CYBERSECURITY

PROTECTION AGAINST THREATS

For Ferrovial, information is a strategic asset that all employees are responsible for. Its integrity, confidentiality and availability must be guaranteed to achieve optimal performance in all business lines.

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 security program and streamline its deployment in all business units. Each business unit also has a Local CISO, whose role is to deploy the security program within his or her local environment. The driving force is the Global Cybersecurity Committee, which meets on a regular basis to monitor and provide continuity in program delivery.

The Global CISO reports directly to the Chief Information Officer and Innovation Officer, who is a member of the Management Committee. On a regular basis, the Global CISO reports to the Committee on the status of the security strategy and program. He is also an invited member on the Management Committees of Ferrovial's Businesses, where he monitors the degree of program implementation in their local environments.

In addition, on an annual basis or at the request of the Board of Directors, the Global CISO provides information on the security strategy and program, as well as the main challenges and threats faced by Ferrovial in this area.

CYBERSECURITY MODEL

Ferrovial has an IT Security Policy approved by the CEO, applicable to all the company's business units, which unequivocally expresses the company's commitment in this context. It is structured around a set of principles that support the company's strategy. This policy is available to all employees and partners on the Intranet and is regularly communicated through various security awareness campaigns and training.

Ferrovial has an IT security and cybersecurity model based on best market practices, including the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and ISO 27001 (since 2011). The objectives of this model are as follows:

- To have a digital and technological environment with the necessary level of security.
- Ensure legal, regulatory and contractual compliance.
- Appropriately manage security incidents and provide resilience to security incidents.
- Homogenize and harmonize security between the different business units and subsidiaries.
- Facilitate digitization, innovation and the adoption of new technologies to support the business.
- Facilitate business opportunities and tendering processes.
- Establish strategic and security partnerships.

The model is based on a set of cybersecurity capabilities based on NIST principles:

Identify, Protect, Detect, Respond and Recover all the assets needed to carry out Ferrovial's business activities.

Since 2019, the IT Security Division has been promoting a new strategic plan that aims to provide advanced security capabilities and strengthen existing ones. The plan's initiatives are ongoing and are expected to be completed by early 2022.

CULTURE

Ferrovial aims to ensure that employees become the first line of defense against potential security events by supporting the generation of a cybersecurity culture within the company. For this reason, the company has a cybersecurity awareness program that has been deployed throughout the organization. Under the slogan, "Being aware makes you safe", it comprises various initiatives, including mandatory cybersecurity training and other training actions, both face-to-face and online, through the intranet and email; preventive campaigns against various threats (phishing, CEO fraud and ransomware); and phishing, vishing and smishing simulations, to name but a few.

It should be noted that employees working within the IT Security Division have specific cybersecurity objectives as part of their annual performance appraisal. Furthermore, all employees are obliged to observe policies on IT security and the appropriate use of technological resources.

RESILIENCE AND CYBER RESILIENCE

Ferrovial has a general security and cybersecurity incident management process. The process is instantiated by threat and potentially malicious event detection capabilities in different domains, response, containment and eradication teams, as well as recovery teams if necessary. The operations described above are formalized in a set of internal policies and procedures.

As established in the security incident management procedure, all Ferrovial employees and partners are obliged to report any suspicious or potentially malicious event in Ferrovial's information systems, and there are different mechanisms for reporting them. Similarly, suppliers

CPD Telefónica, Madrid, Spain.

working with Ferrovial are contractually obliged to report any incident that may affect company assets.

It should be noted that cyber threats are one of the risks considered in the corporate risk map. A detailed description of the same, its potential impact and the control measures implemented can be consulted in the risk section of this report.

Recovering from cyber attacks

Ferrovial has Contingency Plans and Recovery Plans to respond to and recover from potentially disruptive events. There is a Crisis Management Protocol, which, when implemented, triggers the involvement of various divisions and areas within Ferrovial in line with the protocols established by each of them.

The key processes and assets for business activity have been identified and this list is updated on a regular basis. Recovery plans have been put in place to ensure the availability of required resources and to recover within the timeframes and ways determined by the business units, according to the criticality specified by them.

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

EXTERNAL VERIFICATION AND VULNERABILITY ANALYSIS

Ferrovial subjects its IT security systems to continuous reviews by independent third parties in order to identify areas for improvement and vulnerabilities. The aim is to ensure continuous improvement of the cyber security program, its capabilities and resources. On an annual basis, various security audits and reviews are conducted including the following:

- Audits associated with ISO 27001 certification.
- Systems audits in the context of the audit of financial statements.
- Audits conducted by the Internal Audit function.
- Various types of ad-hoc security reviews with different scopes, according to annual planning (Red Team, Test Intrusion, GRC, etc.)
- Conducting recurrent Compromise Assessment exercises combined with threat hunting exercises, in order to detect potential attacks not detected by event correlation systems.
- Vulnerability reviews in data centers, perimeters and cloud environments.
- Annual control reviews of critical suppliers of the Information Systems and Innovation General Directorate.
- Cybersecurity rating review through specialized market service.
- Participation in cyber-exercises.
- Crisis simulations.
- Annual control assessment campaigns (security model, ICFR, Crime Prevention Model, etc.)