CYBERSECURITY

Protected assets

The strategic importance of digital products and services (IT), operational technology (OT), internet-connected assets (IoT) and the information generated and used in all processes and operations that support business activities are essential for the creation of value for stakeholders.

100%
SUCCESSFULLY MANAGED SECURITY INCIDENTS

126,800
SIMULATED PHISHING EMAILS RECEIVED BY EMPLOYEES

26,250
SINGLE USERS INCLUDED IN PHISHING SIMULATIONS

32,900
SUSPICIOUS PHISHING EMAILS REPORTED BY USER

Ferrovial has an adequate organizational structure, a robust security model and the necessary resources to guarantee the confidentiality, integrity and availability of its digital assets.

ORGANIZATION AND LEADERSHIP

Ferrovial's Global Chief Information Security Officer (CISO) and the Local CISOs of divisions and subsidiaries form the organizational structure and adequate resources to implement the Cybersecurity program.

The Global Cybersecurity Community composed of all the security professionals of the business units and subsidiary companies, as well as their different IT managers, monitors and provides continuity to the development of the security program.

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

The Global CISO participates 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 handled. It also reports periodically to the Board of Directors, providing information about the strategy, the security program and the main security risks and threats, as well as their management.

During 2022, the strategic security plan, initiated in 2019, was completed. The security program for 2023 focuses on developing advanced threat protection capabilities, improving security in the lifecycle of digital products and services and third-party risk management, fostering an appropriate cybersecurity culture, as well as increasing detection and response capabilities in industrial environments.

MODEL

The Corporate Cybersecurity Policy, approved by the CEO, applies to all divisions and subsidiaries. It is structured around a set of principles and objectives that reinforce the business strategy. It is implemented from the Security Model based on organization, people, processes and technologies, and 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).

The Cybersecurity Model follows the ISO 27001 continuous improvement principle (Plan, Do, Check, Act). The strategy is implemented through a program comprising initiatives that enable new capabilities or improving existing ones. It is monitored periodically by Ferrovial's governance bodies and is benchmarked against the results of audits and reviews, compliance with KGIs and security KPIs or new cybersecurity threats.

The company is evolving its strategy by deploying protection, detection and response capabilities to address threats such as those associated with the Russian-Ukrainian conflict, the proliferation of ransomware attacks, supply chain or email compromises (BEC), phishing or smishing. Among other measures, detection capabilities have been enhanced, systematic compromise and attack simulations have been carried out, and security training and awareness campaigns have been increased.

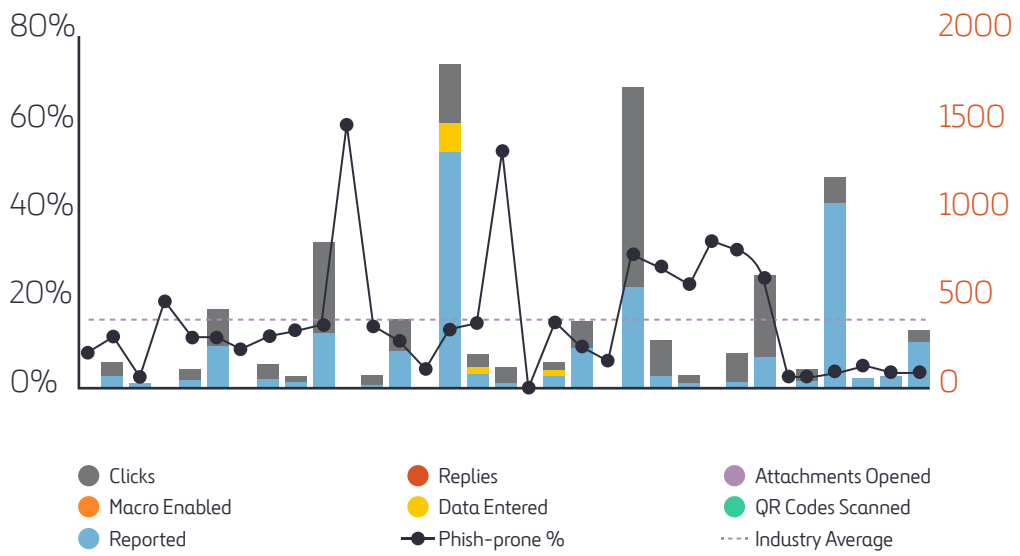
CULTURE

Ferrovial has implemented a cybersecurity culture program with the aim of enabling employees and collaborators to become the first line of defense against cyberthreats. It encompasses different initiatives that are carried out continuously in the organization, such as monthly phishing simulations and periodic smishing and vishing simulations. Following the simulations, the level of risk of suffering this type of attack is measured and the following training, awareness and coaching cycles are adapted to the specific needs identified.

Media such as the intranet and Yammer are also used for the dissemination of relevant news and pills on security matters, including those related to the most common threats that employees and collaborators must face, both professionally and privately.

It is worth noting that employees of the Cybersecurity Department have specific security objectives within their annual performance evaluation.

PHISHING SECURITY TESTS



LEGAL, REGULATORY AND CONTRACTUAL COMPLIANCE

The Security Compliance area, integrated in the Cybersecurity Department, is responsible for identifying the applicable legislation and the security requirements necessary to guarantee compliance in this matter.

The most relevant regulations covered by the Security Model are, but not limited to, the following: the General Data Protection Regulation (RGPD and LOPDGDD), the Internal Control System for Financial Information (SCIIF), the SWIFT (Society for Worldwide Interbank Financial Telecommunication) regulations, the NIS Directive, the Crime Prevention Model typified in the Criminal Code, the National Security Scheme (ENS), ISO 27001 and the different local regulations of the geographies in which Ferrovial operates relating to the protection of Essential Services and Critical Infrastructures. When new regulations are identified or modifications are made to the requirements of those already identified, the Security Model is updated. In addition, specific programs have been implemented for compliance with data protection, Criminal Code, SCIIF, SWIFT and ISO 27001.

The Cybersecurity Department also ensures compliance with the security requirements defined in the bidding specifications, tenders and contracts in the different business units.

DETECTION, CORRELATION AND CYBER THREAT INTELLIGENCE

The company has two SOCs (Security Operations Centers) that provide coverage for security events that occur in its data centers, perimeters, workstations and cloud environments. These services act when they receive alerts generated by SIEM (Security Information and Event Management) tools, upon detecting the use cases defined by the Cybersecurity Department.

Ferrovial has cyberintelligence capabilities that provide information on threat actors and their techniques and tools, enabling the deployment of controls to prevent successful attacks. In addition, formal collaboration agreements are maintained with national and international cybersecurity agencies with which information related to cybersecurity threats and incidents is shared and received.

RESPONSE TO CYBER-ATTACKS

The company has a CSIRT (Computer Security Incident Response Team) that intervenes when events detected by the SOC are likely to become security incidents. It integrates DFIR (Digital Forensics and Incident Response) capabilities that make it possible to analyze events in order to contain them, mitigate them and prevent their recurrence. It is especially relevant the identification of IoCs (Indicators of Compromise) and TTPs (Tactics, Techniques and Procedures) to improve protection and detection mechanisms.

The indicated capabilities and processes are formalized through incident management procedures 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 specified in a set of processes and playbooks.

Detection and response capabilities are systematically tested with Breach & Attack simulations supported by technologies already available on the market.

20,000
ACCESSES BLOCKED TO MALICIOUS DOMAINS ON A MONTHLY BASIS

1,300
SECURITY EVENTS ANALYZED MONTHLY

130,000
PHISHING EMAILS BLOCKED ON A MONTHLY BASIS

750
ATTEMPTS TO ACCESS CORPORATE RESOURCES BLOCKED ON A MONTHLY BASIS (MALICIOUS/ UNTRUSTED ORIGIN)

RESILIENCE AND CYBER RESILIENCE

The company has established Contingency and Recovery Plans to respond to and recover from disruptive events. The Crisis Management Protocol involves different Ferrovial departments and divisions, in accordance with the protocols established for each of them. Response and recovery plans for incidents and disruptive events are tested at least once a year.

Moreover, the company has a cyber insurance policy that offers, among others, various types of coverage such as financial, incident response and legal coverage for disruptive events and cyber incidents that may occur in the context of the activity carried out by Ferrovial, its business units and subsidiaries.

Ferrovial has participated in the National Cyber Exercises 2022 organized by the Spanish National Cybersecurity Institute (INCIBE) and the Cybersecurity Coordination Office (OCC), testing the structure, procedures and capabilities that articulate the detection, response and recovery from cyber incidents.

EXTERNAL VERIFICATION AND VULNERABILITY ANALYSIS

The company continuously reviews its Security Model to identify areas for improvement and vulnerabilities. Security audits and reviews are carried out annually, among which the following stand out:

- Audits associated with ISO 27001 certification.
- Security audits within the framework of the EEFF audit (ITGC and ITCC).
- Audits performed by Internal Audit Department (Third Line of Defense).
- Ad hoc security reviews according to annual planning (Red Team, Pentesting, etc.).
- Recurrent breach & attack exercises combined with threat hunting.
- 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 (INCIBE and OCC).
- Crisis simulations.
- Security Model assessment campaigns.

The Cybersecurity Department gathers, assigns, plans and monitors the implementation of the different action plans resulting from assessments, reviews and audits.