DIGITALIZZAZIONE

DOPPIA MATERIALITÀ

TEMI MATERIALI:
- Trasformazione digitale

PILASTRO DEL PIANO DI SOSTENIBILITÀ

ACCELERATORI DELLA CRESCITA
- Digitalizzazione

OBIETTIVI DI SVILUPPO SOSTENIBILE (SDG)

Enel continua ad agire in maniera integrata, facendo leva su persone, tecnologie e processi per ridurre il rischio cyber, in un contesto caratterizzato dall'aumento delle minacce informatiche, in termini di sofisticazione, frequenza e impatto. Proseguono le azioni per la riduzione delle emissioni di CO_2 attraverso il contenimento delle pagine stampate e il monitoraggio del consumo di energia elettrica al di fuori del normale orario di lavoro di PC, laptop e monitor, ottimizzando l'uso e il dimensionamento delle piattaforme digitali per ridurre l'impatto ambientale.

Di seguito i risultati 2023 relativi al precedente Piano di Sostenibilità 2023-2025, il conseguente stato di avanzamento e i target del Piano di Sostenibilità 2024-2026 ridefiniti, aggiunti o superati rispetto al Piano precedente.

ATTIVITÀ	RISULTATI 2023	TARGET 2024-2026	SDG PREVALENTI
CYBER SECURITY			
Esecuzione di cyber exercise che coinvolgono impianti/siti industriali	**67** cyber exercise svolti	**155** cyber exercise nel periodo 2024-2026(1)	4 9
Azioni di verifica di sicurezza informatica (Ethical Hacking, Vulnerability Assessment ecc.)	**1.861** azioni di verifica svolte	**3.600** azioni di verifica nel periodo 2024-2026(1)	9
Diffusione della cultura della sicurezza informatica e cambiamento dei comportamenti delle persone al fine di ridurre i rischi	**19** eventi di cyber security knowledge sharing eseguiti	**45** eventi di cyber security knowledge sharing nel periodo 2024-2026	4 9
SOLUZIONI DIGITALI			
Attività per la riduzione delle emissioni di CO_2	**-54,5 mln** di pagine stampate (*vs* 2019)	**-17 mln** di pagine stampate nel 2026 (*vs* 2019)	12 13
	6,9 mln di riunioni svolte tramite servizi di videocomunicazione	Estensione dell'utilizzo dei sistemi di videocomunicazione	12 13
	16,4 mln di ore di inutilizzo al di fuori del normale orario di lavoro	Azioni per la riduzione delle ore di inutilizzo di PC, laptop, monitor	12 13
	65 nuove interconnessioni e-API Digital Ecosystem	**90** nuove interconnessioni e-API Digital Ecosystem nel periodo 2024-2026	9 12

(1) Il target è stato ridefinito per una maggiore focalizzazione.

Obiettivi

Nuovo | Ridefinito | Superato

Avanzamento

Non in linea | In linea | Raggiunto

N.A. = non applicabile, obiettivo non presente nel Piano di Sostenibilità 2023-2025

DIGITALIZZAZIONE

67

CYBER EXERCISE

50 nel 2022 **+34%**

1.861

CONTROLLI DI ASSURANCE (ETHICAL HACKING, VULNERABILITY ASSESSMENT)

1.587 nel 2022 **+17,3%**

19

EVENTI PER LA DIFFUSIONE DELLA SICUREZZA INFORMATICA

19 nel 2022 **0%**

La trasformazione digitale rappresenta un fattore imprescindibile per le aziende del settore energetico, poiché è in grado di offrire soluzioni e tecnologie per affrontare le sfide della transizione energetica, per ottimizzare la gestione delle reti, migliorare l'esperienza dei clienti, abilitare lo sviluppo delle energie rinnovabili e agevolare l'esperienza lavorativa, garantendo alti livelli di servizio e di efficienza operativa. Attraverso un nuovo modello organizzativo e operativo semplificato, l'unità di Global Information & Communication Technology, all'interno della Funzione Global Services, si pone l'obiettivo di:

- garantire e aumentare l'**efficienza** dei livelli di servizio offerti dalle soluzioni digitali;
- incrementare l'**efficacia**, con particolare focus sui processi di demand management, adoption e controllo dei costi ricorrenti;
- potenziare l'**internalizzazione**, preservando il know-how sulle tecnologie chiave tramite piani di insourcing, aumentando la formazione e adottando strumenti per incrementare la produttività.

Una trasformazione digitale sostenibile

Tecnologie digitali come l'intelligenza artificiale, i big data, l'IoT e il cloud possono generare grandi benefíci in termini di efficientamento dei processi aziendali, ma è necessario prestare attenzione all'impatto che le stesse possono generare sull'ambiente e sulle persone. La trasformazione digitale di Enel, dunque, mira non solo a utilizzare le soluzioni digitali per realizzare un progresso sostenibile, ma anche a farne uso sulla base di specifici criteri di sostenibilità. Per questo motivo, **le principali linee d'azione del 2023** hanno riguardato:

- **decarbonizzazione** e riduzione delle emissioni legate alle soluzioni digitali;
- **circolarità** dei dispositivi digitali e dei materiali che compongono gli asset digitali del Gruppo;
- promozione dell'**inclusione sociale** attraverso lo sviluppo di tecnologie assistive e soluzioni che assicurino accessibilità e generino valore soddisfacendo bisogni sociali;
- promozione delle **migliori performance ambientali** e adozione dei princípi a **tutela dei diritti umani** con i fornitori di prodotti e soluzioni digitali.

Enel è inoltre tra i promotori in Italia, insieme alla Fondazione per la Sostenibilità Digitale, della prima **Prassi di Riferimento UNI/PdR 147:2023**, che definisce requisiti e linee guida per un digitale più sostenibile e inclusivo by-design. La Prassi di Riferimento individua 58 indicatori di sostenibilità applicabili in tutte le fasi del ciclo di vita di un progetto di trasformazione digitale: dall'avvio alla pianificazione, dall'esecuzione fino al monitoraggio. Gli indicatori sono collegati ai Sustainable Development Goal (SDG) per comprendere in quale misura un determinato progetto di trasformazione digitale sia in grado di sfruttare tutte le potenzialità del digitale, nel rispetto dei criteri di sostenibilità economica, sociale e ambientale. In particolare, Enel ha applicato la Prassi al progetto, adottato su scala globale, di digitalizzazione dei misuratori di energia prelevata e immessa in rete. Ciò ha permesso di evidenziare tra i punti di forza gli obiettivi di innovazione (SDG 9), di consumo responsabile e di crescita economica grazie al riuso del software (SDG 8 e 12), mentre è emerso come punto di miglioramento la parità di genere del team di sviluppo, prevalentemente maschile (SDG 5). Inoltre, la Prassi è stata applicata al progetto Data Governance per lo sviluppo di un motore di ricerca che consenta di ritrovare agevolmente la documentazione relativa ai contratti attivi grazie a una serie di filtri sui metadati del contratto (data stipula, fornitore, prodotti/servizi ecc.). Tra i punti di forza del progetto emergono gli obiettivi di innovazione (SDG 9), di condivisione della conoscenza all'interno della community aziendale (SDG 4 e 11), di buon equilibrio in termini di ore di lavoro necessarie alle attività di sviluppo (SDG 3 e 8), mentre si è evidenziato tra i punti di miglioramento la valorizzazione delle informazioni, ancora poco condivise (SDG 12).

Enel ha, infine, avviato nel 2023 un progetto, a livello globale, per la **valutazione del rischio etico nell'impiego dell'intelligenza artificiale** da parte del Gruppo, in linea con quanto richiesto dalle nuove normative a livello europeo (AI Act). Il progetto ha evidenziato l'esigenza di gestire il design delle soluzioni digitali attraverso una metodologia volta a individuare i rischi, le implicazioni sociali e l'impatto delle tecnologie, e di sviluppare un modello di compliance-by-design per definire le strategie più adeguate di mitigazione dei rischi individuati. Come risultato, è stato redatto un documento di "raccomandazioni" per il Gruppo, contenente gli elementi da considerare in fase di design delle nuove soluzioni digitali.

Inclusività dei portali web per creare valore

Enel ha definito e sviluppato un modello per valutare i portali web a disposizione dei clienti e dei colleghi in termini di inclusività digitale, tenendo in considerazione gli impatti di sostenibilità sociale, ambientale ed economica. Il framework Inclusive Web Portal©, che nel 2023 è stato codificato attraverso copyright, individua 89 requisiti che, considerando l'esperienza utente e l'accessibilità digitale come elementi centrali, mirano a garantire l'inclusività digitale, dando rilevanza, oltre alle diversità persistenti, anche alle diverse abilità di circostanza, le diversità anagrafiche, economiche, lavorative, culturali, linguistiche, etniche e di identità di genere. Il modello permette di individuare le azioni da compiere per promuovere un ambiente digitalmente inclusivo che possa creare valore e rispondere ai bisogni di tutti gli stakeholder, in modo che nessuno sia lasciato indietro nel processo di trasformazione digitale.

I principali driver della trasformazione digitale

Transizione circolare della catena del valore del digitale

I dispositivi digitali sono costituiti da materiali che, se non gestiti correttamente, possono essere dannosi per l'ambiente quando vengono smaltiti; per questo motivo Enel attua, a livello di Gruppo, una strategia comune finalizzata a ridurre i rischi e a cogliere le opportunità derivanti dalla gestione dei dispositivi digitali. In particolare, vengono analizzati i flussi di materie prime in entrata e in uscita, al fine di definire la pianificazione dei fabbisogni e valutare i rischi e gli impatti degli asset digitali in termini di circolarità. Tale analisi ha consentito di identificare i principali materiali critici presenti nei computer e monitor che compongono la flotta aziendale – ferro, rame, alluminio e acciaio – e di effettuare la pianificazione delle quantità di materiali critici necessari a Enel fino al 2030 (per approfondimenti si veda il capitolo "Economia circolare").

Valorizzazione dei dispositivi digitali attraverso il riuso e il riciclo

La dismissione dei dispositivi aziendali genera scarti il cui smaltimento merita particolare attenzione. Per questo motivo, la gestione circolare degli asset digitali, nei diversi Paesi del Gruppo, avviene salvaguardando in primo luogo l'estensione della vita utile dei dispositivi, mediante la vendita degli stessi ai dipendenti e a terze parti, o mediante un processo di donazione a enti del terzo settore, gestito da una specifica procedura di Gruppo, che promuove il riuso, e dunque l'inclusione digitale (17.880 dispositivi venduti nel 2023 e 38 donati). In alternativa, viene promosso il riciclo di tali dispositivi (22 tonnellate di apparati riciclati nel 2023) che, categorizzati come rifiuti elettronici, vengono smaltiti presso alcuni fornitori che acquistano i dispositivi stessi per poi riciclarli.

Valorizzazione dei dati attraverso la condivisione

Il passaggio da architetture monolitiche e "silos" di dati a modelli sistemici, distribuiti ed enterprise-wide permette alle informazioni di ottenere maggiore scalabilità, qualità e velocità di circolazione all'interno di un'organizzazione. In particolare, l'ecosistema e-API (Enel Application Programming Interface) è l'ambiente digitale, costituito da interfacce software, attraverso le quali tutte le società del Gruppo possono condividere rapidamente e in tempo reale le informazioni che normalmente resterebbero confinate all'interno di specifiche applicazioni verticali ("silos" informativi). Questo ecosistema ha contribuito ad accelerare l'adozione di soluzioni digitali, a ridurre le ridondanze dei dati all'interno del Gruppo e, più in generale, a ridurre la quantità di tempo e di risorse impiegate nello scambio di flussi informativi. Nel 2023 sono state realizzate 65 nuove interconnessioni e-API alle applicazioni del Gruppo, che hanno permesso di evitare ulteriori costi di sviluppo software.

Impatto ambientale delle soluzioni digitali

Le tecnologie digitali possono contribuire alla lotta al cambiamento climatico e alla transizione energetica fornendo soluzioni orientate all'efficientamento energetico e alla decarbonizzazione; al contempo, tuttavia, le stesse generano emissioni che impattano negativamente sull'ambiente. Il Digital Carbon Footprint Framework© di Enel, che nel 2023 è stato codificato attraverso copyright, ha consentito di quantificare le emissioni prodotte dalle soluzioni digitali in uso in tutto il Gruppo. Ciò ha consentito di identificare un piano di azioni orientato al contenimento e alla riduzione delle emissioni che, attraverso pratiche di ottimizzazione del dimensionamento del cloud, di incremento dell'alimentazione rinnovabile dell'infrastruttura digitale e di green coding (modalità di sviluppo software che mira a limitare il consumo di energia necessario all'esecuzione di algoritmi), ha permesso di ottenere una riduzione del 36% delle emissioni di CO_2 da fonti digitali al 2023 rispetto al 2018, a fronte di un incremento della capacità elaborativa dei sistemi del 206% e di un incremento della capacità di data storage pari al 90%.

Il digitale per le persone

Awareness per la sostenibilità digitale

Nel 2023 è stata realizzata una campagna di comunicazione interna a livello globale dal titolo "Sustainability by/in digital", finalizzata a condividere la cultura della sostenibilità digitale tra le persone di Enel, mirando a diffondere maggior consapevolezza sugli impatti che i comportamenti digitali hanno sull'ambiente in termini di consumi energetici e di emissioni generate, e a sensibilizzare a un uso consapevole delle tecnologie digitali. La campagna interattiva ha previsto la pubblicazione a livello globale di 3 news sulla Intranet aziendale che hanno riguardato: la prima Prassi di Riferimento UNI/PdR 147:2023, che definisce requisiti e linee guida per un digitale più sostenibile e inclusivo; il decalogo delle azioni da attuare per contenere l'impatto ambientale del digitale; la guida su come utilizzare le nuove tecnologie digitali, limitando i consumi energetici e le relative emissioni generate. Le news sono state accompagnate da newsletter e sondaggi per invitare le persone di Enel a testare la propria conoscenza sulle tematiche della sostenibilità digitale.

Accessibilità digitale per l'inclusione di colleghi e clienti in condizioni di vulnerabilità

Le tecnologie assistive svolgono una funzione fondamentale nel consentire l'inclusione e la partecipazione sociale delle persone in condizioni di vulnerabilità, consentendo loro di superare problemi funzionali e di ridurre la dipendenza da terzi. Per questo motivo, Enel ha disposto un catalogo di hardware e software assistivi per i quali le persone del Gruppo possono ottenere immediata assistenza tecnica attraverso team dedicati. Alcuni esempi sono rappresentati da Jaws, programma di lettura dello schermo con sintesi vocale per i colleghi non vedenti; Zoom text, che consente ai colleghi ipovedenti di ingrandire qualsiasi applicazione a schermo e modificare colori e forma del cursore del mouse; Pedius, che consente ai colleghi sordi di comunicare attraverso le tecnologie di sintesi e riconoscimento vocale, grazie alle quali l'utente può usare la sua voce naturale o scrivere. Infine, è disponibile Veasyt, servizio di video interpretariato professionale nella lingua dei segni, via web o app per eventi e formazione.

Riunioni virtuali

- **6,9 milioni** di riunioni
- **552,8mila tonnellate** di CO_2 evitata

Servizio di stampa

- **81 milioni** di pagine stampate
- **6,4 tonnellate** di CO_2 prodotta

Continua a essere operativo in tutte le sedi del Gruppo il servizio di stampa, che si avvale di stampanti di nuova generazione già predisposte per un utilizzo ecosostenibile. La peculiarità di tale servizio, unitamente a un utilizzo più razionale delle stampe, dovuto a una maggiore consapevolezza, e alla digitalizzazione dei documenti, ha consentito negli anni una riduzione del consumo di carta e conseguentemente un minore impatto sull'ambiente.
Inoltre, servizi come messaggistica istantanea (chat), audio conferenza e videoconferenza sfruttano appieno il modello di condivisione che, attraverso internet, consente di condividere e godere anche in tempo reale di contenuti da personal computer, smartphone o tablet, riducendo la necessità di spostamenti e quindi le emissioni di anidride carbonica.

PC Power Management Italia

- **16,4 milioni** di ore di inutilizzo
- **35,1 tonnellate** di CO_2

Nel 2023 è proseguito il monitoraggio del consumo di energia elettrica al di fuori del normale orario di lavoro relativamente alle postazioni informatiche (desktop, laptop, monitor) delle persone Enel che lavorano in Italia. Tale misurazione è possibile grazie alla presenza sulle postazioni informatiche di una funzionalità Microsoft (System Center Configuration Manager), che permette di individuare quando una postazione risulta accesa e non utilizzata. Rispetto agli anni precedenti, è stato registrato un aumento delle ore di inutilizzo dovuto all'ampliamento del perimetro di dispositivi analizzati; ciononostante, il decremento delle emissioni risulta costante grazie a una migliore performance energetica dei nuovi PC acquisiti nel 2023.

Verso un'elettrificazione cyber-safe

Nell'era della trasformazione digitale, la **cyber security** assume un ruolo fondamentale per garantire la normale operatività delle imprese, anche in considerazione del notevole aumento degli attacchi informatici nonché del loro grado di sofisticazione e impatto.

Studi di settore confermano che la percezione del rischio cyber è in costante crescita, in linea con il trend degli anni precedenti, nonostante questi ultimi siano stati fortemente caratterizzati da conflitti e tensioni geopolitiche. Per questo le agenzie di sicurezza nazionali hanno messo in guardia istituzioni pubbliche e private da potenziali minacce informatiche contro le infrastrutture critiche, spesso generate da attivisti di organizzazioni internazionali e nazionali. Negli ultimi anni molti degli attacchi più rilevanti a livello globale sono stati effettuati sfruttando la catena di fornitura e la compromissione di terze parti, consentendo agli attaccanti di colpire clienti, partner e fornitori del target primario; in questo modo è notevolmente aumentato il numero delle vittime e gli attacchi sono passati sempre più inosservati, realizzando il cosiddetto "scale effect". Si osserva, inoltre, come le vulnerabilità rilevate nei prodotti software di ampio utilizzo siano in costante aumento e come queste vengano sfruttate sempre più rapidamente dai criminali informatici. In particolare, le vulnerabilità di tipo "zero-day" rappresentano un grande rischio perché vengono sfruttate dai criminali informatici per eseguire l'attacco, prima che gli sviluppatori di software ne vengano a conoscenza e prima che possano rilasciare un aggiornamento correttivo (patch).

Con riferimento al settore energetico, la maggior parte degli attacchi informatici include quelli di tipologia ransomware, una modalità sempre più diffusa che determina l'esfiltrazione (copia, trasferimento o recupero non autorizzati) dei dati della vittima e la cifratura degli stessi, offrendo ai responsabili dell'attacco un'ulteriore leva per riscuotere il pagamento del riscatto. Unitamente a tale tipologia, nel 2023 si registra un aumento degli attacchi di Social Engineering, il primo step eseguito dai criminali informatici prima di sferrare l'attacco vero e proprio. Questa tipologia fa leva sulla difficoltà della vittima nel riconoscere l'attacco, sfruttando emozioni come paura e senso di urgenza per spingerla a compiere una determinata azione (per esempio, inviare denaro, divulgare informazioni sensibili o condividere credenziali di accesso). Inoltre, analisi e studi di mercato affermano che esiste una forte probabilità di aumento delle minacce informatiche nei prossimi anni, a causa di un utilizzo sempre più intensivo dell'Intelligenza Artificiale generativa da parte dei criminali informatici, per affinare le tecniche di attacco, sfruttando con successo le debolezze legate al fattore umano.

L'aumento delle minacce informatiche a livello globale costituisce pertanto un importante fattore di rischio per il Gruppo, in quanto un attacco cyber potrebbe causare errori nella normale esecuzione dei processi aziendali, con conseguenti inefficienze, perdite di clientela, interruzioni della produzione e del business in generale. In tali circostanze, il Gruppo potrebbe non essere in grado di condurre in maniera efficace la sua normale operatività.
A tali sfide si aggiunge l'evoluzione del panorama normativo e regolamentare in materia di sicurezza informatica, che ha portato alla definizione di requisiti di sicurezza complessi e talvolta non convergenti. Difatti, sebbene le normative puntino agli stessi obiettivi, definiscono formalismi, scadenze e tempistiche differenti, rendendo onerosa e complessa l'operatività necessaria.

In un simile contesto, già da diversi anni **Enel** ha adottato un approccio strategico e integrato per la gestione del rischio informatico. In particolare, sono state implementate diverse iniziative che agiscono sul fattore umano (per esempio, campagne di awareness, phishing simulato), iniziative che agiscono attraverso l'implementazione di soluzioni tecniche di protezione (per esempio, sistemi antivirus, antispam, autenticazione multifattoriale) e iniziative per la diffusione dei principi di cyber security nei processi aziendali (per esempio, progettazione e manutenzione impianti, gestione della clientela, procurement).

Politiche e modello di gestione

In linea con le esigenze del settore industriale energetico, il Gruppo ha adottato una visione sistemica dei temi della cyber security, nonché una strategia globale di analisi, prevenzione e gestione degli eventi di sicurezza informatica.
Da settembre 2016, all'interno della Funzione Global Information and Communication Technology (GICT) è stata costituita l'unità di **Cyber Security**, a diretto riporto del Chief Information Officer (CIO), e il cui responsabile ricopre il ruolo di Chief Information Security Officer (CISO) del Gruppo. L'unità è impegnata a garantire la governance, la direzione e il controllo delle tematiche di cyber security, la definizione della strategia, delle politiche e delle linee guida, in conformità con le normative nazionali e internazionali, il supporto di ingegneria per la protezione degli ambienti del Gruppo, il monitoraggio della "risk po-

sture" mediante controlli basati su processi e tecnologia, e ancora il presidio e l'implementazione dei requisiti di compliance derivanti da normative in tema di cyber security, unitamente all'adozione delle soluzioni tecniche e di procedure volte alla mitigazione di possibili debolezze rilevate. L'unità lavora in sinergia con le Linee di Business e con le unità tecniche responsabili della progettazione e della gestione dei sistemi, grazie alle figure dei Cyber Security Risk Manager e dei Cyber Security Response Manager. Un approccio valido alla gestione del rischio informatico deve attribuire responsabilità anche alle Linee di Business, consentendo decisioni ben informate sulla gestione e sulla postura del rischio. Il CISO e i Cyber Security Risk Manager costituiscono difatti il Cyber Risks Operating Committee, che ha lo scopo di valutare trasversalmente il rischio cyber e ha l'obiettivo di definire i criteri di accettazione del rischio, in base alla "risk posture" di Gruppo. Il Cyber Security Committee, presieduto dal CEO di Gruppo e composto dalle sue prime linee, approva la strategia di sicurezza informatica e controlla periodicamente (almeno annualmente) i progressi della sua attuazione. Nel 2023 il Comitato si è riunito una volta nel mese di luglio e, per il 2024, sono previsti i consueti incontri per l'avanzamento della strategia. Tutte le aree partecipano attivamente all'attuazione della strategia di cyber security attraverso un piano operativo integrato e allineato agli obiettivi del Gruppo. Inoltre, il rischio cyber, la strategia di cyber security e le relative iniziative sono oggetto di costante approfondimento da parte dei principali board esecutivi e di controllo (per esempio, Board of Directors, Comitato Controllo e Rischi, Collegi Sindacali, Organismi di Vigilanza ecc.) per tutte le Legal Entity e i Paesi di presenza del Gruppo.

Attraverso la politica di Gruppo adottata nel 2017, il "**Cyber Security Framework**", si indirizzano i princípi e i processi operativi che sono a supporto di una strategia globale di analisi, prevenzione e gestione dei rischi. Tale framework, basato su una visione 'sistemica', è trasversalmente applicabile al più tradizionale settore dell'Information Technology (**IT**), così come agli ambienti di Operational Technology (**OT**), legati al mondo industriale, e dell'Internet of Things (**IoT**). Nell'ambito dell'applicazione del framework, è stata definita anche la metodologia di Cyber Security Risk Management, anch'essa applicabile a tutti gli ambienti IT, OT e IoT, che racchiude tutte le fasi necessarie per effettuare l'analisi dei rischi e definire il relativo piano di mitigazione, in coerenza con gli obiettivi di cyber security stabiliti. Per bilanciare i vantaggi ottenuti dall'operatività e dall'uso dei sistemi IT/OT/IoT con il rischio che da questi può potenzialmente derivare, sono infatti fondamentali decisioni ben informate che siano basate sul rischio.
Enel ha inoltre creato il proprio "**Cyber Emergency Readiness Team**" (CERT), per gestire e rispondere in modo proattivo agli incidenti cyber, incentivando la collaborazione e lo scambio di informazioni all'interno di una rete di partner internazionali accreditati. Con il perfezionamento dell'accordo con il CERT nazionale statunitense, il numero di accreditamenti ha raggiunto quota 9: Romania, Italia, Cile, Argentina, Perù, Colombia, Brasile, Spagna e USA. Il CERT del Gruppo fa anche parte di Trusted Introducer, un servizio che comprende 508 CERT distribuiti in 75 Paesi. A settembre 2018 Enel ha aderito anche a FIRST (Forum of Incident Response and Security Teams), la più grande ed estesa comunità del settore con 710 membri dislocati in 106 Paesi. Il modello operativo del CERT H24 7/7, composto da un team interno di analisti di sicurezza che lavorano a turnazione, è completamente dedicato alla protezione dell'Azienda dalle minacce di cyber security.

Definizione della strategia di sicurezza informatica

La strategia di cyber security definisce gli obiettivi e le priorità al fine di indirizzare e coordinare le iniziative di investimento per il Gruppo nel suo complesso e garantire l'aderenza alle politiche di cyber security, la definizione di target, il reporting manageriale e il monitoraggio continuo delle attività di sicurezza in corso.
Tale processo è guidato dal CISO e fa leva su una stretta integrazione e sinergia con le diverse aree di business, che comunicano le proprie esigenze, analizzano le opportunità, gestiscono eventuali criticità e propongono possibili iniziative.

In particolare, la definizione della strategia è un'attività iterativa, basata sulla condivisione e sul consolidamento del target di "risk posture" del Gruppo. I diversi attori coinvolti analizzano le varie opzioni e le possibili iniziative all'interno della rispettiva area di business per valutarne la fattibilità, garantire il consenso e il relativo finanziamento. L'unità di Cyber Security guida il processo e, insieme agli altri attori rilevanti, consolida progressivamente, in un documento di proposta di cyber security strategy, aspetti come lo scenario futuro, gli obiettivi e le possibili iniziative strategiche, con una stima del budget di alto livello e la definizione delle priorità.

Cyber security incident management

La molteplicità e la complessità degli ambienti in cui il Gruppo opera (dati, industry e persone) e delle componenti tecnologiche (per esempio, sistemi business-critical come SCADA – Supervisory Control and Data Acquisition, smart grid e contatori elettronici), sempre più integrate nella vita digitale del Gruppo, ha reso necessaria la definizione di un sistema strutturato di cyber security. Da qui, il modello di cyber defense basato su una visione sistemica che integra il settore IT (a partire dal cloud fino al data center e al cellulare), l'OT (tutto ciò che riguarda il settore industriale, come il telecontrollo degli impianti) e l'IoT (l'estensione della comunicazione e dell'intelligenza artificiale al mondo degli oggetti).

Il CERT, attraverso i sistemi di monitoraggio, raccoglie ogni giorno 5 miliardi di eventi relativi agli asset aziendali da circa 5mila data source, li mette in correlazione sfruttando l'analisi automatica e produce in media 300 incidenti giornalieri. Gli incidenti sono classificati secondo una specifica matrice di impatto (Enel Cyber Impact Matrix), su una scala da 0 a 4, avvalendosi delle migliori capacità di correlazione degli eventi derivanti dall'adozione di servizi all'avanguardia.

La stragrande maggioranza degli incidenti è classificata al **livello 0/1**, non ha un impatto significativo sui sistemi del Gruppo ed è automaticamente o semi-automaticamente bloccata e/o gestita dalle difese aziendali in essere, che in questo modo prevengono e/o riducono l'impatto di potenziali attacchi cyber. Gli incidenti classificati al **livello 2/3/4** hanno un impatto potenziale sul Gruppo e sono gestiti dagli analisti del CERT coinvolgendo gli stakeholder interessati. Grazie ai servizi di protezione, ogni giorno, nel 2023 **il CERT ha bloccato in media 1,1 milioni di e-mail a rischio, 46 virus, 206 attacchi a portali web e 1,6 milioni di connessioni a siti pericolosi**.

Nel corso del 2023 il CERT di Enel ha risposto a: **48 incidenti di sicurezza informatica con livello di impatto 2; 2 incidenti con livello di impatto 3; 0 incidenti con il più alto livello di impatto, il 4**.

Nei casi rilevati, al fine di consentire una risposta efficiente e rapida, così da minimizzare gli impatti su persone, servizi e asset, sono state attivate tutte le procedure definite per la relativa gestione. In particolare, quando un incidente di cyber security si traduce in una potenziale violazione dei dati, vengono immediatamente intraprese le azioni necessarie, in linea con la politica del Gruppo Enel "**Data Breach Management**". Nell'eventualità che possa generarsi una situazione di crisi che metta a rischio la business continuity aziendale, gli asset, la reputazione e/o la redditività del Gruppo, le opportune azioni sono intraprese immediatamente, in linea con la specifica politica di Gruppo in materia di "Gestione degli eventi critici".

La politica "**IT Service Continuity Management**", inoltre, formalizza un processo avente l'obiettivo di ridurre a un livello accettabile il rischio che impatta sulla disponibilità dell'infrastruttura IT, di supportare le esigenze di business continuity e di garantire il ripristino dei servizi IT in base ai risultati derivanti da una Business Impact Analysis, nel momento in cui si dovesse verificare una grave interruzione, anche causata da un incidente.

Di seguito si riportano i dettagli relativi al numero degli eventi di sicurezza informatica registrati nel corso del 2023.

	2023
Numero totale di violazioni della sicurezza delle informazioni[1]	**0**
Numero totale di clienti, consumatori e dipendenti impattati dalle violazioni che hanno interessato il Gruppo[2]	**0**

(1) Il valore riferito alla numerosità del KPI "Numero totale di violazioni della sicurezza delle informazioni" è relativo agli incidenti cyber di livello 4 (non contemplando eventuali violazioni derivanti da incidenti "non digitali").

(2) Il valore riferito alla numerosità del KPI "Numero totale di clienti, consumatori e dipendenti impattati dalle violazioni che hanno interessato il Gruppo" si riferisce al numero di clienti, consumatori e dipendenti impattati dagli incidenti cyber di livello 4.

Principali progetti e iniziative

Tutti i progetti, i programmi e le iniziative di cyber security mirano a evitare, mitigare o porre rimedio ai rischi di sicurezza informatica per l'intero Gruppo. Di conseguenza, tutte le attività, gestite con un approccio risk-based e secondo il principio di security by design, generano un processo di due diligence continuo che include anche attività di self assurance.
Di seguito si riportano i progetti di maggior rilievo.

CYBER EXERCISE

Nel corso degli ultimi anni i cyber exercise sono diventati parte integrante delle attività volte alla **prevenzione**, **reazione** e **gestione** degli **incidenti cyber**. Si tratta nello specifico di esercitazioni periodiche svolte simulando **reali attacchi informatici** (senza impatto sui sistemi o limitazione alla normale operatività) e coinvolgono sia le strutture tecniche sia i business di riferimento. Le simulazioni eseguite hanno come obiettivo allenare la capacità di risposta dei soggetti coinvolti, verificare i processi e le tecnologie in campo, soddisfare i requisiti normativi e generare consapevolezza, indirizzando così eventuali esigenze di miglioramento di aspetti tecnici e/o organizzativi.
Le simulazioni sono sempre seguite da un'attività di assessment che mira ad analizzarne gli esiti, da un punto di vista quantitativo e qualitativo, fornendo eventuali spunti di "**lesson learned**", ove necessario.
Nel corso del 2023 sono stati eseguiti **67 cyber exercise** a livello globale, il che conferma quanto questa attività sia diventata una prassi consolidata nel Gruppo.

CYBER SECURITY GLOBAL REGULATORY COMPLIANCE

Negli ultimi anni si è assistito a **un'evoluzione del panorama normativo e regolamentare in ambito cyber security**, anche in termini di complessità delle normative, che prescrivono adempimenti trasversali e richiedono contemporaneamente miglioramenti in termini di governance, requisiti tecnico-specifici, controlli periodici, notifiche di eventi critici, vincoli e prescrizioni in tema di approvvigionamento di beni e servizi, con processi di verifica e adeguamento continui nel tempo.
Per gestire tale complessità e per efficientare le iniziative volte al **raggiungimento della compliance in ambito infrastrutture critiche** nei Paesi in cui il Gruppo è presente, Enel ha disegnato e gestito un **programma strutturato** per **l'analisi**, **l'adeguamento** e il **monitoraggio** a livello **globale** dei **requisiti normativi di differenti compliance**, garantendo e coinvolgendo sempre maggiormente le Linee di Business. Il programma ha identificato **processi e strumenti globali comuni**, implementati per soddisfare sia i requisiti comuni a tutte le compliance sia le specificità delle normative locali.
A supporto di tale processo, è stato disegnato e implementato un sistema informativo, il "**Cyber Security Global Regulatory Compliance Scheme**", per analizzare i numerosi requisiti normativi, rispetto al framework di Cyber Security del Gruppo, identificando eventuali gap sia a livello di singola normativa di Paese sia a livello di Gruppo.
Grazie a tale strumento, è possibile individuare in modo efficace ed efficiente le misure di adempimento da gestire e da monitorare nel programma di Cyber Security Regulatory Compliance.

PLAYBOOK ISO27001 – CERTIFICAZIONE ALLO STANDARD ISO

Enel ha colto il crescente interesse nel mercato per la **Certificazione di Sicurezza delle Informazioni ISO 27001**, avviando percorsi di certificazione a questo standard ISO conseguendolo già per diverse Legal Entities. Nello specifico, **Enel X**, **Enel X Way**, **Gridspertise**, **Enel Grids** ed **Enel Global Services** hanno raggiunto un importante traguardo per la cyber security di Gruppo, ottenendo la certificazione ISO 27001. Questo importante risultato certifica il sistema di gestione della sicurezza delle informazioni per i **processi core**, nell'ottica di fornire ai clienti prodotti e servizi trusted. Considerata la complessità del Gruppo, partendo dalle esperienze maturate nel leading del percorso di certificazione allo standard ISO 27001 delle varie Legal Entity del Gruppo, è stato disegnato uno **strumento gestionale digitale** che rende **efficiente, ripetibile, scalabile e sostenibile** il conseguimento della certificazione. Lo strumento, chiamato **Playbook ISO 27001**, realizza un **riferimento operativo per il Gruppo**, indicando le informazioni fondamentali da preparare durante la certificazione e fornendo una mappatura requisiti-processi di Gruppo. In particolare, il Playbook fornisce alle Legal Entity anche la mappa dei riferimenti dei responsabili e delle evidenze dei processi trasversali del Gruppo, valorizzando e ottimizzando sia le specificità delle Linee di Business sia l'effort delle Aree Global a servizio trasversale del Gruppo.

Collaborazioni con organismi ed enti esterni

La rete di relazioni con le realtà esterne e le organizzazioni rappresenta un elemento chiave nella strategia di cyber security, per condividere le migliori pratiche e i modelli operativi, sviluppare e rafforzare i canali di condivisione delle informazioni e contribuire alla definizione di standard e normative. Nel corso del 2023 sono stati forniti feedback per promuovere l'armonizzazione dell'attuale panorama normativo in materia e l'adozione di un approccio basato sul rischio e sul principio di security by design, in considerazione delle difficoltà nella gestione delle normative sulla sicurezza informatica a livello globale, caratterizzate da una grande eterogeneità dei requisiti di sicurezza e dei metodi di implementazione. Tenendo in considerazione il contesto di compliance normativa, **nel 2023 non sono state rilevate non-conformità a standard o regolamenti in tema di sicurezza informatica**.

Negli ultimi anni è stato definito e sviluppato un solido network, interagendo anche con stakeholder rilevanti del settore energetico quali ANEEL (Agência Nacional de Energia Elétrica),ONS (Operador Nacional do Sistema Elétrico) in Brasile e CNO (Consejo Nacional de Operación) in Colombia. Nel 2023 il Gruppo ha rappresentato **Eurelectric** per supportare la Commissione europea nell'armonizzazione delle legislazioni e degli standard di cyber security nell'ambito del settore Energia e delle Infrastrutture Critiche.

In Italia è stato inoltre istituito un canale di comunicazione con l'**Agenzia per la Cybersicurezza Nazionale** (**ACN**) per affrontare le sfide della sicurezza informatica. Nello specifico, Enel è tra le quattro **aziende pilota** che hanno partecipato al progetto volto alla realizzazione dell'**Hyper SOC**, ossia un'infrastruttura per la raccolta, la correlazione e l'analisi di eventi di interesse, con l'obiettivo di individuare rapidamente le minacce emergenti e di coordinare le risposte per fronteggiarle efficacemente. Nell'ambito di tale iniziativa, il primo risultato è stato l'attivazione del portale di interscambio di informazioni in tempo reale con l'ACN, per intercettare precocemente possibili "modelli" di attacco complessi.

In aggiunta, grazie alla collaborazione con altri partner esterni, è stato inaugurato il **Cyber Harbour**, un centro di innovazione che unisce esperti di cyber security, aziende, investitori e mondo accademico, per favorire la realizzazione di progetti innovativi e competitivi in ambito sicurezza informatica, a favore del sistema Paese Italia.

Inoltre, Enel ha partecipato ai gruppi di lavoro del World Economic Forum e contribuito negli ultimi anni alla pubblicazione di diversi rapporti, tra cui "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain", "Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors" e "Cyber Resilience in the Electricity Industry: Facilitating Global Interoperability of Cyber Regulations in the Electricity Sector".

Formazione e informazione

Il "**Cyber Security Awareness Program**" è diventato un'iniziativa costante e continuativa a livello di Gruppo, volta a diffondere la cultura della sicurezza informatica e ad aumentare la consapevolezza in merito alle minacce e agli attacchi che hanno come obiettivo il vettore umano. Tale programma contribuisce difatti alla digitalizzazione, poiché crea una cultura della sicurezza informatica, cambia il comportamento delle persone al fine di ridurre il rischio cyber, sviluppa competenze tecniche sulla sicurezza informatica e rende le persone la prima linea di difesa aziendale contro le minacce informatiche. Si avvale di diversi canali di comunicazione e strumenti di diffusione, comprendendo sia campagne di comunicazione sia iniziative di formazione dedicate per cluster di persone. Nello specifico, nel corso del 2023, sono stati realizzati 19 eventi di knowledge sharing a livello Globale su tematiche di cyber security e sono state eseguite diverse iniziative anche a livello locale, mirate a diffondere e aumentare la cultura della sicurezza informatica, con l'obiettivo di cambiare il comportamento delle persone al fine di ridurre i rischi informatici.
Le iniziative in ambito awareness sono state eseguite tramite "TheRedPill", la piattaforma unica per tutto il Gruppo attraverso cui viene reso esecutivo il programma "People Cyber Empowerment Journey" (un programma costituito da campagne di phishing simulato e moduli di awareness).

"THEREDPILL"

Nel 2023 sono state portate avanti, a livello globale, le iniziative di sensibilizzazione in ambito cyber security, grazie alla piattaforma di awareness di Gruppo "**TheRedPill**", con l'obiettivo di generare e potenziare la consapevolezza sulle principali tematiche cyber, indirizzare eventuali esigenze di upskilling e reskilling e insegnare come difendersi da eventuali attacchi informatici. Nello specifico, sono proseguite le **campagne di phishing simulato** (8 nel 2023) rivolte a tutta la popolazione aziendale Enel e sono stati condotti 19 **eventi volti alla diffusione della cultura di sicurezza informatica**.
Nell'ambito del programma di awareness del "People Cyber Empowerment Journey", avviato nel 2022, sono state definite e lanciate tutte le campagne di sensibilizzazione previste (12 campagne). Sono state inoltre avviate iniziative specifiche per i **nuovi assunti**, con l'obiettivo di promuovere la consapevolezza sulla sicurezza informatica sin dai primi giorni di impiego. Tra queste, il corso "**Cyber Security Essentials**", volto a fornire le conoscenze necessarie per affrontare le sfide di sicurezza informatica e promuovere la consapevolezza digitale, un **Modulo Anti-Phishing** per riconoscere le possibili e-mail con contenuto dannoso, e l'inserimento nel "**Welcome Book**" aziendale di contenuti specifici legati alla sicurezza informatica.