2. Governance/La Governance	55	Non sono state comunicate preoccupazioni critiche al più alto organo di governo in quanto non sono state riscontrate nel periodo di rendicontazione
	2-22	Dichiarazione sulla strategia di sviluppo sostenibile	Lettera agli Stakeholder	4	
	2-25	Processi volti a rimediare agli impatti negativi	1. Identità e strategia/Analisi di materialità	32	
	2-27	Conformità e leggi e regolamenti	2. Governance/Compliance normativa in ambito ESG	59	Nel corso del triennio rendicontato non si sono verificati eventi che hanno dato origine a sanzioni e/o contenziosi per non conformità a leggi, normative in materia ambientale, sociale ed economica.

	2-28	Appartenenza ad associazioni	4. Capitale relazionale/Il valore delle partnership	71	
	2-29	Approccio al coinvolgimento degli stakeholder	1. Identità e strategia/Analisi di materialità	32	
	2-30	Contratti collettivi	6. Capitale umano/I Dipendenti	117	
TEMI MATERIALI					
GRI 3: Temi materiali 2021	3-1	Processo di determinazione dei temi materiali	1. Identità e strategia/Analisi di materialità	32	
	3-2	Elenco di temi materiali	1. Identità e strategia/Analisi di materialità	32	
GOVERNANCE, ETICA E COMPLIANCE					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	2. Governance	54	
GRI 205: Anticorruzione	205-3	Episodi di corruzione accertati e azioni intraprese	2. Governance/Compliance normativa	59	Nel corso del triennio 2023-2025 non si sono verificati episodi di corruzione
GRI 206: Comportamento anticoncorrenziale	206-1	Azioni legali per comportamento anticoncorrenziale	2. Governance/Compliance normativa	59	Nel corso del triennio 2023-2025 non sono state rilevate azioni legali
GRI 207: Imposte	207-1	Approccio alla fiscalità	5. Capitale economico-finanziario/Approccio fiscale	111	
GENERAZIONE E DISTRIBUZIONE DI VALORE ECONOMICO E FINANZIARIO					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	5. Capitale economico-finanziario	109	

GRI 201: Performance economiche 2016	201-1	Valore economico direttamente generato e distribuito	5. Capitale economico-finanziario/Il valore economico generato e distribuito	110	
RICERCA & SVILUPPO E INNOVAZIONE					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	3. Capitale infrastrutturale/Innovazione e digitalizzazione	61	
PRIVACY E SICUREZZA DEI DATI E DELLE INFORMAZIONI					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	4. Capitale relazionale/Privacy dei clienti e perdita di dati dei clienti	85	
GRI 418: Privacy dei clienti	418-1	Denunce comprovate riguardanti le violazioni della privacy dei clienti e perdita di dati	4. Capitale relazionale/Privacy dei clienti e perdita di dati dei clienti	84	Nel corso del triennio 2023-2025 non si sono verificate denunce comprovate né fughe, furti o perdite di dati dei clienti
SODDISFAZIONE E GESTIONE DELLE RELAZIONI CON I CLIENTI					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	4. Capitale relazionale	77	
GRI 417: Marketing ed etichettatura	417-3	Casi di non conformità riguardanti comunicazioni di marketing	4. Capitale relazionale/Attività di marketing	85	Nel corso del triennio 2023-2025 non si sono verificati casi di non conformità
CONDIZIONI DI LAVORO, CLIMA INTERNO E WELFARE AZIENDALE					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	6. Capitale umano	114	
GRI 401: Occupazione	401-1	Assunzioni e turnover	6. Capitale umano/Turnover	118	

GRI 401: Occupazione	401-2	Benefit previsti per i dipendenti	6. Capitale umano/Welfare aziendale	123	
GRI 401: Occupazione	401-3	Congedo parentale	6. Capitale umano/I congedi parentali	120	
FORMAZIONE E SVILUPPO DELLE COMPETENZE					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	6. Capitale umano	114	
GRI 404: Formazione e istruzione	404-1	Ore medie di formazione annua per dipendente	6. Capitale umano/Formazione e competenze	121	
SALUTE E SICUREZZA SUL LAVORO					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	6. Capitale umano/Salute e sicurezza sul lavoro	124	
GRI 403: Salute e sicurezza sul lavoro	403-2	Identificazione dei pericoli, valutazione dei rischi	6. Capitale umano/Salute e sicurezza sul lavoro	124	
GRI 403: Salute e sicurezza sul lavoro	403-3	Servizi di medici del lavoro	6. Capitale umano/Salute e sicurezza sul lavoro	124	
GRI 403: Salute e sicurezza sul lavoro	403-9	Infortuni sul lavoro	6. Capitale umano/Salute e sicurezza sul lavoro	125	Nel corso del triennio 2023-2025 non si sono registrati infortuni sul lavoro né malattie professionali
GRI 403: Salute e sicurezza sul lavoro	403-10	Malattie professionali	6. Capitale umano/Salute e sicurezza sul lavoro	125	Nessuna malattia professionale nel triennio
SUPPORTO/IMPATTO SULLA COMUNITÀ E SUL TERRITORIO LOCALE					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	4. Capitale relazionale/Le relazioni con il territorio	98	

GRI 413: Comunità Locali	413-1	Attività che prevedono il coinvolgimento delle comunità locali	4. Capitale relazionale/Le relazioni con il territorio	98	
EFFICIENZA ENERGETICA					
GRI 3: Temi materiali 2021	3-3	Gestione dei temi materiali	7. Capitale ambientale	127	
GRI 302: Energia	302-1	Energia consumata all'interno dell'organizzazione	7. Capitale ambientale/Consumi energetici	128	
GRI 305: Emissioni	305-1	Emissioni dirette di GHG (Scope 1)	7. Capitale ambientale/Emissioni	129	
GRI 305: Emissioni	305-2	Emissioni indirette di GHG (Scope 2)	7. Capitale ambientale/Emissioni	129	
ALTRI INDICATORI RENDICONTATI					
PRESENZA SUL MERCATO					
GRI 202: Presenza sul mercato 2016	202-2	Proporzione di senior manager assunti dalla comunità locale	6. Capitale umano/I Dipendenti	116	
PRATICHE DI APPROVVIGIONAMENTO					
GRI 204: Pratiche di approvvigionamento 2016	204-1	Proporzione di spesa verso fornitori locali	4. Capitale relazionale/La gestione della supply chain	92	
ACQUA E SCARICHI IDRICI					
GRI 303: Acqua e scarichi idrici 2018	303-3	Prelievo idrico	7. Capitale ambientale/Utilizzo responsabile delle risorse naturali	130	

RIFIUTI					
GRI 306: Rifiuti	306-3	Rifiuti prodotti	7. Capitale ambientale/Utilizzo responsabile delle risorse naturali	131	
DIVERSITÀ					
GRI 405: Diversità e pari opportunità	405-1	Diversità negli organi di governo e tra i dipendenti	2. Governance/La Governance + 6. Capitale umano/Diversità	55 117	
DISCRIMINAZIONE					
GRI 406: Non discriminazione	406-1	Episodi di discriminazione e misure correttive	6. Capitale umano/Diversità	118	Nel corso del triennio 2023-2025 non si sono verificati episodi di discriminazione

HQ / REGGIO EMILIA
VIA BRIGATA REGGIO, 37
42124 REGGIO EMILIA - ITALIA
TEL. 0522.388111

SPACES ISOLA / MILANO
VIA POLA, 11
20124 MILANO - ITALIA

BUREAU / PIACENZA
VIA DAL VERME, 33
29121 PIACENZA - ITALIA

BUREAU / VARSAVIA
RONDÓ DASZYŃSKIEGO 2B
00-843 VARSAVIA - POLONIA

