OPEN POWER FOR A BRIGHTER FUTURE.

WE EMPOWER SUSTAINABLE PROGRESS.

Le nostre performance 2022
Digitalizzazione

Le nostre performance

Ambizione emissioni zero ed elettrificazione pulita

sono al centro della nostra strategia che stiamo realizzando in maniera sostenibile e innovativa, promuovendo una **just transition**.

Le persone sono protagoniste del progresso sostenibile,

non solo le nostre, ma anche i clienti, i fornitori, le comunità, le istituzioni, la comunità finanziaria, i media, le imprese e le associazioni di categoria.

L'innovazione, l'economia circolare, la digitalizzazione e la finanza sostenibile

rappresentano gli acceleratori della crescita e abbracciano e potenziano trasversalmente tutti i temi strategici.

Tutela della natura e rispetto dei diritti umani

sono il nostro impegno quotidiano per le generazioni presenti e future.

Digitalizzazione

Temi materiali (I livello) → **Piano** → **SDG**

- Innovazione, economia circolare e trasformazione digitale

- Digitalizzazione

Di seguito i risultati 2022 relativi ai target del precedente Piano di Sostenibilità 2022-2024, il conseguente stato di avanzamento e gli obiettivi del Piano di Sostenibilità 2023-2025, eventualmente ridefiniti, aggiunti o superati rispetto al Piano precedente.

Cyber security

SDG	Attività	Risultati 2022	Avanzamento	Target 2023-2025	Tag
4 9 11	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 erogati	●●●	**15** eventi di cyber security knowledge sharing erogati all'anno	S T
9 11	Azioni di verifica di sicurezza informatica (Ethical Hacking, Vulnerability Assessment ecc.)	**1.587** azioni di verifica svolte	●●●	**1.400** azioni di verifica all'anno	T
9 11	Esecuzione di cyber exercise che coinvolgono impianti/siti industriali	**50** cyber exercise svolti	●●●	**186** cyber exercise nel periodo 2023-2025	S T

Per saperne di più

I **cyber exercise** sono esercitazioni volte alla simulazione di un incidente di sicurezza informatica, eseguite con l'obiettivo di allenare la capacità di reazione dei soggetti coinvolti e di verificare i processi e le tecnologie in campo. Le esercitazioni sono condotte dal Cyber Emergency Readiness Team (CERT) di Enel e coinvolgono sia le strutture tecniche sia i business di riferimento. La simulazione eseguita genera consapevolezza e indirizza eventuali esigenze di miglioramento di aspetti tecnici od organizzativi.

I Industriali · A Ambientali · S Sociali · G Governance · T Tecnologici

Obiettivi: Nuovo · Ridefinito · Superato

Avanzamento: ●○○ Non in linea · ●●○ In linea · ●●● Raggiunto

N.A. = non applicabile

Soluzioni digitali

SDG	Attività	Risultati 2022	Avanzamento	Target 2023-2025	Tag
12 13	Attività per la riduzione delle emissioni di CO_2	**-54,8 mln** di pagine stampate (vs 2019)	●●●	**-17 mln** di pagine stampate nel 2025 (vs 2019)	A S T
		7,3 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	A S T
		7,3 mln di riunioni svolte tramite servizi di videocomunicazione	●●○	Estensione dell'utilizzo dei sistemi di videocomunicazione	A S T
9 12	Riuso e scambio di informazioni nell'e-API Digital Ecosystem	**63** nuove interconnessioni e-API	●●●	**100** nuove interconnessioni e-API nel periodo 2023-2025	S T

Per saperne di più

L'**e-API Digital Ecosystem** è l'ambiente digitale grazie al quale tutte le società del Gruppo Enel possono condividere in modo semplice, veloce e automatizzato le informazioni normalmente confinate all'interno di specifiche applicazioni verticali ("silos" informativi). Grazie alla tecnologia abilitante delle API (Application Programming Interface), i flussi di dati e le funzionalità di Enel sono trattati come "data-as-a-product", favorendo la sostenibilità attraverso un reale riuso e scambio di informazioni e una riduzione di tempo e risorse necessari.

Digitalizzazione

1.587

CONTROLLI DI ASSURANCE (ETHICAL HACKING, VULNERABILITY ASSESSMENT)

1.580 nel 2021

+0,4%

6

CAMPAGNE PHISHING SIMULATO

4 campagne nel 2021

+50%

19

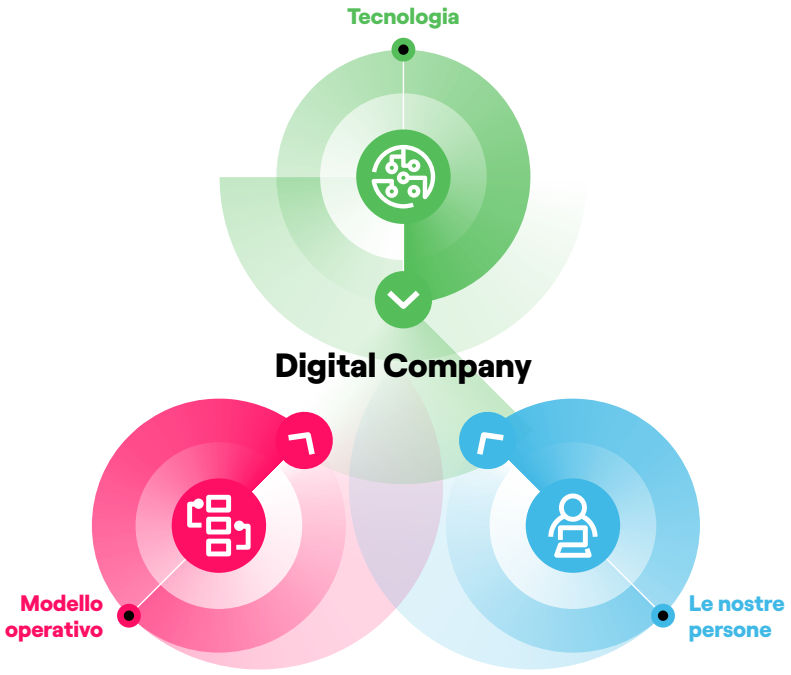
EVENTI PER LA DIFFUSIONE DELLA SICUREZZA INFORMATICA

18 eventi nel 2021

+5,6%

La tecnologia rappresenta uno strumento imprescindibile per innovare, guidare e abilitare la costruzione di modelli di sviluppo sostenibile.
Le tecnologie digitali, sia quelle consolidate sia quelle d'avanguardia, sono infatti in grado di fornire un grande contributo al miglioramento dell'efficienza energetica, alla decarbonizzazione, allo sviluppo di processi aziendali e produttivi automatizzati, favorendo l'economia circolare e promuovendo nuovi modelli di business. Attraverso tali piattaforme è possibile raggiungere crescenti livelli di scalabilità e di efficienza, riducendo i costi marginali.
In particolare:

- le nostre **piattaforme digitali globali** promuovono la crescita delle energie rinnovabili fornendo interfacce comuni e soluzioni intelligenti, grazie a tecnologie come Digital Twin e Intelligenza Artificiale, che migliorano le attività di sviluppo del business, di ingegneria e costruzione, di funzionamento e manutenzione;
- il miglioramento della qualità del servizio, dell'efficienza e della resilienza delle nostre infrastrutture di rete è guidato da un'unica piattaforma digitale, **Grid Blue Sky**, che standardizza e ottimizza le fasi di ingegneria, di funzionamento e manutenzione, ponendo i clienti al centro di ogni attività;
- la nostra base clienti globale è gestita dalla piattaforma **Customer Operations**, che rende smart, replicabili e automatizzati i processi di assistenza ai clienti, di attivazione di servizi, di pagamento e fatturazione. Stiamo inoltre sfruttando le piattaforme digitali di Enel X per offrire a livello globale prodotti e servizi innovativi per i segmenti B2C, B2B e B2G;
- l'esperienza lavorativa di tutte le nostre persone è sempre più supportata dal digitale, consentendo loro di focalizzarsi su attività a maggior valore aggiunto e garantendo la loro sicurezza.



La digitalizzazione sostenibile e il digitale per la sostenibilità

La nostra trasformazione digitale mira a impiegare soluzioni digitali quali strumenti per lo sviluppo di un futuro sostenibile, e a svilupparle sulla base di criteri di sostenibilità. Le principali linee d'azione del 2022 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 dell'adozione dei princípi per i diritti umani con i fornitori di prodotti e soluzioni digitali. Per ulteriori informazioni si vedano i capitoli "Gestione dei diritti umani" e "Catena di fornitura sostenibile".

Diverse sfide sono state lanciate nell'ambito della piattaforma openinnovability.com al fine di coinvolgere l'ecosistema nella loro risoluzione (si veda il capitolo "Innovazione").
Inoltre, in linea con gli obiettivi di decarbonizzazione al 2030, nel 2022 nelle gare di servizi professionali digitali, sono stati inseriti alcuni fattori premianti basati sul Global Warming Potential con il fine di assegnare un maggiore punteggio tecnico ai partecipanti caratterizzati da minori emissioni di gas serra in termini di CO_{2eq}.

Nel 2022 abbiamo predisposto e pubblicato la **Policy per la Sostenibilità Digitale**, che fissa l'orientamento verso la sostenibilità delle iniziative del Gruppo considerando il digitale come elemento centrale. Con tale Policy ci impegniamo a garantire che le soluzioni digitali aziendali siano conformi ai criteri di sostenibilità, oltre a promuovere un utilizzo sostenibile delle tecnologie in tutti i processi aziendali, in tutte le fasi di vita delle iniziative e nei diversi Paesi del Gruppo.
Abbiamo inoltre avviato nel 2022 un progetto per la **creazione di un framework aziendale per valutare e mitigare il rischio etico correlato all'uso delle intelligenze artificiali** e garantirne un utilizzo sicuro ed efficiente, in linea con le novità legislative a livello europeo.

PIATTAFORME: rapidità ed efficacia per rispondere ai continui cambiamenti

Roberto Bianchessi
Head of Platformization Services – Global Digital Solutions

La nuova strategia aziendale che trasforma la complessità in opportunità

"Le piattaforme hanno un ruolo fondamentale per l'Azienda, ovvero quello di essere 'fabbriche di fiducia' per tutti i colleghi. Permettono di condividere la conoscenza, abilitando nuovi modelli operativi e di business."

Le piattaforme digitali rappresentano uno dei pilastri della strategia di Enel, essendo, insieme agli ecosistemi, strumenti basati sulla massima condivisione delle informazioni e della fiducia reciproca.
Essere "platform-oriented" ci consente di creare un vantaggio competitivo, dal momento che le piattaforme digitali abilitano nuovi modelli di business (per esempio, sharing economy) e operativi.
La Enel Digital Platform è il passo finale per realizzare appieno il potenziale digitale di Enel: permette di avere accesso facilitato a tutte le basi di dati aziendali, rompendo silos e barriere informative, stimolando la collaborazione e la sostenibilità digitale.
Il riuso dei dati e lo sviluppo consapevole dei software, infatti, hanno impatti diretti sulla riduzione delle emissioni di carbonio. La stessa Piattaforma Enel sarà un ecosistema di tecnologie, metodologie, servizi e competenze profondamente radicate nella cultura aziendale. L'obiettivo è favorire ecosistemi digitali di sviluppo partecipativi e fortemente basati sul valore dei dati, nella logica dell'operatività agile e attraverso l'utilizzo della tecnologia cloud.
Per questo motivo, nel 2022 Enel ha deciso di lanciare l'iniziativa Platform School per diffondere tra tutte le persone Enel le potenzialità della Platformization attraverso un modello educativo del tipo "train the trainer": formatori interni all'Azienda, abili nel condividere nozioni strategiche, guidano la trasmissione dei saperi attraverso video e minipillole di approfondimento.

I principali driver della trasformazione digitale

Cloud

Il cloud rappresenta un abilitatore strategico fondamentale che consente l'utilizzo di risorse informatiche, sia infrastrutturali sia applicative, e che, sfruttando appieno le possibilità di accesso messe a disposizione dalla rete, permette di ridurre gli sprechi legati ai consumi di risorse inutilizzate. La migrazione delle applicazioni sul cloud ha permesso di ridurre notevolmente la domanda di utilizzo di energia e di conseguenza il consumo di risorse. Dal 2019 a oggi, a fronte di un aumento considerevole di storage dati e capacità elaborativa, è stata registrata una riduzione delle emissioni di CO_2 del 52%.

Unified Communications and Collaboration (UCC)

Servizi come messaggistica istantanea (chat), telefonia IP, audio conferenza e videoconferenza sfruttano appieno il modello di condivisione che, attraverso internet, consente di condividere e godere di contenuti da personal computer, smartphone o tablet, riducendo la necessità di spostamenti e quindi le emissioni di anidride carbonica.

Data sharing ed Enel Application Programming Interface (e-API)

L'ecosistema e-API è l'ambiente digitale attraverso il quale tutte le società del Gruppo possono condividere rapidamente e in tempo reale, attraverso interfacce e tracciati dati standard, 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, e a ridurre le ridondanze dei dati all'interno del Gruppo e, più in generale, la quantità di tempo e di risorse impiegate nello scambio di flussi informativi. Nel 2022 sono state realizzate 63 nuove interconnessioni e-API.

Machine learning e predictive maintenance

Adottiamo le tecnologie di machine learning per condurre analisi predittive in relazione alla manutenzione delle reti di distribuzione elettrica e degli impianti di generazione, identificando in anticipo possibili errori e intervenendo prima del verificarsi di guasti sui principali componenti. Ridurre il rischio di malfunzionamenti ha un impatto rilevante non solo a livello economico ma anche sull'ambiente e sulla sicurezza delle persone. L'uso di tali tecnologie consente, quindi, una migliore qualità del servizio fornito, rendendolo più sostenibile nel tempo, un uso ottimizzato delle risorse interne e ispezioni focalizzate sugli apparati più esposti al rischio di guasto.

Circolarità dei dispositivi digitali

La dismissione dei dispositivi aziendali genera rifiuti il cui smaltimento merita particolare attenzione. Per questo motivo, la gestione circolare degli asset digitali, nei diversi Paesi del Gruppo, avviene salvaguardando sia l'estensione della vita utile dei dispositivi, mediante la vendita degli stessi ai dipendenti o a terze parti (13.427 dispositivi venduti nel 2022), sia lo smaltimento di tali dispositivi in accordo ai princípi di riciclo, per un totale di 33 tonnellate di apparati nel 2022; i dispositivi, categorizzati come rifiuti elettronici, vengono smaltiti presso alcuni fornitori, che poi ricicleranno i dispositivi stessi.

Digital Carbon Footprint

Nel 2022 abbiamo avviato diverse iniziative per monitorare e ridurre le emissioni legate al digitale, volte principalmente a ottimizzare e consolidare l'utilizzo dell'infrastruttura cloud, promuovere la gestione circolare e sostenibile degli asset digitali e incentivare lo sviluppo e l'utilizzo consapevole e responsabile di software e hardware.

In questo contesto abbiamo sviluppato un Digital Carbon Footprint Framework che ci ha permesso di confermare che, a fronte di un incremento di capacità computazionale dei nostri sistemi del 200% e di un incremento della capacità di data storage pari al 107%, siamo riusciti a ottenere una riduzione del 26% delle emissioni di CO_2 da fonti digitali tra il 2018 e il 2022.

Il digitale per le persone

A scuola di "Digital Sustainability"

Nel 2022 abbiamo messo a disposizione delle nostre persone un percorso formativo sulla "Sostenibilità Digitale", costituito da 10 video, per meglio comprendere in che modo il digitale ci guida verso il raggiungimento degli obiettivi di sviluppo sostenibile dell'Agenda 2030 delle Nazioni Unite. Tale percorso formativo, realizzato in collaborazione con la Fondazione per la Sostenibilità Digitale, si propone inoltre di aumentare la consapevolezza di tutti noi sui comportamenti legati all'utilizzo delle tecnologie digitali, consentendoci di comprendere il contributo che possiamo apportare nel quotidiano alla sostenibilità. I video sono oggi disponibili in cinque lingue e si contano oltre 50mila visualizzazioni tra le persone Enel di tutto il mondo.

Accessibilità e inclusività dei sistemi digitali

L'utilizzo dei dati e della logica a piattaforma, unito all'accessibilità e inclusività dei sistemi digitali, permette l'accesso a nuovi modelli di business solidale e a nuove offerte di servizi e prodotti anche ai clienti vulnerabili.

L'accessibilità delle soluzioni digitali va prevista già nella fase di progettazione e per tale ragione nel 2022 è stata creata l'unità organizzativa Digital Accessibility, con lo scopo di agire come punto di contatto per il Gruppo per supportare la gestione di iniziative in materia e lo sviluppo di prodotti e servizi digitali facili da usare e conformi alla normativa e agli standard di riferimento.

Una nuova vita per i nostri PC

L'iniziativa di donazione dei personal computer alla fine della loro vita utile aziendale è stata ideata e attuata con lo scopo di creare un impatto sociale positivo a favore di soggetti pubblici e privati, che svolgono a diverso titolo attività di rilevanza sociale e/o che perseguono scopi di pubblica utilità. Dando una nuova vita ai PC, per il secondo anno di seguito, rafforziamo sia il nostro impegno a sostegno delle comunità nei Paesi in cui operiamo, promuovendo l'inclusione digitale, sia l'economia circolare dei dispositivi digitali, assicurando l'estensione di vita utile degli apparati attraverso il riuso. Nel 2022 sono stati donati 213 dispositivi.

Riunioni virtuali[1]

Oltre **7,3 milioni** di riunioni
Più di **639,3mila tonnellate** di CO_2 evitata

Servizio di stampa[2]

81 milioni di pagine stampate
5,8 tonnellate di CO_2 prodotta

Continua a essere operativo in tutte le sedi del Gruppo il servizio di stampa, basato su modelli di stampanti di nuova generazione già predisposti per un utilizzo più ecosostenibile. La peculiarità di tale servizio, unitamente a un utilizzo più razionale delle stampe e alla digitalizzazione, ha consentito negli anni una riduzione del consumo di carta e conseguentemente un minore impatto sull'ambiente.

(1) Oltre 7,3 milioni di riunioni nel 2021, quasi 5,1 milioni nel 2020 e 244mila nel 2019, rispettivamente con un contributo di CO_2 evitata pari a 587,5mila tonnellate nel 2021, 444,7mila tonnellate nel 2020 a fronte di 242,1mila nel 2019.
(2) 83 milioni di pagine stampate nel 2021, 88 milioni di pagine stampate nel 2020 e 136 milioni nel 2019, che rispettivamente hanno prodotto 6,5, 8,4 e 12,5 tonnellate di CO_2.

PC Power Management – Italia[3]

7,3 milioni di ore di utilizzo
48,8 tonnellate di CO_2 prodotta

Nel 2022 è proseguito il monitoraggio del consumo di energia elettrica al di fuori del normale orario di lavoro[4] relativamente alle postazioni informatiche (desktop, laptop, monitor) delle nostre persone che lavorano in Italia. Tale misurazione è possibile grazie alla presenza sulle postazioni informatiche di una funzionalità Microsoft (System Center Configuration Manager), che ha permesso di individuare quando una postazione risulta accesa e non utilizzata. A valle delle analisi effettuate sono definite specifiche azioni di sensibilizzazione volte alla mitigazione del consumo elettrico. Anche quest'anno vi è stato un decremento nelle ore di inutilizzo, dovuto sia alle azioni di sensibilizzazione portate avanti nel tempo sull'efficientamento energetico, sia ai nuovi strumenti informatici messi a disposizione delle nostre persone durante la pandemia da Covid-19, che hanno permesso una riduzione delle emissioni. Il potenziamento dell'utilizzo di dispositivi mobili ha infatti consentito di ridurre il numero di dispositivi fissi nelle sedi del Gruppo, e di conseguenza l'ammontare di tempo in cui i dispositivi risultano accesi fuori dall'orario di lavoro.

(3) 12 milioni di ore di utilizzo nel 2021, 18 milioni nel 2020 e 32 milioni nel 2019, che rispettivamente hanno prodotto 77,4, 159,6 e 321,1 tonnellate di CO_2.
(4) Lunedì-venerdì (dalle 19 alle 7); sabato e domenica. Il monitoraggio ha escluso i server e i personal computer che, per loro natura, devono essere sempre operativi. Nello specifico l'indicatore rappresenta l'ammontare di CO_2 associata al consumo elettrico dei desktop, laptop e monitor, cui poi viene applicato il valore medio di emissione di CO_2 per unità di energia elettrica prodotta (gCO_2/kWh) relativo al mix di fonti in Italia.

Verso una elettrificazione cyber-safe

Nell'era della trasformazione digitale, la **cyber security** assume un ruolo fondamentale per garantire l'operatività delle imprese.
Le tipologie di attacchi informatici sono cambiate drasticamente negli ultimi anni: il numero è cresciuto in modo esponenziale, così come il loro grado di sofisticazione e impatto, per queste ragioni è sempre più difficile identificarne tempestivamente la fonte. Studi di settore confermano che la percezione del rischio cyber è in costante crescita. Rispetto agli anni precedenti, le cause dell'aumento degli attacchi informatici includono anche tensioni geopolitiche. Il conflitto tra Russia e Ucraina ha infatti aumentato l'attenzione in questo senso. In particolare, tutte le agenzie di sicurezza statali hanno messo in guardia Istituzioni pubbliche e private da potenziali minacce informatiche contro le infrastrutture critiche.
Nel 2022 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". È interessante osservare, inoltre, che la maggior parte degli attacchi al settore energetico 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.
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 scoperte prima che gli sviluppatori di software ne vengano a conoscenza e prima che possano rilasciare un aggiornamento correttivo (patch).
In un simile contesto di cyber-warfare, l'unica difesa possibile è data da processi e tecnologie, messi a punto ed evoluti nel tempo e volti a mitigare il rischio informatico. Oltre alla costante applicazione della strategia di cyber security, abbiamo quindi previsto specifiche misure straordinarie, anche volte a rafforzare la "cyber security posture"[(5)], consapevoli del fatto che il rischio cyber, nel complesso e interconnesso settore elettrico, assume proporzioni diverse, divenendo un rischio di portata ecosistemica. In tale scenario, per esempio, un blackout su larga scala avrebbe ramificazioni socio-economiche tra famiglie, imprese e istituzioni vitali.
Elemento chiave diventa quindi la condivisione e la cooperazione sui temi di cyber security tra tutti gli stakeholder, siano essi aziende, organi legali o di controllo, fornitori, clienti o dipendenti.

Politiche e modello di gestione

In linea con le esigenze del settore industriale energetico e in coerenza con l'approccio strategico Open Power che lo caratterizza, abbiamo adottato una visione sistemica dei temi della cyber security, nonché una strategia globale di analisi, prevenzione e gestione degli eventi di sicurezza informatica. Il percorso della cyber security a supporto della trasformazione digitale del Gruppo si basa sulla definizione, valorizzazione e adozione di un modello di governance, infrastrutture e servizi di sicurezza, al fine di sfruttare al meglio le opportunità disponibili, anche coadiuvate da tecnologie all'avanguardia, per aumentare la resilienza informatica di infrastrutture e applicazioni.
Da settembre 2016, all'interno della Funzione Global Digital Solutions 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 policy 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 posture" mediante controlli basati su processi e tecnologia, e ancora il presidio e l'attuazione 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 gestione dei sistemi, grazie alle figure dei Cyber Security Risk Manager e dei Cyber Security Response Manager. Il CISO e i Cyber Security Risk Manager costituiscono inoltre il Cyber Security 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 periodica-

(5) Per "Cyber Security Posture" si intende lo stato di adozione da parte della società dei princípi di sicurezza informatica.

mente i progressi della sua attuazione. Il Comitato, come stabilito nell'incontro di aprile 2021, si riunisce con cadenza semestrale; nel 2022 si sono tenuti due incontri (maggio e ottobre).
Il 2022 è stato caratterizzato, inoltre, da 3 incontri del Comitato Controllo e Rischi con l'obiettivo di approfondire aspetti legati alle procedure organizzative (sia a livello tecnico sia di governance), al processo di crisis management, al modello operativo del CERT e ai relativi processi che lo caratterizzano.
Tutte le aree partecipano attivamente all'attuazione della strategia di cyber security attraverso un piano operativo integrato e allineato agli obiettivi del Gruppo. Inoltre, la strategia e le iniziative di cyber security sono oggetto di costante approfondimento dei principali board esecutivi e di controllo (per esempio, Board of Directors, Organismi di Vigilanza ecc.) per tutte le legal entity e i Paesi di presenza del Gruppo.

Attraverso la policy di Gruppo adottata nel 2017, il "**Cyber Security Framework**", si indirizzano, inoltre, 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, nel 2017 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 inoltre 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 USA, il numero di accreditamenti ha raggiunto quota 9: Romania, Italia, Cile, Argentina, Perù, Colombia, Brasile, Spagna e USA. Il CERT di Enel fa anche parte di Trusted Introducer, un servizio che comprende 464 CERT distribuiti in 72 Paesi. A settembre 2018 ha aderito anche a FIRST (Forum of Incident Response and Security Teams), la più grande ed estesa comunità del settore con 602 membri dislocati in 99 Paesi. Nel corso del 2022, inoltre, il modello operativo del CERT è stato potenziato con la creazione di un team interno di analisti di sicurezza. Il nuovo modello operativo ha superato quello precedente, implementando l'internalizzazione delle attività di monitoraggio e gestione degli incidenti e potenziando, quindi, le attività h24.

Definizione della strategia di sicurezza informatica

La strategia di cyber security ingloba le attività legate alla definizione di obiettivi e priorità, al fine di indirizzare e coordinare le iniziative di investimento per il Gruppo nel suo complesso e garantire l'aderenza alle policy 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 operiamo (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 integrati nella vita digitale del Gruppo, hanno 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 3 miliardi di eventi relativi agli asset aziendali da 7mila data source, li mette in correlazione sfruttando l'analisi automatica, e produce in media un centinaio di "incident". 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 2022 **il CERT ha bloccato in media 1,2 milioni di e-mail a rischio, 57 virus, 172 attacchi a portali web e 1,3 milioni di connessioni a siti pericolosi**.

Nel corso del 2022 il CERT di Enel ha risposto a: **175 incidenti di sicurezza informatica con livello di impatto 2; 16 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 policy del Gruppo Enel "**Personal 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 Enel, le opportune azioni sono intraprese immediatamente, in linea con la specifica policy di Gruppo in materia di "Gestione degli eventi critici".
La policy "**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.

La tecnologia di EDR (Endpoint Detection and Response) è volta al blocco delle violazioni attraverso l'uso di feature innovative e paradigmi avanzati, in grado non solo di identificare i virus e i malware presenti sugli endpoint, ma anche di rilevare sequenze sospette di eventi tecnici che potrebbero rivelarsi parte di un tentativo di attacco.

Relativamente al numero degli eventi di sicurezza informatica registrati nel corso del 2022, di seguito si riportano i dettagli.

	2022
Numero totale di violazioni della sicurezza delle informazioni o altri incidenti di sicurezza informatica[1]	0
Importo totale delle multe/sanzioni pagate in relazione a violazioni della sicurezza delle informazioni o altri incidenti di sicurezza informatica	0
Numero totale di clienti e dipendenti impattati da data breach che hanno interessato il Gruppo	0
Numero totale di data breach[2]	0

(1) Il valore riferito alla numerosità del KPI "Numero totale di violazioni della sicurezza delle informazioni o altri incidenti di sicurezza informatica" è relativo agli incidenti di livello 4.
(2) Il KPI "Numero totale di data breach" si riferisce al numero di eventi occorsi per effetto di un incidente di sicurezza informatica (ciò implica che la numerosità riportata non contempla eventuali disclosure occorse per effetto di incidenti non digitali).

Inoltre, al fine di rafforzare la capacità di prevenzione, reazione, e gestione degli incidenti, con il coinvolgimento del personale attivo negli ambienti di produzione, sono stati eseguiti alcuni **cyber exercise**, esercitazioni volte alla simulazione di un reale attacco. Al termine di ciascuna esercitazione sono stati prodotti report contenenti le azioni di dettaglio circa lo svolgimento della simulazione, con l'obiettivo di valutare, in un'ottica di continuo miglioramento, qualità e completezza del materiale fornito a supporto delle decisioni, tempi di esecuzione per ogni fase e coerenza con le procedure. Nel 2022, in particolare, sono stati eseguiti 50 cyber exercise in ambienti industriali in 11 Paesi di presenza del Gruppo.

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.

CERT – RISK MONITORING EXTENSION

"**CERT – Risk Monitoring extension**". Il CERT impiega tecnologie emergenti come SOAR (Security Orchestration, Automation and Response) e machine learning a supporto dei Big Data, che consentono di automatizzare e velocizzare le attività di gestione degli incidenti e di sfruttare una migliore visibilità sulle minacce informatiche, aumentando l'efficienza nella gestione di quelle nuove e delle relative indagini. In particolare, grazie al sistema SOAR, attraverso la definizione di flussi operativi, è possibile automatizzare task ripetitivi; mentre attraverso il machine learning, una branca dell'intelligenza artificiale, è possibile apprendere o migliorare le capacità di rilevamento sulla base dei dati disponibili.
Queste tecnologie consentono di accelerare, arricchire e tracciare in modo consistente le attività necessarie durante le fasi di analisi e gestione di un incidente, fornendo un grande supporto all'analista che può così parallelizzare e concentrarsi sui compiti più complessi che richiedono l'intervento umano.

MULTI-FACTOR AUTHENTICATION (MFA)

"**Multi-Factor Authentication (MFA)**" è una soluzione cloud utilizzata per imporre il metodo di identificazione per gli utenti durante la procedura di autenticazione. L'adozione della MFA permette di riconoscere una persona che accede a un sistema tramite un secondo fattore di autenticazione, fruibile tramite SMS o app installata sullo smartphone. La soluzione MFA è in linea con il quadro regolatorio ed è fortemente raccomandata per contrastare le minacce emergenti di furto di credenziali, anche basate su tecniche di social engineering (per esempio, il phishing o eventuali comportamenti degli utenti non aderenti alle policy). L'adozione della soluzione è a regime per tutti gli utenti.

CONTROLLI DI ASSURANCE

Controlli di assurance (Ethical Hacking, Vulnerability Assessment). Tali attività vengono svolte in maniera costante sia con l'ausilio di strumenti automatici sia manualmente, al fine di valutare e quantificare eventuali debolezze in ambienti IT, OT e IoT (applicazioni, sistemi, dispositivi IoT, architetture e/o infrastrutture). Nel 2022 sono stati eseguiti 1.587 controlli. A valle degli stessi è possibile identificare le misure più idonee per eliminare o mitigare le vulnerabilità o le minacce rilevate e, di conseguenza, gli eventuali exploit dannosi associati.

DMARC "E-MAIL FRAUD DEFENSE"

DMARC "E-mail Fraud Defense". La soluzione completa la mappa applicativa a copertura delle minacce di spam, phishing e dei tentativi di frode. Grazie a quest'ultima, tutti i domini di posta elettronica di Enel sono stati configurati per consentire il blocco delle e-mail con un indirizzo mittente falso che sfrutta il brand di Gruppo. Il deployment è avvenuto sull'intero perimetro, fornendo così una copertura totale dei domini.

Collaborazioni con organismi ed enti esterni

In linea con l'approccio Open Power, consideriamo la rete di relazioni con le realtà esterne e le organizzazioni 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 2022 abbiamo fornito feedback in consultazioni pubbliche che hanno contribuito al disegno normativo in tema di cyber security, anche attraverso azioni di drafting legislativo, promuovendo l'armonizzazione dell'attuale panorama normativo in materia e l'attuazione di un approccio basato sul rischio e sul principio di security by design. Fra le collaborazioni avute, si annoverano quelle volte alla costruzione di assetti più omogenei nella definizione della tassonomia degli incidenti di sicurezza, di più organici criteri di classificazione degli stessi, unitamente a una modalità più armonica nelle procedure di notifica in contesti europei. Queste collaborazioni sono anche guidate da un composito panorama normativo in materia di cyber security, sia in termini di aumento delle norme prodotte sia in termini di complessità, principalmente dovuta alle nuove normative che si aggiungono ogni anno, oltre che all'eterogeneità dei requisiti e dei metodi di adozione.
In questo senso, il processo mirato alla compliance normativa può avere un forte impatto, sia sui processi aziendali sia sull'infrastruttura tecnologica, richiedendo un grande sforzo in termini di gestione e monitoraggio.
Inoltre, tenendo in considerazione il contesto di compliance normativa, **nel 2022 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) e ONS (Operador Nacional do Sistema Elétrico) in Brasile e CNO (Consejo Nacional de Operación) in Colombia. Abbiamo preso parte, per esempio, al team di Confindustria Digitale, che ha lo scopo di dare contributi allo sviluppo dell'ecosistema digitale italiano, abbiamo 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" e "Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors".
Inoltre, Enel X, Gridspertise ed Enel Grids hanno raggiunto un importante traguardo nel campo della sicurezza delle informazioni, ottenendo la **certificazione ISO 27001**. Questo importante risultato certifica alcuni processi dotati di un sistema di gestione della sicurezza delle informazioni – politiche, procedure e linee guida per fornire ai clienti prodotti e servizi trusted.

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 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. Si avvale, inoltre, 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 2022, 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. A titolo esemplificativo, nell'ambito di tali iniziative, la Policy no. 1097 "Rules of Behavior for Digital People", è stata integrata con una guida rapida, disponibile in tutte le principali lingue adottate dal Gruppo (5 differenti lingue), volta ad agevolare una veloce consultazione dei temi per indirizzare il corretto uso di risorse digitali. Sono stati inoltre predisposti e diffusi bollettini e notizie attraverso la intranet aziendale, e messi a disposizione documenti per mantenere un aggiornamento costante su tali temi. Tutto ciò è stato reso possibile anche grazie alla piattaforma di awareness "TheRedPill", la piattaforma di Gruppo attraverso cui sono stati erogati contenuti e moduli formativi volti a potenziare la cultura in ambito di sicurezza informatica, consentendo il miglioramento continuo delle iniziative di formazione e l'esecuzione di campagne di phishing simulato. L'obiettivo è generare e potenziare la consapevolezza sulle principali tematiche di cyber security, di indirizzare eventuali esigenze di upskilling e reskilling e di insegnare come difendersi da eventuali attacchi. Nel 2021, anno in cui ha avuto luogo l'aggiornamento della piattaforma, sono state lanciate quattro campagne globali di phishing simulato, un knowledge assessment e una campagna di sensibilizzazione. Nel 2022 sono state lanciate ulteriori iniziative a livello globale, quali la diffusione del modulo "Antiphishing Kit", o il lancio del

"People Cyber Empowerment Journey", ovvero il programma che mira a portare le persone di Enel a essere la prima linea di difesa informatica. Inoltre, sono state disegnate e lanciate 6 campagne di phishing simulato, 3 campagne di sensibilizzazione relative alla protezione dell'identità digitale, alla protezione dei dati e dei device, e 19 eventi volti alla diffusione della cultura di sicurezza informatica (c.d. "knowledge sharing").

In aggiunta alle iniziative di diffusione e comunicazione, nel corso del 2022 sono proseguite le campagne di phishing simulato rivolte all'intera popolazione Enel, con l'obiettivo di allenare i dipendenti a riconoscere le e-mail malevole. A seguito dei risultati ottenuti dalle campagne di phishing, sono state realizzate iniziative specifiche per aumentare la sensibilità e la consapevolezza dei dipendenti (per esempio, specifiche infografiche, istruzioni e linee guida sono state condivise con coloro i quali non sono stati in grado di riconoscere l'e-mail di phishing).
Il progetto **Open Tech Journey** è proseguito con l'obiettivo di rendere disponibili corsi di formazione incentrati su temi tecnologici, promuovendo le capacità interne per diffondere la conoscenza su temi strategici e per gestire esigenze di upskilling e reskilling. In tale ambito è stata attivata la **Cyber School**, con un'offerta di sette corsi sui principali temi legati alla cyber security. Tutti i corsi sono stati ingegnerizzati e resi disponibili a tutta la popolazione Enel in modalità e-learning, con l'obiettivo di raggiungere competenze multi-specialistiche nelle diverse realtà aziendali del Gruppo.

Concept design e realizzazione
Gpt Group

Revisione testi
postScriptum di **Paola Urbani**

Pubblicazione fuori commercio

A cura di
Comunicazione Enel

Enel
Società per azioni
Sede legale 00198 Roma
Viale Regina Margherita, 137
Capitale sociale Euro 10.166.679.946 i.v.
Registro Imprese di Roma, Codice Fiscale 00811720580
R.E.A. 756032 Partita IVA 15844561009