# Bilancio di Sostenibilità

2023

CYBEROO

# Superheroes are always ready for action.

Siamo una società italiana specializzata nella difesa della cyber security. Vigiliamo sulla sicurezza dei tuoi dati, per lasciarti la libertà di focalizzarti sul tuo business.

CYBEROO

# Indice

LETTERA AGLI STAKEHOLDER ..... 5
NOTA METODOLOGICA ..... 7
1. IDENTITÀ E STRATEGIA ..... 10
2. GOVERNANCE ..... 53
3. CAPITALE INFRASTRUTTURALE ..... 65
4. CAPITALE RELAZIONALE ..... 80
5. CAPITALE ECONOMICO FINANZIARIO ..... 101
6. CAPITALE UMANO ..... 106
7. CAPITALE AMBIENTALE ..... 119
GRI INDEX ..... 125

# “CREDIAMO CHE UNO SVILUPPO REALMENTE SOSTENIBILE SIA BASATO SUL BENESSERE DELLE PERSONE E SULL’ATTENZIONE ALL’AMBIENTE, METTENDO IN CONDIVISIONE RISORSE, COMPETENZE E SPERIMENTANDO SOLUZIONI INNOVATIVE.”

**Fabio Leonardi**
CEO

# Lettera agli stakeholder

L'esercizio appena concluso è stato ancora caratterizzato dalle conseguenze sulle economie mondiali degli effetti della guerra in Ucraina e dall'elevata inflazione. Tuttavia, il Gruppo Cyberoo, che opera principalmente nel mercato della Cybersecurity, ha saputo reagire nel corso del 2023 arrivando a chiudere l'esercizio con un utile di gruppo di euro 3.963.448.

Siamo molto soddisfatti delle performance ottenute, ma questo aumenta ancora di più la responsabilità che abbiamo verso le persone che lavorano nella nostra organizzazione e verso le comunità e il territorio in cui operiamo.

Siamo consapevoli che la nostra crescita debba essere anche sostenibile e non possa prescindere dall'adottare soluzioni che siano in grado di portare benessere alla società in cui viviamo.

Tutto questo è possibile grazie all'innovazione, da sempre il cuore pulsante attorno al quale ruotano idee, progetti, servizi, design e processi di sviluppo. È in virtù di questa consapevolezza che nonostante un trend macroeconomico critico ed incerto, abbiamo rafforzato i nostri investimenti in ricerca e sviluppo, sviluppando nuovi progetti di cybersecurity che ci hanno consentito di proporre ai nostri clienti soluzioni tecnologiche sicure ed affidabili. Tutto questo conferma la nostra attenzione al cliente e ribadisce la qualità e la sicurezza che contraddistinguono da sempre i nostri prodotti.

La redazione del Bilancio di sostenibilità di Cyberoo è parte di questo percorso e costituisce non solo un'importante opportunità per la rappresentazione dei risultati economici, sociali ed ambientali, ma anche per evidenziare le linee strategiche di medio-lungo periodo e la loro coerenza con uno sviluppo sostenibile.

Il modello di business sostenibile e la creazione e condivisione di valore per gli Stakeholder è da sempre parte del nostro DNA e ci guida nella gestione quotidiana dell'impresa. Crediamo che uno sviluppo realmente sostenibile sia basato sul benessere delle persone e sull'attenzione all'ambiente, mettendo in condivisione risorse, competenze e sperimentando soluzioni innovative.

Un modello di business sostenibile richiede, infatti, lo sviluppo coerente del tessuto sociale e degli ecosistemi che ci ospitano. Crediamo in una cultura

d'impresa che connette e condivide idee e soluzioni attraverso un complesso intreccio di attori e partner che collaborano per la creazione di valore condiviso nel lungo periodo. Abbiamo creato molti prodotti innovativi in questi anni ma le sfide e il miglioramento continuo sono l'essenza del nostro sviluppo. Tutto questo rappresenta il nostro punto di partenza per iniziare un percorso nella sostenibilità per la crescita dell'azienda, del territorio e del mondo che ci circonda.

**Fabio Leonardi**
CEO

# Nota Metodologica

Il presente documento rappresenta il secondo 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.

Il Bilancio di sostenibilità è stato redatto rendicontando una selezione dei "GRI Sustainability Reporting Standards" pubblicati dal Global Reporting Initiative (GRI 2021), come indicato nel GRI Content Index del presente documento, secondo l'opzione di rendicontazione "With reference".

Si sottolinea che il Gruppo Cyberoo non ricade nel campo di applicazione del D.Lgs. n. 254 del 30 dicembre 2016 il quale, in attuazione delle Direttiva 2014/95/UE, ha previsto l'obbligo di redazione di una Dichiarazione Non Finanziaria ("DNF") per gli enti di interesse pubblico che superano determinate soglie quantitative. Il presente Bilancio di sostenibilità è pertanto redatto su base volontaria e non rappresenta una DNF.

I principi generali applicati per la redazione della Bilancio di sostenibilità sono quelli stabiliti dai GRI Standard: rilevanza, inclusività, contesto di sostenibilità, completezza, equilibrio tra aspetti positivi e negativi, comparabilità, accuratezza, tempestività, affidabilità, chiarezza.

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 di Cyberoo S.p.A., Cyberoo51 S.r.l., MFD International S.r.l., Cyberoo Docetz S.r.l. e di Cyberoo PL Sp z.o.o (società di diritto polacco) al 31 dicembre 2023.

Il Bilancio di sostenibilità è redatto con cadenza annuale. 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.

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 11/07/2024 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 dei servizi e dei prodotti ICT (Information & Communication Technology), ed è specializzato nel fornire alla propria clientela una vasta gamma di servizi e soluzioni tecnologiche a supporto del business delle imprese con focus sulla cyber security.

L'attività si rivolge al mercato delle medie imprese con un portfolio di soluzioni enterprise ampio e variegato, sviluppate con l'utilizzo delle più avanzate tecnologie e con una catena del valore unica, sia tra i player nazionali che internazionali.

Il Gruppo, supporta le imprese nella sicurezza, nonché nel miglioramento e nella digitalizzazione dei propri processi organizzativi e di business, al fine di offrire soluzioni e servizi personalizzati ad alto contenuto tecnologico, combinando l'apprendimento artificiale con l'intelligenza umana dei migliori professionisti sul mercato per garantire sicurezza, continuità e resilienza agli investimenti delle imprese clienti.

Il Gruppo realizza una strategia volta alla protezione e al monitoraggio, oltre che alla gestione, del valore delle informazioni di ogni ecosistema IT, con lo scopo di semplificare la complessità aziendale.

I servizi offerti del Gruppo sono declinati in tre linee di business principali: cyber security services, managed services e digital transformation.

## Le dimensioni

Il Gruppo Cyberoo ha realizzato ricavi per euro 20 milioni e conta, nelle proprie sedi, di un numero complessivo di 94 dipendenti (al 31 dicembre 2023).

| Ricavi per Industry (milioni di euro) | 2021 | | 2022 | | 2023 | |
|---|---|---|---|---|---|---|
| | Ricavi | % | Ricavi | % | Ricavi | % |
| Cyberoo S.p.A. | 7,40 | 74,3% | 13,98 | 81,8% | 18,17 | 80% |
| Cyberoo51 S.r.l. | 1,60 | 16,0% | 2,11 | 12,3% | 2,64 | 11,6% |
| MFD International S.r.l. | 0,77 | 7,7% | 0,76 | 4,4% | 0,90 | 4,0% |
| Cyberoo Docetz S.r.l. | 0,19 | 1,9% | 0,24 | 1,4% | 0,99 | 4,4% |
| Cyberoo P1 Sp z.o.o | - | - | - | - | - | - |
| **Totale*** | **9,96** | **100%** | **17,10** | **100%** | **22,70** | **100%** |

*Importo al lordo delle fatture Intercompany

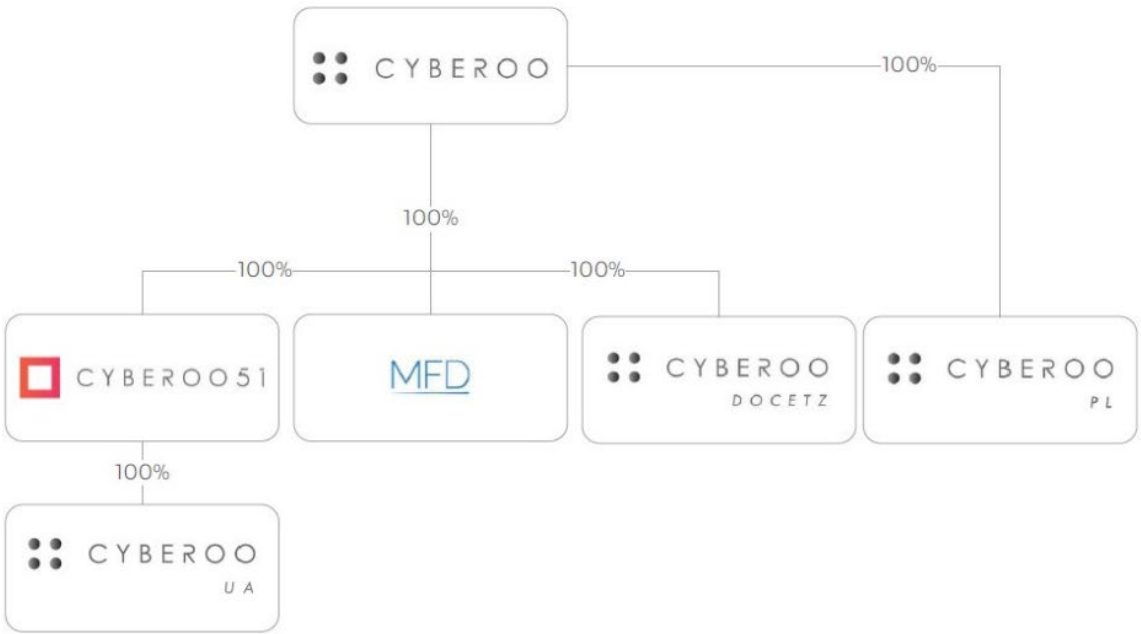
| Ricavi per tipologia di servizio (milioni di euro) | 2021 | | 2022 | | 2023 | |
|---|---|---|---|---|---|---|
| | **Ricavi** | **%** | **Ricavi** | **%** | **Ricavi** | **%** |
| Cyber Security & Device Security | 4,31 | 48,9% | 11,01 | 70,8% | 15,48 | 77,4% |
| Managed Services | 4,32 | 49,1% | 4,36 | 28,0% | 4,37 | 21,8% |
| Digital Transformation | 0,18 | 2,0% | 0,17 | 1,15% | 0,16 | 0,8% |
| **Totale** | **8,81** | **100%** | **15,5** | **100%** | **20,01** | **100%** |

| Ricavi per area geografica (milioni di euro) | 2021 | | 2022 | | 2023 | |
|---|---|---|---|---|---|---|
| | **Ricavi** | **%** | **Ricavi** | **%** | **Ricavi** | **%** |
| Italia | 8,81 | 100% | 15,5 | 100% | 20,01 | 100% |

## Il Gruppo

Il Gruppo, con headquarter a Reggio Emilia e sedi operative in Italia e all'estero, opera nel settore dell'Information Technology è costituito da 6 entità legali.

La struttura del Gruppo al 31 dicembre 2023 è di seguito rappresentata:



Cyberoo S.p.A. detiene una partecipazione pari al 100% del capitale sociale di Cyberoo51 S.r.l. (CYBEROO51), di MFD International S.r.l. (MFD), di Cyberoo Docetz S.r.l. (EX CYBER DIVISION) e di Cyberoo PL Sp z.o.o (società di diritto polacco).

Occorre precisare che Cyberoo51 S.r.l. detiene l'intero capitale della società Cyberoo UA LLC (società di diritto ucraino).

## Cyberoo51 S.r.l.

CYBEROO51, costituita nel 2014, svolge attività di consulenza nel settore delle tecnologie informatiche offrendo soluzioni software personalizzate e di cloud computing, nonché pianificando la corretta strategia di marketing e l'assistenza nelle scelte di comunicazione delle aziende.

In particolare, CYBEROO51 offre i seguenti servizi: servizi consulenziali e software personalizzati, servizi di digital marketing, software as a Service.

CYBEROO51 detiene una partecipazione pari al 100% del capitale sociale di Cyberoo UA, società con sede in Ucraina, a Ternopil, che svolge, per le società appartenenti al Gruppo, servizi in settori quali: *cyber security management, networking management, service desk; backup management, antivirus, antispam, cloud Service, IT consulting.*

## MFD International S.r.l.

MFD, costituita nel 2017, svolge servizi di telemarketing e gestione di call center inbound e outbound principalmente rivolti a società facenti parte del Gruppo.

## Cyberoo Docetz S.r.l.

Cyberoo Docetz S.r.l. (ex Cyber Division), acquisita per il 100% nel gennaio del 2023 è attiva nel campo della cyber security e, nello specifico, nei segmenti Offensive Security e Incidente Response.

## 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 2° livello dell'I-SOC Cyberoo insieme alle molteplici figure dei cybersecurity specialists.

## Storia, evoluzione e crescita

La storia Cyberoo ha inizio nel **2008** con la nascita di **AT Store**, società specializzata nella vendita di device. Nell'agosto dello stesso anno **Sedoc Digital Group**, storica azienda informatica emiliana nata nel 1973, acquisisce il 51% delle quote di AT, ultimandone l'acquisizione nell'aprile 2010. Nel dicembre 2011, AT Store acquisisce un ramo aziendale da Sedoc Digital Group e inizia l'attività di *Printing Management*, nuovo servizio per la gestione e monitoraggio delle stampanti in partnership con HP.

Nel 2015 AT Store diventa un ***Managed Service Provider (MSP)***, ossia un'azienda che fornisce servizi informatici di gestione e monitoraggio, anche a distanza.

Nel 2016 viene aperto il primo Hub in Ucraina per ampliare il focus sui *Managed Security Services*.

Il 2017 è l'anno di svolta. La stampante multifunzione diventa uno strumento per attaccare i dispositivi collegati alla rete locale ed eseguirvi codice malevolo. Dopo l'attacco hacker «Faxploit», la società cambia modello di business e diventa un ***Managed Security Service Solution (MSSP)*** e successivamente di Cyber Security ampliando l'offerta alla gestione, monitoraggio e protezione di tutta l'infrastruttura IT dei clienti, specializzandosi così nella fornitura di servizi di sicurezza informatica.

Nel 2018 è nato CYBEROO Lab: un network di HUB tecnologici proprietari con l'ambizione di creare soluzioni intelligenti e competitive nel mercato internazionale, a supporto della sicurezza e continuità operativa.

Nel 2019 l'azienda cambia nome in **Cyberoo**, lancia sul mercato 3 soluzioni innovative: Cypeer e Cyber Security Intelligence (CSI), che compongono la Cyber Security Suite, e la Titaan Suite, che a sua volta è costituita da tre moduli (Titaan Atlaas, Titaan Croono e Titaan Hyperioon). Il 7 ottobre 2019 Cyberoo viene quotata su Euronext Growth Milan (ex AIM Italia), il mercato di Borsa Italiana riservato alle PMI, risultando la **prima società di cyber security quotata a Piazza Affari**.

A dicembre 2019 Cyberoo ha siglato un accordo con l'Università di Ternopil "Ivan Puluj National Technical University" in Ucraina, volto alla ricerca e sviluppo e alla selezione dei migliori talenti in ambito di cyber security. Cyberoo ha concordato con l'Università un percorso formativo innovativo, con un forte investimento sulle risorse umane coinvolte. Conformemente ai programmi e agli argomenti condivisi con l'Università, Cyberoo si è resa disponibile allo svolgimento di tirocini e concorsi per borse di studio, con l'obiettivo di selezionare le migliori risorse e garantirsi la progressiva crescita delle competenze specializzate in ambito di cyber security.

Ad aprile 2021 Cyberoo ha avviato anche una collaborazione che la vede partecipare, come membro del Comitato di Indirizzo, al corso di Laurea in "Innovazione e Imprenditorialità Digitale" presso la Facoltà di Economia e Giurisprudenza dell'Università Cattolica del Sacro Cuore, campus di Cremona. Cyberoo punta così a definire insieme all'Università Cattolica nuove linee di ricerca volte al trasferimento tecnologico nell'ambito della sicurezza informatica, attraverso un processo di sensibilizzazione dei giovani e contribuendo alla formazione di risorse altamente specializzate in ambito IT.

In data 27 luglio, Cyberoo finalizza l'acquisizione del 51% di Cyber Division S.r.l., azienda novarese a elevata focalizzazione nelle attività di Vulnerability Assessment, Penetration Test ed Ethical Hacking, oltre a quelle di Incident Response.

Il 25 ottobre Cyberoo viene nominata "Representative Vendor" nella "2021 Gartner Market Guide For MDR Services", la più importante e autorevole ricerca internazionale sui servizi gestiti di sicurezza informatica. Prima e unica azienda italiana a ottenere l'ambito riconoscimento.

Nell'estate 2022 Cyberoo ha annunciato al mercato e ai propri partner il nuovo MDR (Managed Detection & Response) che integra funzioni di Automatic Remediation potenziate e all'avanguardia, avviando così un nuovo corso per la cyber sicurezza aziendale. Un importante investimento per un valore di circa 1,5 milioni di euro.

Cypeer Pure e Cypeer Sonic sono le due configurazioni del nuovo MDR che funziona con ampio ricorso all'intelligenza artificiale e al machine learning, e che segna un ulteriore importante cambio di passo per le attività di Response e Automatic Remediation.

A luglio 2022 Cyberoo riprende il percorso di internazionalizzazione e porta le proprie soluzioni sul mercato tedesco. Lo sbarco in Germania è stato reso possibile grazie al partner distributore ICOS.

A settembre 2022 Cyberoo si riconferma tra i principali player internazionali nel segmento dei servizi di Managed Detection and Response (MDR). Gartner, infatti, ha citato Cyberoo tra le circa 50 principali aziende mondiali specializzate in questo specifico segmento.

Per Gartner quello degli MDR è uno dei settori più dinamici del mercato della cybersecurity. Cresciuti del 48,9% dal 2020 al 2021, i servizi di Managed Detection and Response dovrebbero raggiungere la loro massima diffusione entro i prossimi cinque anni.

Il 17 gennaio 2023 Cyberoo ha avviato Cyberoo Docetz S.r.l. con l'obiettivo di accelerare la crescita strutturale dell'organizzazione e rispondere in modo efficace alle attività in ambito di cyber security e consulenza aziendale.

A febbraio dello stesso anno, il Gruppo viene riconosciuto per la seconda volta come "Representative Vendor" nella prestigiosa "Market Guide For MDR Services 2023" di Gartner.

Il 22 maggio 2023 Cyberoo ha approvato il suo primo Bilancio di Sostenibilità. Il documento, riferito all'esercizio 2022, è stato redatto su base volontaria rendicontando una selezione degli standard internazionali "GRI Sustainability Reporting Standards - 2021", secondo l'opzione di rendicontazione "Referenced". Con questa pubblicazione Cyberoo fa un ulteriore importante passo nel percorso intrapreso di Corporate Social Responsibility.

Il 23 maggio 2023, viene inaugurata in Polonia la nuova sede. Si tratta di un importante I-SOC (Intelligence - Security Operation Center), nel quale vengono rafforzate le attività I-SOC di secondo livello, con un ampio gruppo di cyber specialist attivi a supporto della struttura operativa di Gruppo H24. Il nuovo modello scalabile garantisce un ulteriore miglioramento del servizio offerto ai clienti e consente a Cyberoo di supportare al meglio la costante crescita della clientela che si affida sempre più ai servizi MDR (Managed Detection and Response) offerti Cyberoo.

**2008**

**Start up:**
Inizia l'attività come distributore di devices con la denominazione di AT Srl.

**2011**

**Print Management:**
Nuovo servizio per la gestione e monitoraggio delle stampanti in partnership con HP.

**2015**

**MSP**
(Managed Server Provider)

**2017**

**Attacchi faxploit**
La stampante multifunzione diventa uno strumento per attaccare i dispositivi collegati alla rete locale ed eseguirvi codice malevolo.

**2017**

**MSP e Cyber Security**
Dopo l'attacco hacker "Faxploit", inizia l'attività di Managed Server Provider e successivamente di Cyber Security ampliando l'offerta alla gestione, monitoraggio, e protezione di tutta l'infrastruttur IT dei clienti

**2019**

**Nuove soluzioni e IPO**
Rilascio sul mercato di nuove soluzioni di Cyber Security e MSP e IPO sul mercato AIM Italia.

**Riassetto societario:**
Acquisizione delle partecipazioni totalitarie in Life Your Brand S.r.l. (il 20 dicembre 2018 da SEDOC) e MFD International S.r.l. (il 22 febbraio 2019 da Fabio Leonardi, Massimo Bonifati e Davide Cignatta), quest'ultima titolare, a sua volta, dell'intero capitale sociale di DFM Virtual Service LLC (con sede in Ucraina).

**Quotazione in borsa**
Il 7 ottobre 2019 Cyberoo viene quotata su Euronext Growth Milan (ex AIM Italia), il mercato di Borsa Italiana riservato alle PMI, risultando la prima società di cyber security quotata a Piazza Affari.

**2021**

**Acquisizione di Cyber Division S.r.l.**
In data 27 luglio, Cyberoo finalizza l'acquisizione del 51% di Cyber Division S.r.l., azienda novarese a elevata focalizzazione nelle attività di Vulnerability Assessment, Penetration Test ed Ethical Hacking oltre a quelle di Incident Response.

**Nomina "Representative Vendor" da Gartner**
Cyberoo viene nominata "Representative Vendor" nella "2021 Gartner Market Guide For MDR Services", la più importante e autorevole ricerca internazionale sui servizi gestiti di sicurezza informatica. Prima e unica azienda italiana a ottenere l'ambito riconoscimento.

**2022**

NEW

**Nuove soluzioni e internazionalizzazione**
Nell'estate 2022 Cyberoo ha annunciato al mercato e ai propri partner il nuovo MDR (Managed Detection & Response) che integra funzioni di Automatic Remediation potenziate e all'avanguardia, avviando così un nuovo corso per la cyber sicurezza aziendale. Un importante investimento per un valore di circa 1,5 milioni di euro.

**Cypeer Pure e Cypeer Sonic**
Sono le due configurazioni del nuovo MDR che funziona con ampio ricorso all'intelligenza artificiale e al machine learning.

**Tra le 50 principali aziende mondiali specializzate in MDR**
A settembre Cyberoo si riconferma tra i principali player internazionali nel segmento dei servizi di Managed Detection and Response (MDR). Gartner, infatti, ha citato Cyberoo tra le circa 50 principali aziende mondiali specializzate in questo specifico segmento.

**2023**

**Nuova sede in Polonia**
Nel maggio 2023, Cyberoo inaugura la sua nuova sede nella capitale polacca, dove svolge attività i-SOC di secondo livello, 24/7, e nella quale prenderanno il via, verso la fine dell'anno, le attività commerciali per l'internazionalizzazione aziendale.

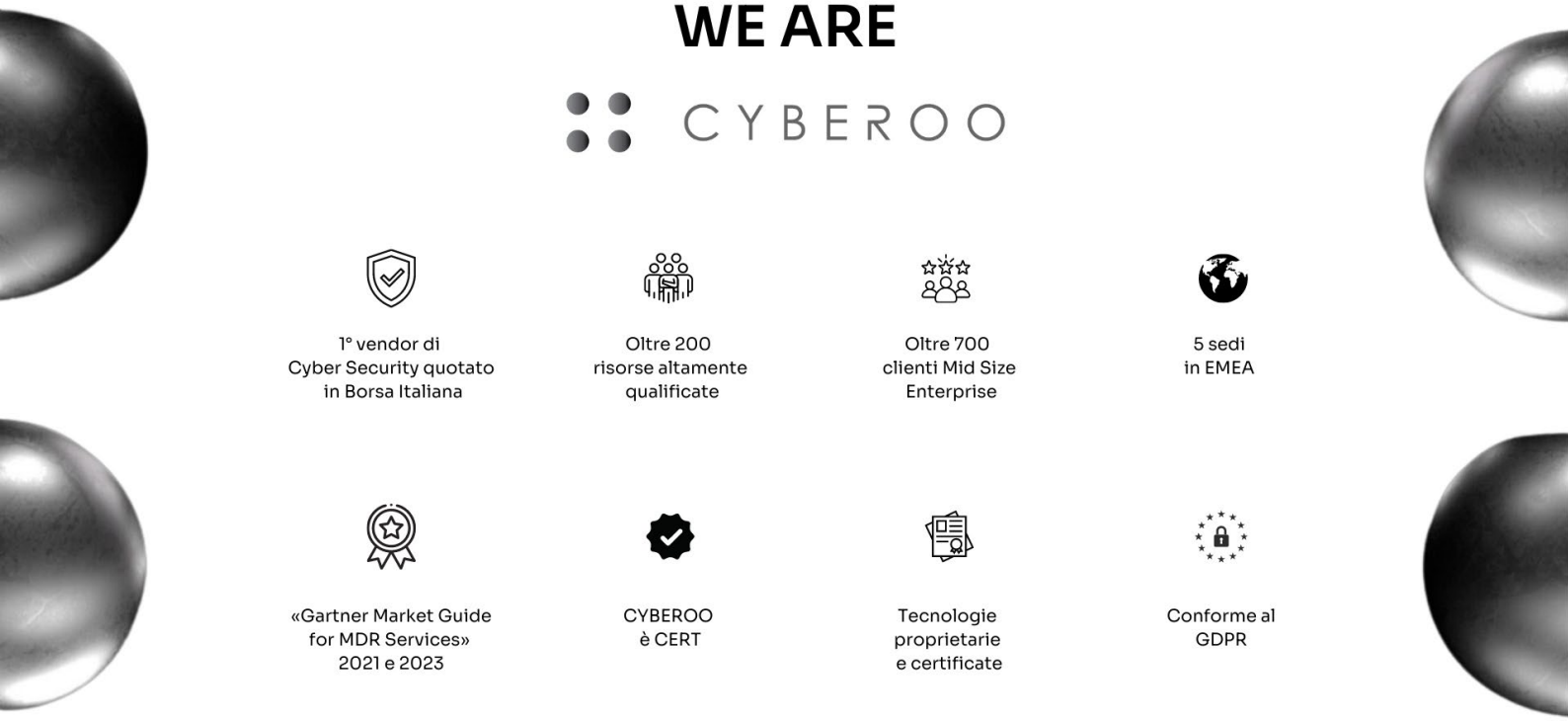
**Nomina "Example MDR Provider" da Gartner**
Cyberoo è nominato in due importanti report sulle tecnologie emergenti di cybersecurity presentati da Gartner.

**Digital Improvements**
Successivamente alle attività di R&D impegnate in campo digitale, Cyberoo introduce il nuovo sito web, il Black Button e l'App CYBShield. Le nuove feature digitali sono volte a velocizzare e facilitare la comunicazione tra le aziende e Cyberoo.

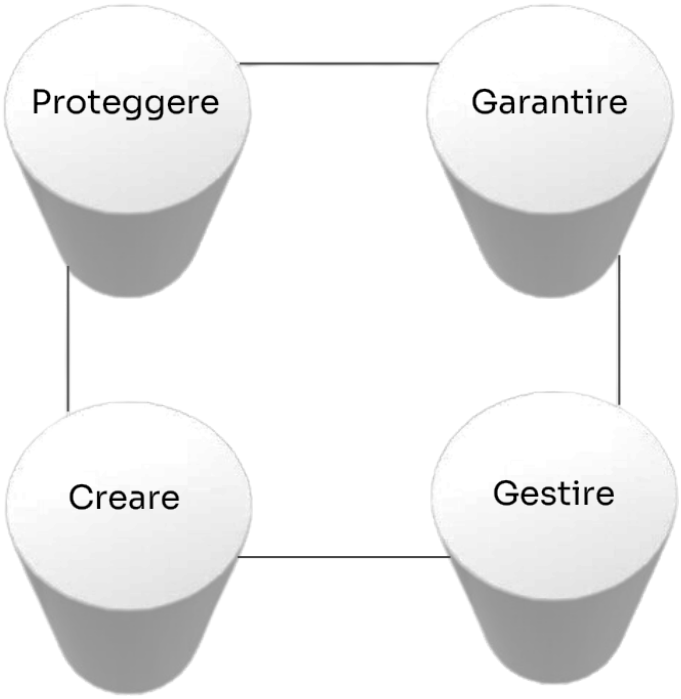
**Cyberoo è CERT**
Cyberoo entra a far parte del circuito CERT (Computer Emergency Response Team) del Trusted Introducer, principale riferimento del settore a livello internazionale.

# Mission e Valori

## Mission




Cyberoo si propone di essere "***il faro made in Italy che illumina le zone oscure e poco chiare del cyber spazio***", una vera e propria guida che accompagni le aziende, le persone e gli enti nel percorso di conoscenza, formazione e difesa oramai imprescindibili per vivere al meglio e in sicurezza le proprie vite nell'ambito del digitale. Un faro che sia però anche polo di ricerca e sviluppo per le più avanzate tecnologie di Detection.




***Proteggere, garantire, creare, gestire***: sono le quattro "torri di vedetta" di Cyberoo (rappresentate nel logo), indispensabili alla salvaguardia cyber del Business delle aziende clienti.

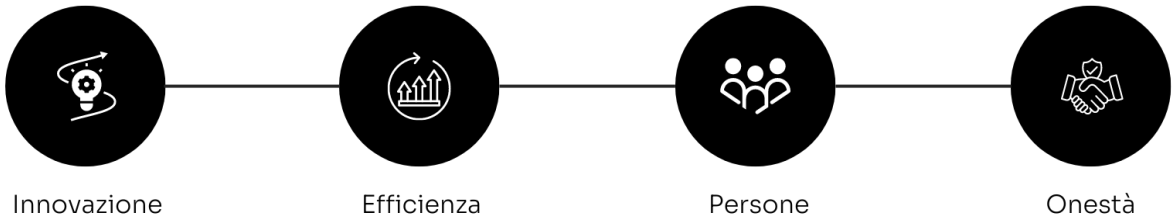
Cyberoo si pone attorno all'attività delle aziende e si colloca come guardiano a tutela delle informazioni e dei dati. Le soluzioni proposte da Cyberoo assolvono a questo scopo mettendo insieme tutte le misure per proteggere i dati da eventi imprevisti, per tutelarne la disponibilità e l'integrità e la riservatezza informatica, garantendo anche un veloce recupero e ripristino in caso di necessità.

Creando nuove soluzioni e algoritmi di intelligenza artificiale, il Gruppo è in grado di monitorare, gestire e proteggere le informazioni dell'ecosistema IT dalle minacce informatiche e dal *cyber crime*, garantendo la sicurezza e le performance dei sistemi.

## 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 dei prodotti attraverso soluzioni innovative che incrementino il valore e le performance delle aziende clienti, affrontare rapidamente le sfide di un mercato in frenetica 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 o aziendale 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 principalmente nel mercato del MDR (Managed Detection and Response), riguardante l'offerta ad una clientela business, principalmente in riferimento alla media e grande azienda.

I servizi MDR forniscono ai clienti le moderne funzionalità di Security Operations Center (SOC) erogate da remoto per rilevare, analizzare, indagare e rispondere attivamente alle minacce informatiche. La definizione classica di MDR prevede che i provider di tali servizi installino all'interno dell'ecosistema del cliente le proprie tecnologie proprietarie che coprono endpoint, reti, servizi cloud, tecnologia operativa (OT)/ Internet of Things (IoT) e altre fonti, per raccogliere log, dati e altre informazioni di contesto utili per analizzare la postura di sicurezza del cliente. I dati raccolti da varie fonti vengono analizzati tramite la piattaforma del provider grazie a sistemi di Intelligenza Artificiale e Machine Learning. Infine, i servizi di individuazione della remediation H24 vengono eseguiti da cybersecurity specialists che completano le capacità di monitoraggio e rilevamento in tempo reale.

L'MDR è quindi un provider di servizi gestiti che prevede l'esternalizzazione delle funzioni di gestione della sicurezza informatica di un'azienda cliente. È un metodo strategico destinato a migliorare le operazioni di un'organizzazione e anche a ridurre i costi su attività che non rappresentano il core business dell'azienda che acquisisce il servizio. L'obiettivo, infatti, tramite il servizio è quello di accedere a risorse estremamente preparate sui temi come la cybersecurity e il monitoraggio dell'ecosistema IT sotto diversi punti di vista. L'adozione di servizi gestiti è anche considerata un modo efficace per rimanere aggiornati sulla tecnologia. Gli MDR sono considerati un'alternativa al modello di esternalizzazione su base fissa o on-demand su cui si basa il classico modello di fornitura ICT. Anche da un punto di vista del pricing, l'MDR normalmente propone canoni ricorrenti, che quindi assicura al cliente un costo certo e non legato a monte ore di lavoro connesso a progetti.

In particolare, secondo Gartner aumenterà vertiginosamente nei prossimi anni la domanda di soluzioni di rilevamento e risposta basate su cloud, come il

rilevamento e la risposta degli endpoint (EDR) e il rilevamento e la risposta gestiti (MDR). Il Global Risk Report del World Economic Forum identifica al quarto posto nella classifica dei rischi più rilevanti per i prossimi due anni quelli legati alla cybersecurity.

In particolare, nel suo report annuale dedicato "Global Cybersecurity Outlook 2024", riporta un netto miglioramento nella consapevolezza dei Consigli di Amministrazione rispetto alle problematiche attuali nel campo della cybersecurity. Tuttavia, il divario tra la consapevolezza e l'attuazione di strategie effettive alla risoluzione di tali problemi è ancora significativamente ampio.

Infatti, lo stesso report illustra come nel 2023 il 29% delle organizzazioni sono state danneggiate da incidenti di sicurezza, e come il 41% di queste abbia subito l'attacco a causa di terze parti presenti all'interno della supply chain. Inoltre, il 54% dell'organizzazioni riporta, ancora, un insufficiente comprensione delle vulnerabilità informatiche relative alla sua filiera.

- Mercato Europeo

Secondo una recente ricerca di BeDisruptive dal titolo "Cybersecurity nel 2024: analisi e tendenze", il mercato della sicurezza informatica in Europa nel 2023 ha superato i 32,43 miliardi di dollari ed è previsto che raggiunga gli oltre 57,75 miliardi di dollari entro il 2028, con un tasso di crescita annuo del 12,23%.
L'Europa detiene la seconda quota di mercato più grande nel settore della sicurezza informatica grazie alle iniziative intraprese dalla Commissione europea per rendere l'Unione europea un attore forte nella lotta contro gli attacchi informatici. La digitalizzazione delle aziende e la trasformazione digitale supportata dai fondi dell'UE hanno aiutato l'industria della sicurezza informatica a guadagnare slancio.
La sicurezza informatica è una priorità, ed è necessario per l'Europa avere la sovranità tecnologica. L'aumento del telelavoro e il conseguente impatto sulle attività di criminalità informatica, durante la crisi Covid-19, ha mostrato quanto siamo tutti dipendenti dalla cybersecurity e quanto ne abbiamo bisogno per un mondo digitale.
La Commissione europea ha intrapreso varie iniziative nel campo della sicurezza informatica al fine di rendere l'Unione europea un attore forte nella lotta agli attacchi informatici, per aumentare le capacità e la cooperazione in materia di sicurezza informatica. Si stima che il costo annuo del crimine informatico per

l'economia globale abbia raggiunto i 5,5 trilioni di euro alla fine del 2020 e raggiungerà i 10,5 trilioni di euro entro il 2025.

L'aggiornamento del panorama normativo europeo in materia di cybersecurity, oggetto di significativi sviluppi nel corso del 2023 dimostra come la sicurezza informatica abbiamo ormai guadagnato un posto di rilievo. I più recenti passaggi di questo iter hanno visto, nel 2022, l'entrata in vigore della Direttiva n. 2555 sulle misure di cybersecurity nell'Unione (NIS2) e del Digital Operational Resilience Act (DORA) nonché, all'inizio del 2023, del Cyber Resilience Act (CRA).

La Direttiva NIS2, pubblicata nella Gazzetta Ufficiale dell'Unione Europea il 27 dicembre 2022 ed entrata in vigore il 16 gennaio 2023, mantiene l'obiettivo di raggiungere un livello comune elevato di cybersicurezza tra gli Stati Membri, migliorando la capacità di garantire uniformità ed efficacia nell'applicazione, e quindi di garantire un'effettiva protezione per la vita sociale ed economica dell'Unione. La normativa impone, in particolare, obblighi di cybersicurezza stringenti in capo a un'ampia platea di organizzazioni operanti in settori ritenuti critici per il funzionamento della società europea.

L'atto sulla resilienza operativa digitale (DORA) garantisce una maggiore resilienza del settore finanziario dell'UE in caso di interruzioni operative gravi e attacchi informatici. Questa normativa armonizza i requisiti di resilienza operativa digitale per tutte le società che forniscono servizi finanziari, compresi fornitori di servizi di criptovalute, banche e fornitori di moneta elettronica.

Tra le nuove proposte e adozioni legislative, emerge il "Cyber Resilience Act" (CRA) che ha attirato l'attenzione negli ultimi mesi, poiché le istituzioni europee hanno concluso i negoziati nel dicembre 2023, aprendo la strada a una possibile approvazione entro il 2024.

Il Regolamento propone una serie di norme volte a incrementare la sicurezza e la resistenza alle minacce informatiche di tutti i prodotti con componenti digitali, dagli smartphones ai giocattoli. Il testo introdurrà requisiti obbligatori di sicurezza informatica per progettare, sviluppare, produrre e distribuire prodotti hardware e software, in modo da garantire la standardizzazione delle norme tra i vari paesi membri. Il regolamento introduce la responsabilità dei produttori nel garantire adeguati supporti e strumenti per individuare e affrontare gli aspetti di vulnerabilità di volta in volta individuati.

- Mercato italiano

A testimonianza dell'interesse, nel 2023 il mercato italiano della cybersecurity ha raggiunto un record: 2,15 miliardi di euro, +16% rispetto al 2022. Il rapporto tra spesa in cybersecurity e PIL in Italia si attesta allo 0,12%, in crescita rispetto al 2022 (era pari allo 0,10%).

In questo contesto, continua a crescere l'interesse delle aziende italiane, sia grandi che PMI, per la cybersecurity, che si conferma principale priorità di investimento nel digitale in Italia. Nonostante l'aumento, questo risultato colloca ancora il nostro Paese all'ultimo posto nel G7, a grande distanza dai primi in classifica, Stati Uniti (0,34%), Regno Unito (0,29%), e da Paesi come Francia o Germania allo 0,19%. Il 62% delle grandi organizzazioni ha aumentato la spesa, ma l'Italia resta ultima tra i Paesi del G7 per rapporto mercato/PIL.

L'81% delle grandi imprese ha definito un piano di sviluppo strutturato in materia, con una strategia di lungo periodo. Tuttavia, il percorso di sviluppo e miglioramento è ancora lungo. Infatti, il 74% delle imprese ha percepito un aumento di tentativi di attacco, il 12% ha subito conseguenze tangibili derivanti da attacchi cyber.

Fin dall'inizio del conflitto ucraino del 2022, il Clusit ha sottolineato come l'Italia sia nel mirino del cybercrime, osservazione comprovata dai dati del 2023 che rappresentano lo stivale come un bersaglio particolarmente facile, dal momento che ha ricevuto ben l'11% degli attacchi rilevati a livello globale (contro un 3,4% del 2021 e un 7,6% del 2022).

Nell'ultimo anno sono stati registrati 2.779 incidenti, il numero maggiore di sempre, ed è interessante notare come già dal 2019 la realtà abbia iniziato a superare le previsioni indicate dai trend, e come tale aumento si dimostri stabile negli ultimi anni.

A conferma di una costante recrudescenza dello scenario degli incidenti, gli eventi degli ultimi cinque anni (2019-2023) sono più della metà (56.3%) degli incidenti classificati in totale dal 2011. A livello di distribuzione mensile, la prima metà dell'anno vede registrare una attività molto più intensa, con un picco massimo ad aprile 2023 con 270 attacchi, anche in questo caso raggiungendo un record negativo mai raggiunto.

Conseguentemente, anche la media mensile dei cyber attacchi è aumentata considerevolmente e arrivata a 232, con una tendenza di crescita costante, considerando che nel 2019 si attestava a poco più della metà.
Sebbene la maggioranza degli attacchi rimanga riconducibile al cybercrime, guardando alle tecniche di attacco, in Italia gravano più che a livello internazionale gli incidenti di social engineering (14% contro l'8,6% globale). Tra le altre tendenze che caratterizzano il panorama delle minacce, si denota l'aumento degli attacchi di tipologia supply chain, che si propagano a cascata tra fornitori e clienti, con possibili impatti significativi sul business delle organizzazioni a livello italiano e internazionale.

## La regolamentazione di settore

Nel mercato in cui opera, Cyberoo è sottoposta ad alcune disposizioni legislative e regolamentari che possono avere un'incidenza significativa sulla sua attività, di seguito sintetizzate.

### 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 ad 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'ambito dell'intelligenza artificiale per il business di Gruppo Cyberoo, si segnala che in data 21 aprile 2021, la Commissione Europea ha presentato una proposta di Regolamento che definisce in modo organico e strutturato il quadro giuridico in relazione all'Intelligenza Artificiale, riconoscendo innumerevoli vantaggi competitivi che l'Intelligenza Artificiale può fornire da un punto di vista economico, sociale ed ambientale. Allo stesso tempo, ha individuato alcune applicazioni che potrebbero generare rischi e avere effetti negativi sul mercato.

È dunque necessario, secondo la Commissione Europea, definire un quadro normativo che stabilisca regole chiare e condivise volte a disciplinare l'applicabilità dell'AI (Artificial Intelligence), in modo tale da creare le condizioni di fiducia per quel che riguarda l'immissione sul mercato e l'utilizzo degli strumenti di IA nell'Unione Europea.

Per queste ragioni, si sono stabilite regole di trasparenza armonizzate per i sistemi di IA che interagiscono con persone fisiche e per quelli utilizzati per generare o manipolare immagini, audio, video o contenuto.

Il nuovo quadro giuridico destinato all'intelligenza artificiale sarà basato su misure che individuano un rischio chiaramente definito, regole che facilitano l'istituzione di codici di condotta volontari e un sistema di governance a sostegno dell'attuazione del regolamento a livello europeo e nazionale.

## 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.

### 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 6 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.

## 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.

**INNOVATION & ENVIRONMENT**

| Linee di azione | Obiettivi | SDGs |
|---|---|---|
| Innovation & Digital Transformation | • Promuovere la digitalizzazione dei processi e della cybersecurity<br>• Sviluppare l'innovazione dei prodotti |  |
| Quality Solutions | • Sviluppare progetti per il controllo e l'ottimizzazione della qualità dei servizi<br>• Sviluppare iniziative per migliorare l'attenzione verso i clienti e la misurazione della loro soddisfazione<br>• Incrementare la sicurezza di prodotto e dei clienti |  |
| Environment | • Migliorare l'impatto ambientale dei trasporti e della logistica<br>• Roadmap verso la carbon neutrality<br>• Sviluppare una strategia di mobility management |  |

**PEOPLE**

| Linee di azione | Obiettivi | SDGs |
|---|---|---|
| Diversity & Inclusion | • Gestire le diversità e le pari opportunità<br>• Assicurare il gender balance nei percorsi di carriera e assunzioni<br>• Valorizzare la meritocrazia e assicurare la parità nei percorsi retributivi e di carriera |  |

| | | |
|---|---|---|
| Education & Culture | • Sviluppare collaborazioni e partnership con il mondo scuola, università, onlus ed enti locali<br>• Sviluppare la cultura delle risorse interne attraverso iniziative di organizzazione e formazione<br>• Sviluppare la formazione su etica e trasparenza |  |
| Wellness & Happiness | • Migliorare le condizioni di lavoro e il clima aziendale<br>• Potenziare la salute e sicurezza sul lavoro<br>• Migliorare la comunicazione interna verso i dipendenti<br>• Sviluppare il sistema di welfare aziendale |  |

## Il modello di business

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 ad 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 ad 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 realizza per le imprese clienti una strategia globale in grado 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.
- **Capacità di offrire soluzioni tecnologiche innovative**: il Gruppo, grazie ad 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.

- **Canoni ricorrenti e pricing competitivo**: il Gruppo opera principalmente con contratti a canone ricorrente annuo. Inoltre, con riferimento alle soluzioni proprietarie, offre servizi ad un pricing competitivo.
- **Appartenenza a Sedoc Digital Group S.r.l.**: Sedoc Digital Group S.r.l. offre grandi opportunità per una forte espansione nel mercato di riferimento, operando come vendor dei prodotti del Gruppo Cyberoo.

## Le linee di prodotti e servizi

I servizi offerti da Gruppo Cyberoo sono declinati in tre linee di business principali: ***cyber security services, managed services e digital transformation*.**

## Cyber security services

Cyberoo affianca ai tradizionali prodotti di security un sistema di gestione degli stessi, volto ad analizzare e controllare gli strumenti e i dati da essi prodotti. In particolare, i servizi ricompresi nell'ambito della cyber security sono:

### *Antispam*

Il servizio Antispam prevede la messa a disposizione dei clienti di un'infrastruttura remota, operativa presso un primario fornitore nazionale, ridondata, ovvero articolata tramite un cluster Active-Active in modalità Software-as-a-Service (SaaS) operativo presso due Centri Dati che si trovano sul territorio Italiano, uno di Livello (Tier) IV e l'altro di Livello (Tier) III, in grado di analizzare i messaggi di posta elettronica, al fine di individuare sia i messaggi indesiderati (SPAM), sia eventuali minacce informatiche (virus, malware...). Grazie all'ambiente cloud, i clienti hanno la possibilità di migliorare l'affidabilità della loro soluzione di posta elettronica: in caso di necessità, possono utilizzare la soluzione offerta da Cyberoo per leggere, inviare e inoltrare le email. Inoltre, sulla base delle proprie esigenze, i clienti possono scegliere di attivare il servizio in modalità 24 ore su 24, 7 giorni su 7.

### *Antivirus*

Il servizio antivirus, acquistato da terzi e declinato in tre differenti versioni (base, pro e FSS) prevede la presa in carico, da parte del personale tecnico e specialistico della sicurezza degli endpoint aziendali. All'interno del servizio viene fornito al cliente tutto il software necessario per la messa in sicurezza degli endpoint aziendali.

Il servizio antivirus si caratterizza per la semplicità di installazione, per una gestione completa e per il profilo della proattività, in quanto, in caso di segnalazione di una postazione infetta, il personale specialistico procede proattivamente con l'intervento di rimozione della minaccia.

### *Web security*

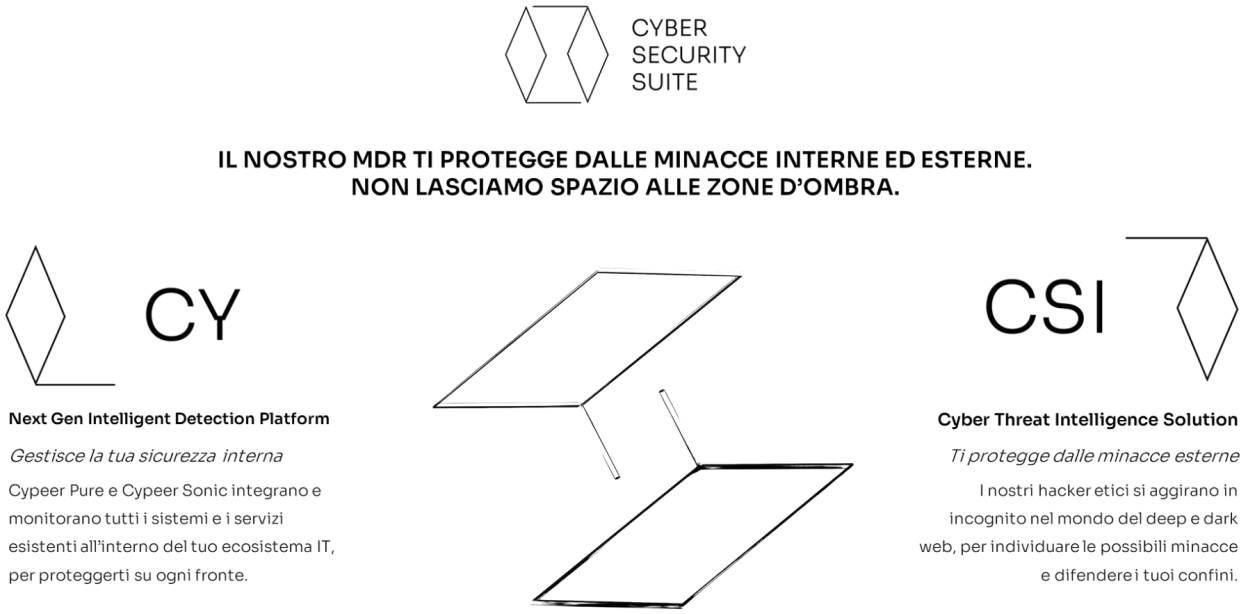
Il servizio di web security consente alle aziende clienti di definire e applicare regole sull'utilizzo di internet, in modo da impedire che i dipendenti assumano un comportamento illecito che potrebbe anche danneggiare l'immagine dell'azienda. Allo stesso tempo, il software fornito mette in sicurezza l'accesso ad internet impedendo gli attacchi cyber e tutelando le persone dall'accesso a siti web compromessi o fraudolenti. Il servizio prevede la registrazione dei siti web visitati dagli utenti del cliente e, ove previsto, il blocco dell'accesso ai siti web. Più in generale, il servizio consente di contrastare le infezioni da malware, di ridurre o calmierare gli effetti del phishing e dei ransomware. Il servizio è, altresì, in grado di regolamentare l'accesso ad internet anche sui dispositivi che operano al di fuori della rete aziendale del cliente. Il servizio, caratterizzato da una soluzione basata sul cloud, consente un controllo e una protezione costante della navigazione internet anche in mobilità e una limitazione dell'accesso ad internet per determinate categorie (white list e black list) e offre altresì report avanzati per l'analisi della sicurezza aziendale anche a disposizione dei clienti.

### *Security awareness*

Alla luce di incidenti che causano fuga di dati sempre più frequenti causati dagli utenti, il servizio di security awareness prevede la messa a disposizione dei clienti di una piattaforma di e-learning in cloud, relativa alla cyber security. All'interno della piattaforma è possibile seguire corsi (disponibili in diverse lingue) connessi alla sicurezza informatica, volti a migliorare la consapevolezza dei dipendenti del cliente sulle minacce presenti sul mercato e in internet. In particolare, il servizio mette a disposizione del cliente anche una piattaforma per lo svolgimento di attacchi di phishing simulati, in modo da valutare le reazioni di ciascun dipendente. La simulazione di attacchi di phishing consente anche di comprendere quanto appreso da ciascun dipendente dai corsi svolti e il rispetto delle procedure aziendali.

### *Cyber Security Suite*

Cyberoo, grazie anche alle proprie competenze e conoscenze in termini di servizi di cyber security e delle differenti tipologie di minacce che si attestano sui clienti, ha sviluppato soluzioni proprietarie innovative di elevata affidabilità. A tal proposito, in aggiunta ai servizi sopra descritti e nell'ambito dei servizi di cyber security, l'Emittente offre servizi relativi a (i) **Cyber Security Intelligence ("CSI")** volti a proteggere i clienti dalle minacce esterne; e (ii) **Cypeer ("CY"),** funzionali alla garanzia della sicurezza interna dell'azienda.



## Cyber Security Intelligence (CSI)


Cyber Security Intelligence (CSI) è il servizio di **Threat Intelligence** che, attraverso la raccolta e l'analisi di informazioni presenti nel deep e dark web, permette di avere una visione completa delle minacce esterne che riguardano la presenza sul web dell'azienda.

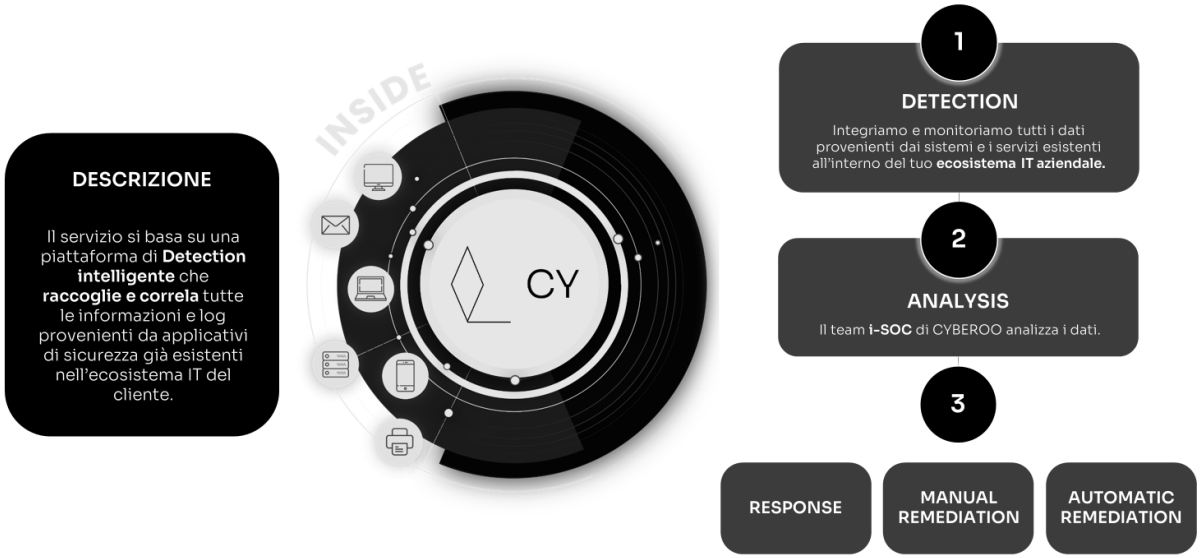
A svolgere il servizio è l'**I-SOC**, che si occupa di:

- verificare gli allarmi e abbattere i falsi positivi, grazie anche all'ausilio di processi automatizzati;
- definire i workaround per identificare un percorso di risoluzione delle problematiche rilevate;
- svolgere attività di OSINT (Open Source Intelligence) quali Data Breach & Data Leakage Identification, Brand Monitoring, Deep & Dark Web Analysis e VIP Users Protection.

CSI permette di accrescere la propria consapevolezza dei rischi e delle minacce dirette e indirette che possono impattare ogni realtà. L'I-SOC attivo H24 notifica, infatti, in near real-time le minacce individuate e le azioni necessarie volte a mitigare o evitare l'impatto. Grazie a ciò, è possibile prendere provvedimenti sulle proprie soluzioni in modo proattivo, contrastando il verificarsi di incidenti di sicurezza.

Questo servizio vanta la capacità di andare oltre a quelle che possono essere le minacce prettamente tecnologiche, ponendo l'attenzione anche e in particolar modo alle minacce di natura fraudolenta. Le informazioni raccolte ed elaborate da CSI sono secretate e disponibili solo agli utenti/sistemi autorizzati alla loro gestione: ogni accesso alle informazioni è dovutamente registrato e i log sono mantenuti secondo gli standard di sicurezza in materia e la normativa vigente.

### Cypeer (CY)




Cypeer è un servizio basato su una piattaforma di detection intelligente, pensato per avere un quadro completo della postura di sicurezza IT dell'azienda da un punto di vista interno, allo scopo di prevenire minacce e attacchi al sistema.

Il servizio permette di aggregare e correlare tutti gli eventi generati dagli apparati di sicurezza già esistenti nell'ecosistema IT, consentendo di avere una visione specifica per ciascuna macchina o soluzione appartenente all'infrastruttura. Eventuali minacce rilevate sono poi prese in esame dall'I-SOC attivo in H24 e segnalate insieme alla remediation proposta per risolvere il problema stesso, grazie a:

- **INTEGRAZIONE CON SOLUZIONI DI SICUREZZA E INFRASTRUTTURA IT:** Cypeer può andare ad integrare qualunque servizio di sicurezza, a patto che questo possa condividere le proprie informazioni attraverso log di sistema e simili.

- **CORRELAZIONE DEGLI EVENTI:** per tutte le fonti di dati agganciate a Cypeer, questo effettua attività di identificazione, correlazione e alerting di anomalie o attacchi cyber che vanno oltre alle capacità native dei singoli servizi.
- **DASHBOARD MULTITENANT PER UN ACCESSO COMPLETO AI DATI:** Cypeer dispone di dashboard multi-tenant per un accesso completo ai casi in gestione da parte dell'I-SOC, allo scopo di avere una visione istantanea e pregressa della postura di sicurezza dell'ecosistema IT.
- **AUTOMATIC REMEDIATION:** Cypeer può attivare remediation automatiche a fronte di allarmi specifici o di condizioni predefinite.
- **REMEDIATION MANUALE:** Cypeer grazie alle persone che compongono il team di remediation e ad un'istanza che non richiede gli accessi di amministratore di sistema sono in grando di intervenire direttamente con Playbook definiti sui sistemi dei clienti laddove non ci sia una catena del soccorso con presenza H24.

È proprio nella remediation che si distinguono Cypeer Dek e Cypeer Sonic e Cypeer Keera:

**Cypeer Dek** permette ai clienti con limitazioni di budget ad accedere ad un eccellente strumento di detection e analisi grazie all'i-SOC e poi implementa la remediation direttamente tramite catena del soccorso identificata sulla base degli schemi MITRE ATT&CK.

In **Cypeer Sonic** oltre agli elementi presenti in Cypeer Dek è possibile implementare automatismi di risposta tramite playbook. Questo fa sì che l'Automatic Remediation sia senza limiti su tutte le tecnologie che offrono la possibilità di essere utilizzate tramite sistemi automatici (che forniscono API).

**Cypeer Keera** aggiunge alle funzionalità di Sonic anche la possibilità di avere un servizio di remediation Night & Weekend per effettuare attività di risposta alle minacce supportando una catena del soccorso 8x5, mentre la versione **Keera +** permette le attività di remediation H24.

## Managed services

Cyberoo, nell'esercizio della propria attività, svolge la funzione di ***Managed Security Service Provider (MSSP).*** I servizi ricompresi in tale linea di business sono riferibili a tre categorie principali: (i) *data center management*; (ii) *cloud management*; e (iii) *device management*.

## Data center management

Il servizio di *data center management* prevede la gestione dei server, fisici o virtuali, degli apparati di rete (switch, router, firewall e fibre channel switch), nonché delle unità dischi (NAS e SAN) presenti all'interno di un centro dati. In particolare, il servizio prevede una gestione proattiva delle eventuali problematiche che possono verificarsi sia lato hardware sia lato software sui dispositivi gestiti, tramite degli interventi remoti o in locale.

Nell'ambito del servizio, Cyberoo offre altresì il servizio di *back up management*, ideato per garantire ai clienti una gestione completa dell'infrastruttura per il salvataggio dei dati e delle macchine virtuali, sia monitorando, controllando e gestendo l'intero processo di salvataggio dei dati, sia eseguendo le eventuali richieste di ripristino dei dati. Il servizio di back up management si caratterizza per il profilo della scalabilità, in quanto la soluzione realizzata è in grado di gestire sia le piccole imprese sia le imprese medie e grandi: il servizio, infatti, essendo tarato sulla effettiva quantità di dati da proteggere, è indipendente dal numero di dispositivi da salvare.

In aggiunta, Cyberoo ha ideato il servizio di *back up in cloud* al fine di garantire al cliente una maggiore affidabilità della salvaguardia dei dati aziendali e l'integrità degli stessi. Grazie a tale servizio, infatti, è possibile archiviare i dati salvati all'interno di un server sicuro, ospitato presso un centro dati. Il servizio comprende anche il controllo e il monitoraggio proattivo di tutto il processo di copia remota dei dati all'interno dello spazio disco remoto. Il software di backup fornito consente di salvare i dati in locale e poi replicarli in cloud al fine di conservarli, a seconda delle specifiche esigenze del cliente, per una, due o quattro settimane.

### Cloud management

Cyberoo mette a disposizione dei propri clienti infrastrutture e applicazioni cloud che garantiscono altissimi livelli di performance grazie alle più avanzate tecnologie disponibili sul mercato. I *cloud services*, oltre a ridurre i costi di infrastruttura, consentono scalabilità e agibilità virtualmente illimitate, nonché un elevato grado di sicurezza e conformità.

In particolare, l'Emittente propone una soluzione Infrastructure as a Service (IaaS), erogabile secondo una duplice modalità:

- *cloud*, dove i dati ed i servizi del cliente sono ospitati presso un data center, di proprietà di soggetti terzi, di primaria importanza nazionale (modalità indicata per aziende multi sede);
- *on premise*, dove i dati ed i servizi sono ospitati in una infrastruttura locale all'interno della sede del cliente (modalità indicata per aziende di produzione o mono sede).

### Device management

Cyberoo effettua la gestione e il monitoraggio utilizzando sistemi basati sull'intelligenza artificiale in grado di rilevare gli eventi di ogni dispositivo distribuito all'interno della rete del cliente, garantendone la massima efficienza operativa.

Il servizio di *help desk* (24 ore su 24, 7 giorni su 7) consente di avere un maggiore controllo delle postazioni, di monitorare lo stato hardware e software delle postazioni stesse e la gestione degli aggiornamenti dei sistemi e delle principali applicazioni.

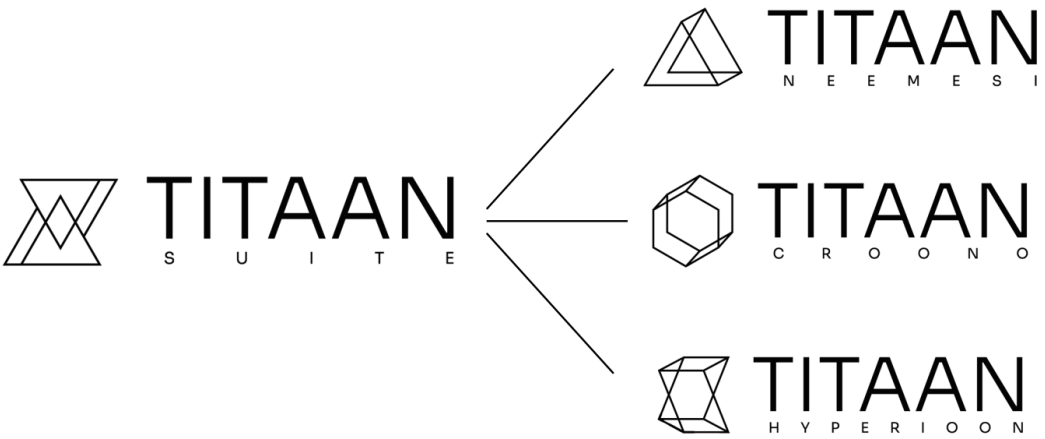
Cyberoo, grazie ad una esperienza pluriennale ed una profonda conoscenza dei servizi riguardanti la gestione dell'ecosistema IT e del mercato degli strumenti di monitoraggio classici, ha ideato, sviluppato e registrato una soluzione innovativa, denominata **Titaan Suite**, che consente una gestione dei servizi ancora più efficiente utilizzando le conoscenze sull'intelligenza artificiale, deep learning e big data.

Titaan è un "*System behaviour analyser (SaaS)*", ossia una piattaforma che supera il paradigma dei classici sistemi di monitoraggio basato sulle soglie statiche in

quanto è in grado di identificare e prevenire le inefficienze sui sistemi, basandosi dunque non su soglie impostate dall'utente, ma sullo studio del comportamento della macchina stessa. Questo avviene attraverso complessi algoritmi di **Intelligenza Artificiale,** che imparano a identificare puntualmente comportamenti anomali, segnalando solamente reali problematiche e non i cosiddetti "falsi positivi".

Con una *dashboard user-friendly*, Titaan è in grado di prevenire le inefficienze sui sistemi e ridurre i costi. Oltre a identificare il problema, la suite è in grado di farne un'analisi causale, andando ad individuare chi e come sta causando un malfunzionamento. È sempre tramite gli algoritmi di IA che Titaan consente di fare un'analisi predittiva fino a 8 settimane sul dimensionamento delle macchine ed eventuali anomalie.

Il servizio Titaan offerto è disponibile in tre differenti versioni: (i) Titaan Neemesi; (ii) Titaan Croono; e (iii) Titaan Hyperioon.




**Titaan Neemesi**

Titaan Neemesi è il modulo che ha lo scopo di mantenere la compliance all'interno dell'infrastruttura IT.

Nello specifico si compone di cinque application: Admin Log, Log Extra AD, Best Practice Analyzer e Active Directory Report.

Il modulo è stato sviluppato con l'obiettivo di:

- garantire la compliance al GDPR e l'inalterabilità del dato e dei log raccolti grazie alla tecnologia Blockchain;
- identificare eventi che si verificano su Active Directory;
- identificare e fornire le Best practice per il GDPR, procedure di certificazione e compliance;
- evitare cali di prestazioni, scarsa affidabilità, conflitti e problemi di sicurezza;
- identificare problemi specifici su alcuni dei più importanti componenti aziendali, politiche di login, permessi, ruoli, sistemi operativi, unità organizzative.

Titaan Nemesi ha la possibilità di aggiungere anche tre add-on:

- Whistleblowing: consente ai dipendenti di fare segnalazioni anonime a fronte di comportamenti non etici all'interno dell'azienda;
- File Integrity: consente di sapere che cosa accade ai file aziendali, chi ne ha accesso, al fine di proteggere il know how aziendale;
- NIS2: fornisce e consente il monitoraggio e l'analisi dei sicurezza necessarie per supportare la compliance NIS2.

### Titaan Croono

Titaan Croono è il modulo che rappresenta **l'inventario degli asset di rete dell'infrastruttura aziendale**. Individua gli apparati di rete e i nodi che sono più carichi a livello di throughput dei dati permettendo di evitare i colli di bottiglia delle prestazioni e di recuperare e redistribuire le risorse hardware in base al carico effettivo. È in grado di disegnare automaticamente la topologia della rete e monitorarne l'hardware. Offre, inoltre, una reportistica omnicomprensiva di tutti gli asset di rete e delle relative informazioni.

### Titaan Hyperioon

Titaan Hyperioon è il terzo modulo della Titaan Suite ed è la soluzione di Observability per infrastrutture On-Premise, Hybrid e Cloud.

È il concentratore di ogni informazione inerente a log e metriche di sistema: Hyperioon, infatti, integra e correla dati da oltre 200 fonti, garantendo una gestione immediata delle problematiche. Tramite l'Intelligenza Artificiale, è in

grado di individuare deviazioni dal comportamento usuale dell'ecosistema IT e inviare alter proattivi, consentendo così di aumentare la velocità di risoluzione delle problematiche.

### Digital transformation

Cyberoo, mediante l'offerta di servizi di digital transformation, 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 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, accentrandoli 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 ed 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 in azienda con modalità innovative, (tramite app). Inoltre, mediante tale soluzione, l'ospite ha altresì la possibilità di visionare l'informativa aziendale sulla privacy aziendale, al fine di tutelare la sua sicurezza e la sua permanenza in azienda.
- ***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.

# 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 |
| **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.

Non tutti gli aspetti materiali sono di uguale importanza, e l'enfasi all'interno di un report ne riflette la loro priorità relativa. Ai fini della redazione del primo bilancio di sostenibilità, ancorché redatto secondo l'opzione di rendicontazione GRI "*With referenced to*", Cyberoo ha effettuato, in coerenza con i GRI Standard, un'analisi di materialità. L'analisi è stata effettuata tenendo inoltre conto di quanto previsto dal D.lgs. 254/2016, che disciplina la redazione della Dichiarazione Non Finanziaria (DNF).

Al fine di identificare i principali impatti che le attività svolte da Cyberoo generano o potrebbero generare sulla sfera ESG, nel corso del 2022 è stato svolto un processo strutturato che ha permesso di definire nel dettaglio il contesto di riferimento all'interno e all'esterno dell'Organizzazione.

Nel 2023 non sono intervenuti eventi significativamente rilevanti tali da prevedere una revisione dell'analisi di materialità. Per questa ragione il management aziendale del Gruppo ha valutato di considerare come "materiali" gli stessi temi e impatti ESG definiti nell'esercizio 2022.

Lo svolgimento dell'analisi di materialità si è articolata nei seguenti passaggi:

| Processo: Fasi | |
|---|---|
| **1** | Identificazione e mappatura stakeholder |
| **2** | Linee guida del piano industriale e relativi obiettivi |
| **3** | Analisi documentale dello scenario di riferimento: normativa settore e megatrend (in particolare politiche EU Green Deal – EU Next Generation Plan e PNRR) |
| **4** | Analisi benchmark di settore: Reporting di sostenibilità dei comparables nazionali ed internazionali |
| **5** | Stakeholder: approfondimento delle attività di engagement di carattere ricorrente svolte nei confronti delle diverse categorie di stakeholder /Aspettative da analisi contesto |
| **6** | Valutazione del management e di alcuni stakeholder (dipendenti, fornitori, investitori, banche e clienti) attraverso un questionario di valutazione |
| **7** | Validazione delle tematiche di materialità e del livello di priorità da parte del top management di Cyberoo (Presidente/Amministratore Delegato/Direttore generale) |

Gli impatti individuati sono stati clusterizzati in base al reciproco livello di affinità, al fine di ottenere un elenco più limitato di 26 tematiche ESG da sottoporre a valutazione quantitativa da parte dei Vertici Aziendali e da un campione rappresentativo delle principali categorie di stakeholder dell'azienda.

Per la valutazione delle tematiche è stato utilizzato un questionario con il quale è stato richiesto di prioritizzare ciascun tema, secondo il livello di rilevanza.

In particolare, la valutazione circa il livello di "rilevanza" degli impatti ESG connessi ad ogni tematica 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).

Al fine di identificare i temi e gli impatti ESG realmente "materiali" per Cyberoo è stata definita la cosiddetta "**soglia di materialità**", considerando come tali, per ogni macro ambito, il 50% dei temi che hanno ottenuto una prioritizzazione più elevata.

Al termine dell'intero processo, i risultati conseguiti sono stati sottoposti a discussione e validazione da parte del Consiglio di Amministrazione di Cyberoo S.p.A. in data 22/05/2023.

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 |
|---|---|---|---|---|
| **Governance** | | | | |
| **Etica e integrità nella condotta del business** | Possibilità di incidere positivamente o negativamente su:<br>• gestione delle risorse finanziarie a beneficio della società e dell'ecosistema economico in cui opera<br>• mantenimento delle relazioni con i principali stakeholder con cui l'Organizzazione interagisce | GRI 2-27<br>GRI 205-3<br>GRI 206-1<br>GRI 207-1 | Processi di verifica dell'allineamento alle normative e agli standard in materia di etica e integrità del business | Codice Etico<br>Modello di Organizzazione, Gestione e Controllo 231/01<br>Predisposizione e asseverazione con cadenza annuale del Bilancio Finanziario |
| **Tutela del brand e reputazione** | Possibilità di incidere positivamente o negativamente su:<br>• sensibilità e consapevolezza della clientela e del mercato sulla sostenibilità<br>• disponibilità di prodotti e servizi con elevate performance ambientali/sociali | GRI 2-6 | Processo di aggiornamento e monitoraggio costante dei brand registrati | Adozione di misure volte a rafforzare la reputazione dell'azienda, incrementando l'apprezzamento da parte dei clienti e valorizzando i brand del Gruppo |

| Tema materiale | Impatti e rilevanza del tema | KPI/GRI Standards | Attività che genera l'impatto | Impegni, politiche e strumenti di monitoraggio |
|---|---|---|---|---|
| **Anticorruzione e compliance** | Possibilità di incidere positivamente o negativamente su:<br>• tutela della legalità in ambiti quali il reimpiego di profitti derivanti da attività illecite, il manifestarsi di episodi di corruzione e concussione, l'adozione di comportamenti anti-competitivi, ecc. | GRI 205-3<br>GRI 206-1 | Attività di monitoraggio e controllo dell'attività di core business<br>Processi di verifica dell'allineamento alle normative e agli standard in materia di etica e integrità del business | Codice Etico<br>Modello di Organizzazione, Gestione e Controllo 231/01 |
| **Governance trasparente e gestione dei rischi di sostenibilità** | Possibilità di incidere positivamente o negativamente su:<br>• tutela della legalità e prevenzione di comportamenti illeciti | GRI 2-27<br>GRI 205-3<br>GRI 206-1 | Processi di monitoraggio e aggiornamento del sistema di gestione dei rischi con integrazione dei rischi ESG | Codice Etico<br>Modello di Organizzazione, Gestione e Controllo 231/01 |
| **Capitale economico-finanziario** | | | | |
| **Solidità e resilienza economica** | Possibilità di incidere positivamente o negativamente su:<br>• gestione delle risorse finanziarie a beneficio della società e dell'ecosistema economico in cui opera (es: settore di riferimento, distretto geografico, ecc.).<br>• mantenimento delle relazioni con i principali stakeholder con cui l'Organizzazione interagisce.<br>• grado di attrazione nei confronti degli investitori e dei prestatori di capitale. | GRI 201-1 | Sviluppo dell'attività di business | Adozione di una strategia competitiva capace di garantire la salvaguardia ed il possibile miglioramento delle performance economico-finanziarie del Gruppo nel corso del tempo |
| **Creazione e distribuzione della ricchezza generata** | Possibilità di incidere positivamente o negativamente su:<br>• gestione delle risorse finanziarie a beneficio della società e | GRI 201-1<br>GRI 203-1 | Sviluppo e rafforzamento delle relazioni con gli stakeholder e relativa | Piano Industriale di Gruppo<br>Stakeholder Engagement |

| Tema materiale | Impatti e rilevanza del tema | KPI/GRI Standards | Attività che genera l'impatto | Impegni, politiche e strumenti di monitoraggio |
|---|---|---|---|---|
| | dell'ecosistema economico in cui opera<br>• mantenimento delle relazioni con i principali stakeholder con cui l'Organizzazione interagisce<br>• capacità di *retention* e *attraction* e sulla stabilità occupazionale delle risorse umane | | distribuzione della ricchezza generata | Adozione di misure in grado di garantire la continuità operativa, la stabilità finanziaria e la redditività del business |
| **Capitale Produttivo** | | | | |
| **Ricerca e innovazione tecnologica** | Possibilità di incidere positivamente o negativamente su:<br>• gestione delle risorse finanziarie a beneficio della società e dell'ecosistema economico in cui opera.<br>• 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 | |
| **Qualità, sicurezza ed affidabilità dei servizi** | Possibilità di incidere positivamente o negativamente su:<br>• benessere della clientela, in termini di assenza di materiali/sostanze tossiche nei prodotti offerti dall'azienda | GRI 416-1<br>GRI 416-2 | Controlli periodici di qualità sui prodotti commercializzati | Test a campione sui prodotti/servizi commercializzati<br><br>Certificazioni di qualità sui prodotti/servizi |
| **Capitale Umano e Relazionale** | | | | |
| **Formazione e sviluppo delle carriere** | Possibilità di incidere positivamente o negativamente su:<br>• opportunità di ciascun collaboratore di intraprendere un percorso di crescita professionale e di realizzare pienamente il proprio potenziale<br>• disponibilità di percorsi finalizzati al | GRI 404-1 | Sviluppo di piani di formazione obbligatoria e specializzata per la crescita professionale dei dipendenti | Impegno per la formazione e addestramento del personale |

| Tema materiale | Impatti e rilevanza del tema | KPI/GRI Standards | Attività che genera l'impatto | Impegni, politiche e strumenti di monitoraggio |
|---|---|---|---|---|
| | rafforzamento e sviluppo delle competenze e delle skill professionali | | | |
| **Partnership con istituzioni ed imprese** | Possibilità di incidere positivamente o negativamente su:<br>• sviluppo della capacità innovativa, produttiva ed economica del territorio e del mercato in cui la stessa azienda opera | GRI 2-28 | Sviluppo di partnership strategiche con imprese, enti locali e associazioni del settore | |
| **Soddisfazione e gestione delle relazioni con i clienti** | Possibilità di contribuire positivamente o negativamente a:<br>• realizzazione e soddisfacimento dei bisogni della clientela in termini di offerta dei prodotti e qualità dei servizi | GRI 418-1 | Attività di customer satisfaction<br>Attività di analisi delle richieste del mercato | Gestione della customer satisfaction |
| **Rispetto dei diritti umani e tutela dei lavoratori** | Possibilità di incidere positivamente o negativamente su:<br>• tutela dei diritti fondamentali dei membri del personale aziendale e di tutti i collaboratori con cui la Società si interfaccia | GRI 401-1<br>GRI 406-1 | Processi di monitoraggio e segnalazione del mancato rispetto dei diritti umani | Codice Etico<br>Monitoraggio degli episodi di discriminazione |
| **Trasparenza delle informazioni sui servizi** | Possibilità di influenzare positivamente o negativamente su:<br>• consapevolezza dei clienti in fase di acquisto<br>• grado di fiducia dei clienti e degli stakeholder nei confronti della Società e della sua reputazione<br>• disponibilità di informazioni sulle caratteristiche dei prodotti e dei servizi offerti | GRI 417-3 | Disponibilità per i clienti di informazioni sulle caratteristiche dei prodotti/servizi offerti | Capacità di comunicare con trasparenza le caratteristiche dei prodotti/ servizi immessi nel mercato, evitando il greenwashing. |
| **Capitale Ambientale** | | | | |

| Tema materiale | Impatti e rilevanza del tema | KPI/GRI Standards | Attività che genera l'impatto | Impegni, politiche e strumenti di monitoraggio |
|---|---|---|---|---|
| **Efficienza energetica** | Possibilità di incidere positivamente o negativamente su:<br>• costi energetici attraverso azioni e progetti di efficientamento energetico<br>• tutela delle comunità locali e del territorio rispetto all'esposizione ad 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 |
| **Lotta al cambiamento climatico** | Possibilità di incidere positivamente o negativamente su:<br>• tutela degli ecosistemi e salvaguardia della biodiversità<br>• tutela delle comunità locali e del territorio rispetto all'esposizione ad eventi atmosferici estremi (es: alluvioni, allagamenti, uragani, desertificazione, ecc.) | GRI 305-1<br>GRI 305-2 | Processo di monitoraggio costante degli impatti sull'ambiente derivante dall'attività di business | Confronto e verifica annuale sui risultati raggiunti sulla riduzione delle emissioni |
| **Gestione dei rifiuti** | Possibilità di incidere positivamente o negativamente su:<br>• tutela degli ecosistemi e della biodiversità<br>• prosperità dei principali stakeholder con cui l'Organizzazione interagisce in termini di disponibilità di risorse materiche nei sistemi naturali e facilità di accesso ad esse<br>• salute e benessere della clientela, in termini di assenza di materiali / sostanze tossiche nei prodotti offerti dall'azienda | GRI 306-3 | Gestione responsabile dello smaltimento dei rifiuti, rispettando le leggi e i regolamenti in vigore | Attenzione alla gestione di fine vita del prodotto<br><br>Utilizzo di packaging sostenibile<br><br>Impegno nell'aumentare la quantità di materiali riciclati |

## Capitolo 2

# GOVERNANCE

# **GOVERNANCE**
# OVERVIEW

## SGI ISO 27001

Sistema di Gestione Integrato per la Qualità e la Sicurezza delle Informazioni (SGI) – ISO 27001

## FAI, CRIT e BNP Paribas

Tre delle nuove collaborazioni con entri territoriali e nazionali

## CERT e Cyberoo

## NESSUNA SANZIONE

Nessuna sanzione e/o contenzioso in essere in materia ambientale, sociale ed economica

# 2. 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 ed accurata informazione agli *stakeholder* relativamente agli sviluppi strategici ed 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 sono in corso le valutazioni per una redazione sia del Codice Etico che del Modello di organizzazione, gestione e controllo D.lgs. 231/2001, le cui implementazioni saranno previste entro il 2024.

## 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);

L'attività di **revisione legale** dei conti è stata affidata a BDO Italia S.p.A., nominata in data 29/04/2022. Tale incarico è conferito fino all'approvazione del bilancio al 31 dicembre 2024.

Il Consiglio di Amministrazione, costituito da sette membri, è stato nominato dall'Assemblea degli azionisti il 29 aprile 2022 e durerà in carica per tre esercizi.

Il Consiglio ha designato Massimo Bonifati nella carica di Presidente.

| 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 | Non esecutivo | Esecutivo | Esecutivo | Non esecutivo | Non esecutivo |
| Altre posizione rivestite nel Gruppo Cyberoo e/o esternamente | - | C.E.O Cyberoo S.p.A. | - | C.M.O. Cyberoo S.p.A. | Head of Service Design & Transition 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 2019 la società ha nominato, nella persona di Emanuele Cervo, il Responsabile della Protezione dei Dati (RPD o DPO) ai sensi dell'art. 37 del Regolamento UE 2016/679 (GDPR).

| Consiglio di Amministrazione – Diversità (genere – classi di età) | | | | | |
|---|---|---|---|---|---|
| Donne | | Uomini | | Totale | |
| Nr | % | Nr | % | Nr | % |
| 3 | 14% | 18 | 86% | 21 | 100% |
| Minori di 30 anni | | Tra 30 e 50 anni | | Maggiori di 50 anni | |
| Nr | % | Nr | % | Nr | % |
| - | - | 12 | 57% | 9 | 43% |

Il Collegio Sindacale, nominato dall'assemblea del 29 aprile 2022, rimarrà in carica sino all'Assemblea che approverà il bilancio di esercizio al 31 dicembre 2024 ed è composto da 3 membri effettivi e 2 supplementari.

| Collegio Sindacale | Gianluca Settepani | Rita Sciaraffa | Alberto Ventura | Mariangela Rossetti | 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 posizione rivestite nel Gruppo Cyberoo e/o esternamente | - | - | - | - | - |

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

## 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

L'Azienda 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 27001:2013**.

Il Sistema di Gestione, implementato da Cyberoo, si basa sulla gestione ed il governo dei suoi processi primari di business (progettazione, realizzazione ed erogazione dei servizi di cybersecurity e monitoraggio Infrastrutture IT) e sulle relative attività che hanno influenza sulle prestazioni aziendali.

Il Sistema di Gestione (SGI) è costituito dall'insieme di responsabilità, procedure, attività, strutture e risorse predisposte per realizzare la Politica per la Qualità e Sicurezza delle Informazioni nel modo più efficace possibile e per garantire al massimo la sicurezza, integrità e disponibilità delle informazioni, ottenendo al tempo stesso un continuo miglioramento.

Al fine di mettere in atto il SGI, l'Azienda ha:

- identificato e documentato i processi operativi;
- stabilito le sequenze e le interazioni tra i processi;

- individuato gli elementi in ingresso (input), gli elementi in uscita (output) per ogni attività aziendale, le responsabilità e i documenti di riferimento;
- individuato i punti di controllo per ogni processo;
- individuato le interfacce e i requisiti di sicurezza dei fornitori esterni (contenuti in appositi documenti contrattuali o attraverso audit eseguiti da Cyberoo).

In ottica di migliorare sempre di più la qualità dei processi, e dunque dei servizi erogati, Cyberoo ha in previsione per i prossimi anni – essendo una delle attività core aziendali – di ottenere la certificazione secondo lo schema **ISO 27035**, relativo alla gestione degli incidenti informatici. Per raggiungere questo obiettivo, si è avviato un primo assesment ed è già stato disegnato il processo di Gestione degli Incidenti.

## Adesione ad iniziative esterne e Membership

### Confindustria

Cyberoo a partire da giugno 2020 è partner di **Confindustria Servizi** attraverso il brand ***RetIndustria,*** che gestisce le convenzioni nazionali di Confindustria e offre ai partner la possibilità di promuovere i propri prodotti e servizi legati all'attività imprenditoriale alle oltre 150.000 aziende associate a Confindustria e alle circa 200 Organizzazioni Confederate (associazioni territoriali, associazioni nazionali di categoria, Confindustrie regionali e Federazioni nazionali di settore).

#### Confindustria Servizi

Confindustria Servizi S.p.A. organizza e gestisce le attività connesse e complementari alla realizzazione di iniziative editoriali, dirette a promuovere la diffusione della cultura d'impresa. Tra le attività principali ci sono la pubblicazione di volumi e riviste, l'invio di newsletter "partner del mese" alle Organizzazioni confederate, partecipazione ad eventi di business networking sul territorio, fisicamente o in modalità remoto.

## RetIndustria

RetIndustria è la rete di Partner che garantisce agli Associati al Sistema Confindustria offerte dedicate, in esclusiva e alle migliori condizioni sul mercato, per risparmiare sui principali prodotti e servizi legati all'attività imprenditoriale.

Cyberoo ogni anno è interessata a fornire al Sistema Associativo i propri servizi di cyber security a condizioni economiche di particolare vantaggio economico: nel 2020 tramite l'iniziativa di solidarietà "*Defence for ITALY*" ha reso disponibili alle aziende associate Confindustria e a tutte le Aziende italiane che ne hanno fatto richiesta, gratuitamente per tre mesi, i servizi innovativi di cyber security, Cypeer e CSI e i servizi di File Integrity e Admin Log, facenti parte della Suite Titaan. Tali soluzioni sono finalizzate a garantire un'elevata sicurezza soprattutto in quell'anno in cui le aziende hanno fatto ampio uso di modalità lavorativa in Smart Working con crescenti e impreviste problematiche di cyber security.

Nel 2021 tramite l'iniziativa "*BSecure*", Cyberoo ha riservato alle aziende associate Confindustria una soluzione di Vulnerability Assessement interno ed esterno e un UpSecurity Analysis gratuiti all'acquisto dell'innovativa Suite di Cyber Security (Cypeer e CSI) o del servizio Cypeer. A fronte di attacchi sempre più sofisticati e di un perimetro aziendale sempre più esteso e difficilmente monitorabile, tali soluzioni supportano le aziende nell'attivare un processo corretto e completo della Cyber Security, portando una maggiore consapevolezza e una cultura positiva all'interno delle imprese.

Nel 2022 Cyberoo, tramite l'iniziativa "*Security Plus*" riserva alle aziende associate Confindustria la promozione Security Plus che rende disponibili i servizi della Cyber Security Suite: Cypeer e CSI. Tramite questi servizi, Cyberoo offre una mensilità gratuita alla sottoscrizione di un contratto di 12 mesi o tre mensilità gratuite alla sottoscrizione di un contratto di 36 mesi.

Nel 2023 Cyberoo ha proseguito con l'iniziativa *"Security Plus"* riservata alle aziende associate.

### Unindustria Reggio Emilia

Sempre a partire dal 2020, Cyberoo è associato a **Unindustria Reggio Emilia**, che in coordinamento con il sistema Confindustria, concorre a tutelare e rappresentare le imprese associate sostenendo le ragioni della libera impresa, del lavoro, dei legittimi interessi e delle aspettative del mondo industriale in tutte le sedi, politiche, istituzionali, economiche e sindacali. Unindustria Reggio Emilia è l'associazione territoriale del sistema Confindustria che rappresenta quasi 1.000 imprese manifatturiere e di servizi della provincia, con circa 50.000 dipendenti.

A settembre 2021 viene annunciata l'apertura del nuovo polo tecnologico di Piacenza e, presidiando così anche il territorio piacentino con una nuova sede, Cyberoo è associata a **Confindustria Piacenza** che in conformità ai principi organizzativi generali del sistema di Confindustria persegue i seguenti scopi:

- favorire il progresso dell'industria piacentina, promuovendo la maggiore solidarietà e collaborazione tra le aziende associate;
- assistere tutelare e rappresentare le medesime in tutti i problemi sindacali, sociali, economici e culturali che direttamente o indirettamente le riguardano;
- promuovere nella provincia, e particolarmente presso gli imprenditori, lo sviluppo sociale, civile ed economico, nonché comportamenti conseguenti nel contesto di una libera società.

### Clusit

Cyberoo a partire da giugno 2021 è socia del **Clusit**, associazione che nasce nel 2000 sulla scorta delle esperienze di altre associazioni europee per la sicurezza informatica quali CLUSIB (B), CLUSIF (F), CLUSIS (CH), CLUSIL (L) che costituiscono un punto di riferimento per la sicurezza informatica nei rispettivi paesi da oltre 20 anni, alle quali si è aggiunta CLUSIQ. Il Clusit si pone i seguenti obiettivi:

- diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini;
- partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello comunitario che italiano;

- contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Nel 2022 Cyberoo ha avuto la possibilità di contribuire ai contenuti della pubblicazione Supply Chain Security, dedicata al tema della cyber security nelle catene di fornitura. Negli anni precedenti Cyberoo ha partecipato in qualità di sponsor e speaker agli eventi *Security Summit*.

**CRIT**

Dal 2020 Cyberoo fa parte del Network Fornitori Accreditati di CRIT S.r.l., azienda modenese che sviluppa progetti di ricerca, trasferimento di conoscenze tecnologiche ed analisi di informazioni tecnico-scientifiche.

La partnership high-tech che nasce lungo l'asse della Via Emilia è finalizzata a sviluppare strategie e soluzioni innovative volte a garantire la continuità operativa delle aziende e la difesa da attacchi informatici di varia natura. In particolare, grazie all'impiego di Intelligenza Artificiale e Big Data sarà possibile creare strategie ad hoc per proteggere, monitorare e gestire in piena sicurezza le infrastrutture IT delle aziende che compongono il panel societario di CRIT.

**FAI**

Dal 2022 ha avviato una collaborazione triennale con il FAI – Fondo per l'Ambiente Italiano che porterà l'azienda a dare il suo contributo per la salvaguardia del patrimonio artistico e ambientale italiano, insieme a quello tecnologico e della sicurezza informatica.

La decisione nasce dalla forte condivisione di valori legati alla protezione e valorizzazione del patrimonio nazionale, principi verso i quali Cyberoo e FAI indirizzano le rispettive attività, ognuno per le proprie aree di competenza.

Da un lato Cyberoo, impegnata nel mettere in sicurezza il perimetro informatico del patrimonio aziendale italiano, e non solo, e dall'altro lato il FAI, ambasciatore della cultura della protezione e valorizzazione dei luoghi dell'arte e della natura. Entrambi quindi impegnati nel dare un futuro migliore al Paese.

Tramite il FAI sono stati organizzati seminari di formazione sul tema della protezione dei dati con **SDA BOCCONI**.

**BNP Paribas**

Il 31 maggio 2023 Cyberoo ha avviato una collaborazione con BNP Paribas Leasing Solutions per la locazione operativa e il finanziamento delle sue principali soluzioni di cyber security: Cyberoo di CSI (Cyber Security Intelligence) e Cypeer. L'opzione della locazione operativa e del finanziamento permetterà alle piccole e medie imprese di avere un accesso a soluzioni di sicurezza informatica evoluta di medio termine, con un prezzo fisso per tre anni, tramite pagamenti di canoni mensili o trimestrali. Questa nuova soluzione risponde alla necessità delle aziende di rateizzare il pagamento dei servizi per la sicurezza informatica a copertura pluriennale.

**Computer Emergency Response Team (CERT)**

Cyberoo comunica, il 29 giugno 2023, di essere entrata nel circuito CERT (Computer Emergency Response Team) del Trusted Introducer, il principale riferimento del settore a livello internazionale.

In qualità di CERT, per Cyberoo si aprono nuove importanti opportunità. Queste includono sia l'ampliamento della visibilità verso aziende che richiedono consulenza e supporto in ambito di sicurezza informatica, sia per la collaborazione con altri player internazionali per lo scambio di informazioni utili alla definizione delle best practices, volte al contrasto dei nuovi cyber threat a vantaggio della sicurezza nazionale e internazionale.

**Bullismo No Grazie**

In data 14 dicembre 2023, Cyberoo decide, insieme al partner Euro Informatica S.p.A., di sostenere "Bullismo No Grazie". Questa associazione no profit è nata con l'obiettivo di prevenire, combattere ed informare sulla diffusione del bullismo e del cyberbullismo, e dei relativi traumi di chi ne è vittima. L'impegno di Cyberoo consiste nel supportare la pubblicazione del calendario "Bullismo No Grazie 2024", al fine di creare uno strumento che aiuti a ricordare i molteplici pericoli in cui possono incorrere i ragazzi ogni giorno e di come tutti abbiamo il dovere di impegnarci nella prevenzione e lotta al bullismo.

## Cybersecurity e Data protection

Il core business di Cyberoo è la Cybersecurity. Essa si concretizza applicando i 3 principi canonici della sicurezza del dato: ***confidenzialità, integrità e disponibilità***. Cyberoo al fine di esser trasparente e monitorata da enti terzi sullo stato di adeguamento delle proprie tecnologie, procedure e linee guida per la sicurezza del dato – specialmente per quanto concerne la gestione dello stesso per il Cliente – ha riconfermato le Certificazioni ISO 27001 per la sicurezza.

All'interno di questo contesto, Cyberoo applica le proprie Soluzioni di Cybersecurity (l'MDR Cypeer e la Soluzione di threat intelligence CSI) prima di tutto alla propria azienda al fine di garantire il più alto livello di protezione.

Per quanto concerne la gestione del dato in ottica privacy, tutte le informazioni raccolte e gestite da Cyberoo per il Cliente sono contestuali a **metadati**, ossia, informazioni non direttamente relative alla persona. Nonostante ciò, le modalità di accesso, gestione e archiviazione delle informazioni rispettano tutti i principi di privilegio minimo, nonché cifratura del dato e ridondanza.

Cyberoo ha inoltre un importante team di *Incident Response*, il quale, supportato dal servizio di analisti, monitora costantemente e agisce in caso di possibile minaccia o attacco all'azienda e/o ai sistemi dei Clienti sotto monitoraggio. Ad oggi, Cyberoo non ha subito alcun tipo di compromissione e diversi attacchi sono stati correttamente identificati e mitigati prima che questi potessero sortire effetti negativi. Anche nell'ambito della difesa dei Clienti, tutti gli attacchi monitorati o i primi stage di compromissione sono stati identificati e correttamente gestiti, e nessuna informazione è stata ad oggi trafugata o compromessa in termini di confidenzialità, riservatezza o disponibilità.

Ad oggi Cyberoo conta 3 livelli di SOC h24 dislocati sul territorio EMEA.

Questi SOC forniscono tre differenti livelli di competenze e conseguente escalation sulla base della natura delle minacce rilevate dalle Soluzioni Cypeer e/o CSI e prese in carico per la loro mitigazione e risposta da parte del team SOC.

Tali team possono richiedere il supporto anche del Team di Incidente Response ove necessario.

Le Soluzioni Cyberoo sono state, inoltre, aggiornate al fine di poter dare evidenza ai SOC del livello di rischio esposto tramite l'esecuzione continuativa di scansioni

volte a rilevare in near-real-time eventuali vulnerabilità che possano impattare i sistemi Cyberoo.

Come accennato, Cyberoo offre diverse Soluzioni per garantire la sicurezza dei dati e dei servizi dei propri Clienti: tale differenziazione nasce dalla necessità di indirizzare correttamente le minacce che, per loro costituzione e natura, possono presentarsi in diverse forme e applicazioni.

## Compliance normativa

Nel corso del 2023, così come negli anni precedenti, non si sono verificati eventi che hanno dato origine a sanzioni e/o contenziosi per non conformità a leggi, normative, regolamenti in materia ambientale.

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.

Capitolo 3

# CAPITALE INFRASTRUTTURALE

## CAPITALE INFRASTRUTTURALE
OVERVIEW

# CRM
# + ITSM

Continuo miglioramento del
sistema interno

# 72

Accordi di partneship su tutto
il territorio nazionale

Gartner®

Primario «Representative Vendor 2023»
in Italia dei servizi di cybersecurity

# 3. Capitale infrastrutturale

## Innovazione e digitalizzazione

Cyberoo persegue una politica di elevata attenzione all'evoluzione tecnologica: in ottica di miglioramento continuo; nel corso del 2022 sono stati chiusi importanti contratti di rinnovamento tecnologico, per consentire al Gruppo di ottimizzare al meglio il proprio lavoro. Nello specifico, Cyberoo ha deciso di **rinnovare completamente il sistema CRM e di ITSM**. In particolare, il nuovo CRM consentirà di gestire al meglio il parco clienti, andando a centralizzare tutte le informazioni sugli stessi (contatti, riferimenti commerciali) così da rendere possibile un tracciamento costante dell'evoluzione delle opportunità.
Il nuovo sistema ITSM, invece, consentirà al Cliente di visualizzare in real time tutto ciò che concerne il suo rapporto verso Cyberoo: ticket aperti, servizi e contratti in essere, monitoraggio delle survey sulla customer satisfaction.

Oltre ai sistemi sopra menzionati, è stato avviato, nel 2022, un massiccio lavoro di **ottimizzazione 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 BPM[1], consentendo così di avere ben chiaro il risultato di ogni fase. Sono state aggiornate e condivise le matrici RACI, per esplicare ancor meglio la correlazione delle responsabilità. La Direzione Aziendale, attenta a questi temi, ha deciso inoltre di finanziare la formazione sulla metodologia Lean[2] e Six Sigma[3] nel corso del 2023, così da poter raggiungere risultati ancora migliori – in ambito di ottimizzazione dei processi – riducendo gli "sprechi" interni e, dunque, poter ottenere una maggiore qualità del servizio e del supporto erogato all'esterno. Il 2024, per concludere, sarà l'anno di applicazione di queste nuove metodologie per raggiungere gli obiettivi di qualità ed eccellenza che il gruppo persegue.

[1] BPM: Business Process Modeling

[2] Lean: un sistema di produzione che, riducendo gli sprechi fino a eliminarli, mira alla qualità totale;

[3] Six Sigma: approccio metodologico, rigoroso e fortemente strutturato orientato al miglioramento radicale dei processi in termini di performance e robustezza.

# 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 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 ad 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 compongano 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 notevole numero di Generic Top-Level Domains (gTLD), ossia tutti i domini utilizzabili per la registrazione di domini web (es: .it, .com, .org, .net, .eu, ecc). 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).

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 CSI permette di rendere automatizzabile 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 ed 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).

## 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 permetta di superare le limitazioni dei tradizionali sistemi “supervised” I principali contenuti innovativi derivano dall’utilizzo delle tecnologie di Machine Learning e Intelligenza Artificiale che si è scelto di utilizzare perché sono le uniche in grado di lavorare in un vantaggio competitivo rispetto alla concorrenza maniera proattiva ed in grado di generare previsioni analizzando in tempo reale elevati volumi di dati (big data). 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.

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 ad 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 2 mesi permettendo il giusto dimensionamento dei sistemi business critical.

**REOS**

Reos è un software di time tracking e reportistica pensato per aziende del comparto SMB ed enterprise. Scopo primario del software è aiutare i decisori aziendali a capire quali tipi di software vengono utilizzati in azienda all'interno delle varie Business Unit e con quali modalità di fruizione.

La soluzione monitora il tempo speso dalle risorse in relazione a:

- navigazione web;
- software utilizzati;
- tempo di utilizzo dei device aziendali;
- classificazione automatica del tempo speso.

La soluzione è pensata per ottimizzare fortemente la produttività delle risorse aziendali, sia mentre sono in sede sia mentre sono in telelavoro e/o in regimi di orario flessibile. Il software risponde a tutti i requisiti fondamentali che riguardano i moderni applet di time tracking. L'utente ha la possibilità di vedere la propria reportistica in merito all'utilizzo del tempo, in questo modo può rendersi conto in autonomia di quali abitudini è possibile modificare per migliorare la propria produttività.

Gli elementi di particolare innovazione sono dati dall'utilizzo di due algoritmi di Machine Learning che sono stati utilizzati per specifiche applicazioni e sono risultati più efficienti rispetto a tutti gli algoritmi esistenti sul mercato.

## PROGETTO GENERALISTA B2B/B2C

Nell'ambito degli archivi digitali i metadati sono le informazioni di cui bisogna dotare il documento informatico per poterlo correttamente formare, gestire e conservare nel tempo.

Il documento informatico è infatti privo della componente materiale costituita dalla carta ed è memorizzato in sistemi che contengono moltissimi oggetti digitali; per poter essere conservato, reso accessibile nel tempo, e per poter essere correttamente inserito nel suo contesto, deve essere posto in relazione ad un insieme di informazioni che lo descrivano a vari livelli. La normativa italiana prevede alcuni metadati minimi che devono essere associati al documento informatico come per esempio: la data di chiusura, l'oggetto, il soggetto produttore, ecc.

Tutti questi elementi servono per attribuire al documento un'identità ben precisa.

Al fine di poter sviluppare un *marketplace* che possa essere adattato ad ogni settore, si è pensato di realizzare uno speciale schema di database che racchiude i metadati che sia facilmente adattabile alle esigenze di vari clienti e permetta di realizzare la complessità e l'architettura dei dati attualmente implementati con singole personalizzazioni. Le attività di R&S sono finalizzate alla progettazione ed allo sviluppo sperimentale di tabelle multidimensionali di associazione che permettono di associare un insieme definito di metadati ad una molteplicità di prodotti.

È stata studiata una particolare architettura di dati che permette di velocizzare la risposta alle query di sistema mediante viste che si possono aggiornare rapidamente. In tal modo si ha la flessibilità di una vista e la consistenza ed integrità del dato di una tabella. La soluzione proposta è l'unica sul mercato che permetta di personalizzare in modo semplice ed efficiente la struttura dei metadati per ogni tipologia di prodotto in vari settori. La tecnologia che si vuole sviluppare è innovativa per il settore dell'e-commerce business in quanto al momento tutte le piattaforme utilizzano DB relazionali personalizzati per singolo progetto e non hanno una struttura facilmente configurabile dall'utente e valida in varie situazioni applicative. I principali contenuti innovativi sono dati dallo studio e sperimentazione di innovativi algoritmi non esistenti sul mercato, basati su tecnologie di Machine Learning e Intelligenza Artificiale che permettono di

analizzare in tempo reale grande quantità di dati e di supportare il decision maker in base alla valutazione dei rischi in real time.

## Premi e riconoscimenti

Grazie alla qualità della Suite proprietaria, del nuovo servizio Cypeer Sonic e all'investimento in Automatic Remediation, a febbraio 2023, Cyberoo è stata riconosciuta, per la seconda volta, come "Representative Vendor" nella prestigiosa "Market Guide For MDR Services 2023" di Gartner. La ricerca internazionale sui servizi gestiti di sicurezza informatica più importante e autorevole, ha riconosciuto Cyberoo come parte del ristretto gruppo dei "**Representative Vendor**" delle nuove frontiere della cybersecurity.

Con questo riconoscimento, Cyberoo si conferma tra i big internazionali della Cybersecurity avanzata e unica italiana tra 12 società europee e 50 nel mondo.


CYBEROO
Cyberoo
Black
Club

## 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 un contratto di distribuzione nazionale e 72 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.;
- Zerouno Informatica S.p.A.;
- Magnetic Media Network S.p.A.
- NPO Sistemi S.r.l.;
- Ergon S.r.l.;
- Vidata S.r.l.;
- Euro Informatica S.p.A.;
- Cyber-Bee-R1 S.p.A.
- WindTre S.p.A.;
- Retelit Digital Service S.p.A.
- Eurosystem S.p.A.
- Reti S.p.A.

Inoltre, nel corso del 2023 Cyberoo ha ampliato le sue operazioni internazionali con tre partnership in Polonia sotto riportate.

- PROSYSTEM SA.
- INTEGRITY PARTNERS SP. Z O. O.
- CC Otwarte Systemy Komputerowe Sp. z o.o

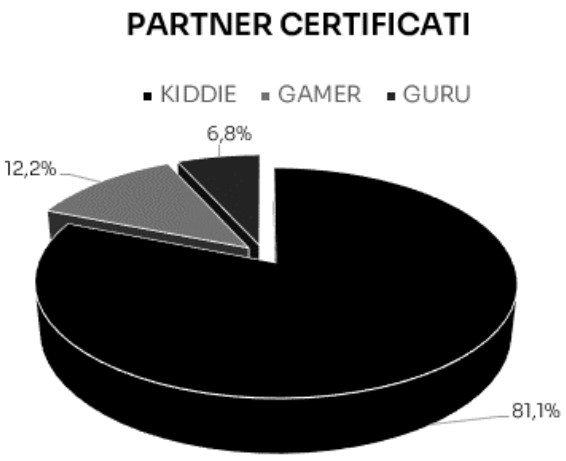
L'azienda ha la possibilità di supportare i clienti e i partner con maggior facilità, avendo asset e personale in loco. I clienti ricevono un supporto diretto e da un servizio 24/7 svolto da personale che parla la loro lingua.

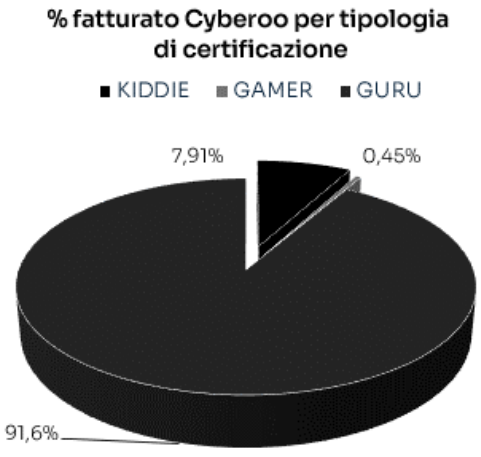
I partner sono inoltre agevolati dalla costruzione di un network e sono in condizione, insieme a Cyberoo, di supportare un maggior numero di aziende nel paese.

## 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 di partnership 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, pre-sales e tecniche:



- **KIDDIE**: il livello è quello di iscrizione iniziale e offre ai partner l'accesso ad 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.

**Capitolo 4**

# CAPITALE RELAZIONALE

# CAPITALE RELAZIONALE
OVERVIEW

0

Nessun data breach
nel 2023

64%

Fornitori situati
in Italia

29 %

Fornitori locali

+55 %

Attività con enti locali,
rispetto al 2022

# 4. Capitale relazionale

## Relazione con i clienti

Cyberoo ha sviluppato, nel corso degli anni, una relazione stabile con le principali aziende che propongono soluzioni e attività specialistiche nell'ambito della Cyber Security sul territorio nazionale ed internazionale.

Il presidio del cliente (partner) costituisce un processo centrale del modello operativo di Gruppo Cyberoo, che opera costantemente per far crescere il valore generato dalla relazione con il cliente stesso.

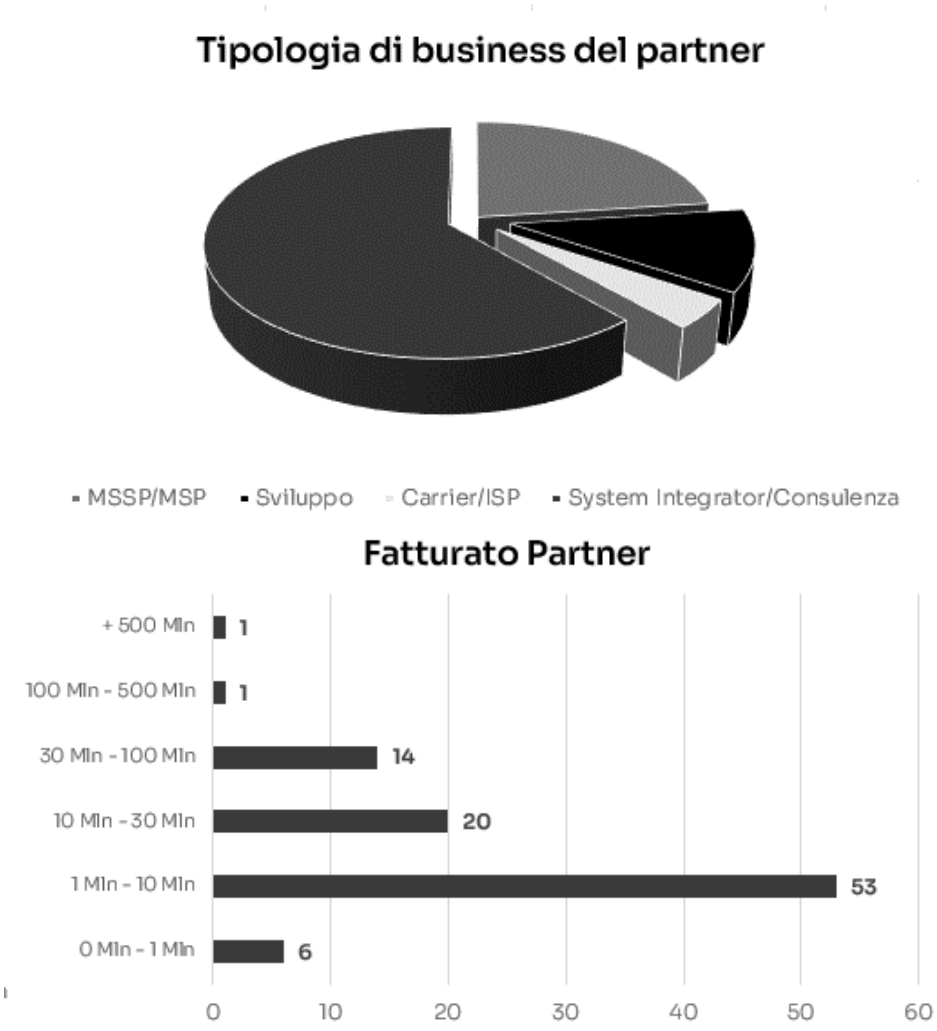
La capacità di soddisfare le esigenze dei clienti rappresenta, infatti, il punto chiave per lo sviluppo di Cyberoo ed è determinante per mantenere e garantire la fiducia del rapporto.

Dall'altro lato, i clienti-partner scelgono Cyberoo poiché vengono garantiti i seguenti fondamentali obiettivi:

- **Valore:** ampliare il proprio portafoglio di offerta con servizi Cyber Security ad alto valore aggiunto, gestiti in modalità H24 con I-SOC altamente specializzato;
- **Fidelizzazione:** i servizi *always on* permettono alle aziende di seguire il cliente in modalità proattiva e continuativa e questo aumenta il grado di fidelizzazione del cliente nei confronti dell'azienda;
- **Ricavi Ricorrenti:** i servizi offerti portano il beneficio economico in termini di ricavi ricorrenti dando maggiore solidità agli economics aziendali.

La base di clienti è caratterizzata da aziende di diversa tipologia che hanno contatti con i clienti finali in funzione della loro propensione alla capacità di indirizzare la tecnologia, di erogare consulenza o di fornire servizi.

Nei grafici seguenti sono riportati i partner per tipologia di business che sviluppano e per fatturato:




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

## La gestione della relazione con i clienti

I partner possono contare su una struttura di risorse altamente qualificate e completamente dedicate allo sviluppo del business da parte di Cyberoo:

- **Channel Manager:** si occupa di sviluppare le strategie di canale e di attivare le relazioni con nuovi Partner;
- **Partner Account Manager:** si affianca ai Partner con l'obiettivo di consolidare e gestire nel lungo termine la relazione, aiutandoli nello sviluppo dell'offerta di cyber security e nelle trattative commerciali con l'End User;
- **Key Account Manager:** sviluppa e mantiene relazioni con l'End User al fine di generare e gestire trattative che verranno assegnate al Partner a seconda di parametri preventivamente definiti;

- **Business Development Manager:** si occupa di supportare il partner nelle attività di formazione e certificazione, analisi del mercato di riferimento, definizione piani di sviluppo del business, presentazioni con i clienti, attività di demo e gestione delle opportunità;
- **Deal Manager:** è la figura interna che si occupa di supportare il partner nella deal registration e per la relativa approvazione.

### Processo di on-boarding dei partner

Il recruitment dei partner avviene sia su base territoriale che in base al modello di sviluppo del business identificato per una data tipologia di cliente. Una volta identificata l'azienda, condiviso il modello di business e raccolta la volontà di diventare partner Cyberoo, segue il processo definito "**on-boarding del partner**", che si articola nei seguenti aspetti:

- Firma del contratto di Partnership e associazione al Cyberoo Black Club;
- Formazione del personale coinvolto del partner (Sales. Pre-sales, Tecnici);
- Condivisione dello Starter kit;
- Definizione del piano commerciale;
- Pianificazione e supporto allo sviluppo del Business (incontri e gestione trattative).

### Formazione e certificazione

Al fine di permettere la completa conoscenza e autonomia del partner sia sul modello di business che sulle soluzioni proposte da Cyberoo, vengono organizzati **corsi specifici di certificazione** per le figure commerciali (sales), di prevendita (Pre-Sales) e tecniche. Vengono svolti con regolarità trimestrale, e sono gratuiti per tutti i partner.

Tra gli argomenti trattati è posta l'attenzione, ad esempio, sugli aspetti di cyber security, su come affrontare il Cyber Crime e viene descritta l'offerta dei servizi Cyberoo (Cyber Security Suite).

### Security Advisor Manager

In seguito all'attivazione delle soluzioni Cyberoo, vengono messe a disposizione dei nostri clienti figure altamente specializzate, note come Security Advisor Manager deputate alla valutazione del livello di servizio offerto. Tali professionisti

pianificano regolari incontri con i nostri clienti, in media on site con cadenza trimestrale, durante i quali vengono definiti sia lo stato attuale dei servizi forniti che un'analisi dettagliata delle principali segnalazioni presenti, al fine di individuare eventuali criticità da sanare attraverso il miglioramento dei processi.

Poiché la consapevolezza della propria postura di sicurezza nello scenario contemporaneo diventa essenziale per poter garantire efficacemente i risultati operativi aziendali, durante la Service Review Cyberoo presenta un documento di **Risk Assessment** volto ad avere contezza di quella che è la situazione del cliente (il livello di rischio) in ambito infrastrutturale, di networking e in tema cybersecurity. Il documento viene poi analizzato da un team di specialisti che, domanda per domanda, va a stabilire il livello di rischio corredando lo stesso di suggerimenti e/o possibili criticità.

Questo ci consente di offrire un servizio di altissimo livello, su misura per le esigenze specifiche di ogni cliente, garantendo la massima efficienza ed efficacia nelle soluzioni implementate.

## Qualità, sicurezza ed affidabilità del servizio

Monitorare costantemente l'andamento dei servizi in essere sul Cliente, permette al Gruppo Cyberoo di raggiungere un duplice obiettivo: **migliorare l'effettiva qualità di erogazione del servizio al cliente e ottimizzare e migliorare internamente i processi interni.**

La direzione aziendale di Cyberoo, sensibile a questa particolare tematica, ha dato vita ad un'intera struttura (***Quality and Customer Relationship Department***) che ha come compito quello di:

- Comprendere, analizzare le aspettative e i bisogni di business dei vari Clienti;
- Garantire la qualità dei processi/servizi in corso di erogazione assicurando il raggiungimento dei target stabiliti a partire dalla fase progettuale;
- Facilitare e migliorare le interazioni tra i vari stakeholders coinvolti, organizzando e supervisionando l'operato degli stessi;
- Sviluppare piani di problem management e service improvement;

- Organizzare riunioni periodiche di rilevazione stato del servizio in aderenza a indicatori e stati di avanzamento del servizio concordati con il Cliente finale;
- Redigere una reportistica inerente le performance, secondo modalità e frequenza concordata;
- Registrare e analizzare i dati relativi ai feedback sul prodotto/servizio;
- Condividere all'occorrenza evoluzioni dei servizi attivi con lo sviluppo di progetti ad hoc (tempi e attività);
- Elevare il livello di fidelizzazione del Cliente/Partner e facilitare la generazione di nuove opportunità.

## Privacy dei clienti e perdita di dati dei clienti

Nessuna contestazione o reclamo è pervenuta da parte dei Clienti in materia di privacy, relativamente a violazioni della normativa sulla protezione dei dati personali (GDPR) che il Gruppo Cyberoo ha trattato in qualità di Titolare o Responsabile del trattamento.

Non sono stati registrati incidenti sulla sicurezza delle informazioni, classificabili come *data breach*, quali divulgazione, furto o perdita di dati dei Clienti.

## Attività di marketing

### Digital360

Cyberoo collabora attivamente con **Digital360**, in qualità di partner digitale per le attività di comunicazione e marketing. Integrando sapientemente storytelling, posizionamento SEO e azioni Social e lavorando sia sui portali del Network Digital360 (outbound) sia su property dell'Azienda (inbound).
L'obiettivo della partnership è valorizzare competenze ed expertise di comunicazione a 360 gradi, generando su base continuativa concrete opportunità di vendita, facendo leva sui contenuti editoriali «gated» (white paper), sugli eventi digitali e sulla Marketing Automation.
Gli altri contenuti digital prodotti con Digtal360, come tool strategici sono:

| Data di inizio Progetto<br>Novembre 2022 | | Data di fine Progetto<br>Novembre 2023 | Completamento Progetto<br>97% |
|---|---|---|---|
| **Contenuti Previsti** | | **Prodotti / Pubblicati** | **In progress** |
| CONTENUTI OPEN | **15** sul **Magazine** | **15** contenuti prodotti e pubblicati | |
| | **3** su **Network Digital360** | **3** contenuti prodotti e pubblicati | |
| | **2 video interviste** su **Network Digital360** | **2** video interviste pubblicate | |
| | **5 Pulse** | **4** Pulse pubblicati | **1** da pianificare |
| | **4 Carousel** | **4** contenuti prodotti e pubblicati | |
| | **3 Linktree** | **3** contenuti prodotti e pubblicati | |
| | **32 contenuti a piano** | **31 contenuti prodotti** | |
| | **30** post social | **60** post aziendali<br>**8** post network | |
| CONTENUTI GATED | **1 Content Syndication** | **Always on** | |
| | **1 Roadshow di tre tappe** | Svolte due tappe | |

In particolare, le attività di marketing di Cyberoo sono dirette soprattutto sui canali **social**: il traffico del sito da gennaio 2020 ad oggi ha totalizzato circa 215 mila sessioni. Negli ultimi 12 mesi, i contenuti societari sono stati diffusi sui **canali social del Network Digital360** Linkedin, Facebook, Twitter e sui canali social di Cyberoo.

La collaborazione con Digital360 continuerà per tutto il 2023 con i seguenti obiettivi:

- potenziare il posizionamento e la reputation di Cyberoo;
- ampliare la community building di Cyberoo;
- potenziare l'automazione dei processi di lead generation ed i processi interni a Cyberoo.

### Marketing Arena

Cyberoo collabora attivamente anche con **Marketing Arena**, in qualità di partner digitale per elaborare una strategia di digital marketing volta ad aumentare la *brand awareness* e la consapevolezza degli utenti sul tema della cyber security.

A questo scopo sono state attivate campagne di *digital advertising* su diversi canali, indirizzate verso la promozione di una landing page per richiesta di informazioni e quiz sulla cyber security in Outgrow (piattaforma integrata sul sito web tramite landing page e dedicata appositamente ai quiz).

La collaborazione proseguirà fino a metà 2023 con budget da destinare all'advertising online sui diversi canali.

I focus per gennaio 2023 sono divisi su 4 campagne:

- Campagna Lead generation in piattaforma LinkedIn;
- Campagna Google Search con nuova Key strategy;
- Campagna Organico;
- Campagna Education.

### 27Digital

Tra il 2022 e il primo semestre del 2023 Cyberoo ha gestito il progetto di rifacimento sito web, con l'obiettivo di comunicare in modo chiaro e semplice la nuova *brand identity*, così composta:

- garantire una qualità di servizio vicina al mondo luxury;
- apparire come punto di riferimento Cyber Security in Italia;
- assicurare un'immagine dall'effetto visivo immediato.

Il nuovo sito web è un'esperienza per l'utente, oltre che essere fruibile anche dall'estero grazie ad un sistema multilingua, comunicando la nuova brand identity tramite uno storytelling e una User Experience unici rispetto alla concorrenza.

## Fornitori: 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 ed approvare un Fornitore (sia di prodotti che servizi) che possa avere influenza sulla qualità e sicurezza delle informazioni dei prodotti e servizi forniti dal Gruppo Cyberoo, l'Azienda 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 macro categorie trattate sono riassumibili in: ***sostenibilità ambientale, etica, rispetto dei diritti e gestione dei fornitori*.**

| NUMERO FORNITORI [4] | FY 2021 | | FY 2022 | | FY 2023 | |
|---|---|---|---|---|---|---|
| | n. | % sul totale | n. | % sul totale | n. | % sul totale |
| Numero di fornitori LOCALI[5] | 163 | **40%** | 164 | **32%** | 188 | **29%** |
| Numero di fornitori situati in ITALIA | 220 | **54%** | 308 | **60%** | 418 | **64%** |
| Numero di fornitori situati in EUROPA | 7 | **2%** | 19 | **4%** | 27 | **4%** |
| Numero di fornitori situati in AMERICA | 6 | **1%** | 12 | **2%** | 11 | **2%** |
| Numero di fornitori situati in ASIA | 2 | **0%** | 3 | **1%** | 1 | **0%** |
| Numero di fornitori situati nel RESTO DEL MONDO | 9 | **2%** | 10 | **2%** | 12 | **2%** |
| **TOTALE FORNITORI** | 407 | **100%** | 516 | **100%** | 657 | **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 aziendalmente si è deciso di orientarsi su fornitori i più locali possibile.

## 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 ad intervalli non superiori a 12 mesi (ad 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.

[4] I dati del biennio 2021 e 2022 sono stati aggiornati, poiché dal 2023 si è utilizzata una metodologia differente per l'estrazione del numero dei fornitori

[5] Per fornitori locali si intende i fornitori provenienti dall'Emilia Romagna

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 2 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 3 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 ad esigenze di vendite transazionali, di canoni di servizio, sia di riapprovvigionamento interno.

## Le relazioni con il territorio

Cyberoo è molto attenta alle questioni che attengono la sfera sociale e del territorio, siano esse comunità locali o internazionali.

Nel 2023 Cyberoo ha svolto incontri, al fine di divulgare i risultati delle valutazioni d’impatto ambientale e sociale, attività di stakeholder engagement ed ha organizzato comitati di impresa e per la sicurezza e la salute sul lavoro.

Rispetto al 2022, come riportato nella tabella sottostante, la Società ha svolto il 73% in più di attività che prevedono il coinvolgimento delle attività locali.

| ATTIVITÀ CHE PREVEDONO IL COINVOLGIMENTO DELLE COMUNITÀ LOCALI, VALUTAZIONI D'IMPATTO E PROGRAMMI DI SVILUPPO | FY 2022 | | FY 2023 | |
|---|---|---|---|---|
| | n. | **% sul totale** | n. | **% sul totale** |
| Valutazioni d'impatto sociale basate su processi partecipativi | - | **0%** | - | **0%** |
| Valutazioni d'impatto ambientale | - | **0%** | - | **0%** |
| Incontri organizzati (conferenze, workshop, focus group, ecc..) per divulgare i risultati delle valutazioni d'impatto ambientale e sociale | 1 | **9%** | 2 | **11%** |
| Programmi di sviluppo comunitari locali | - | **0%** | - | **0%** |

| | | | | |
|---|---|---|---|---|
| Attività di stakeholder engagement | 10 | **91%** | 15 | **79%** |
| Comitati di consultazione aperti alla comunità locale e processi che includono categorie vulnerabili | - | **0%** | - | **0%** |
| Comitati di impresa, comitati per la sicurezza e la salute sul lavoro | - | **0%** | 2 | **11%** |
| Procedimenti formali di gestione dei reclami provenienti dalla comunità locale | - | **0%** | - | **0%** |
| **TOTALE ATTIVITÀ** | **11** | **100%** | **19** | **100%** |

## CRIT

A luglio 2020, Cyberoo è entrata a far parte del Network Fornitori Accreditati di CRIT, realtà modenese che sviluppa progetti di ricerca, trasferimento di conoscenze tecnologiche ed analisi di informazioni tecnico-scientifiche.

Questa partnership ha consentito al Gruppo di usufruire dei servizi di innovazione collaborativa offerti da CRIT ed entrare in contatto con altre realtà innovative italiane e di consentire al network e soci del CRIT di elevare il livello di expertise nell'ambito della sicurezza informatica.

Con CRIT, Cyberoo ha realizzato i seguenti progetti:

- nel 2020, un webinar intitolato "**DEEP & DARK WEB: la parte sommersa della rete**", un evento formativo volto ad aggiornare le imprese del network CRIT sui pericoli connessi al *Deep & Dark Web* destinato a una piattaforma interna riservata agli associati. In quella che viene definita "La parte sommersa della rete" è infatti possibile trovare una moltitudine di informazioni sensibili e strategiche offerte in via illegale. Un vero e proprio bottino digitale (costituito da password, informazioni sulla proprietà intellettuale, dati economici e finanziari delle aziende, ecc.), utilizzabile da malintenzionati e criminali informatici per ottenerne profitto o, molto peggio, come principio di un attacco più complesso. Grazie alla competenza dei tecnici qualificati di Cyberoo, i partecipanti al webinar hanno potuto accrescere e qualificare le proprie conoscenze in materia di sicurezza informatica ed attivare efficaci strategie difensive;
- nel 2021, è stata svolta **formazione online**: un ciclo di 3 webinar da 50 minuti l'uno circa per cui Cyberoo ha messo a disposizione relatori esperti, occupandosi di sviscerare in capitoli i macro-argomenti della Cyber Security fondamentali per accrescere le competenze di ogni dipendente di

azienda e manager del network del CRIT. In questa formazione, gli esperti di Cyberoo si sono messi a disposizione per mostrare come andare oltre il semplice firewall o antivirus, guidando i partecipanti nel mondo del Deep e Dark Web e per elevare la sicurezza delle aziende e proteggere l'identità digitale;

- nel 2022 un webinar intitolato "**AGE OF CYBERCRIME: Strumenti, metodologie e strategie di difesa**", un evento formativo volto ad aggiornare le imprese del network CRIT (personale tecnico come IT Manager, CISO e CIO) e manager clienti di Cyberoo. In questo webinar, Cyberoo ha messo a disposizione alcuni cyber security specialist e ripercorso l'evoluzione del *cyber crime* in Italia e le migliori strategie con cui le organizzazioni possono difendersi dagli attacchi informatici. Al webinar si sono iscritte 89 persone a cui sono seguite attività di follow-up tramite newsletter di Cyberoo e del CRIT, con condivisione delle slide di presentazione utilizzate durante l'evento e il video registrato.
- Nel 2023 è stato sviluppato un ciclo di tre webinar incentrati su diversi aspetti della sicurezza da una panorami degli attacchi e i limiti dei servizi di Endpoint Protection della protezione della filiera di fornitura fino all'importanza della Cyber Resilience e la gestione del rischio.

### Confindustria – RetIndustria Servizi

In collaborazione con RetIndustria Servizi nel 2022, Cyberoo ha realizzato un webinar "**LA RETE CONFINDUSTRIA PER LA SICUREZZA DELLE AZIENDE ITALIANE**" dedicato esclusivamente alle Confindustrie e associazioni di territorio. Il Gruppo ha messo a disposizione personale interno per formare le Confindustrie sulle minacce informatiche provenienti da luoghi esterni all'ecosistema aziendale, e per comprendere come tutelare la *business continuity* delle aziende del territorio italiano.

## Collaborazioni con Università, scuola ed enti di ricerca

### Unindustria Reggio Emilia - Istituto Scaruffi

Cyberoo, appartenente al Club Digitale di Unindustria Reggio Emilia, a marzo del 2022, poi proseguito nel 2023, ha avviato un progetto di collaborazione didattica

con l'**Istituto Tecnico Superiore Scaruffi-Levi-Tricolore**, volto all'avvicinamento dei ragazzi alle tematiche del lavoro e dell'impresa. Il progetto ha coinvolto due classi del quinto anno dell'indirizzo Sistemi Informativi Aziendali, per un totale di 28 giovani, prevedendo una serie di incontri durante i quali è stata data loro la possibilità di confrontarsi con la realtà aziendale in un percorso di conoscenza che li ha portati a respirare momenti di vita professionale e casi di operatività concreta legata al mondo IT e della cyber security, dalle nozioni base ai rischi del deep e dark web fino ai recenti attacchi hacker a danno di multinazionali e istituzioni.
Il progetto, durante le settimane di realizzazione ha previsto anche lo svolgimento di un elaborato in autonomia, che ha visto gli studenti alla prova con un caso concreto di attacco hacker. Dopo un'analisi OSINT (Open Source Intelligence) infatti, i ragazzi sono stati chiamati a valutare l'impatto sulla reputazione aziendale generato da una fuga di dati e sulle possibili azioni da intraprendere per limitare il danno a carico dell'impresa.

### Confindustria Area Emilia Centro

Con **Confindustria Area Emilia Centro** Cyberoo ha realizzato nel 2022 due progetti:

- *Pillole formative* : 5 video da 15 minuti l'uno, destinati a una piattaforma interna riservata agli associati; Cyberoo si è occupata di sviluppare i macro-argomenti della Cyber Security;
- *Formazione online*: Cyberoo ha incontrato due classi quarte del Liceo Steam Emilia di Bologna tramite live webinar. Mettendo a disposizione una figura del marketing e uno specialista Cyber Security, il Gruppo ha presentato l'attività dell'azienda attraverso i temi principali del mondo della sicurezza informatica, con l'obiettivo di formare e sensibilizzare gli alunni sul tema e sul mondo del lavoro.

### Università Cattolica Del Sacro Cuore

Cyberoo ad aprile del 2021 ha avviato una collaborazione che la vede partecipare, come membro del Comitato di Indirizzo, al corso di laurea in "Innovazione e Imprenditorialità Digitale" presso la facoltà di Economia e Giurisprudenza dell'Università Cattolica del Sacro Cuore, campus di Cremona. La convezione prevede il contributo attivo di Cyberoo nella definizione e realizzazione di lezioni,

seminari e project work che valorizzano il percorso accademico dei futuri manager, anche con l'esperienza sul campo mediante stage e tirocini formativi in azienda.
Forte di una qualificata esperienza nei campi della digital transformation e della cyber security, Cyberoo punta a definire insieme all'Università Cattolica nuove linee di ricerca volte al trasferimento tecnologico nell'ambito della sicurezza informatica, attraverso un processo di sensibilizzazione dei giovani e contribuendo alla formazione di risorse altamente specializzate in ambito IT.
La convenzione si inserisce in uno scenario caratterizzato da un "ritardo digitale" che, stando ai dati 2020 della Commissione Europea, vede l'Italia classificarsi agli ultimi posti in Europa per quanto riguarda il livello di digitalizzazione del sistema economico e il conseguente ritardo anche sul fronte delle competenze digitali. Con il nuovo corso di laurea magistrale attivato dalla Cattolica, la sfida è colmare progressivamente questo ritardo ma anche coniugare saperi diversi e competenze tecnico-scientifiche inerenti la digitalizzazione e la cyber security, a conferma della necessità di una formazione sempre più ampia, trasversale.
In aggiunta, insieme all'Università Cattolica del Sacro Cuore, Cyberoo ha realizzato i seguenti progetti:

- per la lezione di Economia digitale, a marzo del 2022, si è approfondito il tema della cyber security, attraverso contenuti sul tema della sicurezza, minacce, rischi, necessità e scelte imprenditoriali;
- a novembre 2022, Cyberoo ha partecipato allo "**SPEED INTERVIEWS-STAGE DAY Circuito di selezione "colloqui lampo"** presso il Campus Santa Monica a Cremona.
- Nel 2023 ben tre studenti del corso di "Innovazione e Imprenditorialità Digitale" sono stati selezionati per uno stage e di cui due sono stati confermati per un contratto di apprendistato.

## CISL

Nel 2023 Cyberoo ha supportato il sindacato CISL nella formazione dei suoi associati che all'interno delle rispettive aziende si occupano delle relazioni sindacali nei processi decisionali.
Le due iniziative di formazione si sono tenute a Napoli il 28 febbraio e a Matera il 5 ottobre e avevano l'obiettivo di dare gli strumenti base della comprensione dei

rischi cyber security e quindi l'importanza di occuparsi dell'argomento anche al fine di tutelare la sicurezza e il benessere dei dipendenti.

## Comunicazione interna ed esterna

### Comunicazione interna

Per quanto riguarda la comunicazione interna aziendale, vengono svolte tutta una serie di attività di comunicazione finalizzate a creare una rete interna di flussi informativi e mirate con lo scopo di diffondere informazioni, saperi e conoscenze, oltre che rendere chiari e condivisi gli obiettivi dell'azienda ai dipendenti.
Vengono presi in considerazione aspetti come la qualità di vita nell'ambiente lavorativo, l'identità di visioni e obiettivi che accomunano il brand ai suoi dipendenti, la volontà di questi ultimi di farsi ambasciatori del brand e dei suoi servizi. Tutto questo contribuisce più in generale a migliorare il clima e l'ambiente di lavoro.
Quanto agli strumenti utilizzati nella strategia di comunicazione interna, ve ne sono alcuni più tradizionali come la posta elettronica, altri invece sfruttano i meccanismi dei nuovi ambienti digitali e collaborativi per favorire le interazioni tra i propri dipendenti.
Cyberoo utilizza anche la intranet aziendale (Microsoft SharePoint) per la gestione dei documenti e dei contenuti ad uso aziendale. L'obiettivo è quello di connettere le persone e consentire la condivisione e la comunicazione nell'Azienda stessa, permettendo una riduzione del numero di e-mail, la possibilità di scambiare file o di archiviarli in cloud lavorare con una logica wiki e collaborativa sullo stesso documento.

## Comunicazione agli investitori finanziari

Cyberoo grazie alla collaborazione con l'agenzia di consulenza *Reputation Value* di Milano, specializzata in comunicazione e ufficio stampa, è capace di interagire e comunicare con ogni mezzo di comunicazione presente nell'attuale contesto mediatico, con lo scopo di far conoscere a un vasto pubblico di lettori qualificati la propria storia, professionalità, capacità di innovazione, attività e soluzioni.
L'attività con Reputation Value è focalizzata nella costruzione dei contenuti relativi a eventi, risultati finanziari, cambiamenti aziendali, novità e successi con particolare attenzione agli aspetti strategici della narrazione e nella loro

veicolazione ai mass media (tramite comunicati stampa, interviste, conferenze stampa, ecc).

Per quanto riguarda le attività di **Investor Relations** (IR), Cyberoo gestisce la comunicazione finanziaria e istituzionale con investitori e intermediari finanziari come banche e analisti, chi si occupa della dematerializzazione delle azioni e della tenuta del libro soci o dei rapporti con Monte Titoli.

Cyberoo intrattiene anche una relazione con gli analisti finanziari che hanno effettuato studi sulla società.

A questo proposito ogni anno vengono organizzate, a seguito della pubblicazione dei dati di bilancio annuali e semestrali, delle conference call con gli investitori, che vengono invitati a partecipare tramite newsletter aziendale.

Durante il 2023, Cyberoo ha partecipato a differenti eventi rivolti agli investitori:

- Mid&Small London – 19 aprile 2023;
- KT&Partners Annual Investors Summit Day – 07 giugno 2023;
- European Midcap Event Paris – 23 giugno 2023;
- Mid&Small Virtual – 28/29 giugno 2023;
- Le Eccellenze del Made in Italy – 27 settembre 2023;
- Madrid Intermonte Virtual – 16 novembre 2023,
- Mid&Small Milano – 22 novembre 2023.

### Confidustria – Farete 2023

Cyberoo, in qualità di Partner RetIndustria, ha partecipato alla **Fiera Farete** che si è tenuta il 6 e 7 settembre 2023 a Bologna, promossa e organizzata da Confindustria Emilia. I due giorno sono stati dedicati al networking e agli incontri B2B tra le imprese.

Una grande vetrina delle produzioni, delle lavorazioni, della subfornitura e dei servizi che anni ha visto la presenza di più di 550 aziende coinvolte, oltre 90 workshop tematici in programma, 77 operatori internazionali provenienti da 21 Paesi, più di 700 appuntamenti B2B.

Con questa occasione, Cyberoo ha avuto la possibilità di incontrare oltre 120 aziende e di essere presente sui materiali di comunicazione della Fiera: catalogo espositori cartaceo e web; “Fare” House Organ di Confindustria Reggio Emilia e nel materiale delle 2.500 shopper consegnate durante la Fiera.

# Le donazioni

Ogni anno nel periodo natalizio Cyberoo devolve un contributo a un ente o associazione che sposi uno dei valori dell'azienda:

- nel 2019, è stata conferita una donazione a ***Fondazione Pangea Onlus***, un'organizzazione no profit che dal 2002 lavora per favorire lo sviluppo economico e sociale delle donne, delle loro famiglie e delle comunità circostanti;
- nel 2021, è stata conferita una donazione a **Treedom s.r.l.**, azienda italiana che si occupa di riforestazione nel mondo. Grazie a questo, Cyberoo ha permesso che fossero piantati 100 alberi tra Africa e Sud America;
- nel 2022 è stata conferita una donazione a **Granello di Senape APS**, una associazione di giovani che, a titolo puramente volontario, offrono aiuto alle persone emarginate dalla società a causa di problemi economici o culturali.
- Nel 2023 Cyberoo ha deciso di sostenere "Bullismo No Grazie", l'associazione no profit nata con l'obiettivo di prevenire, combattere ed informare sui fenomeni dilaganti, e dei relativi traumi di chi ne è vittima, del bullismo e del cyberbullismo.

**Capitolo 5**

# CAPITALE ECONOMICO FINANZIARIO

# CAPITALE ECONOMICO FINANZIARIO
OVERVIEW

20 mil. €
Valore economico generato

14,8 mil. €
Valore economico distribuito

# 5. Capitale economico-finanziario

## Andamento della gestione

Il bilancio del Gruppo Cyberoo, relativo all'esercizio 2023, si è chiuso con un utile di 3.963.448 euro rispetto al risultato positivo di 2.787.941 euro realizzato nell'esercizio 2022. I ricavi del Gruppo hanno oltrepassato i 20 milioni di euro, con un incremento del 29% rispetto ai 15.5 milioni di euro realizzati 31 dicembre 2022. Positivo è stato anche l'andamento dei principali indicatori economici:

- l'EBITDA del 2023 è risultato pari al 46,3% dei ricavi ed è in crescita del 37,7% rispetto all'esercizio precedente;
- l'EBIT, pari a 6,07 milioni di euro, è incrementato del 39,8% rispetto al 2022.

## Il valore economico generato e distribuito

Il prospetto che evidenzia il valore generato e distribuito viene elaborato sulla base del Conto Economico del bilancio di esercizio, con l'obiettivo di dare evidenza del valore economico direttamente generato dal Gruppo Cyberoo e la sua distribuzione agli stakeholder interni ed esterni.

Il **Valore Economico generato** si riferisce al Valore della produzione come da Bilancio di esercizio (Ricavi e Altri ricavi operativi), al netto delle perdite su crediti ed integrato dei proventi finanziari. Il **Valore Economico trattenuto**, che per il 2023 è pari a 5,59 milioni Euro, è relativo alla differenza tra Valore Economico generato e distribuito e comprende gli ammortamenti dei beni materiali ed immateriali oltre alla fiscalità differita.

| VALORE AGGIUNTO | 2021 | 2022 | 2023 |
|---|---|---|---|
| Ricavi | 10.254.276 | 17.287.908 | 20.013.526 |
| Altri proventi | 225.075 | 275.268 | 271.209 |
| Proventi finanziari | 20.580 | 9.873 | 95.252 |
| **Totale valore economico generato** | **10.499.931** | **17.573.049** | **20.379.987** |
| Costi operativi | 4.482.549 | 6.202.565 | 6.945.130 |
| Remunerazione del personale | 3.540.893 | 4.589.142 | 5.596.319 |

| | | | |
|---|---|---|---|
| Remunerazione dei finanziatori | 108.301 | 239.838 | 489.446 |
| Remunerazione degli investitori | - | - | - |
| Remunerazione della Pubblica Amministrazione | 108.337 | 1.311.687 | 1.716.523 |
| Liberalità esterne | - | 49.700 | 35.250 |
| **Totale valore economico distribuito** | **8.240.080** | **12.392.933** | **14.782.668** |
| **Valore economico trattenuto** | **2.259.851** | **5.180.116** | **5.597.319** |

## 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.

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 ad una specifica azienda, degli attacchi potenziali in termini di confidenzialità, integrità e disponibilità dei dati e dei servizi.

## Approccio fiscale

Il Gruppo Cyberoo si impegna ad applicare la legislazione fiscale in vigore, assicurando che siano osservati lo spirito e lo scopo che la norma e l'ordinamento prevedono per la materia oggetto di interpretazione. Nei casi in cui la disciplina fiscale alimenti dubbi interpretativi o difficoltà applicative, viene perseguita una linea interpretativa ragionevole, avvalendosi della consulenza di qualificati professionisti esterni.

La sede fiscale del Gruppo è in Italia, dove vengono corrisposte le imposte.

L'approccio alla fiscalità del Gruppo Cyberoo è improntato alla trasparenza ed alla totale aderenza alle normative locali, curando l'ambito della compliance e intercettando tutte le novità normative per ottemperare nelle tempistiche previste.

L'obiettivo del Gruppo, in questo ambito, è assicurare che:

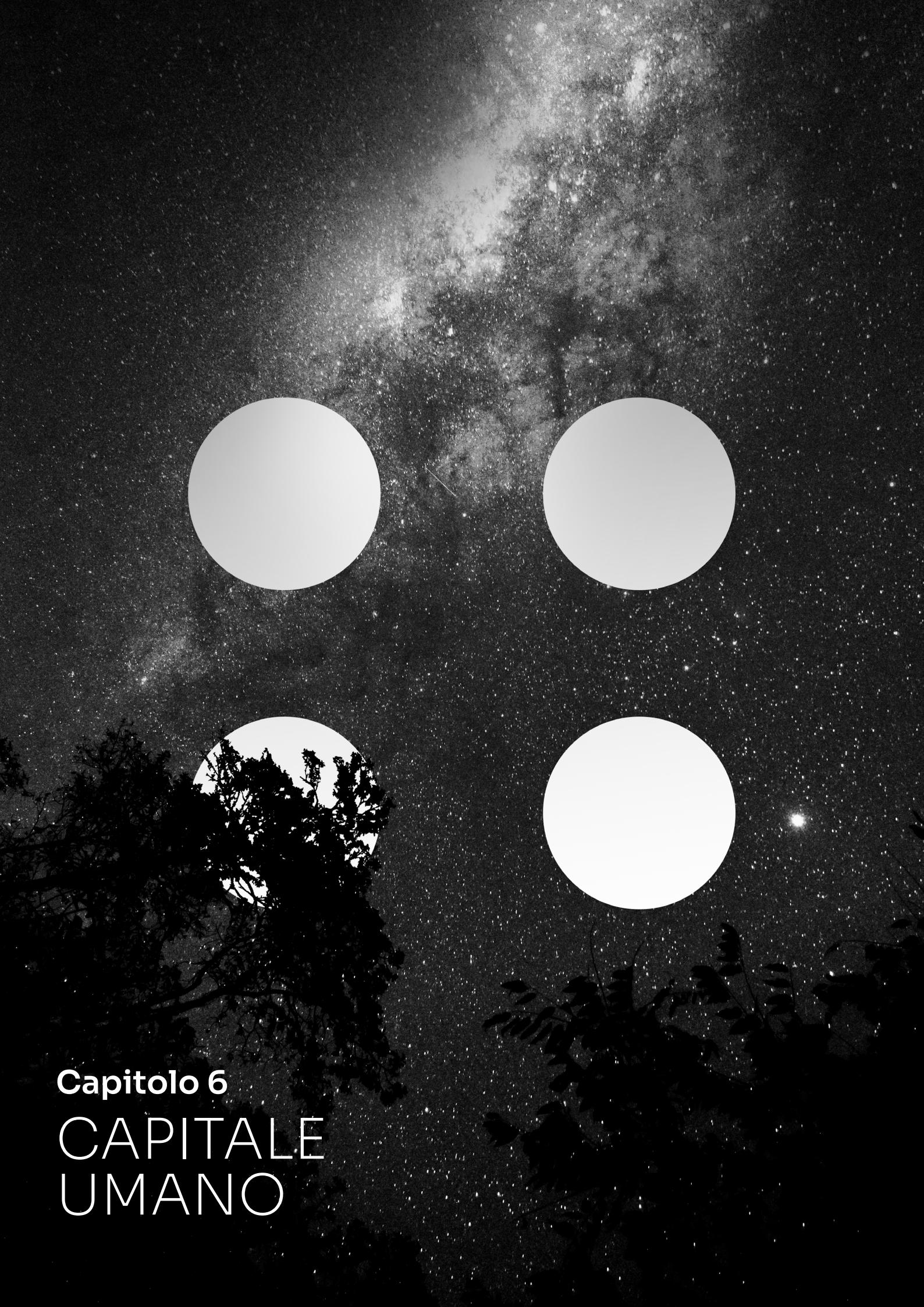
- le dichiarazioni sul reddito e sul valore aggiunto vengano redatte in conformità alla disciplina vigente;
- il calcolo delle imposte avvenga nel rispetto dei principi tributari elaborati dalle norme vigenti e dalle circolari emesse dai vari uffici dell'amministrazione finanziaria;
- le operazioni di compensazione dell'IVA e le richieste di rimborso delle imposte abbia per oggetto crediti fiscali realmente sussistenti, certi e verificabili;
- le dichiarazioni sul valore aggiunto originate da rapporti transfrontalieri vengano depositate nel rispetto delle tempistiche e della disciplina tributaria.

Gli impatti fiscali sono tenuti in debita considerazione nella redazione della pianificazione strategica e operativa aziendale e rappresentano un essenziale elemento di valutazione del conseguente impatto economico-sociale.

La governance del controllo fiscale è demandata alla Direzione Amministrativa e Bilancio che, anche tramite il supporto di consulenti esterni, vigila sulla correttezza delle operazioni ed applica la corretta normativa.

Tutte le richieste effettuate al Gruppo Cyberoo dalle autorità fiscali vengono gestite all'interno del corretto flusso informativo con un approccio da parte del Gruppo di totale trasparenza e dialogo costruttivo: i dati fiscali ed il loro dettaglio sono regolarmente esposti nel bilancio annuale di esercizio e nella relativa Nota integrativa e quindi messi a disposizione dei soci e di tutti gli stakeholder.

Nel corso del triennio 2021-2023 non sono stati registrati contenziosi o contestazioni di tipo fiscale e, alla data del presente documento, non sono in essere contenziosi di carattere fiscale di rilievo.



**Capitolo 6**

# CAPITALE UMANO

# **CAPITALE UMANO**
# OVERVIEW

100 %
Assunti a tempo
indeterminato

97 %
Contratti full-time

62 %
Dipendenti con età compresa
tra i 30 e i 50 anni

50 %
Senior Manager assunti
dalla comunità locale

# 6. 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 l'Azienda 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 inter-aziendale mirate a rafforzare il legame tra Azienda e 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 Cyber Security.

Alta è 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 ed 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 l'azienda 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, registrando un aumento del 25% rispetto al 2022 e del 32% rispetto al 2021.

| Numero dipendenti [6] | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **Donne** | **Uomini** | **Totale** | **Donne** | **Uomini** | **Totale** | **Donne** | **Uomini** | **Totale** |
| | 17 | 54 | **71** | 19 | 56 | **75** | 21 | 73 | **94** |

## Le forme di impiego

| Numero dipendenti per tipologia di contratto / per genere | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| **Numero dipendenti** | **Donne** | **Uomini** | **Totale** | **Donne** | **Uomini** | **Totale** | **Donne** | **Uomini** | **Totale** |
| Contratto a tempo indeterminato | 17 | 53 | 70 | 19 | 56 | 75 | 21 | 73 | **94** |
| Contratto a tempo determinato | - | 1 | 1 | - | - | - | - | - | **-** |
| **Totale** | **17** | **54** | **71** | **19** | **56** | **75** | **21** | **73** | **94** |

[6] 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.

| Numero dipendenti per tipo di impiego / genere | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **Donne** | **Uomini** | **Totale** | **Donne** | **Uomini** | **Totale** | **Donne** | **Uomini** | **Totale** |
| Contratto full time | 16 | 53 | 69 | 18 | 55 | 73 | 20 | 71 | **91** |
| Contratto part time | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 2 | **3** |
| Contratto con orario variabile | - | - | - | - | - | - | - | - | **-** |
| **Totale** | **17** | **54** | **71** | **19** | **56** | **75** | **21** | **73** | **94** |

| Numero dipendenti per tipologia di contratto / per genere | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| | **Donne** | **Uomini** | **Totale** | **Donne** | **Uomini** | **Totale** | **Donne** | **Uomini** | **Totale** |
| Stagisti e tirocinanti | - | - | - | - | 1 | 1 | 3 | - | **3** |
| CO.CO.CO | 1 | - | 1 | - | - | - | - | - | **-** |
| **Totale** | **1** | **-** | **1** | **-** | **1** | **1** | **3** | **-** | **3** |

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

Nel 2023, il 100% dei dipendenti è assunto tramite contratto a tempo indeterminato a dimostrazione della stabilità e valorizzazione del capitale umano all'interno di Cyberoo. Il part time viene richiesto principalmente per motivi familiari.

## Diversità

La componente maschile è preponderante, spiegata anche dalle caratteristiche del settore IT: la percentuale media di donne nel settore della cyber security in Italia, infatti, è del 15% circa. Cyberoo con il 22% di presenza femminile in organico è quindi in una posizione favorevole rispetto alla media del mercato: la totalità dei dipendenti di genere femminile, occupa una posizione impiegatizia (21 teste su 94). Il 96% della popolazione aziendale è rappresentata dalla figura degli impiegati.

| Dipendenti per categoria/ genere | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| | Donne | Uomini | Totale | Donne | Uomini | Totale | Donne | Uomini | Totale |
| Dirigenti | - | - | - | - | - | - | - | - | - |
| Quadri[7] | - | 3 | 3 | - | 3 | 3 | - | 4 | **4** |
| Impiegati | 17 | 51 | 68 | 19 | 53 | 72 | 21 | 69 | **90** |
| Operai | - | - | - | - | - | - | - | - | **-** |
| **Totale** | **17** | **54** | **71** | **19** | **56** | **75** | **21** | **73** | **94** |

Di seguito si riportano le percentuali di dipendenti divise per categoria e genere, rapportati al totale dei dipendenti al 31 dicembre 2021, 2022 e 2023. Il rapporto tra la percentuale dei dipendenti donne e uomini risulta abbastanza costante nel tempo, in particolare nell'area degli impiegati.

| Dipendenti per categoria/ Genere % | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| | Donne | Uomini | Totale | Donne | Uomini | Totale | Donne | Uomini | Totale |
| Dirigenti | - | - | - | - | - | - | - | - | **-** |
| Quadri | - | 4% | 4% | - | 4% | 4% | - | 4% | **4%** |
| Impiegati | 24% | 72% | 96% | 25% | 71% | 96% | 22% | 74% | **96%** |
| Operai | - | - | - | - | - | - | - | - | **-** |
| **Totale** | **24%** | **76%** | **100%** | **25%** | **75%** | **100%** | **22%** | **78%** | **100%** |

Nel 2023 la maggior parte dei dipendenti di Cyberoo ha un'età compresa tra i 30 ed i 50 anni (62%), i quali risultano per il 98% impiegati e per il restante 2% quadri.

| Dipendenti per categoria/ fascia d'età | 2021 | | | | 2022 | | | | 2023 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Fino a 29 anni | Da 30 a 50 anni | Oltre 50 anni | Totale | Fino a 29 anni | Da 30 a 50 anni | Oltre 50 anni | Totale | Fino a 29 anni | Da 30 a 50 anni | Oltre 50 anni | Totale |
| Dirigenti | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Quadri | - | 1 | 2 | 3 | - | 1 | 2 | 3 | - | 1 | 3 | **4** |
| Impiegati | 19 | 41 | 8 | 68 | 17 | 47 | 8 | 72 | 27 | 57 | 6 | **90** |
| Operai | - | - | - | - | - | - | - | - | - | - | - | **-** |
| **Totale** | **19** | **42** | **10** | **71** | **17** | **48** | **10** | **75** | **27** | **58** | **9** | **94** |

[7] La percentuale di Senior manager (quadri) presso le sedi operative dell'Azienda che sono stati assunti dalla comunità locale è pari al 50%.

| Dipendenti per categoria /fascia d'età % | 2021 | | | | 2022 | | | | 2023 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Fino a 29 anni | Da 30 a 50 anni | Oltre 50 anni | Totale | Fino a 29 anni | Da 30 a 50 anni | Oltre 50 anni | Totale | Fino a 29 anni | Da 30 a 50 anni | Oltre 50 anni | Totale |
| Dirigenti | - | - | - | - | - | - | - | - | - | - | - | **-** |
| Quadri | - | 1% | 3% | 4% | - | 1% | 3% | 4% | | 1% | 3% | **4%** |
| Impiegati | 27% | 58% | 11% | 96% | 22% | 63% | 11% | 96% | 29% | 61% | 6% | **96%** |
| Operai | - | - | - | - | - | - | - | - | - | - | - | **-** |
| **Totale** | **27%** | **59%** | **14%** | **100%** | **22%** | **64%** | **14%** | **100%** | **29%** | **62%** | **9%** | **100%** |

L'azienda 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.

## Turnover

Nel triennio 2021-2023 la popolazione aziendale è cresciuta passando da 71 unità al 31/12/2021 a 94 unità al 31/12/2023. È stato assunto principalmente personale già qualificato e con elevata esperienza nelle attività che compongono il business aziendale, con età compresa tra i 30 e i 50 anni.

Le percentuali del turnover sono state calcolate, in aderenza alla richiesta del GRI Standard, sul totale dei dipendenti al 31 dicembre di ciascun anno, andando a confrontare la percentuale di turnover positivo con quella di turnover negativo. Il primo risulta essere sempre più alto, a conferma della crescita dell'azienda riuscendo non solo a coprire le uscite ma ad aumentare annualmente la numerosità dei dipendenti, sintomo di un'azienda che è riuscita a mantenere sempre vivo il proprio trend di crescita.

| Assunzioni[8] | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| | Donne | Uomini | Totale | Donne | Uomini | Totale | Donne | Uomini | Totale |
| Fino a 29 anni | 1 | 10 | 11 | 4 | 6 | 10 | 7 | 9 | 16 |
| Da 30 a 50 anni | 7 | 19 | 26 | 3 | 16 | 19 | 4 | 16 | 20 |
| Oltre 50 anni | - | 4 | 4 | 1 | - | 1 | 0 | 1 | 1 |
| **Totale** | **8** | **33** | **41** | **8** | **22** | **30** | **11** | **26** | **37** |

[8] All'interno delle tabelle "Assunzioni" e "Cessazioni" sono inclusi, nel triennio di riferimento, anche i tirocinanti e gli stagisti.

| Cessazioni | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| | Donne | Uomini | Totale | Donne | Uomini | Totale | Donne | Uomini | Totale |
| Fino a 29 anni | - | 2 | 2 | 2 | 2 | 4 | 0 | 5 | 5 |
| Da 30 a 50 anni | 4 | 18 | 22 | 2 | 16 | 18 | 6 | 6 | 12 |
| Oltre 50 anni | - | 2 | 2 | 1 | 3 | 4 | 0 | 1 | 1 |
| **Totale** | **4** | **22** | **26** | **5** | **21** | **26** | **6** | **12** | **18** |

| Tasso di turnover | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| | Donne | Uomini | Totale | Donne | Uomini | Totale | Donne | Uomini | Totale |
| Turnover negativo - cessazioni | 24% | 41% | **37%** | 26% | 38% | **35%** | 29% | 16% | **45%** |
| Turnover positivo - assunzioni | 47% | 61% | **76%** | 42% | 39% | **40%** | 52% | 36% | **88%** |

## I congedi parentali

| Congedi parentali | 2021 | | | 2022 | | | 2023 | | |
|---|---|---|---|---|---|---|---|---|---|
| | Donna | Uomo | Totale | Donna | Uomo | Totale | Donna | Uomo | Totale |
| Dipendenti che hanno avuto diritto al congedo parentale | 1 | 1 | **2** | - | - | **-** | 4 | 4 | **8** |
| Dipendenti che hanno usufruito del congedo parentale | 1 | 1 | **2** | - | - | **-** | 4 | 4 | **8** |
| Dipendenti che sono tornati al lavoro durante il periodo di rendicontazione dopo aver usufruito del congedo parentale | 1 | 1 | **2** | - | - | **-** | 1 | 4 | **5** |
| Dipendenti che sarebbero dovuti tornare al lavoro durante il periodo di rendicontazione dopo aver usufruito del congedo parentale | 1 | 1 | **2** | - | - | **-** | 1 | 4 | **5** |
| 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 | 1 | **2** | - | - | **-** | 1 | 3 | **4** |

## Formazione e competenze

L'Azienda per gli anni 2021, 2022 e 2023 ha strutturato dei percorsi di formazione su più livelli e moduli con focus sulla crescita dei propri dipendenti in termini di collaborazione e comunicazione efficace.

Nello specifico sono stati organizzati con la scuola di Formazione e coaching **Creattività** degli incontri formativi sia online che in presenza, così strutturati:

- ***Modello Brainbow***: dedicato a tutta la popolazione aziendale e volto a migliorare la gestione delle relazioni interpersonali sia in campo privato che professionale;
- ***Corsi di Public Speaking***: dedicati alle figure commerciali, per andare a migliorare la loro comunicazione nei confronti di clienti e stakeholder esterni all'Azienda;
- ***Corsi sulla Leadership & Gestione del Feedback***: rivolto alle figure manageriali, che in Azienda hanno la responsabilità della gestione e mentoring di altre risorse, in qualità quindi di team leader.

Le ore di formazioni dedicate ai dipendenti sono state negli anni via via crescenti. Per il prossimo triennio sarà intenzione dell'azienda consolidare e confermare tali attività, cercando di strutturare anche percorsi di formazione e-learning: le ore di formazione sono aumentate esponenzialmente nel triennio, passando da 56 ore annue nel 2021 a 101 ore di formazione nel 2022 fino ad arrivare a 1.228 nel 2023.

## 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 3 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 accordo individuale per 3 giorni a settimana, valido per tutti i dipendenti a prescindere dalla funzione lavorativa.

Dal 2023 tutti i 94 dipendenti del Gruppo sono coperti da assicurazione per invalidità e disabilità.

Sarà intenzione del Gruppo consolidare questo modus operandi e continuare ad 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 ed 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 ed 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 ed aggiornato un documento che contiene il piano di lavoro e gli interventi di miglioramento **(Piano di miglioramento)**. Sono stati inoltre organizzati per il 2023 i corsi 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 ed organismi di controllo e certificazione e si coordina con le rappresentanze dei lavoratori per la sicurezza e gli Amministratori.

## Gli infortuni

Nel corso del 2023, così come nel 2021, non sono stati registrati infortuni mentre nel 2022è stato registrato un solo infortunio (in itinere).

| **Infortuni sul lavoro** [9] | **2021** | **2022** | **2023** |
|---|---|---|---|
| Mortali | - | - | - |
| Incidenti gravi | - | - | - |
| Altri Incidenti[10] | - | 1 | - |
| Totale Incidenti registrati | - | 1 | - |
| Di cui: Incidenti in itinere | - | 1 | - |

[9] 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.

[10] Incidente inferiore a un mese.

| | | | |
|---|---|---|---|
| Giorni assenza per infortuni | - | 4 | - |
| Totale ore lavorate | 121.873 | 125.565 | 157.638 |
| **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[11]** | **-** | **7,96** | **-** |

[11] Il dato riguardante il tasso di infortuni sul lavoro registrabili per il 2022 è stato aggiornato

Capitolo 7

# CAPITALE AMBIENTALE

# **CAPITALE AMBIENTALE**
OVERVIEW

Con 24bottles il gruppo ha ridotto di 80 grammi/
per dipendente le emissioni di $CO_2$ in atmosfera

-21,28

Tonnellate di rifiuti prodotti, equivalente
al -51% rispetto al 2022

# 7. 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.

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 energetici

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 (server[12]);
- Gas per il riscaldamento della sede centrale;
- Diesel, benzina e GPL per l'alimentazione delle auto aziendali. Relativamente a questo punto, il Gruppo sta realizzando un monitoraggio della situazione per avere 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.

Nella successive tabella sono riportati i consumi energetici relativi al triennio 2021 - 2023.

I dati mostrano un aumento dei consumi di energia del 36% nel 2023, rispetto all'anno precedente, che riflette la ripresa delle attività a seguito della situazione pandemica vissuta (Covid-19), con un impatto importante sui consumi relativamente alla componente mobilità. Allo stesso modo, anche le relative emissioni pari a tCO2e (calcolate secondo l'approccio *market-based*), sono aumentate nel 2023 del 27%.

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

Le società del Gruppo hanno, infatti, fatto leva sulle criticità presentate dalla pandemia per incentivare, ad esempio, lo *Smart Working*, creando soluzioni finalizzate a garantire il lavoro a distanza in maniera efficace, consentendo di proteggere, prima di tutto, la salute di collaboratori e dei dipendenti e assicurare, allo stesso tempo, una riduzione delle emissioni causate dalla mobilità del personale.

| **Energia consumata (GJoule)**[13] | **2021** | **2022** | **2023** |
|---|---|---|---|
| **Energia elettrica** | | | |
| Energia elettrica acquistata | | | |
| *Di cui da fonti non rinnovabili* | *210* | *217* | *229* |
| *Di cui da fonti rinnovabili* | - | - | - |
| **Carburanti** | | | |
| GPL | 5 | - | - |
| Diesel | 1.359 | 1.708 | 2.377 |
| Benzina | 60 | 64 | 96 |
| **Totale** | **1.634** | **1.989** | **2.702** |

[13] I fattori di conversione utilizzati per trasformare le differenti quantità energetiche in GJ sono tratti dal database Defra 2023 (UK Department for Environment, Food and Rural Affairs). I dati relativi all'anno fiscale 2022 sono stimati sulla base dei dati relativi al biennio precedente in quanto non disponibili alla data della redazione del presente documento.

Rispetto alla precedente rendicontazione il consumo di gas è stato considerato all'interno della quota dei consumi derivanti dal teleriscaldamento.

## Emissioni

Per dare un contributo indiretto alla compensazione delle emissioni, il Gruppo Cyberoo ha deciso nel corso del 2021 di finanziare interventi specifici di plantumazione: con l'aiuto di **Treedom**, sono stati piantati 100 alberi da frutto in Kenya, Tanzania e Colombia contribuendo così a sottrarre più di 10 tonnellate di CO2 dall'atmosfera (nei primi 10 anni).

Con l'aiuto, invece, di **24bottles** è stata realizzata e fornita una bottiglia per ciascun dipendente con l'obiettivo di ridurre l'utilizzo di bottiglie di plastica monouso, evitando di rilasciare in atmosfera circa 80 grammi di CO2 (per ogni bottiglia di plastica monouso).

| **Emissioni GHG Scope 1 (tCO2e) – Scope 1[14]** | **2021** | **2022** | **2023** |
|---|---|---|---|
| **Emissioni dirette** | | | |
| GPL | 0,3 | - | - |
| Gasolio | 102 | 128 | 168 |
| Benzina | 4 | 5 | 6 |
| **Emissioni complessive – Totale Scope 1** | **106,3** | **133** | **174** |
| **Emissioni GHG Scope 2 (tCO2e) – Location Based[15]** | | | |
| **Emissioni indirette** | | | |
| Energia elettrica acquistata | 14 | 15 | 19 |
| **Emissioni Complessive – Totale Scope 2** | **14** | **15** | **19** |
| **Totale emissioni Scope 1 + Scope 2** | **120,3** | **148** | **193** |
| **Emissioni GHG Scope 2 (tCO2e) – Market Based[16]** | | | |
| **Emissioni indirette** | | | |
| Energia elettrica acquistata | 27 | 27 | 29 |
| **Emissioni Complessive – Totale Scope 2** | **27** | **27** | **29** |
| **Totale emissioni Scope 1 + Scope 2** | **133,3** | **160** | **203** |

[14] La fonte dei fattori di emissione utilizzati per il calcolo delle emissioni di GHG dirette è il database Defra 2023 (UK Department for Environment, Food and Rural Affairs).

I dati delle emissioni relativi al triennio sono stati rettificati in quanto i consumi di gas sono stati conteggiati all'interno del teleriscaldamento.

[15] La fonte dei fattori di emissione utilizzati per il calcolo delle emissioni di GHG indirette Location Based è *Terna Confronti internazionali 2020*.

[16] La fonte dei fattori di emissione utilizzati per il calcolo delle emissioni di GHG indirette Market Based è l'*European Residual Mixes "AIB"* ultimo aggiornamento (31.05.2021).

# Utilizzo responsabile delle risorse naturali

## Acqua

L'acqua per le società del Gruppo Cyberoo non è una risorsa critica in quanto non è utilizzata ai fini industriali. La gestione dell'approvvigionamento idrico e dello smaltimento è affidata alla capogruppo per la quasi totalità, la quale adotta specifiche politiche di gestione dei reflui.

Le società si impegnano a monitorare costantemente i propri consumi, per individuare eventuali perdite ed intervenire con tempestività, riducendo al minimo il proprio impatto ambientale in questo senso.

| Acqua consumata (in ML)[17] | 2021 | 2022 | 2023 |
|---|---|---|---|
| Risorse idriche di terze parti - fornitori idrici<br>*Di cui: Acqua dolce (≤1.000 mg/l di solidi disciolti totali)* | 41 | 134 | 279 |
| **Totale (in ML)** | **41** | **134** | **279** |

I **prelievi di acqua** di Cyberoo avvengono dalla rete dell'acquedotto pubblico e riguardano prevalentemente utilizzi di tipo sanitario in quantità modeste.

Il consumo di acqua è aumentato nel 2023: sono stati consumati circa 279 mL nel 2023 rispetto ai 134 mL nel 2022.

## Rifiuti

Le società del Gruppo Cyberoo adottano tutte le misure necessarie per lo smaltimento dei dispositivi tecnologici che sono comunque la minima parte siccome la gestione dei dispositivi è affidata alla Capogruppo. Per i rifiuti assimilabili a quelli civili, Cyberoo ha introdotto la raccolta differenziata.

| Rifiuti prodotti (in t)[18] | 2021 | 2022 | 2023 |
|---|---|---|---|
| **Rifiuti non pericolosi** | 34,82 | 36,34 | 16,60 |
| **Rifiuti pericolosi** | 0,42 | 5,24 | 3,70 |
| **Totale rifiuti prodotti** | **35,24** | **41,58** | **20,30** |

[17] I dati del biennio 2021 e 2022 sono stati aggiornati, poiché dal 2023 si è utilizzata una metodologia differente per l'estrazione dei dati sul prelievo di acqua

[18] 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.

Nel 2023 i rifiuti prodotti pari a 20,30 tonnellate (di cui l'82% dei rifiuti prodotti, sono non pericolosi) sono in diminuzione di più della metà rispetto al 2022, in quanto il gruppo ha ottimizzato la gestione dei rifiuti smaltendone una minore quantità.

# GRI 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 secondo l'opzione "with reference" con i GRI Standards per il periodo 1° gennaio 2023 - 31 dicembre 2023. |
| **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/II Gruppo | 11 | |
| | **2-2** | Entità incluse nella rendicontazione di sostenibilità dell'organizzazione | Nota Metodologica | 7 | |
| | **2-3** | Periodo di rendicontazione, frequenza e punto di contatto | Nota Metodologica | 7 | |
| | **2-4** | Revisione delle informazioni | Nota Metodologica | 7 | |
| | **2-5** | Assurance esterna | Nota Metodologica | 7 | 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 | 28 | |
| | **2-7** | Dipendenti | 6. Capitale umano/I Dipendenti | 108 | |
| | **2-8** | Lavoratori non dipendenti | 6. Capitale umano/I Dipendenti | 109 | |
| | **2-9** | Struttura e composizione della governance | 2. Governance/La Governance | 53 | |
| | **2-10** | Nomina e selezione del massimo organo di governo | 2. Governance/La Governance | 53 | |
| | **2-11** | Presidente del massimo organo di governo | 2. Governance/La Governance | 53 | |
| | **2-14** | Ruolo del massimo organo di governo nella rendicontazione di sostenibilità | Nota Metodologica | 7 | |
| | **2-16** | Comunicazione delle criticità | 2. Governance/La Governance | | 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 | 5 | |
| | **2-25** | Processi volti a rimediare agli impatti negativi | 1. Identità e strategia/Analisi di materialità | 43 | Rientra nel management approach dei temi materiali |

| | | | | | |
|---|---|---|---|---|---|
| | **2-27** | Conformità e leggi e regolamenti | 2. Governance/Compliance normativa | 62 | Nel corso del 2023 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 | 3. Capitale infrastrutturale/Il valore delle partnership | 75 | |
| | **2-29** | Approccio al coinvolgimento degli stakeholder | 1. Identità e strategia/Analisi di materialità | 43 | |
| | **2-30** | Contratti collettivi | 6. Capitale umano/I Dipendenti | 108 | |
| **TEMI MATERIALI** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-1** | Processo di determinazione dei temi materiali | 1. Identità e strategia/Analisi di materialità | 43 | |
| | **3-2** | Elenco di temi materiali | 1. Identità e strategia/Analisi di materialità | 43 | |
| **ETICA E INTEGRITÀ NELLA CONDOTTA DEL BUSINESS** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 2. Governance | 53 | |
| **GRI 205: Anticorruzione 2016** | **205-3** | Episodi di corruzione accertati e azioni intraprese | 2. Governance | 53 | Nessun episodio di corruzione accertato nel corso del |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | presente esercizio |
| **GRI 206: Comportamento anticoncorrenziale 2016** | **206-1** | Azioni legali per comportamento anticoncorrenziale, antitrust e pratiche monopolistiche | 2. Governance/Compliance normativa | 62 | |
| **GRI 207: Imposte 2019** | **207-1** | Approccio alla fiscalità | 5. Capitale economico-finanziario/Approccio fiscale | 102 | |
| **ANTICORRUZIONE E COMPLIANCE** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 2. Governance | 53 | |
| **GRI 205: Anticorruzione 2016** | **205-3** | Episodi di corruzione accertati e azioni intraprese | 2. Governance | 53 | |
| **GRI 206: Comportamento anticoncorrenziale 2016** | **206-1** | Azioni legali per comportamento anticoncorrenziale, antitrust e pratiche monopolistiche | 2. Governance/Compliance normativa | 62 | |
| **GOVERNANCE TRASPARENTE E GESTIONE DEI RISCHI DI SOSTENIBILITÀ** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 2. Governance | 53 | |
| **GRI 205: Anticorruzione 2016** | **205-3** | Episodi di corruzione accertati e azioni intraprese | 2. Governance | 53 | |
| **GRI 206: Comportamento anticoncorrenziale 2016** | **206-1** | Azioni legali per comportamento anticoncorrenziale, antitrust e pratiche monopolistiche | 2. Governance/Compliance normativa | 62 | |

| | | | | | |
|---|---|---|---|---|---|
| **TUTELA DEL BRAND E REPUTAZIONE** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 3. Capitale infrastrutturale | 65 | |
| **CREAZIONE E DISTRIBUZIONE DELLA RICCHEZZA GENERATA** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 5. Capitale economico-finanziario | 101 | |
| **GRI 201: Performance economiche 2016** | **201-1** | Valore economico direttamente generato e distribuito | 5. Capitale economico-finanziario/Il valore economico generato e distribuito | 101 | |
| **SOLIDITÀ E RESILIENZA ECONOMICA** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 5. Capitale economico-finanziario | 101 | |
| **GRI 201: Performance economiche 2016** | **201-1** | Valore economico direttamente generato e distribuito | 5. Capitale economico-finanziario/Il valore economico generato e distribuito | 101 | |
| **GRI 203: Impatti economici indiretti 2016** | **203-1** | Investimenti infrastrutturali e servizi finanziati | 5. Capitale economico-finanziario/Gli investimenti | 102 | |
| **RICERCA E INNOVAZIONE TECNOLOGICA** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 3. Capitale infrastrutturale/Innovazione e digitalizzazione | 65 | |

| | | | | | |
|---|---|---|---|---|---|
| **QUALITÀ, SICUREZZA E AFFIDABILITÀ DEI SERVIZI** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 4. Capitale relazionale | 80 | |
| **GRI 416: Salute e sicurezza dei clienti 2016** | **416-1** | Valutazione degli impatti sulla salute e sulla sicurezza per categorie di prodotto e servizi | 4. Capitale relazionale/Qualità, sicurezza e affidabilità dei servizi | 83 | |
| | **416-2** | Episodi di non conformità riguardanti impatti sulla salute e sulla sicurezza di prodotti e servizi | 4. Capitale relazionale/Qualità, sicurezza e affidabilità dei servizi | 83 | Nel corso del 2023 non si sono verificati casi di non conformità riguardanti impatti sulla salute e sulla sicurezza di prodotti e servizi offerti |
| **LOTTA AL CAMBIAMENTO CLIMATICO** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 7. Capitale ambientale | 119 | |
| **GRI 305: Emissioni 2016** | **305-1** | Emissioni dirette di GHG (Scope 1) | 7. Capitale ambientale/Emissioni | 122 | |
| | **305-2** | Emissioni indirette di GHG da consumi energetici (Scope 2) | 7. Capitale ambientale/Emissioni | 122 | |
| **EFFICIENZA ENERGETICA** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 7. Capitale ambientale | 119 | |

| | | | | | |
|---|---|---|---|---|---|
| **GRI 302: Energia 2016** | **302-1** | Energia consumata all'interno dell'organizzazione | 7. Capitale ambientale/Consumi energetici | 120 | |
| **RISPETTO DEI DIRITTI UMANI E TUTELA DEI LAVORATORI** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 6. Capitale umano | 106 | |
| **GRI 401: Occupazione 2016** | **401-1** | Assunzioni e turnover | 6. Capitale umano/I Dipendenti | 112 | |
| **GRI 406: Non discriminazione 2016** | **406-1** | Episodi di discriminazione e misure correttive adottate | 6. Capitale umano/Diversità | 109 | Nel 2023 non si sono verificati episodi di discriminazione |
| **SODDISFAZIONE E GESTIONE DELLE RELAZIONI CON I CLIENTI** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 4. Capitale relazionale | 80 | |
| **GRI 418: Privacy dei clienti 2016** | **418-1** | Denunce comprovate riguardanti le violazioni della privacy dei clienti e perdita di dati dei clienti | 4. Capitale relazionale/Qualità, sicurezza e affidabilità dei servizi | 83 | |
| **FORMAZIONE E SVILUPPO DELLE CARRIERE** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 6. Capitale umano | 106 | |
| **GRI 404: Formazione e istruzione 2016** | **404-1** | Ore medie di formazione annua per dipendente | 6. Capitale umano/Formazione e Competenze | 113 | |

| | | | | | |
|---|---|---|---|---|---|
| **TRASPARENZA DELLE INFORMAZIONI SUI PRODOTTI** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 4. Capitale relazionale | 80 | |
| **GRI 417: Marketing ed etichettatura 2016** | **417-3** | Casi di non conformità riguardanti comunicazioni di marketing | 4. Capitale relazionale/Attività di marketing | 84 | Nel corso del 2023 non si sono verificati casi di non conformità riguardanti comunicazioni di marketing. |
| **PARNERSHIP CON ISTITUZIONI ED IMPRESE** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 3. Capitale infrastrutturale/Il valore delle partnership | 75 | |
| **GESTIONE DEI RIFIUTI** | | | | | |
| **GRI 3: Temi materiali 2021** | **3-3** | Gestione dei temi materiali | 4. Capitale ambientale | 119 | |
| **GRI 306: Rifiuti 2020** | **306-3** | Rifiuti prodotti | 7. Capitale ambientale/Utilizzo responsabile delle risorse naturali | 123 | |
| **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 | 110 | |

| | | | | | |
|---|---|---|---|---|---|
| **PRATICHE DI APPROVVIGIONAMENTO** | | | | | |
| **GRI 204: Pratiche di approvvigionamento 2016** | **204-1** | Proporzione di spesa verso fornitori locali | 4. Capitale relazionale/Fornitori: la gestione della supply chain | 86 | |
| **ACQUA E SCARICHI IDRICI** | | | | | |
| **GRI 303: Acqua e scarichi idrici 2018** | **303-3** | Prelievo idrico | 7. Capitale ambientale/Utilizzo responsabile delle risorse naturali | 123 | |
| **OCCUPAZIONE** | | | | | |
| **GRI 401: Occupazione 2016** | **401-3** | Congedo parentale | 6. Congedi parentali | 113 | |
| **SALUTE E SICUREZZA SUL LAVORO** | | | | | |
| **GRI 403: Salute e sicurezza sul lavoro 2018** | **403-2** | Identificazione dei pericoli, valutazione dei rischi e indagini sugli incidenti | 6. Capitale umano/Salute e sicurezza sul lavoro | 115 | |
| | **403-3** | Servizi di medicina del lavoro | 6. Capitale umano/Salute e sicurezza sul lavoro | 115 | |
| | **403-9** | Infortuni sul lavoro | 6. Capitale umano/Salute e sicurezza sul lavoro | 115 | |
| **DIVERSITÀ E PARI OPPORTUNITÀ** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **GRI 405: Diversità e pari opportunità 2016** | **405-1** | Diversità negli organi di governo e tra i dipendenti | 6. Capitale umano/Diversità | 109 | |
| **COMUNITÀ LOCALI** | | | | | |
| **GRI 413: Comunità locali 2016** | **413-1** | Attività che prevedono il coinvolgimento delle comunità locale, valutazioni d'impatto e programmi di sviluppo | 4. Capitale relazionale/Le relazioni con il territorio | 91 | |

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

**SPACES ISOLA / MILANO**
VIA POLA, 11
20124 MILANO

**BUREAU / PIACENZA**
VIA DAL VERME, 33
29121 PIACENZA

CYBEROO