CYBERSECURITY

Business continuity

Digital (IT), industrial (OT), connected (IoT) products and services and information are strategic assets for Ferrovial for which all employees are responsible. Its integrity, confidentiality and availability must be guaranteed to achieve optimal performance in all business lines.

100%

Successfully managed security incidents

113,000

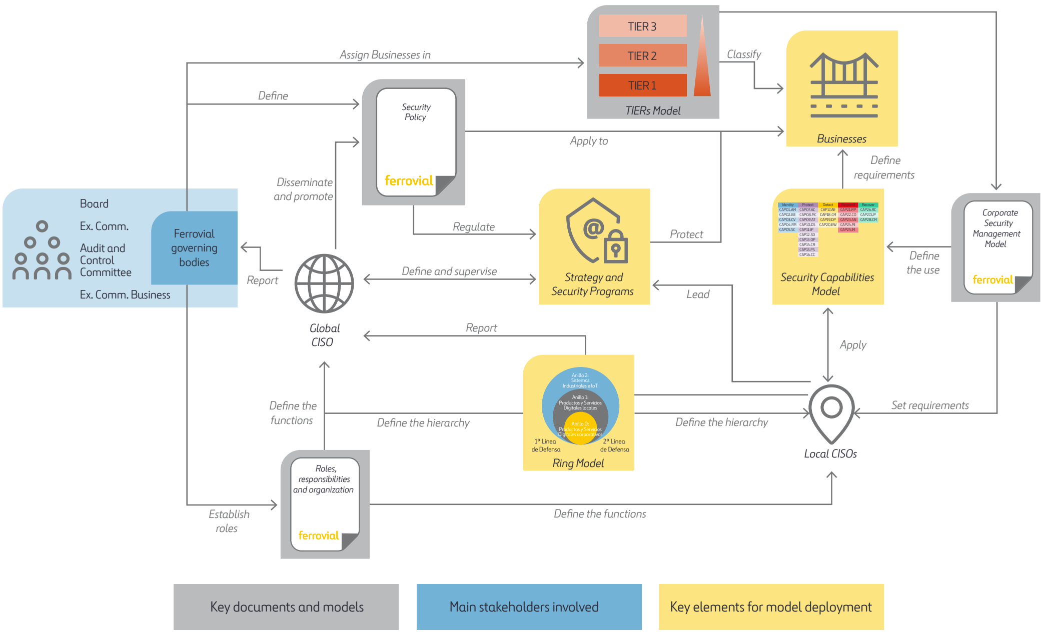
Simulated phishing emails received by employees

18,543

Single users included in phishing simulations

14,000

SMS sent in smishing campaigns


Board
Ex. Comm.
Audit and Control Committee
Ex. Comm. Business
Ferrovial governing bodies
Assign Businesses in
Define
Security Policy
ferrovial
Disseminate and promote
Report
Global CISO
Regulate
Define and supervise
Report
Define the functions
Define the hierarchy
Roles, responsibilities and organization
ferrovial
Establish roles
Define the functions
TIER 3
TIER 2
TIER 1
TIERs Model
Classify
Apply to
Businesses
Define requirements
Protect
Strategy and Security Programs
Lead
Identity
Protect
Detect
Respond
Recover
CAP01.AM CAP02.BE CAP03.GV CAP04.RM CAP05.SC
CAP07.AC CAP08.MC CAP09.AT CAP10.DS CAP11.IP CAP12.SD CAP13.OP CAP14.CR CAP15.PS CAP16.CC
CAP17.AE CAP18.CM CAP19.DP CAP20.EW
CAP21.RP CAP22.CO CAP23.AN CAP24.MI CAP25.IM
CAP26.RC CAP27.UP CAP28.CM
Security Capabilities Model
Corporate Security Management Model
ferrovial
Define the use
Apply
Anillo 2: Sistemas Industriales e IoT
Anillo 1: Productos y Servicios Digitales locales
Anillo 0: Productos y Servicios Digitales corporativos
1ª Línea de Defensa
2ª Línea de Defensa
Ring Model
Define the hierarchy
Local CISOs
Set requirements
Key documents and models
Main stakeholders involved
Key elements for model deployment

The company has an optimal organizational structure, a robust security model and resources to guarantee the integrity of its assets.

CYBERSECURITY ORGANIZATION AND LEADERSHIP

Ferrovial has appointed the position of Global Chief Information Security Officer (CISO), providing him with an organizational structure and the necessary resources to implement the Cybersecurity (Security) program. Likewise, each business unit and subsidiary company has a Local CISO.

The driving force in security is the Global Cybersecurity Committee, which provides monitoring and continuity to the development of the security program. In addition, there is a Global Cybersecurity Community, composed of all the security professionals in the business units and subsidiary companies, as well as their IT managers.

The Cybersecurity department reports to the governing bodies of Ferrovial. The Global CISO reports periodically to Ferrovial's Management Committee and to the Management Committees of Ferrovial's businesses, generally reporting on the security strategy and program, as well as the main security risks and threats.

On a regular basis, the Global CISO reports to the Board of Directors providing information on the security strategy and program, the main security risks and threats faced by Ferrovial and how they are being managed. It must also participate in the Audit and Control Committee at its request, providing information on the security strategy and program, on the level of internal control, on the main security risks and threats and how they are being managed.

Since 2019, the Cybersecurity Department has been promoting a new strategic plan approved by Ferrovial's Management Committee, which is expected to be completed throughout 2022.

CYBERSECURITY MODEL

Ferrovial has a General Cybersecurity Policy, approved by the CEO, applicable to all business units and subsidiaries. It is structured around a set of principles and objectives that support the company's strategy.

It is implemented through the Security Model based on organization, people, processes and technologies, formalized in a Security Regulatory Body that takes as a reference the best market practices, highlighting the NIST CSF and the ISO 27001 standard (Ferrovial has been certified since 2012).

It is based on a set of security capabilities supported by the NIST CSF principles: Identify, Protect, Detect, Respond and Recover all the assets needed to carry out Ferrovial's business activities.

The Cybersecurity Model complies with the principle of continuous improvement established by ISO 27001 (Plan, Do, Check, Act). The strategy is implemented through a program comprising security capabilities and projects that implement new capabilities or strengthen existing ones. The strategy is reviewed periodically by Ferrovial's Governing Bodies and uses as reference the results of audits and reviews, compliance with KGIs and Security KPIs or new cybersecurity threats.

Ferrovial has adapted its security strategy and capabilities to respond to the threats arising from the COVID-19 pandemic, such as the proliferation of phishing attacks, disinformation campaigns, attacks on employees and collaborators working remotely, etc. This situation has required leveraging existing Zero-Trust architectures and has encouraged the rapid adoption of SASE (Secure Access Service Edge) models and advanced XDR (Extended Detection & Response) monitoring and correlation capabilities.

SECURITY CULTURE

Ferrovial aims to ensure that employees and collaborators become the first line of defense against cyber threats, supporting the generation of a security culture. The security awareness program "Being aware, makes you safe" has been deployed, comprising various initiatives such as mandatory security training and other training actions (face-to-face or online), news and pills on the intranet and via mail; preventive and systematic campaigns against phishing, ransomware, or CEO fraud, as well as vishing, phising and smishing simulations. After the simulations, the level of risk of suffering these types of attacks is measured and the users to be made aware of and sensitized are identified based on their results obtained.

It should be noted that employees of the Cybersecurity Department have specific objectives in the area of security as part of their annual performance evaluation.

COMPLIANCE

There is a Security Compliance area within the Cybersecurity Department. It is responsible for the identification of applicable legislation and Security requirements necessary to guarantee compliance articulated through the Security Model.

The most relevant regulations covered by the Security Model are the General Data Protection Regulation (RGPD and LOPDGDD, by its Spanish acronyms), the Internal Control over Financial Information System (SCIIF), the NIS Directive, the Crime Prevention Model typified in the Criminal Code, the National Security Framework (ENS) and ISO 27001. When new standards are identified, or modifications are made to the requirements of those already identified, the Security Model is enriched. In addition, specific compliance programs have been established for data protection, the Criminal Code, the SCIIF and ISO 27001.

The Cybersecurity Department ensures compliance with the security requirements defined in the bidding specifications, tenders and contracts in Ferrovial's businesses.

THREAT DETECTION, CORRELATION AND CYBERINTELLIGENCE

Ferrovial has two SOC (Security Operations Center) that provide coverage for events occurring in its data centers, perimeters, workstations and cloud environments. These services act as they receive alerts generated by SIEM (Security Information and Event Management) tools, upon detecting security events defined by the Cybersecurity Department.

The available cyber intelligence capabilities provide information on threat actors and their techniques and tools, enabling the deployment of controls to prevent successful attacks. Furthermore, there are formal collaboration agreements with national and international cybersecurity agencies with which information on threats and cyber incidents is shared and received.

CYBER ATTACKS RESPONSE

Ferrovial has an Incident Management procedure based on the National Cyber Incident Notification and Management Guide (INCIBE-CERT) and the ISO/IEC 27035 standard, which operations (response, containment and eradication) are formalized through a set of policies and playbooks.

The process incorporates the lessons learned from the different events and incidents managed. It is especially relevant to identify IoC (Indicators of Compromise) and TTPs (Tactics, Techniques & Procedures) to improve protection and detection mechanisms.

RESILIENCE AND CYBER RESILIENCE

Ferrovial has Contingency and Recovery Plans to respond to and recover from disruptive events. The Crisis Management Protocol involves various departments and areas within Ferrovial, in accordance with the protocols established by each of them. Response and recovery plans for incidents and disruptive events are tested periodically.

Additionally, the company has a cyber insurance policy that covers possible disruptive events and cyber incidents that may occur in the context of business activity.

EXTERNAL VERIFICATION AND VULNERABILITY ANALYSIS

Ferrovial continuously reviews its Security Model to identify areas for improvement and vulnerabilities. Various security audits and reviews are carried out on an annual basis, among which the following stand out:

- Audits associated with ISO 27001 certification.
- Security audits in the context of the EEFF audit (ITGC and ITCC).
- Audits conducted by the Internal Audit department (Third Line of Defense).
- Ad-hoc security reviews according to annual planning (Red Team, Pentesting, etc.).
- Recurrent Compromise Assessment exercises combined with threat hunting exercises.
- Vulnerability reviews in data centers, workstations, perimeters and cloud environments.
- Vulnerability reviews in source code.
- Security reviews of vendors (Vendor Risk Management).
- Review of Ferrovial's cybersecurity rating.
- Participation in national cyber exercises.
- Crisis simulations.
- Security Model assessment campaigns.

The Cybersecurity Department groups, assigns, plans and monitors the implementation of the different action plans that arise as a result of the assessments, reviews and audits indicated.