OPEN POWER FOR A BRIGHTER FUTURE.

WE EMPOWER SUSTAINABLE PROGRESS.

Our performance 2022
Digitalization

enel

Our performance

Ambition of zero emissions and clean electrification

lies at the heart of the strategy we are implementing in a sustainable and innovative way, to favor a **just transition**.

People are the mainstays of sustainable progress,

not only ours, but also customers, suppliers, communities, institutions, the financial community, the media, companies and trade associations.

Innovation, circular economy, digitalization and sustainable finance

are the growth accelerators, and embrace and enhance all strategic themes across the board.

Protection of nature and respect for human rights

form our daily commitment to the current and future generations.

Digitalization

Below the 2022 results related to the targets of the previous 2022-2024 Sustainability Plan, the resulting progress and the targets of the 2023-2025 Sustainability Plan, which may be redefined, added to, or surpassed with respect to the previous Plan.

Cyber security

SDG	Activities	2022 results	Progress	2023-2025 targets	Tag
4 9 11	Disseminating the IT security culture and changing people's behaviour in order to reduce risks	**19** cyber security knowledge-sharing events executed	●●●	**15** cyber security knowledge-sharing events executed each year	S T
9 11	Information security verification activities (Ethical Hacking, Vulnerability Assessment, etc.)	**1,587** verification activities carried out	●●●	**1,400** verification activities each year	T
9 11	Execution of cyber exercises involving plants/industrial sites	**50** cyber exercises carried out	●●●	**186** cyber exercises in the period 2023-2025	S T

Read more

Cyber exercises are drills aimed at simulating a cyber security incident, carried out with the objective of training the reaction capacity of the involved subjects and testing the processes and technologies in the field. The exercises are conducted by Enel's Cyber Emergency Readiness Team (CERT) and involve both technical and business reference structures. The simulation performed generates awareness and addresses possible needs for improvement of technical or organizational aspects.

I Industrial E Environmental S Social
G Governance T Technological

Goals: New, Redefined, Outdated

Progress: Not in line, In line, Achieved

N.A. = not applicable

Digital solutions

SDG	Activities	2022 results	Progress	2023-2025 targets	Tag
12 13	Activities to reduce CO_2 emissions	**-54.8 mil** printed pages (vs 2019)	●●●	**-17 mil** printed pages in 2025 (vs. 2019)	E S T
		7.3 mil hours of downtime outside normal working hours	●●○	Activities to reduce PC, laptop and monitor downtime	E S T
		7.3 mil meetings held via video communication services	●●○	Extended use of video communication systems	E S T
9 12	Reuse and exchange of information in the e-API Digital Ecosystem	**63** new e-API interconnections	●●●	**100** new e-API interconnections in the period 2023-2025	S T

Read more

The **e-API Digital Ecosystem** is the digital environment through which all the companies of Enel Group can easily, quickly and automatically share information normally confined within specific vertical applications ("silos" of information). Thanks to the enabling technology of the API (Application Programming Interface), Enel's data flows and functionalities are treated as "data-as-a-product", fostering sustainability through a real reuse and exchange of information and a reduction of time and resources needed.

Digitalization

1,587

ASSURANCE CHECKS (ETHICAL HACKING, VULNERABILITY ASSESSMENT)

1,580 in 2021

+0.4%

6

SIMULATED PHISHING CAMPAIGNS

4 campaigns in 2021

+50%

19

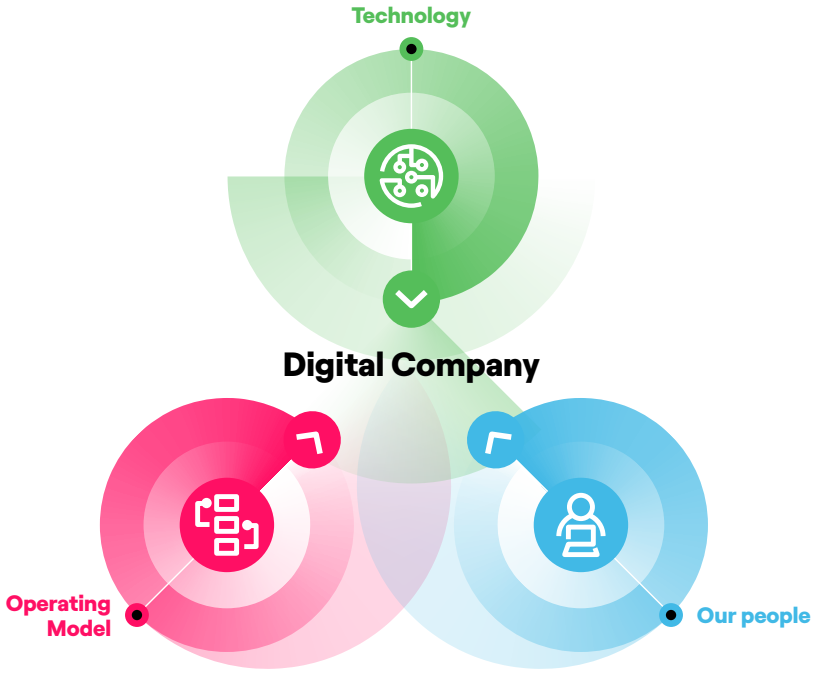
EVENTS TO RAISE AWARENESS OF CYBER SECURITY

18 events in 2021

+5.6%

Technology is essential in order to innovate, guide and enable the creation of sustainable development models.
Indeed, digital technologies, both established and cutting-edge, contribute significantly to improving energy efficiency, decarbonization, and the development of automated business and production processes, thus promoting the circular economy and new business models.
Through such platforms, increasing levels of scalability and efficiency can be achieved, reducing marginal costs.
Specifically:

- our **global digital platforms** promote the growth of renewable energy by providing common interfaces and smart solutions, thanks to technologies such as Digital Twin and Artificial Intelligence, which improve business development, engineering and construction, operation and maintenance;
- improving service quality, efficiency and the resilience of our grid infrastructure is driven by a single digital platform, **Grid Blue Sky**, which standardizes and optimizes the engineering, operation and maintenance phases and places the customer at the heart of every activity;
- our global customer base is managed by the **Customer Operations** platform, which renders the customer support, service activation, payment and billing processes smart, replicable and automated. We also leverage Enel X's digital platforms to globally offer innovative products and services for the B2C, B2B and B2G segments;
- the working life of all our people is increasingly supported by digital, allowing them to focus on higher value-added activities and ensuring their security.



Sustainable digitalization and digital for sustainability

In our digital transformation, we aim to use digital solutions as tools for the development of a sustainable future, and to develop them on the basis of sustainability criteria.
The main actions taken in 2022 concerned:

- decarbonization and reduction of emissions linked to digital solutions;
- circularity of the digital devices and materials comprising the digital assets of the Group;
- promotion of social inclusion through the development of assistive technologies and solutions that ensure accessibility and generate value by meeting local needs;
- promotion of best environmental performance and adoption of human rights principles with the suppliers of digital products and solutions. For more information, see the chapters on "Managing human rights" and "Sustainable supply chain".

Several challenges have been launched on the openinnovability.com platform with a view to incorporating environmental considerations in their resolution (see chapter on "Innovation").

Furthermore, in line with the 2030 decarbonization targets, a number of criteria based on Global Warming Potential were included in tenders for digital professional services in 2022, which allow participants with lower greenhouse gas emissions in terms of CO_{2eq} to gain a higher technical score.

In 2022, we drafted and published our **Digital Sustainability Policy**, which establishes the sustainability orientation of the Group's initiatives and considers digital to be a key factor. With this Policy, we are committed to ensuring that the Company's digital solutions comply with sustainability criteria, as well as promoting the sustainable use of technology in all business processes, at all stages of the initiatives and in the different countries of the Group.
We also launched a project in 2022 to create a **corporate framework in which to assess and mitigate the ethical risk related to the use of artificial intelligence** and ensure its safe and efficient use, in line with legislative changes at European level.

PLATFORMS: ensuring a rapid and effective response to continuous change

Roberto Bianchessi

Head of Platformization Services – Global Digital Solutions

The new Company strategy that transforms complexities into opportunities

"Platforms play a key role in the Company in that they build trust for all our colleagues. They make it possible to share knowledge, enabling new operational and business models."

The digital platforms are one of the pillars of Enel's strategy, since they are, together with the ecosystems, tools based on maximum information sharing and mutual trust.
Being platform-oriented allows us to create a competitive advantage as digital platforms enable new operational and business models (e.g., sharing economy).
The Enel Digital Platform is the final step in realizing Enel's full digital potential: it allows easy access to all Company databases, breaking down silos and information barriers, and fostering collaboration and digital sustainability.
The reuse of data and conscious software development have a direct impact on the reduction of carbon emissions.

This Enel Platform will be an ecosystem of technologies, methodologies, services and skills deeply embedded in the corporate culture. The goal is to foster participative and strongly data-driven digital development ecosystems, based on an agile approach to operations and the use of cloud technology.
For this reason, in 2022 Enel decided to launch the Platform School initiative to spread the potential of Platformization among all Enel people through a "train the trainer" educational model: in-house trainers, skilled in sharing strategic concepts, guide the transmission of knowledge through video and bitesize information materials.

Key drivers of the digital transformation

Cloud computing

The cloud represents a fundamental strategic enabler which allows us to use IT resources (both in terms of infrastructure and applications) and which, by making full use of the access possibilities provided by the network, allows to reduce waste tied to the consumption of unused resources. The migration of applications to the cloud made it possible to significantly reduce the demand for energy and consequently the consumption of resources. From 2019 to date, while data storage and processing capacity have increased considerably, there has been a 52% reduction in CO_2 emissions.

Unified Communications and Collaboration (UCC)

Services such as instant messaging (chat), IP telephony, audio and video conferencing take full advantage of the sharing model which, through the internet, allows content to be shared and enjoyed from personal computers, smartphones or tablets, thereby reducing the need to travel and, in turn, lowering carbon dioxide emissions.

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

The e-API ecosystem is the digital environment where all Group companies can share quickly and in real time – through standard interfaces and data paths – information that would normally remain confined to specific vertical applications (information silos). This ecosystem has helped speed up the adoption of digital solutions, reduce data redundancies within the Group and, more generally, reduce the amount of time and resources spent on exchanging information flows. A total of 63 new e-API interconnections were implemented in 2022.

Machine learning and predictive maintenance

We adopt machine learning technologies to conduct predictive analysis in relation to the maintenance of electricity distribution networks and generation plants, identifying possible errors in advance and acting before faults occur on the main components. Reducing the risk of malfunctions has a significant impact not only in economic terms, but also in relation to the environment and personal safety. Therefore, using these technologies improves the quality of service provided, making it more sustainable over time, while ensuring an optimized use of internal resources and inspections focusing on the equipment most exposed to the risk of failure.

Circularity of digital devices

The decommissioning of Company equipment generates waste, the disposal of which merits special attention. For this reason, the circular management of digital assets in the Group's various countries is achieved by safeguarding both the extension of the devices' service life, by selling them to employees or third parties (13,427 devices sold in 2022), and disposing of these devices in line with recycling principles, amounting to a total of 33 tons of equipment in 2022; devices categorized as electronic waste are disposed of at certain suppliers, who will then recycle the devices themselves.

Digital Carbon Footprint

In 2022, we launched several initiatives to monitor and reduce digital-related emissions, mainly aimed at optimizing and consolidating the use of cloud infrastructure, promoting circular and sustainable management of digital assets, and encouraging the conscious and responsible development and use of software and hardware.

In this context, we developed a Digital Carbon Footprint Framework, which confirmed that with a 200% increase in the computational capacity of our systems and a 107% increase in data storage capacity, we were able to achieve a 26% reduction in CO_2 emissions from digital sources between 2018 and 2022.

Digital for people

"Digital Sustainability" school

In 2022, we made available to our people a training course on "Digital Sustainability", consisting of 10 videos, to better understand how digital technology guides us towards achieving the UN 2030 Agenda's Sustainable Development Goals. This training course, delivered in collaboration with the Digital Sustainability Foundation, also aims to raise awareness of behaviors related to the use of digital technologies, enabling us to understand the contribution we can make in our daily lives to sustainability. The videos are now available in five languages and have over 50 thousand views among Enel people around the world.

Accessibility and inclusiveness in digital systems

The use of data and platform logic, coupled with the accessibility and inclusiveness of digital systems, allows access to new joint business models and the offer of new services and products, including to vulnerable customers.

The accessibility of digital solutions must be provided for at the design stage, which is why the Digital Accessibility organizational unit was created in 2022 in order to act as a point of contact for the Group and support the management of related initiatives and the development of digital products and services that are easy to use and compliant with the relevant regulations and standards.

A new life for our PCs

The initiative to donate personal computers that have reached the end of their service life has been implemented with the aim of creating a positive social impact on public and private entities, which carry out various kinds of activities of social relevance and/or which pursue public benefit purposes. By giving PCs a new life, for the second year we are reinforcing our commitment to supporting communities in the countries where we operate, by promoting digital inclusion and enhancing the circular economy of digital devices, thereby extending the equipment's service life through reuse. 213 devices were donated in 2022.

Video communication(1)

More than **7.3 million** meetings
More than **639.3 thousand tons** of CO_2 avoided

Printing service(2)

81 million pages printed
5.8 tons of CO_2 produced

The printing service, based on new generation printer models set up for a more eco-sustainable use, continues to be in operation at all Group offices. Together with a more rational use of prints and digitalization, the service has made it possible to reduce paper consumption over the years and, in turn, reduce the impact on the environment.

(1) More than 7.3 million meetings in 2021, almost 5.1 million in 2020 and 244 thousand in 2019, respectively avoiding contributing 587.5 thousand metric tons of CO_2 in 2021, 444.7 thousand in 2020 and 242.1 thousand in 2019.
(2) 83 million pages printed in 2021, 88 million in 2020 and 136 million in 2019, which respectively produced 6.5, 8.4 and 12.5 tons of CO_2.

PC Power Management – Italy[3]

7.3 million hours of use
48.8 tons of CO_2 produced

In 2022, we continued to monitor electricity consumption outside normal working hours[4] of the IT workstations (desktops, laptops, monitors) of our people working in Italy. This was measured thanks to a Microsoft function (System Center Configuration Manager) on the workstations, which can identify when a workstation is on and not being used. Following the analysis, specific awareness-raising initiatives were defined, aimed at reducing electricity consumption. Also this year, there has been a decrease in the hours of inactivity. This is thanks to both our awareness-raising activities on energy efficiency and to the new IT tools made available to our people during the Covid-19 pandemic, which enabled a reduction in emissions. The greater use of mobile devices has in fact made it possible to reduce the number of fixed devices in the Group's offices and, in turn, cut down the amount of time that devices are on outside working hours.

(3) 12 million hours of use in 2021, 18 million in 2020 and 32 million in 2019, which respectively produced 77.4, 159.6 and 321.1 tons of CO_2.
(4) Monday-Friday (from 7pm to 7am); Saturday and Sunday. Monitoring is not carried out on servers and personal computers which, by their nature, must be operational at all times. Specifically, the indicator represents the amount of CO_2 associated with the electricity consumption of desktop computers, laptops and monitors, calculated after applying the average CO_2 emission value per unit of electricity generated (gCO_2/kWh) in relation to the mix of sources present in Italy.

Towards cyber-safe electrification

In the era of digital transformation, **cyber security** is taking on a key role in ensuring business operations.
Typical cyber-attack types have changed radically in recent years: the number has grown exponentially, as has their level of sophistication and impact, making it is increasingly challenging to identify the source in a timely manner. Sector studies confirm that the perception of cyber risk is continuously growing. As compared to previous years, the causes for increased cyberattacks also include geopolitical tensions. In fact the conflict between Russia and Ukraine has increased attention about this issue. In particular, all state security agencies have warned public and private institutions about potential IT threads against critical infrastructures.
In 2022, many of the world's major attacks were carried out by leveraging the supply chain and through compromised third parties, which allowed attackers to target the primary target's customers, partners, and suppliers. This caused a sharp rise in the number of victims and attacks went increasingly undetected (the so-called "scale effect"). It is also interesting to observe that the majority of the attacks in the energy sector include ransomware, an increasingly used method that causes the exfiltration (unauthorized copy, transfer or recovery) of the victim's data and its encryption, which gives the people responsible for the attack an additional lever for receiving payment of ransom.
It is also seen how the vulnerabilities detected in commonly used software products are continuously increasing and how they are taken advantage of with greater speed by cyber criminals. In particular, the zero-day type vulnerabilities represent a large risk because they are discovered before software developers become aware of them and before they can release a patch.
In a similar context of cyberwarfare, the only possible defense is given by processes and technologies, which have been developed and evolved over time to mitigate the IT risk. On top of constantly applying the cyber security strategy, we have set out special measures, also in order to reinforce the "cyber security posture",[5] aware of the fact that overall, cyber risks can become a risk of ecosystemic proportions within the broader context of the complex and interconnected electricity industry. For example, a large-scale blackout in this scenario would have socio-economic ramifications throughout the population, companies and key institutions.
The key elements are therefore sharing and cooperation on cyber security issues with participation among all stakeholders including companies, legal institutions, supervisory bodies, suppliers, customers, and employees.

Policies and management models

In line with the needs of the energy industrial sector and with the Open Power strategic approach that characterizes it, we have adopted a systemic vision of cyber security issues, as well as a global strategy of analysis, prevention and management of cyber security events. The cyber security path to support the Group's digital transformation is based on creating, enhancing and adopting a security governance model, infrastructure and services in order to make full use of opportunities – including with the help of cutting-edge technologies – to boost the cyber resilience of our infrastructure and applications.
Since September 2016, the **Cyber Security** unit has been operating within Global Digital Solutions Function, reporting directly to the Chief Information Officer (CIO) who works under the Group Chief Information Security Officer (CISO). The unit is committed to ensuring the governance, direction and control of cyber security issues, establishing strategy, policies and guidelines in compliance with national and international regulations, engineering support for the protection of the Group's environments, monitoring of the risk posture through checks based on processes and technology, as well as monitoring and implementing compliance requirements tied to cyber security regulations, and adopting technical solutions and procedures to mitigate any weaknesses detected. The unit works synergically with the Business Lines and with the technical units responsible for systems design and management, thanks to the Cyber Security Risk Managers and Cyber Security Response Managers. CISO and the Cyber Security Risk Managers also make up the Cyber Security Operating Committee, which aims to evaluate cyber risks across the business and determine the risk acceptance criteria based on the Group's risk posture. The Cyber Security Committee, chaired by the Group's CEO and made up of his/her front lines, approves the cyber security strategy and periodically checks its progress. As determined at the meeting of April 2021, the Committee meets every six months. Two meetings were held in 2022 (May and October).
In 2022, the Control and Risk Committee held 3 meetings with the objective of addressing in more depth the aspects related to organizational procedures (on a technical and governance level), the crisis management process,

(5) "Cyber Security Posture" refers to the state of society's adoption of cyber security principles.

the CERT operating model and the relative processes that characterize them.
All areas actively participate in implementing the cyber security strategy by way of an integrated operating plan in line with the Group's objectives. Moreover, cyber security strategy and initiatives are a key focus area for the principal executive and control bodies (e.g. Board of Directors, Supervisory Bodies, etc.) for all the legal entities and Countries where the Group is present.

Moreover, the Group policy adopted in 2017 (the "**Cyber Security Framework**") addresses the principles and operational processes that support a global strategy of risk analysis, prevention and management.
This Framework, based on a 'systemic' vision applies across the more traditional Information Technology (**IT**) sector, as well as to Operational Technology (**OT**) environments tied to the industrial world and the Internet of Things (**IoT**). In applying this Framework, the Cyber Security Risk Management method was established in 2017. The method is applicable to all IT, OT and IoT environments and includes all of the phases required to carry out a risk analysis and define the related mitigation plan, in line with the stated cyber security goals. To balance the advantages obtained by the operation and use of IT/OT/IoT systems with the risk that can potentially derive from them, well-informed, risk-based decisions are of fundamental importance.
Enel has also created a "**Cyber Emergency Readiness Team**" (CERT) to ensure proactive management and responses to cyber incidents, while also encouraging collaboration and exchanges of information within a network of accredited international partners. Having entered into an agreement with the US national CERT, there are now 9 accreditations with: Romania, Italy, Chile, Argentina, Peru, Colombia, Brazil, Spain, and the US. Enel's CERT is also part of Trusted Introducer – a service that includes 464 CERTs in 72 countries. In September 2018 Enel also joined FIRST (Forum of Incident Response and Security Teams), which is the largest and most widespread community in the sector, with 602 members spread across 99 countries. Furthermore, in 2022 the CERT operating model was strengthened with the creation of an internal team of security analysts. The new operating model has exceeded the previous one, implementing the internalization of the incident monitoring and management activities and therefore, strengthening the activities 24x7.

Definition of the IT security strategy

The cyber security strategy covers setting objectives and priorities to direct and coordinate investment initiatives for the Group as a whole, and to ensure adherence to cyber security policies, setting targets, management reporting, and constant monitoring of ongoing security activities.
This process is guided by CISO and uses close integration and synergy with the various business areas, which communicate their needs, analyze opportunities, manage any criticalities, and make proposals for initiatives.
Devising strategies is an iterative activity based on sharing and consolidation of the Group's risk posture target. The various actors involved analyze the options and potential initiatives within their respective business areas in order to assess the feasibility, guarantee consensus, and the necessary funds. The Cyber Security unit guides the process and, together with the other key players, gradually consolidates aspects such as future scenario, objectives, and possible strategic initiatives in a cyber security strategy proposal document, with a high-level budget estimate and prioritization.

Cyber security incident management

The multiplicity and complexity of the areas in which we operate (data, industry, and people) and of the technological components (e.g. business critical systems such as SCADA – Supervisory Control and Data Acquisition, smart grids and smart meters) increasingly integrated in the Group's digital life, have made it necessary to configure a structured cyber security system. This leads to the need for a cyber defense model based on a systemic vision that integrates the IT sector (starting from the cloud down to the data center and mobile phone), the OT (everything concerning industrial sector, such as generation plant remote control) and the IoT (extension of communication and artificial intelligence to the world of things).
Through the monitoring systems, CERT collects 3 billion events every day relating to the company's assets from 7 thousand data sources, correlates them through automatic analysis, and produces a hundred "incidents" on average. The incidents are classified based on the Enel Cyber Impact Matrix (on a scale of 0 to 4), making use of the best events correlation capabilities thanks to the adoption of highly advanced services.
The vast majority of "incidents" are classified as **0/1**; these have no significant impact on Group systems and are automatically or semi-automatically intercepted and/or managed by the existing company defenses; this way they are able to prevent and/or mitigate the impact of potential cyber-attacks.
Incidents classified as **2/3/4** have a potential impact on the Group and are managed by CERT analysts, involving any affected stakeholders. Thanks to the protection services, every day, in 2022 **CERT intercepted on average 1.2 million at risk e-mails, 57 viruses, 172 web portal attacks, and 1.3 million connections to harmful websites every day**.

In 2022 Enel CERT responded to: **175 cyber security incidents with impact level 2; 16 incidents with impact level 3; and 0 incidents with the highest impact level of 4**.
In the cases detected, to ensure an efficient and rapid response and minimize the impact on people, services and assets, all the relevant management procedures have been put in place.
Specifically, when a cyber security incident translates into a potential data breach, the necessary actions are taken immediately, in line with the Enel Group "**Personal Data Breach Management**" policy. Should a crisis situation arise that threatens the Enel Group's business continuity, assets, reputation and/or profitability, the appropriate actions are taken immediately, in line with the specific Group policy on "Critical events management".
Moreover, the "**IT Service Continuity Management**" policy formalizes a process to bring the risk affecting the availability of IT infrastructure down to an acceptable level, support business continuity requirements, and restore IT services based on the results deriving from a Business Impact Analysis when a severe interruption occurs, including when caused by an accident.

EDR (Endpoint Detection and Response) technology blocks violations by using innovative features and advanced paradigms not only to identify viruses and malware on endpoints, but also to detect suspicious sequences of technical events that could prove to be part of an attempted attack.

Detailed below is the number of cyber security events recorded in 2022.

	2022
Total number of cyber security breaches or other cyber security incidents[1]	0
Total amount of fines/sanctions paid related to cyber security breaches or other cyber security incidents	0
Total number of customers and employees impacted by data breaches affecting the Group	0
Total number of data breaches[2]	0

(1) The value reported for the KPI "Total number of cyber security breaches or other cyber security incidents" refers to Level 4 incidents.
(2) The KPI "Total number of data breaches" refers to the number of events that occurred as a result of a cyber security incident (i.e. the number reported does not include any disclosures occurring as a result of non-digital incidents).

Furthermore, in order to boost our capacity to prevent, react to and manage incidents, some **cyber exercises** simulating a real attack were carried out, involving staff working in the production environments. At the end of each exercise, reports were produced containing details of the actions taken during the simulation, to assess – with a view to continuous improvement – the quality and completeness of the materials provided to help with decision-making, the execution times for each phase, and how well the procedures had been followed. In 2022, in particular, 50 cyber exercises were carried out in industrial environments in 11 Countries where the Group is present.

Main projects and initiatives

All cyber security projects, programs, and initiatives are designed to avoid, mitigate or remediate cyber security risks for the entire Group. As a result, all activities are managed with a risk-based approach following the security by design principle to ensure a continuous due diligence process that also includes self-assurance activities.

CERT – RISK MONITORING EXTENSION

"**CERT – Risk Monitoring extension**". CERT uses emergency technologies such as SOAR (Security Orchestration, Automation and Response) and machine learning to support Big Data, which make it possible to automate and streamline incident management activities and make use of improved visibility of cyber threats, increasing efficiency in managing new ones and the related investigations. In particular, thanks to the SOAR system, through the definition of operating flows it is possible to automate repetitive tasks, whereas through machine learning, a branch of artificial intelligence, it is possible to learn or improve detection capacities based on available data.
These technologies make it possible to consistently accelerate, enrich and trace the necessary activities during the analysis and management phase of an incident, providing considerable support to the analyst who can therefore parallelize and concentrate on more complex tasks that require human intervention.

MULTI-FACTOR AUTHENTICATION (MFA)

"**Multi Factor Authentication (MFA)**" is a cloud solution used to enforce the identification method for users during the authentication procedure. Adopting MFA enables a person accessing a system to identify himself/herself through a second authentication factor via SMS or an app installed on his/her smartphone. The MFA solution is in line with the regulatory framework and is strongly recommended to counter emerging threats of theft of credentials, including those using social engineering techniques (e.g., phishing or potential user behavior not in line with policy). The adoption of the solution is operational for all users.

ASSURANCE CHECKS

Assurance checks (Ethical Hacking, Vulnerability Assessment). These activities are carried out on an ongoing basis both using automated tools and manually, to assess and quantify any weaknesses in IT, OT and IoT environments (applications, systems, IoT devices, architectures and/or infrastructures). 1,587 checks were performed in 2022. Following these checks, we can identify the best measures to eliminate or mitigate the detected vulnerabilities or threats and, in turn, any associated harmful exploits.

DMARC "E-MAIL FRAUD DEFENSE"

DMARC "E-mail Fraud Defense". This solution completes the application map covering threats of spam, phishing and fraud attempts. Thanks to this, all of Enel's e-mail domains are configured to permit blocking e-mails with an incorrect sender address that exploits the Group brand. Deployment took place across the entire perimeter, thereby providing complete coverage of the domains.

Collaborations with external bodies and agencies

In line with the Open Power approach, we believe that networking with external entities and organizations is a key element in the cyber security strategy, to share best practices and operational models, develop and strengthen information sharing channels, and help establish standards and regulations. In 2022, we provided feedback in public consultations to help draw up cyber security regulations, including by drafting legislations, promoting a harmonization of the current regulatory landscape in this area, and implementing a risk-based approach and the principle of security by design. Collaborations carried out also aim to construct more homogeneous structures for defining the taxonomy of security incidents, more organic criteria for their classification, as well as more harmonious notification procedures in European contexts. These collaborations are also guided by a complex regulatory landscape in the cyber security area, both in terms of an increase in standards produced as well as in terms of complexity, mainly due to the new regulations that are added every year, in addition to the heterogeneity of requirements and the methods of adoption.

In this sense, the process aimed at regulatory compliance can have a strong impact both on company processes ad well as on the technological infrastructure, requiring a major effort in terms of management and monitoring.

Moreover, taking into account the context of regulatory compliance, **no cases of non-compliance with standards or cyber security regulations were detected in 2022**.

In recent years, a solid network has been established and developed by interacting with key stakeholders in the energy sector such as ANEEL (Agência Nacional de Energia Elétrica) and ONS (Operador Nacional do Sistema Elétrico) in Brazil and CNO (Consejo Nacional de Operación) in Colombia. We took part, for example, in the Confindustria Digitale team, which aims to help develop the Italian digital ecosystem, we participated in the working groups of the World Economic Forum, and contributed in recent years to the publication of several reports including "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain" and "Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors".

Furthermore, Enel X, Gridspertise and Enel Grids have reached an important goal in the area of IT security by obtaining **ISO 27001 certification**. This important result certifies some processes that have an IT security management system – policies, procedures and guidelines for providing customers with trusted products and services.

Training and information

The "**Cyber Security Awareness Program**" has become a constant and ongoing initiative at Group level; it used to disseminate our cyber security culture and raise awareness of threats and attacks that exploit the human vector. This program contributes in fact to digitalization, because it creates a culture of IT security, changes the behavior of people in order to reduce the cyber risk, develops technical IT security skills and makes people the first line of company defense. It also uses various communication channels and dissemination tools, including both communication campaigns as well as dedicated training initiatives for clusters of people. Specifically, 19 knowledge sharing events were held in 2022 on a Global level on the issues of cyber security and various initiatives were held also on a local level. For example, within the scope of these initiatives, Policy no. 1097 "Rules of Behavior for Digital People" was integrated with a quick guide, available in all the main languages adopted in the Group (5 different languages) targeted towards facilitating a quick consultation of topics for directing the correct use of digital resources. Bulletins and news were also created and disseminated through the company intranet and documents were made available to stay always up to date on these issues. All of this was made possible also thanks to the awareness platform "TheRedPill", the Group platform through which training content and modules are delivered in order to strengthen the IT security culture, allowing the continuous improvement of training initiatives and the performance of simulated phishing campaigns. Its objective is to raise awareness of the main cyber security issues, address any upskilling and reskilling needs and teach how to defend against possible attacks. Four global simulated phishing campaigns, a knowledge assessment and an awareness campaign were launched in 2021 – the year the platform was updated. During 2022, additional initiatives were launched on a global level, such as the dissemination of the "Antiphishing Kit" module, or the launch of the "People Cyber Empowerment Journey", or the program that aims to make Enel people the first line of IT defense. Furthermore, 6 simulated phishing campaigns, 3 awareness campaigns related to digital identity protection, data and device protection, and 19 events targeted to disseminating the culture of IT security were designed and launched (so-called "knowledge sharing").

In addition to the dissemination and communication initiatives, during 2022 the simulated phishing campaigns targeted toward the entire Enel population continued, in order to train employees to recognize malicious e-mails. Following the results obtained by the phishing campaigns, specific initiatives were created to increase employee sensitivity and awareness (for example, specific infographics, instructions and guidelines were shared with those who were not able to recognize a phishing e-mail).

The **Open Tech Journey** project also continued to provide access to training courses focused on technological topics, promoting internal skills to spread awareness of strategic topics and manage upskilling and reskilling needs. This was the background to the creation of the **Cyber School**, which delivered seven courses on the main cyber security topics. All the courses were engineered and made available to the entire Enel population in e-learning mode, in order to reach multi-specialistic skills in the various companies of the Group.

Concept design and realization
Gpt Group

Copy editing
postScriptum di **Paola Urbani**

Publication not for sale

Edited by
Enel Communications

Disclaimer
This Report issued in Italian has been translated into
English solely for the convenience of international readers

Enel
Società per azioni
Registered Office 00198 Rome - Italy
Viale Regina Margherita, 137
Stock Capital Euro 10,166,679,946 fully paid-in
Companies Register of Rome and Tax I.D. 00811720580
R.E.A. of Rome 756032 VAT Code 15844561009