CYBERSECURITY

PROTECTED ASSETS

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

Ferrovial has consolidated an adequate organizational structure, a robust security model and has allocated the necessary resources to guarantee the confidentiality, integrity and availability required by its digital assets

100%
Successfully managed security incidents

127,565
Phishing scam emails received by employees

7,858
Unique users included in phishing simulations

6,083
Suspicious phishing emails reported monthly by users

24,454
Training actions completed by users

13,375
Accesses blocked monthly to malicious domains

80,195
Phishing and malicious emails, blocked on a monthly basis

7,294
Monthly blocked access attempts to corporate resources with malicious or untrusted origin (November and December average).

GOVERNANCE

Ferrovial has a Cybersecurity Governance model aligned with the business that supports the fulfillment of the company's objectives. The model considers it key to have an adequate Cybersecurity risk management program, as well as Cybersecurity capabilities (controls) to manage it.

A Cybersecurity risk assessment is performed annually in all Ferrovial's business units and subsidiaries, evaluating the exposure of the company's assets to cyber threats and the impact they may have on them. The level of compliance with Cybersecurity capabilities is also assessed and a roadmap is required to be drawn up to ensure that the level of risk remains within the acceptance thresholds in accordance with the risk appetite defined by the company.

Ferrovial's Governing Bodies supervise the level of cybersecurity risk on a regular basis and monitor the achievement of the roadmap and ensure the provision of resources should they be necessary.

The company has a Global Chief Information Security Officer (CISO) and Local CISOs, designated for their respective divisions and subsidiaries. Their roles and responsibilities in cybersecurity matters have been defined, as well as the relationship model between the different business units.

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

The Global CISO at the request of the Audit and Control Committee, provides 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. 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.

Throughout 2023, advanced threat protection capabilities were strengthened and training and awareness-raising actions were promoted to maintain an adequate cybersecurity culture. Improvements were implemented in security in the life cycle of digital products and services, as well as in the management of risks associated with the supply chain and detection and response capabilities in industrial environments.

Artificial Intelligence (AI) has been a protagonist throughout 2023 and will continue to be so during 2024 in the different perspectives in which Ferrovial is working: as a transformer of business operations, analyzing how to protect against the new capabilities it offers to threat agents and as a potential tool to support Cybersecurity.

During 2024, in preparation for Ferrovial's planned listing on the Nasdaq, the strategic programs aimed at adapting to the technical and organizational requirements required by Sarbanes-Oxley (SOX) that began in mid-2023, as well as the SEC Final Rules on Cybersecurity, will continue to be carried out.

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, formalized in a Security Regulatory Body that takes as a reference the best practices in the market, highlighting the NIST CSF and the ISO 27001 standard (Ferrovial has been certified since 2012).

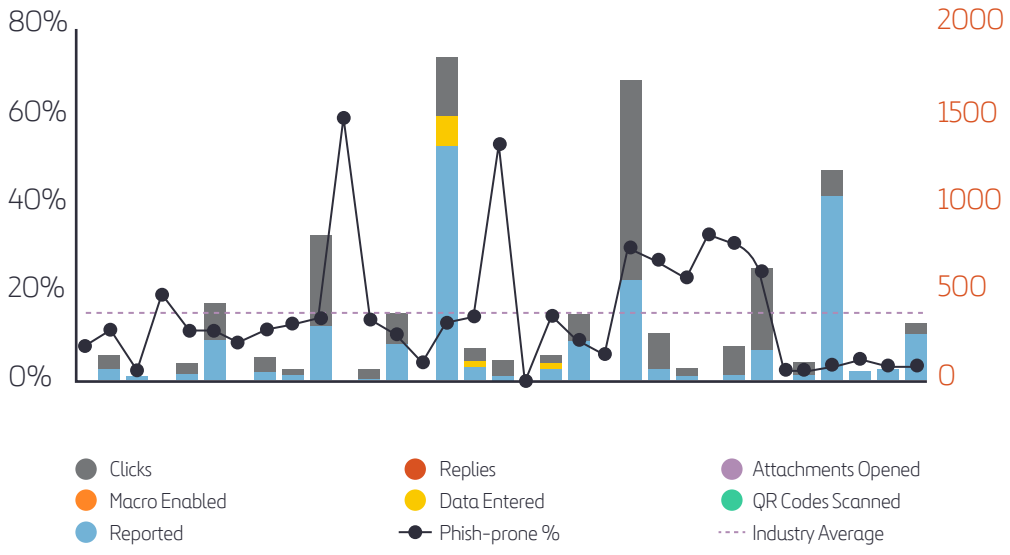
The Cybersecurity Model follows the ISO 27001 continuous improvement principle (Plan, Do, Check, Act). The strategy is implemented through a program comprising initiatives that enable new capabilities or improve existing ones. It is monitored periodically by Ferrovial's governance bodies and is benchmarked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

The company continuously evolves and adapts is updating its cybersecurity strategy, through its protection, detection and response capabilities to address the evolving cyber threat horizon, with a special focus on the increased sophistication and media impact of ransomware attacks, email compromise (BEC) or supply chain compromise and the instrumentalization of AI in targeted phishing, smishing, vishing or QRishing attacks.

CULTURE

During 2023, Ferrovial has committed to evolving the cybersecurity culture, systematizing and increasing the vision of cybersecurity within the company. To this end, a user-centric approach has been adopted, in accordance with the needs of its function and with the active participation of users, identifying and reporting suspicious emails received.

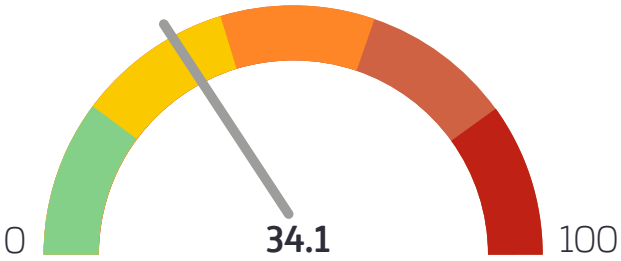
PHISHING SECURITY TESTS



The frequency of phishing drills has been increased, including its different variants: vishing, smishing and QRishing, which are now carried out every two weeks. After the drills, the level of risk of suffering this type of attack is measured and the following cycles of education, awareness and training are adapted to the specific needs identified.

Users are provided with a view of their own risk rating and the risk rating of the people in their team. This risk is nourished by their role in the company and by the information on cybersecurity culture, including their performance in drills and their participation in the training actions carried out.

PERSONAL RISK SCORE



Their risk score is based on a number of factors, such as job title, phishing test results and training completed.

It is worth noting that the company has the ability to measure and analyze the level of cybersecurity culture in real time, facilitating targeted awareness actions with a high level of granularity.

Regarding training, users have completed different training actions, both general and specific according to the requirements derived from the role in the company, risk level, specific cyber-attacks, etc.

The management of the security culture is carried out with a specific platform, which combines simulation management, training management (LMS) and cybersecurity culture measurement.

The company uses e-mail, the intranet and Yammer as its preferred means of publishing relevant security news and pills. These media include information and guidelines on the most common threats faced by employees, both in their professional and private lives.

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 ensure compliance in this area.

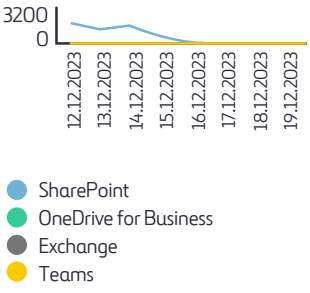
The most relevant regulations covered by the Security Model are, but not limited to, the following: The General Data Protection Regulation (RGPD and LOPDGDD), the Internal Control System for Financial Information (SCIIF), the SWIFT (Society for Worldwide Interbank Financial Telecommunication) regulations, 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.

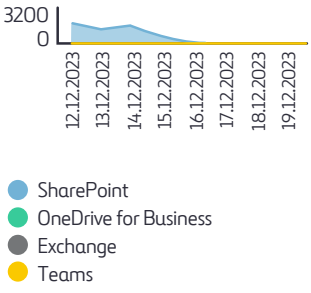
When new regulations are identified or modifications are made to the requirements of those already identified, the Security Model is updated. In addition, specific programs have been implemented for compliance with data protection, Criminal Code, SCIIF, SWIFT and ISO 27001, and the process of adapting to SOX and the SEC Final Rules on Cybersecurity has begun.

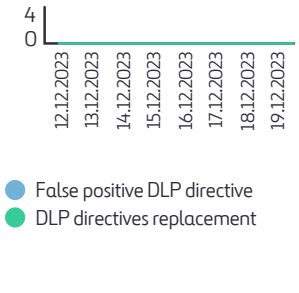
Likewise, the Cybersecurity Department ensures compliance with the security requirements defined in the bidding documents, tenders and contracts in the different businesses.

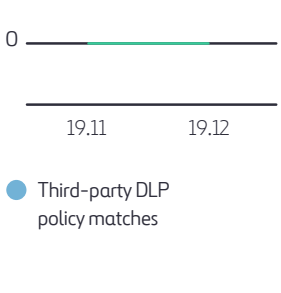
THREAT DETECTION, CORRELATION AND CYBERINTELLIGENCE

To protect its data centers, perimeters, workstations, mobile devices and cloud environments, the company has two SOCs (Security Operations Centers). These services act when they receive alerts generated by SIEM (Security Information and Event Management) tools and when they detect use cases defined by Cybersecurity Department that imply their activation.



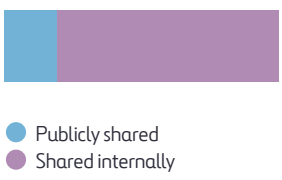


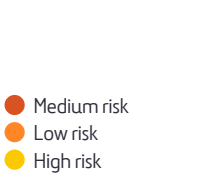




Users currently sharing most files from cloud applications

User	Share files
... .com	XXX
... .com	XXX
... .com	XXX
... .com	XXX





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, detection and response capabilities have been increased. Retroactive investigation, real-time vulnerability detection and information protection capabilities have been incorporated. Security processes have also been enhanced by taking advantage of advances in artificial intelligence.

Finally, the company maintains formal collaboration agreements with national and international cybersecurity agencies, allowing it to share and receive information related to cybersecurity threats and incidents.

CYBERATTACK RESPONSE

The company has a CSIRT (Computer Security Incident Response Team) that intervenes when events detected by the SOC may become security incidents. This team integrates DFIR (Digital Forensics and Incident Response) capabilities to analyze events in order to contain them, mitigate them and prevent their recurrence. The identification of IoCs (Indicators of Compromise) and TTPs (Tactics, Techniques and Procedures) are key to improving protection and detection mechanisms.

Ferrovial has a cyber-incident management protocol based on best market practices (INCIBE-CERT National Guide for Notification and Management of Cyber-Incidents, the ISO/IEC 27035 standard, and the NIST Computer Security Incident Handling Guide. One of the key elements within the protocol is communication to stakeholders (regulators, authorities, customers, etc.) and communication mechanisms have been established considering the deadlines and agreements established for this purpose.

Detection and response capabilities are systematically tested with Breach & Attack simulations supported by technologies already available on the market. It should be noted that there were no material breaches of Ferrovial's information systems during 2023.

RESILIENCE AND CYBER RESILIENCE

The company has established Contingency Plans and Recovery Plans to respond to and recover from disruptive events. The Crisis Management Protocol involves different divisions and divisions of Ferrovial, 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.

Similarly, within the activities of the Vendor Risk Management (VRM) process, critical suppliers must provide evidence of periodic testing to ensure compliance with established service level agreements.

Over the course of 2023, Ferrovial has carried out various initiatives and table-top simulations, testing in a crisis situation the organizational structure, procedures and capabilities required in the coordination of detection, response and recovery actions in the event of cyber-incidents.

In addition, the company has a cyber insurance policy that offers different 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. These coverages include financial, incident response and legal.

THIRD PARTY RISK MANAGEMENT

Ferrovial has a third-party risk management (VRM) program that establishes the security requirements that third parties must comply depending on the service to be provided for the company, considering, among other things, the level of access to its resources and information.

The program establishes formal evaluations of third parties throughout the life cycle of their relationship with Ferrovial. These evaluations are based on reports issued by third parties, certifications, ratings or other audit and review techniques that provide the necessary information to determine the level of control and security of third parties.

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:

- Internal and third party audits associated with the renewal of ISO 27001 certification.
- Security audits within the framework of the consolidated financial statements audit (ITGC and ITCC).
- Self-assessment of ITGC/ICFR controls.
- External audit SWIFT (Society for Worldwide Interbank Financial Telecommunication).
- Audits performed by Internal Audit (Third Line of Defense).
- SOX IT readiness assessment.
- 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 the source code.
- Review of Ferrovial's cybersecurity rating.
- Supplier security risk reviews (Vendor Risk Management).
- Crisis simulations (table-top exercises).
- Security Model assessment campaigns.
- Review of the company's Cybersecurity culture level.

The Cybersecurity Management groups, assigns, plans and monitors the implementation of the different action plans derived from the assessments, reviews and audits performed.