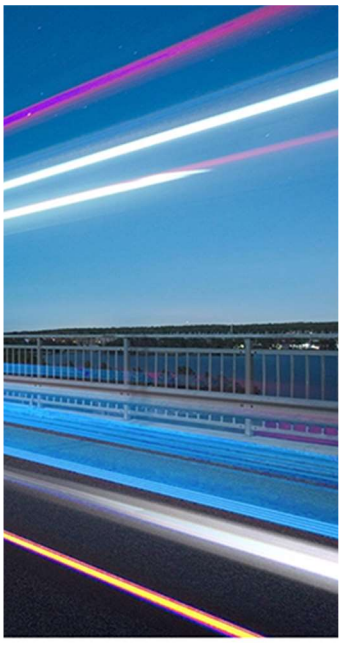
CYBERSECURITY POLICY

TRANSPORT SYSTEMS
TRAINS
BUSES
SIGNALLING
COMPONENTS
SERVICES

Your Way
to Future Mobility

The following English translation is provided by the Company for information purposes only, based on the original and official document in Spanish available on the Company's website. In the event of any discrepancy between the English version and the Spanish original document, the latter will prevail.

INDEX



1. INTRODUCTION AND OBJECT

The Board of Directors of CONSTRUCCIONES Y AUXILIAR DE FERROCARRILES, S.A., in the exercise of its non-delegable functions of defining the general strategies of the Company and its Group (hereinafter "CAF" or "Group") and taking into account the regulatory developments driven from the European Union and their projection in our country, as well as the recommendations, practices and standards established by the supervisory authorities and organizations of recognized prestige, has approved at its meeting held on 10 October 2024, the present Cybersecurity Policy (the "Policy"), which establishes the basic principles and commitments in the field of information security and cybersecurity.

In accordance with the general provisions of the Group's Code of Conduct and taking into account the provisions of the Sustainability Policy and the General Risk Control and Management Policy, the basic principles set out in this Policy will enable the Group to deploy Cybersecurity strategies, procedures and standards, aligned with business objectives, for the protection of CAF's data, systems and operations. In addition, the Policy aims to deploy processes and technologies that enable the Group to offer products and services that users, customers and other stakeholders can trust.

2. SCOPE

This Policy is applicable to and must be complied with by all the entities that make up CAF.

This Policy applies to all employees, shareholders, officers or members of a governing body of any CAF entity, regardless of their position or geographic location.

Likewise, this Policy is applicable to third parties in the value chain with whom CAF has established some kind of commercial relationship (Business Partners) and in particular to project partners, agents, suppliers and customers.

In order to define the specific requirements for the different types of Business Partners, objective factors will be taken into account, such as whether CAF has operational control or decisive influence over the third party, or similar criteria recognized in the main international best practice guides. In the event that CAF does not have such operational control or lacks significant influence, reasonable measures proportionate to the risk shall be adopted, such as, for example and among others, the analysis of the equivalent policies of the Business Partner in the subject matter of this Policy, to ensure their compatibility and alignment with this Policy, or any other measures that may be effective in ensuring respect by third parties of the General Principles of CAF's Code of Conduct, in general, and the content of the Supplier Code of Conduct, for the latter.

With respect to investee companies that do not belong to CAF because they do not have a sufficient shareholding to ensure control, CAF shall ensure that their principles of action are consistent with the provisions of this Policy, always respecting the legislation applicable in each case.

3. BASIC PRINCIPLES AND CYBERSECURITY COMMITMENTS

In order to achieve the implementation of the commitments, CAF will be guided by the basic principles of security, confidentiality, integrity, availability, authenticity and traceability of information, which govern this Cybersecurity Policy.

In this sense:

- Confidentiality ensures that the information is only accessible to users authorized to access it and that it cannot be disclosed to third parties without proper authorization.
- Integrity ensures that data is kept free from unauthorized modification and that existing information has not been altered by unauthorized persons or processes.
- Availability ensures that information and information systems are accessible and usable when required by authorized users.
- Authenticity is the ability to ensure that the origin and identities associated with the information are indeed those that appear in the attributes of the information. This is linked to the principle of non-repudiation, which ensures that the user cannot deny authorship of an act in the system or the linkage to a data or dataset.
- Traceability ensures that it is possible to determine at any time the identity of the persons accessing the information and their activity in relation to it, as well as the different states and routes that the information has followed.

On this basis, this Policy responds to the following commitments:

Commitment 1: To promote and continuously improve cybersecurity management in order to comply with legal and contractual obligations, while incorporating good security practices and the ethical use of the organization's resources, satisfying the needs and expectations of our customers and other stakeholders.

Cybersecurity management is understood as the set of activities, controls and technical and organizational measures for effective management of cybersecurity risks, which ensure the comprehensive security of information systems, networks and the information stored in such systems, including the prevention, detection, response and recovery from incidents.

This commitment extends to compliance with legal and contractual obligations, best safety practices and the ethical use of the organization's resources, meeting the needs and expectations of customers and other stakeholders.

CAF's cybersecurity management model is based on recognized benchmarks and standards, and on national and international regulations and standards. This allows both the deployment of controls and measures, as well as risk management appropriate to each area, taking into account the current environment and threats, and those that arise in the development of business and as a result of new regulatory requirements.

In any case, continuous supervision and monitoring will be carried out to ensure the effectiveness and continuous improvement of the model.

Commitment 2: Promote a culture of cybersecurity among our people and external collaborators, involving them in the achievement of the objectives.

A culture of cybersecurity for people involves:

The establishment, deployment, maintenance and communication of cyber security policies, standards and procedures that are fundamental to defining cyber security principles, objectives and responsibilities.

These elements provide clear guidelines for the use of technology, data management and incident response, thus promoting the integration of cyber security in all areas of the organization and establishing cyber security by design, as defined below, as the basis for our activities. In addition, it is essential to define training plans that train the entire organization in cybersecurity, adapting them to their areas of activity and responsibility. To complement this, cybersecurity awareness is crucial, involving the education and awareness of everyone in the organization about cybersecurity risks, current threats and best practices to prevent incidents.

On the other hand, overseeing compliance with best practices requires establishing clear agreements on expected security standards, conducting regular assessments of implemented controls and continuously monitoring cyber security performance. In this context, it is essential to maintain fluid and transparent communication with Business Partners to address any security vulnerabilities or incidents quickly and efficiently. Integrating all these components ensures robust and effective cyber security, protecting the organization from potential threats and guaranteeing the continuity of its operations.

Commitment 3: Ensure the protection of people from accidents and incidents arising from or related to our products and services.

This Policy establishes the obligation to protect people from any harm or incident related to our digital products and services. This means establishing cybersecurity by design, i.e. designing, developing and delivering products and services with robust security measures, aligned with customer needs, regulations and existing threats, and integrating cybersecurity throughout the development lifecycle. The objective is none other than to identify and correct vulnerabilities throughout the process. In addition, CAF extends vulnerability management and incident monitoring to the operation and maintenance phases, protecting people and reducing the risks associated with possible incidents.

Commitment 4: Adopt a zero-tolerance approach to actions or attitudes that are detrimental to cybersecurity and, in case of conflict between competing interests, give priority to security.

A zero-tolerance policy is established for any action or attitude that could compromise the cybersecurity of systems and data. This involves mitigating and managing risks, implementing immediate corrective measures for any breach, and prioritizing security in all decisions and resource allocation. In the event of a conflict between security and other

interests, such as functionality or efficiency, security must always prevail. This approach requires committed leadership, clear communication, continuous training and constant evaluation to ensure a safe and secure digital environment.

Commitment 5: To protect data of all kinds relating to CAF and its stakeholders, in terms of intellectual and industrial property, commercial secrets, personal data or other areas.

This Policy provides for the comprehensive safeguarding of data concerning CAF and its stakeholders. This includes rigorous protection of intellectual property, industrial property, trade secrets and personal data, among other sensitive areas. The implementation of robust security measures, such as encryption, access control and staff training, is essential to prevent unauthorized access, disclosure or misuse of this information. Similarly, measures covering the physical and environmental security of information systems and networks need to be implemented to protect such systems against unexpected system failures, human error, malicious acts or natural phenomena to ensure business continuity.

By protecting these intangible assets, CAF not only preserves its competitive advantage and reputation, but also fulfils its legal and ethical responsibilities to its various stakeholders. It also involves establishing clear communication channels for users to report incidents and receive assistance, as well as having incident response plans in place to mitigate any negative impact on users' security and privacy.

Commitment 6: Promote cybersecurity throughout the value chain.

Cybersecurity is actively encouraged at all levels of the value chain, promoting the implementation of and compliance with global cybersecurity and information security and data protection standards among suppliers, subcontractors and customers. Strategic alliances are established with actors committed to cybersecurity, promoting responsible practices that minimize the risk of incidents and protect the integrity of systems and data.

4. METRICS AND OBJECTS

To ensure compliance with the principles and commitments established in the Cybersecurity Policy, CAF has defined a robust monitoring and control system based on performance indicators and clearly defined short, medium and long-term objectives.

Periodic monitoring of performance indicators allows for the evaluation of progress towards the achievement of previously defined short, medium and long-term objectives. This practice facilitates the identification of areas requiring attention and improvement, making it possible to make the right decisions and implement appropriate corrective measures. In this way, a continuous cycle of continuous improvement is ensured, and performance and efficiency is optimized at all levels of the organization.

To ensure their effectiveness, performance indicators should meet the following criteria:

- Relevance: Indicators should accurately and meaningfully measure and reflect progress towards the achievement of a specific objective, providing information that can be used for decision-making and action.

- True representation: Data sources should be reliable, and measurement methods should be standardized. The information presented through the indicators should be complete, neutral and accurate.
- Timeliness: The frequency of measurement of indicators should be adequate for timely decision-making.
- User-friendliness: They should be easily understandable and interpretable for both collectors and analysts.
- Effective communication: The results of the indicators should be communicated clearly and concisely to all levels of the organization.

The most relevant indicators will form part of the non-financial information report in accordance with the Group's sustainability best practices.

The purpose of this approach is to ensure that good corporate governance, ethics and sustainability are cross-cutting themes in decision-making at all levels of CAF and especially in risk management, so that its activities generate value for both its shareholders and its other stakeholders.

5. CYBERSECURITY GOVERNANCE AND MANAGEMENT

CAF's governance of information security, and in particular cybersecurity, is structured through the following levels:

a) Board of Directors

The Board of Directors lays the foundations for the Group's internal governance on cybersecurity by defining the strategic objectives in this area, and in particular through the following competencies:

- Approve this Corporate Policy.
- Conduct regular monitoring of cybersecurity in the organization.
- Promote, together with management, a culture of cybersecurity throughout the organization, with the aim of raising awareness of best practices to prevent and mitigate cybersecurity risks.
- Give the Audit Committee direct oversight on cybersecurity.
- Ensure the availability of the material and human resources and capabilities necessary to achieve the objectives of the Cybersecurity Function.
- Update, at the request of the Audit Committee, this Policy, in accordance with the provisions of section 7 of this Policy.

b) Audit Committee

The Audit Committee is responsible for supervising and evaluating the Group's financial and non-financial risk management and control systems, including technological risks.

The Audit Committee shall also have the following powers.

- Oversee the implementation of this Policy, as well as the Cybersecurity Function.

- Regularly and periodically collect reports on the management of the cybersecurity function from the Corporate Head of the Cybersecurity Function, at least once a year.

  Such reports shall contain at least the status of cybersecurity and significant incidents handled, if any.

- Propose to the Board the updating of this Policy, in accordance with the provisions of section 7 of this Policy.

c) Corporate Technology Director

The Corporate Technology Director will:

- Set the Group's Technology guidelines and, in particular, for the management of cybersecurity, coordinating this function with the other technological areas of the Group.
- Recibe the direct report of the Corporate Head of the Cybersecurity Function on the achievement of strategic objectives and KPIs defined at corporate level.
- Facilitate the involvement of senior management in cybersecurity matters in those high-level fora in which the Corporate Head of the Cybersecurity Function is not directly involved.
- Establish the CAF areas to be represented in the Corporate Cybersecurity Committee.

d) Cybersecurity Function and Corporate Head of the Cybersecurity Function

The Cybersecurity Function is the internal body responsible for the development, implementation and application of the strategic guidelines set by the Board of Directors in the area of cybersecurity. It may report functionally to the Board of Directors, the Audit Committee or senior management, independently of the heads of network and information systems.

Its head (the "Corporate Head of the Cybersecurity Function") shall be a person with the appropriate knowledge, experience and competencies to perform the function and shall have sufficient decision-making capacity and influence in the organization.

Among its main competencies, the Cybersecurity Function will ensure the assessment, control, management and monitoring of cybersecurity risks, and the implementation of appropriate cyberresilience mechanisms, ensuring proper reporting to the appropriate forums. It will also define the performance indicators associated with cybersecurity and promote training and awareness-raising initiatives in the organization.

The Corporate Head of the Cybersecurity Function shall report to the Technology Directorate and, in any event, shall report periodically to the Audit Committee on the performance of his/her duties, in line with best practices in this area.

The Cybersecurity Function will be regularly assessed as part of the risk management and control system.

e) Corporate Cybersecurity Committee

The Group shall have a Corporate Cybersecurity Committee to adopt relevant resolutions on information security matters that may substantially affect the Group's activity.

The Corporate Cybersecurity Committee shall have an appropriate number of areas of the organization represented, in addition to the Corporate Technology Director and the Corporate Head of the Cybersecurity Function.

There may be other collegiate structures for the development of the competences of the Corporate Head of the Cybersecurity Function, which shall act under the coordination of the same.

Cybersecurity crisis committees will also be set up and the Cybersecurity Function will be involved in other crisis committees as required.

f) Business Management

Business Management is defined as the highest body responsible for a specific business activity division within the CAF Group.

The key responsibility of the Business Management in cybersecurity matters will be the implementation of this Policy, ensuring the definition of deployment plans for the development, supervision and control within the Business itself, for which the Business Cybersecurity Manager will be designated.

g) Business Cybersecurity Manager

The Business Cybersecurity Manager will coordinate all Business-level efforts related to cybersecurity, such as the deployment of corporate cybersecurity guidelines in the Business and the establishment of cybersecurity competencies, enabling corporate training and awareness plans, and identifying any specific needs that the Business may have.

6. INTERNAL INFORMATION SYSTEM (WHISTLEBLOWING CHANNELS)

All members of the Group have an obligation to report behavior or conduct identified in the work or professional context that may contravene the principles and parameters set out in this Policy, including any known actions or conduct that may be an indication of risk.

For such purpose, they must use the Group's Internal Reporting System, in accordance with the provisions of the Group's Internal Reporting System Policy, by accessing the same through the corporate website. This mechanism is also accessible to any third party outside the Group for the purpose of reporting breaches of this Policy.

The Internal Reporting System provides the safeguards of trust, confidentiality (including protection of the identity of the reporting person) and prohibition of retaliation reflected in the Internal Reporting System Policy and should be employed in good faith, based on a reasonable belief of the existence of a breach or a risk of a breach occurring.

7. REVIEW AND UPDATE

CAF's Board of Directors, at the request of the Audit Committee, shall update the Policy, in particular when any of the following circumstances arise:

- Relevant regulatory changes affecting the content of this Policy are approved.

- Areas of improvement or deficiencies in the content of this Policy are detected as a result of reviews and verifications of the Policy.

8. APPROVAL AND DISSEMINATION

This Policy is approved by the Board of Directors on 10 October 2024, from which date it becomes effective.

In order to facilitate its content for interested parties and recipients, this Policy will be published on CAF's website, as well as on the Group's internal channels.