V 3.0 – March 2026

Security

Keeping your trust

mapfre

Index

Guillermo Llorente,
Corporate Director of Security at Mapfre

For Mapfre, people are our most important asset and that is why our main mission is to protect them, both on a personal level and in terms of the data they give us, guaranteeing the service we provide and the trust they place in us.

To achieve this, the Security Function was established to protect Mapfre's tangible and intangible assets and ensure their operational resilience. This mission is reflected in the Strategic Security Framework, which, with a risk management approach, serves as the backbone of the Corporate Security and Privacy Policies, Business Continuity Policies, and the associated Internal Regulations. All of this is always within the strictest compliance with current legislation and Mapfre's Code of Ethics and Conduct.

SECURITY is an integral part of the entire organization and its culture and Mapfre's vision is for every initiative to incorporate security as a fundamental attribute. Therefore, to maintain the continuity of the service we provide and the privacy of the information entrusted to us, security requirements are integrated, by default and by design, into every application, service, device, or facility; in short, into every project we implement.

To oversee the normal development of our activity, Mapfre has a Security Operations Center (Global SOC), which is part of the FIRST network (Forum of Incident Response and Security Teams) and the Spanish National SOC Network. This network monitors and analyzes the security of Mapfre's Networks and Information Systems worldwide and coordinates and implements the response to security incidents that may occur at any entity within the Group.

When all of this is not enough and attacks materialize, serious crises or natural disasters appear, Mapfre has developed and implemented Crisis Management and Business Continuity Plans in its entities that are tested annually and whose objective is to enable the continuity of service to our clients even in the worst circumstances.

All of this has made it possible to detect and respond to the needs of an increasingly challenging security environment, enabling that in 2024, Mapfre has not had to report any serious cyber incidents to the regulatory authorities of the countries in which it operates.

In conclusion, the continuity of the service we provide, as well as the security and privacy of our clients, are fundamental and essential elements of the nature and vocation of service of our company, constituting a personal and unavoidable Commitment of all of us who are part of Mapfre.

Guillermo Llorente
Corporate Director of Security

Strategic Approach

01

The leadership aspiration at Mapfre and its global nature are reflected across all the Group's activities and serve as a guiding principle in the actions related to security. Security is also a field in which Mapfre seeks to be a benchmark

1.1

Characteristics of the Function of Security at Mapfre

The Security Function at Mapfre is responsible for protecting its tangible and intangible assets and business processes on an ongoing basis against security risks, ensuring the safety of people, regulatory compliance, information security, privacy, the operational resilience of services provided to our clients, the preservation of our good reputation, and our sustainability. All of this is done with the strictest respect for the law and Mapfre's ethical principles.

The 4 fundamental pillars on which it is based on are the are:

GLOBAL for the entire Company.

It applies to all personnel, resources, facilities, technological assets and all processes and activities across the various entities, bodies and areas of Mapfre, regardless of their geographical location and corporate structure.

Ensure RESILIENCE.

Enabling the normal development of the business and providing detection, response and recovery capabilities in the event of risks that affect the operational reliability and/or the integrity of the Group's assets.

SERVICE oriented.

The Security Function is service-oriented, considering the organization as its client. It aims to meet the needs that may be demanded and to support the organization throughout its transformation process.

Must PROVIDE VALUE.

By providing differentiation, reliability, and competitive advantage to the company. It will evolve according to the Group's needs in order to remain permanently integrated into the business, adapting, aligning, and contributing at all times to Mapfre's corporate strategy and image, reinforcing the trust placed in it by its clients and other stakeholders.

1.2

Mission of the Security Function

The Security Function has the following mission:

To prevent the occurrence and mitigate the impact of security risks that may cause damage to Mapfre, its reputation or its staff, as well as disrupt or limit its operational and/or financial capacity.

Thus, in addition to enabling the normal development of the activity of the different Business Units and entities of the Group, the Security Function has the following specific missions:

- **Protect PEOPLE and other Mapfre assets,** including third-party data to which Mapfre has access, ensuring regulatory compliance, ethical and responsible conduct and the preservation of the company's good reputation.

- **Enabling RESILIENCE of business and support processes,** prioritizing those identified as critical and that affect the Group's obligations to third parties.

1.3

Vision of the Corporate Security Function

To ensure adequate and sustainable protection in a challenging environment, security, privacy, responsible use of data and operational resilience are essential elements inherent to the company's activity, integrated into its business processes and in line with Mapfre's responsibility towards its employees, customers, shareholders, suppliers, partners and the society in which it operates.

The Security Function contributes to Mapfre's leadership in security, privacy and operational resilience through innovative, effective and efficient solutions.

It is governed by parameters of strict proportionality, establishing protection mechanisms in accordance with the risk and value of the assets, providing an adequate level of control that will result in an increase in the quality of processes, products and services.

Additionally, the Security Function ensures legal and regulatory compliance regarding the protection of people, facilities, ICT security, privacy, operational resilience, AI, and the prevention of antisocial or illegal acts.

The Security Function is governed by the strict ethical and governance standards of the Mapfre Group and its Strategic Security Framework. Its operating model is based on best practices and international standards, structured through a **Risk Management process** that, in a logical, standardized, and systematic way, identifies and assesses Risks and Assets, defines and implements protection measures, verifies the effectiveness of controls, and allows for determining the best treatment for each Risk.

1.4

Principles of the Security Function

The Security Function of the Mapfre Group is governed by the following Principles:

1. Ethical and responsible conduct, ensuring strict compliance with applicable legislation and the Group's Code of Ethics and Conduct in all actions.

2. Comprehensive Approach, taking the Asset to be protected as the center of its activity and protecting it against all types of Threats and Risks within the scope of Security, Privacy and Operational Resilience, regardless of how they materialize.

3. Proportionality, establishing security measures based on the asset's value, the risk, availability, and the cost of the measures and the means of protection and control. All of this within the risk management process and in accordance with the risk tolerance levels established by the Group.

4. Incorporation from the design stage, understanding SECURITY as a continuous process that must be part of all business processes and activities, incorporating security, privacy and operational resilience criteria from their conception and maintaining them throughout their life cycle.

5. Preventive action, anticipating damages to avoid them or reduce their consequences, within the concept of due diligence.

6. Security in Depth and Tiered, Applying a strategic, multi-layered approach to defense to protect assets and mitigate risks, so that if one measure fails, the following ones continue to provide protection, combining different physical, logical, technical, and organizational controls.

7. Responsiveness, possessing the necessary capacity to respond quickly, effectively, and in a coordinated manner to any threat or incident, minimizing its impact and preventing further damage once the risk has materialized. Actions are carried out promptly, both in terms of timing and resources, anticipating events whenever possible and proactively managing crisis situations, with the aim of preserving the Group's operational resilience at all times.

8. Centralized Management, which allows for a unified response to risks by concentrating resources and personnel under a single leadership and planning framework. This approach fosters consistency throughout the organization, aligns policies, criteria, and principles, and leverages synergies. Given the complexity of the system, the overall security level will always depend on its weakest link. Therefore, achieving a homogeneous level (a common baseline) across the Group is essential to ensuring effective protection.

9. Integration. To ensure consistent and effective corporate management of Security, Privacy, and Operational Resilience, these disciplines are integrated across all business processes. Their implementation is coordinated with all areas of the Mapfre Group, maximizing synergies and enhancing value creation throughout the organization.

10. Security culture, ensuring that security, privacy, responsible use of data and operational resilience are part of the corporate culture, raising awareness and providing relevant training and information on these matters to board members, employees, customers, suppliers and partners.

1.5

Integrated Model of Security

Mapfre applies a **holistic approach to Security,** integrating the management of all aspects related to the Security of people, their assets and their business, in a single Corporate Directorate with a global presence and scope of action.

The responsibilities of the Corporate Security Division (DCS) include the following areas:

- Security of People.
- Security of Facilities.
- Security Information Systems (Cybersecurity).
- Privacy and Protection of Personal Data and Artificial Intelligence.
- Operational Resilience: Crisis Management and Business Continuity Committee.
- Fight against fraud.
- Security Intelligence.
- Regulatory and legal compliance regarding Security, Operational Resilience, Privacy and Artificial Intelligence.
- Third-party and supplier security risks.

Security measures are based on a risk management model, ensuring adequate protection of Mapfre's corporate assets.

Security risk management is also integrated into the Mapfre Group's risk management system, forming part of the information periodically reported to the Group's Board of Directors' Risk, Sustainability and Compliance Committee.

The model also incorporates **security intelligence capabilities** , designed to transform relevant information into useful knowledge to anticipate threats and guide strategic decisions.

This approach has formed the basis of the model for the development of the **Security Function** at Mapfre, governed by the Code of Ethics and Conduct and based on international standards and best practices, such as, among others:

ISO 27001 and 27002 in Information Systems Security.

ISO 22301 Business Continuity.

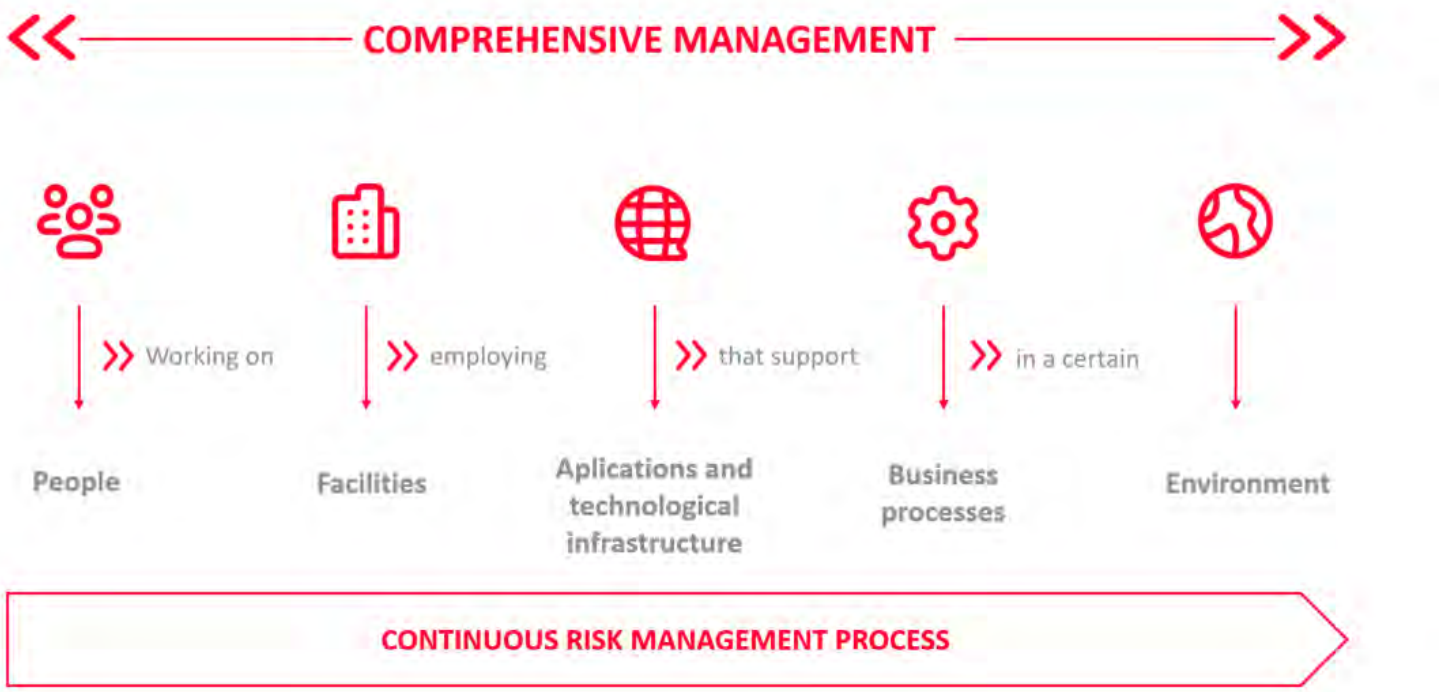
ISO 9001 for quality management.

ISO 27701 for privacy management

ISO 29100 relating to the protection of privacy.

PCI DSS. On payment card data security.

ISO 31030 on travel risk management.



1.6

Global Approach

Our concept of Security as **UNIQUE** for the entire Mapfre organization, and of a **COMPREHENSIVE nature** against all types of threats in a global entity like our Group, implies having a **Global Security structure,** which allows a homogeneous and coherent response to risks, both global and local, acting simultaneously and in a coordinated manner across both dimensions.

Global Dimension

- Protection against global threats.
- Global regulatory compliance.
- Searching for and maximizing synergies.
- Aligned with Mapfre's Global Strategy.

Specific Dimension

- Protection against local threats.
- Local regulatory compliance.
- Communication with Regulators, Authorities and local Security Forces.
- Capturing and adapting to the needs, threats, and habits/customs in each entity, country, and market.

1.7

Security Document System

Reflecting the aforementioned principles and in accordance with the Institutional and Business Principles, as well as the Code of Ethics and Conduct, Mapfre has a Security Document System, the cornerstone of which is the set of corporate policies. These policies outline Mapfre's commitment to guaranteeing the protection of its assets, ensuring regulatory compliance regarding security and privacy, the operational resilience of services provided to third parties, the preservation of the company's good reputation and image, and its sustainability. These policies have been approved by the Board of Directors of Mapfre, SA and are mandatory throughout the Group.

Corporate Security and Privacy Policy , which establishes Mapfre's guidelines and commitments regarding security and privacy.

Business Continuity Policy , which establishes the framework to ensure operational resilience and recovery of critical functions after disruptive incidents, protecting people and ensuring the continuity of essential processes and services.

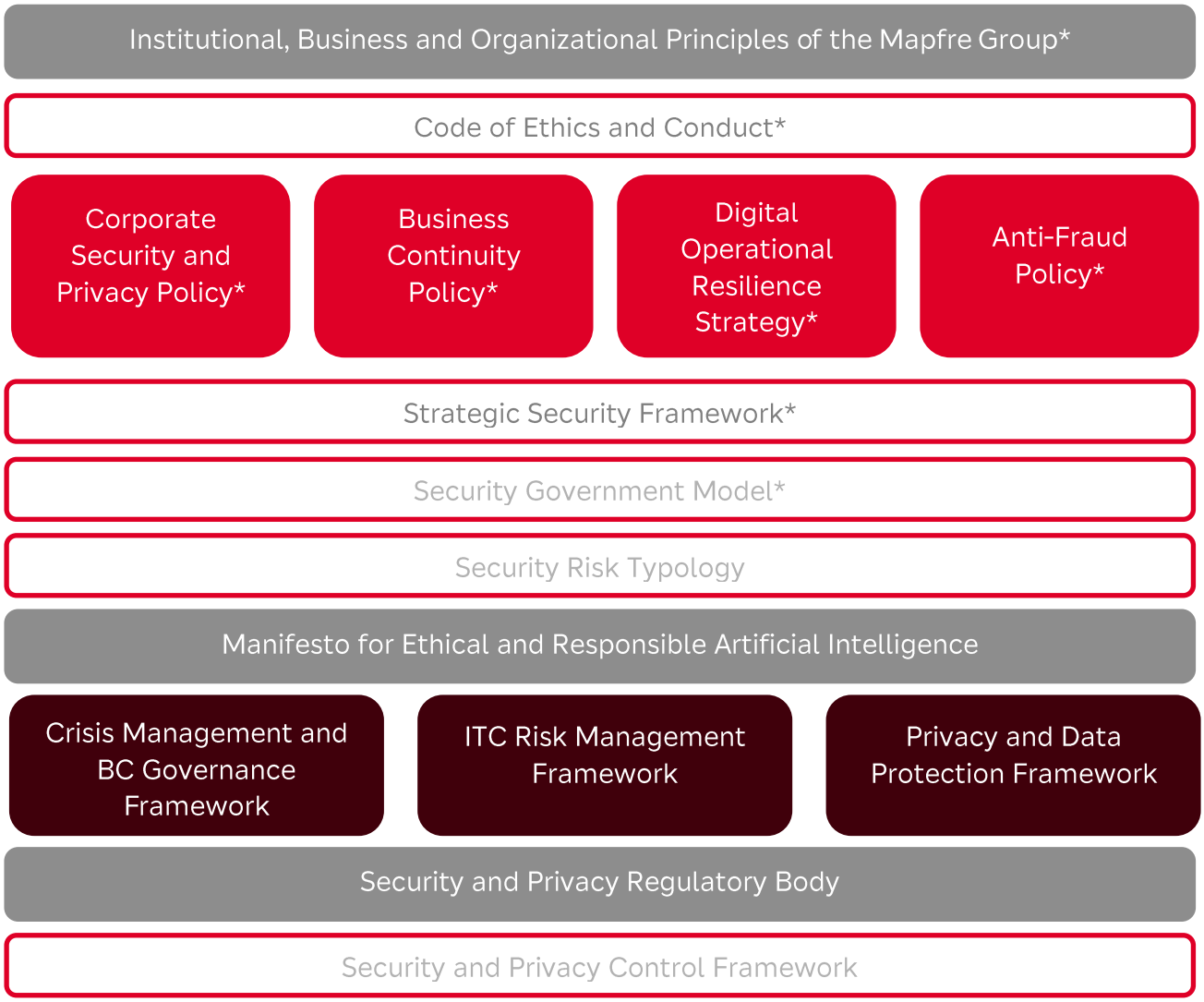
Digital Operational Resilience Strategy, which establishes the framework for managing ICT-related risks and ensuring the continuity of critical services, protecting information, guaranteeing security and operational resilience.

Anti-Fraud Policy, which establishes the guidelines, procedures and responsibilities for preventing, detecting, investigating and prosecuting fraud in all its forms.

The following links provide access to the code of ethics and conduct, as well as corporate security policies:

- Code of Ethics and Conduct
- Corporate Security and Privacy Policy
- Business Continuity Policy

These Policies constitute the starting point for the development of the remaining components of the Security Document System, as shown in the following figure:

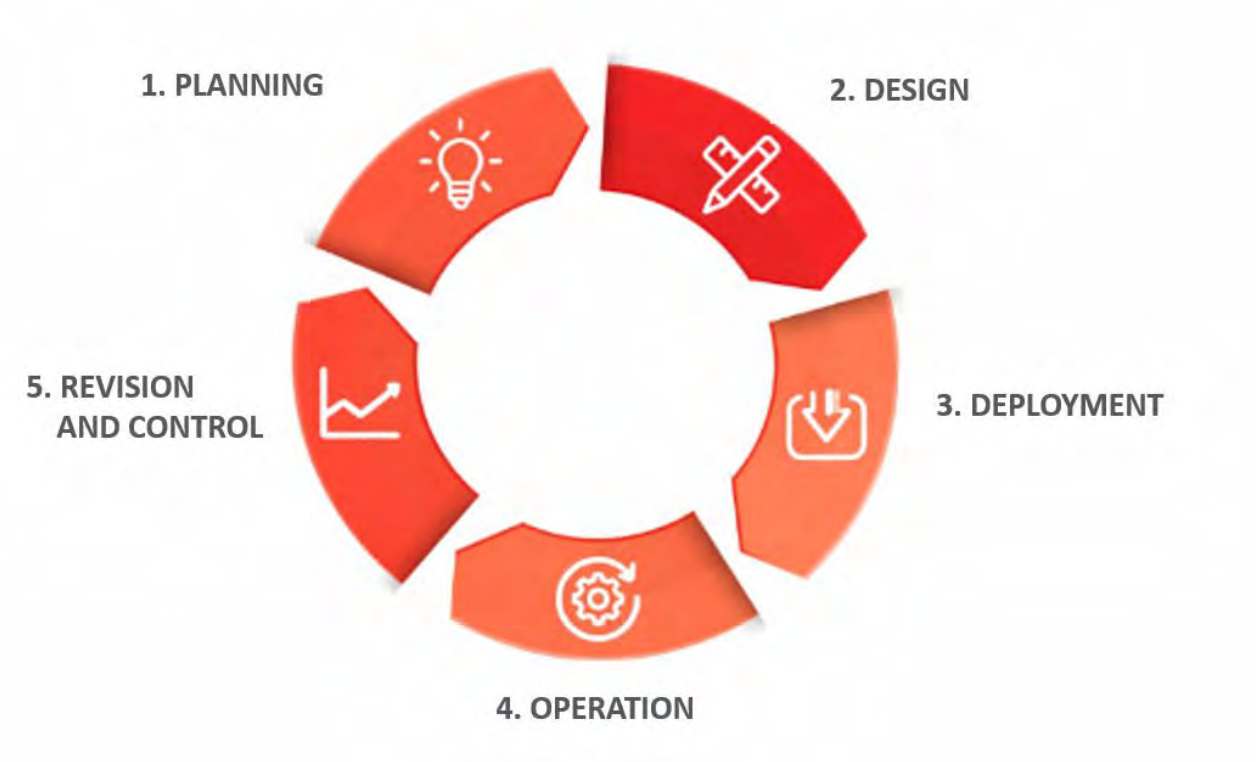


* Approved by the Board of Directors of Mapfre.

1.8

Process of Continuous Security Improvement

To carry out its mission, Security at Mapfre follows a **continuous improvement process** that also allows it to align plans and projects in this area with the Group's Strategy, the threats of the environment and the needs of our clients.



Security Organization

02

The Government of Security requires an **Organization** that adequately articulates the Function while been aligned with the **global dimension and the corporate organizational** structure.

2.1

Security Organization Structure

Mapfre's Security Organization integrates the human teams, means and resources of all kinds intended to protect the Group's tangible and intangible assets, with the aim of preserving the company's operational resilience.

It is structured in different levels of responsibility aligned with the Group's corporate governance structure, as follows:

- Mapfre Board of Directors
- Mapfre Executive Committee
- Corporate Committee on Security, Crisis and Resilience
- Corporate Committee on Privacy, Data Protection and Responsible AI
- Corporate Security Department

2.2

Mapfre SA Board of Directors

At the apex of Mapfre's security governance model is the Board of Directors of Mapfre SA, which is ultimately responsible for controlling the Group's risks, and specifically those related to ICT and security. This responsibility is exercised, within their respective areas, by the Boards of Directors of the various Mapfre Group entities.

2.3

Mapfre Executive Committee

Mapfre's Executive Committee, acting on behalf of the Board of Directors, directly oversees security management, thus demonstrating senior management's commitment to and support for the security function. This responsibility is exercised, within their respective areas, by the management committees of the Group's various entities.

2.4

Corporate Security, Crisis and Resilience Committee

It is the highest executive body of the Security Organization, ensuring that business objectives and needs govern the activity of the Security Function, while guaranteeing that security, privacy and operational resilience are considered a constituent element of corporate business processes.

When the situation requires it, this Committee becomes the Group's Crisis Committee, exercising the functions assigned in the Business Continuity Policy and Governance Model.

The Committee is chaired by the First Vice President of the Mapfre Group, and its members include the Senior Management members responsible for its main business areas and corporate functions.

The composition of the Committee as of the date of writing this document is as follows:

CHAIRMAN of the Committee:

- First Vice Chairman of the Board of Directors of Mapfre SA**

MEMBERS of the Committee:

- CEO of IBERIA**
- CEO of the INTERNATIONAL Insurance Unit**
- CEO of NORTH AMERICA*
- Chief Financial Officer (CFO)**
- General Manager of Legal Affairs (General Secretary of Mapfre)*
- Corporate General Manager of Technology and Data*
- General Manager of People, Strategy and Sustainability*
- General Manager of Business*
- General Manager of External Relations and Communication
- Corporate Chief Security Officer (Corporate CSO)

** Member of the Board of Directors and the Executive Committee of Mapfre SA.

* Member of the Executive Committee of Mapfre SA.

2.5

Corporate Privacy, Data Protection and Responsible AI Committee

A specific operational committee, subordinate to the Corporate Security, Crisis and Resilience Committee, for supervision and coordination in the area of privacy and protection of personal data and responsible Artificial Intelligence, which supports Data and Artificial Intelligence Protection Officer or Data Protection and Artificial Intelligence Officer (DAIPO) responsible for the performance of their duties.

It is the former Corporate Privacy and Data Protection Committee that has expanded its powers in the area of responsible use of AI systems.

2.6

Corporate Security Department

Mapfre's Corporate Security Directorate (DCS) is the global body responsible for directing, planning and executing the Corporate Security Function, in its various areas of operation:

- Security of People.
- Security of Facilities.
- Information Systems Security (Cybersecurity).
- Personal Data and Artificial Intelligence Privacy and Protection.
- Operational Resilience: Crisis Management and Business Continuity.
- Fraud Prevention.
- Security Intelligence.
- Regulatory and legal compliance in matters of Security, Operational Resilience, Privacy and Artificial Intelligence.
- Third-party and supplier security risks.

2.7

Highly Qualified Human Team

Mapfre, through the team of highly qualified experts of the **Corporate Security Directorate (DCS),** has managed to equip itself with the best capabilities to fulfill its mission and serve an increasingly globalized, complex and demanding environment.

The **high specialization and technical qualification** of our personnel stands out as a fundamental part of the value contribution to the company and our clients, and has been recognized by public and private authorities on numerous occasions.

This high level of specialization is evidenced by the more than **300 individual certifications** held by DCS staff across all disciplines of Security, Privacy, and Business Continuity, with a total of 125 certified employees as of the date of this report. See Appendix A.1 for a list of certifications.

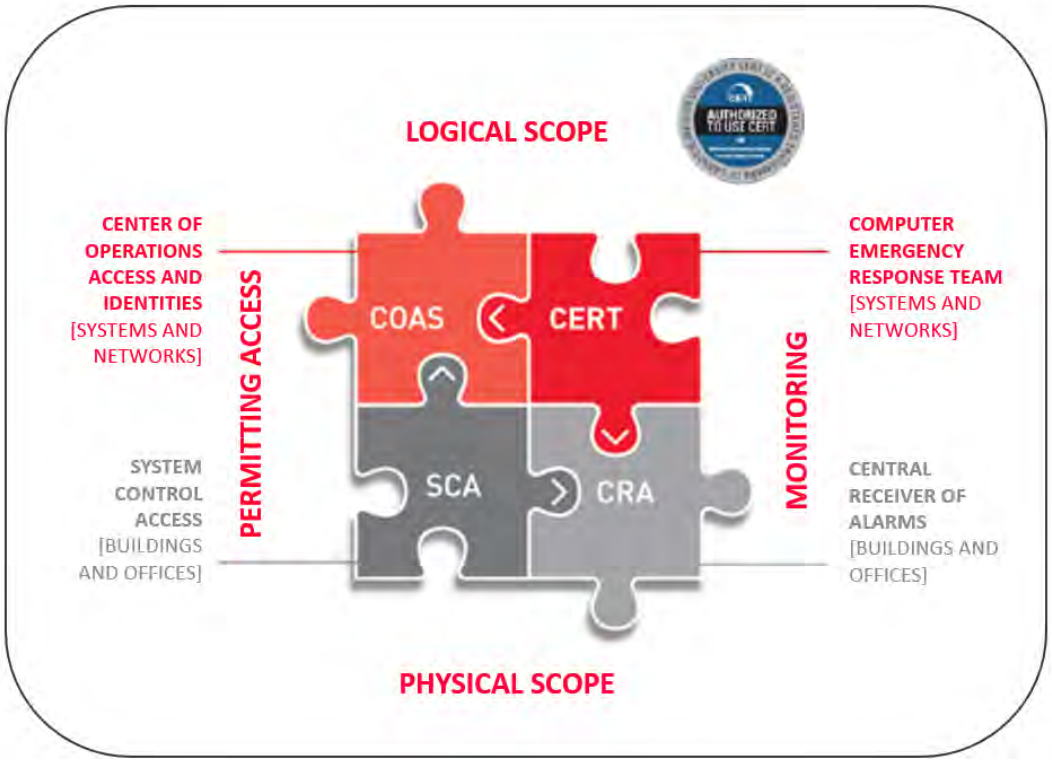
2.8

Global Security Operations Center (Global SOC)

Mapfre's **Global Security Operations Center (Global SOC)** is the body, certified as **" Computer Emergency Response Team" (CERT),** which provides the Group with monitoring, identity management and access control capabilities, and incident response at a global level.

This body embodies Mapfre's comprehensive and integrated security model, forming its core. It enables and controls access to Mapfre's Information Systems and facilities, monitors various physical and logical events, and responds to security incidents of any kind.

The Global SOC is integrated into the **"Forum of Incident Response and Security Teams " (FIRST)** and is in constant contact with the main private and government CERTs in the world, as well as in the National Network of SOCs of the Spanish CCN-CERT, and is part of the CSIRT.es network, which facilitates collaboration and the exchange of information between public cybersecurity operations centers in order to identify threats and respond early to possible incidents.



SECURITY PLATFORMS OPERATIONS CENTER

(Operation of Systems and Security Tools)

The **Global SOC** is certified to **ISO 27001 and ISO 22301,** as well as to Spain's National Security Scheme (ENS). Additionally, it was **the first Spanish Certified Equipment Trainer (CERT) to obtain ISO 9001 certification** and was recognized by the **Gartner Group as a success story** in the design, implementation, and operation of a comprehensive security model.

ISO 9001 certification validates the effective management of SOC processes. It helps identify inefficiencies and areas for improvement in a continuous improvement process and allows for the assessment of customer satisfaction.

ISO 27001 certification in Information Security confirms that an organization has a risk management model and controls appropriate to its risk levels. The organization's risk position and the suitability and effectiveness of the implemented controls are periodically assessed.

ISO 22301 certification in Business Continuity demonstrates the ability to identify potential current and future risk scenarios, determine critical functions and strengthen their protection against potential emergencies, and ensure service continuity in unforeseen situations.

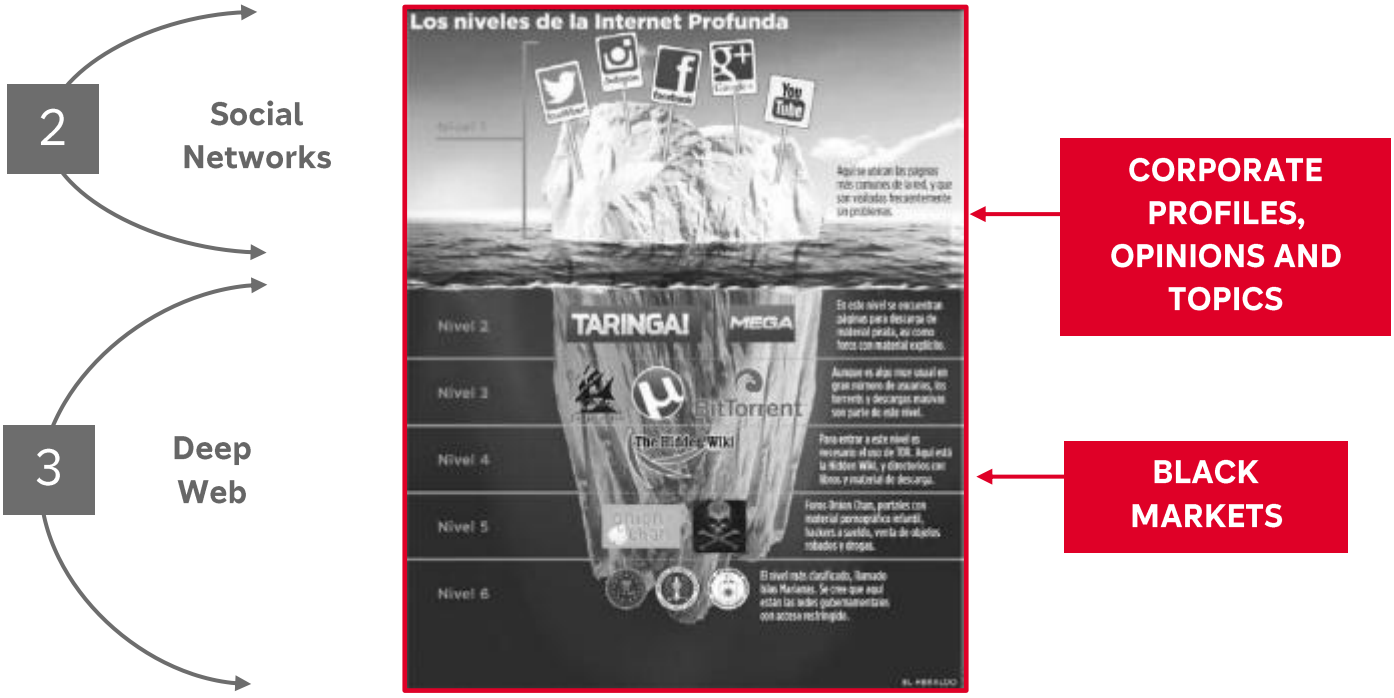
National Network of Security Operations Centers (RNSOC): In Q1 2023, Mapfre became the **first private entity** (not a provider of ICT services to the Public Administration) to join the RNSOC of the CCN-CERT. The RNSOC comprises more than 200 entities classified into two access levels: Gold and Silver. **Mapfre was included as a Gold member** , once again becoming the first non-technology private company to achieve this status.

Mapfre's Global SOC has obtained the **Spanish National Security Scheme (ENS) Conformity Certification in the MEDIUM category** , reinforcing the robustness of its information protection and management model. This certification accredits controls, processes, and capabilities aligned with official standards, guaranteeing highly reliable monitoring, detection, and response services. For our clients, this translates into greater confidence, resilience, and a level of security verified by an independent body.

The Global **SOC** monitors all activity events from the networks, systems, and users generated in the technological areas where Mapfre operates. More than 4 billion events are managed daily and analyzed using intelligence rules to generate alerts for potential anomalies .

The generated alerts are managed globally by specialized teams, in a 24x7x365 mode, in which a rigorous process of identification, analysis, evaluation, containment, resolution, escalation and registration of the alerts is applied.

The Global SOC monitors:



Security and Privacy Compliance

03

Mapfre's governing bodies have always had a special concern for good corporate governance, and have therefore adopted a set of principles and standards that govern their actions, grouped together in the Code of Ethics and Conduct that guarantees strict compliance with the laws and their obligations, as well as with the good practices of the sectors and territories in which our activities are carried out.

Mapfre has created a Security Regulatory Body, based on ISO 27002, ISO 27701, ISO 22301, and ISO 29100 standards, and further enhanced by other widely recognized industry standards, such as the NIST CSF Cybersecurity Framework, the PCI-DSS standard, and Spain's National Security Scheme (ENS). This Regulatory Framework is mandatory for all processes and activities in which the Group's entities participate.

The Regulatory Body, made up of more than 100 documents, is constantly being adapted, just like Mapfre, to the different legislations that appear in the countries where it operates.

Regarding compliance monitoring, special mention should be made of the applicable European Union Regulations, which Mapfre adopts as **reference standards for the entire Group:**

- **General Data Protection Regulation (GDPR),** the benchmark standard in privacy matters, whose strict compliance constitutes the guarantee offered to our clients that we will make proper use of the personal data they entrust to us, guaranteeing their privacy and confidentiality.

- **Digital Operational Resilience Regulation (DORA),** Mapfre's objective is to guarantee not only compliance with this legislation, but also to sufficiently demonstrate that it can withstand and respond to any type of disruption and threat related to ICT and recover from them within the agreed timeframes.

- **EU Artificial Intelligence Act (AI Act),** currently Work continues on adapting to this Regulation to meet the requirements within the established deadlines, but beyond this project, Mapfre, since 2022, has established guidelines and controls to ensure that AI is used responsibly at all times, **demonstrating ethical and responsible use** of the systems that use it.

Mapfre collaborates with public institutions and in sectoral forums, in order to enable both the most correct development and the most efficient implementation of the various laws in the field, as well as the most appropriate compliance.

Mapfre has a regulatory observatory and analysis system for the multiple pronouncements by regulators in the countries where it operates, with the aim of ensuring that, from the design stage, all processes always comply with the applicable regulations on security, privacy, data protection and resilience.

Mapfre, within the management process of **Third-party security risk** includes cybersecurity criteria, privacy, responsible use of AI, and operational resilience in the homologation, selection, and acquisition processes of technological solutions and services, incorporating into all its contracts with third parties clauses **on security, data protection, use and/or development of AI systems , and operational resilience,** requiring compliance from all its collaborators, in order to ensure prudent and diligent behavior in the management of its security and the personal data entrusted to it.

Therefore, we can guarantee that Mapfre has the regulations, internal procedures **and** the necessary control measures to meet the regulatory and **customer requirements** applicable to us in matters of security, privacy, responsible use of AI and digital operational resilience, monitoring and ensuring compliance at all levels of the company through the implementation of the mechanisms required by its own regulatory framework.

All the above considerations allow us to firmly convey Mapfre's willingness and ability to **comply with the requirements of security, privacy, responsible use of AI and resilience.** required by the laws of all the countries where it operates.

Security of People and Facilities

04

Mapfre considers **the security of everyone in its facilities, whether employees, customers, suppliers or visitors,** as a priority and an indispensable objective. Consequently, it has defined guidelines and implemented procedures and tools to ensure their adequate protection.

Risk Analysis:

Mapfre's main establishments and facilities undergo regular security risk analyses that cover all potential threats: natural disasters, fires, unauthorized access, theft or corruption of information stored on various media, and other risks. Based on these analyses, appropriate security measures are considered and implemented.

Fire Protection:

Mapfre's internal regulations establish fire protection requirements for all its facilities, whether owned or not. These requirements mandate, at a minimum, adequate compliance with applicable regulations, with particular attention to areas critical to the safety of personnel and the operation of the business. It is worth noting that, in its commitment to sustainability, Mapfre uses clean and environmentally friendly agents in its fire suppression systems.

Self-Protection and Emergency Plans:

Implemented and updated in all facilities where Mapfre operates; adapted to the regulatory requirements established in each area, including the performance of drills with the frequency established by the regulations and at least once (1) a year. During 2025, 548 emergency drills were carried out at Mapfre facilities.

Security and Access Control Systems:

In response to the identified risks in both buildings and offices, Mapfre has implemented physical access control systems, based on a prior risk analysis, as well as video surveillance, alarm systems, and/or security personnel for monitoring and overseeing these systems. Those areas whose security has the greatest impact on Mapfre's operations and business have enhanced security measures, designed according to a layered and in-depth defense model.

Mapfre's Global SOC continuously monitors and supervises these systems, ensuring a fast and effective response in incident management. Most of the installed security systems are based on IP technology, using Mapfre's own proprietary communication networks.

These measures are further reinforced by drills and training and awareness activities, which are carried out periodically and systematically.

Travel and Event Safety:

Mapfre's commitment to the safety of its employees and partners also extends to their travel. Employees have access to a comprehensive system that protects them when traveling abroad. This system analyzes upcoming trips, identifies and assesses associated risks, and contacts travelers destined for higher-risk areas, all while being always monitored by the Global Security Operations Center (SOC).

In addition, travelers have access to a Self-Protection Guide with travel safety tips, as well as specific Safety Guides for trips to destinations considered medium or high risk. These guides contain information about different regions of the country, useful contacts, including the SOC's 24/7 helpline, and safety advice regarding the country's risks.

As a result, Mapfre has obtained Travel Risk Management certification in accordance with the ISO 31030 standard “Travel risk Management. Guidance for organizations” for the management of international travel originating in Spain, for employees of the Group.

The ISO 31030 certification is a recognition of Mapfre's advanced practices in managing risks associated with travel, ensuring that the Group's employees have the best protection, safety and support measures on their international trips.

Cybersecurity

05

Mapfre has established a **Cybersecurity** prevention and protection model based on the following pillars:

The technology security architecture, through which the foundations of cybersecurity in the company are created, by selecting the best solutions for each of the areas.

Integrating security from the design and by default in all new initiatives: the construction of new solutions, the contracting of new services, etc. In other words, integrating cybersecurity from the design stage is a basic quality requirement for all Mapfre processes.

Proactive third-party risk management, applying specific methodologies to verify that they have the appropriate level of security and verify that the risks derived from the service they provide are adequately controlled

The education of all Mapfre personnel in Security matters and the specific training of those who may have access to third party information, whether recipients (clients) or providers of a service (providers).

TECHNOLOGY

- Baseline Definition of Cybersecurity.
- Specific tools: the best in the Market.
- Search for added value.

CYBERSECURITY AND PRIVACY "from the cradle to the

- Integrated from the design and by default in all business initiatives
- Included in the construction and acquisition of solutions and services, as well as in the establishment of agreements with third parties.
- Evaluating the impact on privacy of new treatments and implementing controls and measures in this regard

CULTURE

- Educating employees, customers and stakeholders.
- Specific training for critical personnel.
- Training for Security personnel and Crisis management exercises, for the management of the entities.
- Training and Awareness Plan, approved by the Corporate Security, Crisis and Resilience Committee.
- Crisis management drills and exercises for management committees and key personnel of the entities.

THIRD PARTY SECURITY RISK

- Covering the life cycle of our relationship with third parties: approval, bidding/contracting, contract execution and completion.
- Level of demand associated with the risk for Mapfre that the activity provided entails.
- Use of Trust Seals (LEET Security) and rating tools to evaluate. the security level of the third party.

5.1

Security by Design

Mapfre considers cybersecurity, privacy, and responsible use **essential quality requirements** in the development of its processes, services, and digital solutions. For this reason, security is integrated **by design and by default** in all new initiatives, whether it involves building technological solutions, evolving existing systems, contracting services, or incorporating third parties into the Group's digital ecosystem.

This approach ensures that the risks of cybersecurity, privacy, and responsible use of AI associated with new projects, products, and services are addressed.

- **Incorporation of appropriate security controls** in the design, development, acquisition and integration phases of solutions.
- **Alignment of security requirements with corporate standards,** industry best practices and applicable regulatory obligations.
- **Active collaboration between technical, business, and security areas to ensure secure solutions** without compromising functionality or user experience.

This model allows Mapfre to reduce risk exposure, improve the effectiveness of controls, and strengthen protection against emerging threats, while facilitating innovation and digital transformation securely. By integrating cybersecurity, privacy, and the responsible use of AI from the design stage, Mapfre ensures that all its digital initiatives meet a **consistent level of protection**, in line with the most demanding standards in the insurance and financial sectors.

5.2

Technology: the highest industry standards

To **protect its technological environment and the data it manages,** Mapfre leverages industry-leading solutions and services. All security solutions undergo a rigorous and comprehensive market review process to select the best possible option for all Group entities.

5.3

Secure Application Development

With a reality increasingly dependent on digital applications and with the presence of an increasingly demanding regulatory environment and best practices, Mapfre considers that security in its applications is not only an operational necessity, but an unavoidable responsibility.

To address these challenges, a strategy has been defined based on:

- **A comprehensive view of the entire software lifecycle,** based on processes that seek to ensure that each initiative—whether it is an in-house development, an integration, or an acquisition—is built and operated under the highest protection standards.
- **Our own security model,** based on the best market practices (SAMM, DSOMM, BSIMM, ...) that includes more than 50 activities to consider throughout the application lifecycle with the aim of understanding its maturity and prioritizing efforts.
- **Daily collaboration between Security and Technology** throughout all stages of the life cycle.
- **Reference architectures and safe patterns** from the design phase, facilitating consistent and reusable solutions.
- **Enterprise development platforms with automated and mandatory controls** that validate code from the earliest stages of development, with advanced security services such as:
    - Detecting **secrets** in the code.
    - Analysis of **dependencies in third-party libraries.**
    - Detecting **information leaks** in repositories.
    - **Static code analysis.**
    - Security validation **in infrastructure as code (IaC).**
- **Updated inventories** for applications and their components facilitate proper risk management, as well as the prioritization of remediation efforts according to their criticality to the business.

Furthermore, security support during development is complemented by **high value-added activities** such as:

- **Monitoring public** code repositories to prevent the exposure of information related to Mapfre.
- **Securing the continuous integration and continuous delivery (CI/CD) environment,** as well as the tools and platforms used to develop software.
- **Ongoing training** (seminars and courses) aimed at empowering development teams in security matters.

With all this, Mapfre is moving permanently and systematically towards a safer digital ecosystem, in which every application and every process reflects our commitment to excellence, protection and trust.

5.4

Identity Management

Mapfre considers it critical to securely manage access to the organization's various assets, establishing Identity and Access Management processes for each user group (employees, collaborators, intermediaries, etc.) that allow for the identification of who has accessed what and with what permissions. Access is granted to users based on the principle of granting the least possible privilege and only when necessary for them to perform their duties.

The **principles** that govern these Identity Management processes are as follows:


Incorporation of Identity and Access Management in the application development lifecycle.


Establishment of a unique and immutable identifier for each user requiring access to the company's information systems.


Definition of a specific user identifier for those accounts that require elevated permissions (administrators, automations, etc.).


Access control managed and controlled by the security area, based on authorization matrices and adequate segregation of duties.


Use of MFA (Multi-Factor Authentication) for customers, collaborator and other sensitive access web portals and, especially, for any type of remote access.


Definition of a robust password policy that is reinforced by protection mechanisms against stolen identities and weak passwords.

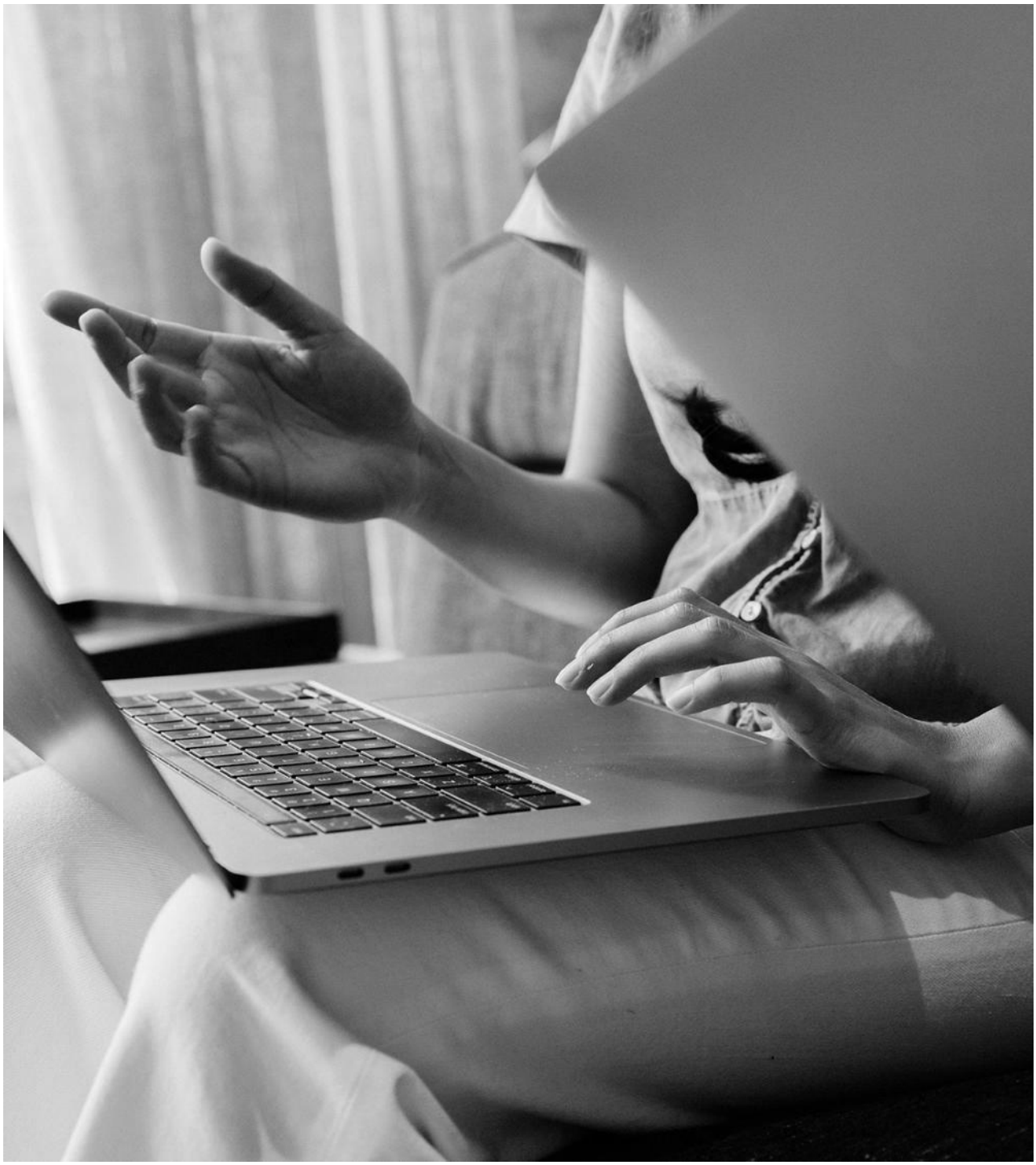

Advanced access protection based on behavioral analytics.

Restriction between productive and non-productive environments regarding the use of identities and access.


Periodic reviews of the accounts and permissions assigned to users.


Exhaustive control and continuous review of the activities of especially privileged users in critical environments, through specific tools that allow centralized management, monitoring and auditing of the use of accounts with high privileges, ensuring their use only when necessary and under strict security controls.

The Identity Governance processes governed by the DCS are intertwined with the rest of the security controls, being operated both automatically (through the Corporate Identity Management Systems), and manually from the Global SOC's Center of Access and Identity Operations (COAS).



5.5

Customer Protection

One of the current trends in the world of cybercrime is the direct, massive, and indiscriminate attack on individuals, in addition to the attacks already seen against organizations and companies across all sectors. With this objective, organized gangs attempt to obtain as much personal information as possible from an individual in order to later use that information for all kinds of fraud and blackmail.

For this reason, protecting our customers and their information in all their interactions with Mapfre has become a **top priority.** In an environment characterized by the growth of digital services and the increase in threats of fraud and identity theft, Mapfre is continuously strengthening the protection of all digital channels.

advanced security capabilities are being deployed to protect digital customer interaction environments. These capabilities enable the application of consistent, robust security controls aligned with best practices in the insurance and financial sectors, dynamically adapting to user profiles, the risk level of each access, and the attack techniques used by cybercriminals.

Among the main security measures implemented, the **use of Multi-Factor Authentication (MFA) stands out,** adding an extra layer of security to the access process. With MFA, access to customer portals requires not only knowledge of credentials (username and password) but also a second, independent factor, significantly reducing the risk of unauthorized access even in the event of a credential breach due to causes beyond Mapfre's control.

Additionally, this protection model incorporates:

- **Risk-based adaptive authentication,** adjusting access controls based on context, user behavior, and the risk level of the access attempt.
- **Protection against identity theft and fraud,** through the detection of anomalous patterns or suspicious activities during the authentication process.
- **Secure and centralized identity management,** ensuring that each client only accesses the services and data that correspond to them.
- **Integration with corporate monitoring and incident response systems,** enabling early detection and coordinated action in the event of potential security incidents.
- **A balance between security and usability,** ensuring high levels of protection without introducing unnecessary friction into the customer's digital experience.

This approach is part of the ongoing evolution of the Group's cybersecurity model, ensuring that customer-facing digital portals and services maintain a level of security that meets current expectations and the most demanding market standards.

5.6

Network Security

Mapfre bases **network protection** on a model of segregation and localization of resources across different layers. At the same time, various network security solutions are applied, for example:

- Double firewall level.
- IDS/IPS for detecting and blocking of attack patterns.
- VLANs Segregation.
- Physical and/or logical isolation between entities.
- Use of Multi-Factor Authentication (MFA) for external access.
- Isolated third-party connection.
- Different Service Providers.
- Protection against distributed denial-of-service (DDoS) attacks
- WAF technologies and load balancers.
- Secure Web Gateway and DLP in the internet connection, Secure Web Gateway and DLP in email, etc.
- DNS-level security.

5.7

Device security (computer stations, servers and mobile devices)

As in the previous case, Mapfre uses various security procedures and solutions to protect the devices used, as well as the information they contain, such as:

- Advanced antimalware protection: Antivirus & EDR.
- Procedural and implemented system for managing vulnerabilities and associated patches.
- Data encryption.
- Device bastioning.
- Inventory, management and monitoring of device security.
- Mobile Device Management for mobile devices and tablets.
- Restricting access to USB ports on user computers.
- Security breach simulation tool.

5.8

Cloud Security

Mapfre is no stranger to digital transformation and, similarly to other companies, has been incorporating cloud technologies into its technology projects for years. Mapfre only uses cloud providers that comply with the highest standards, regulations, and security certifications (including ISO 27001, ISO 27018, SOC 1, SOC 2, SOC 3, PCI-DSS, and GDPR).

Mapfre's priority suppliers are:

Additionally, the various cloud initiatives must have at least the same security controls as those existing in corporate data processing centers, and should not in any way imply a decrease in the previously existing level of security.

Examples of the security controls used to achieve the above are:

- Security Architectures for the leading IaaS providers.
- Adaptation of current security controls.
- Cloud Access Security Broker (CASB).
- Cloud Security Posture Management (CSPM).
- Cloud Workload Protection Platform (CWPP).
- Shadow IT control, etc.
- Incident monitoring and response.

Monitoring cloud activity is a top priority for Mapfre. More than 500 million events (as of the date of this document) generated in these clouds are monitored daily and analyzed using advanced data processing filters. All alerts and potential anomalies are managed by the Global SOC as one of its core areas of responsibility.

5.9

Vulnerability and Patch Management

One of the key security processes to ensure an adequate level of protection for any information system involves patching systems and resolving vulnerabilities effectively and within appropriate timeframes.

Mapfre has a formalized, implemented, and mature vulnerability and patch management process that covers everything from early identification to certification of resolution by specialized teams. This process ensures that information systems are updated regularly and systematically with the latest patches released by software vendors.

In addition to the capabilities associated with the Security Technical Review Reference Center, Mapfre has support agreements with leading technology manufacturers for the early notification of vulnerabilities and continuously monitors any vulnerabilities that may affect the technology used in our information systems. Mapfre also participates in the main CERT/SOC associations, where information on vulnerabilities, particularly zero-day vulnerabilities, is exchanged.

Whenever a new vulnerability is identified or disclosed, the cybersecurity team assesses it based on its criticality and potential impact on Mapfre's systems, resulting in a classification. All identified vulnerabilities are managed for resolution within timeframes appropriate to their criticality. For the most critical vulnerabilities, an urgent procedure is activated to resolve them globally in less than 24 hours across all potentially affected information systems.

5.10

Incident Monitoring and Response

As previously stated in this document, Mapfre brings together its **cybersecurity monitoring and incident response capabilities in the Global SOC,** operating as:

- **SOC with dedicated staff at Mapfre's facilities,** with permanent availability (in 24/7/365 format).
- **Global security SOC stratified in 3 levels** of action with capacity and autonomy for immediate response to threats.
- **Automatic threat collection system** based on MISP.
- **Orchestration and automation system** of safety operation.
- **Security monitoring systems** with an intake of more than 4 billion daily monitored events (as of the date of writing this document).
- **Specific monitoring scenarios** for critical environments.
- **Connection to different groups and collaboration networks** national and international scope (First, CSIRT, FS-ISAC, National Network of SOC's).
- **Regular participation in CyberEx** , cyber exercises organized by the National Cybersecurity Institute of Spain (INCIBE), in coordination with the Cybersecurity Office (OCC).
- **Isolated laboratory** for forensic analysis.

The high level of training of the people, the tools and procedures implemented, as well as the network of contacts with organizations of a similar nature in the public and private sectors, enable Mapfre to carry out the early and effective detection and response to any cybersecurity incident.

Since the entry into force of DORA, NIS2, CRA and AI Act, Mapfre and the rest of the Group companies **have not had to notify any relevant incident to the** competent supervisory authorities.

5.11

Quantum Computing

The arrival of quantum computing will bring about a paradigm shift in the use of cryptography across all organizations, industries, and sectors. Following a detailed and in-depth analysis of the environment and its own situation, Mapfre has defined a crypto agility plan that will be implemented over the coming years. This plan includes the necessary actions to deploy Post-Quantum Cryptography (PQC) capabilities at all levels and across all information systems of the company.

This plan establishes the monitoring of technological advances in Quantum Computing, as well as collaboration with all components of the value chain as a basis to ensure timely evolution of all information systems involved in the service we provide to our clients.

5.12

Cyber Insurance

Mapfre Group entities have specific **cyber risk insurance coverage,** which includes both damage to their own assets and potential liabilities to third parties should such events occur. In terms of coverage and ensured limits, the protection contracted is consistent with and appropriate to the risk, the activity, and the size of a company like ours.

During 2025, **no events occurred that required the activation of this coverage.** This reinforces the effectiveness of the prevention, detection, and response model and the level of operational resilience achieved by the Group, with the policy remaining in place as a risk transfer instrument for scenarios of significant impact.

Technical Security Reviews

06

Mapfre considers it a priority and an essential objective to guarantee security through **rigorous technical reviews**. In this regard, it has established guidelines, procedures and tools that allow the evaluation, control and minimisation of risks, ensuring compliance with the highest safety standards in all its operations.

With the aim of enabling all entities that make up the Mapfre Group to benefit from the knowledge, experience, resources, infrastructure and tools existing at the corporate level in matters of ethical hacking and security analysis, the **Technical Security Review Reference Center has been established,** made up of highly specialized personnel, services and tools.

REFERENCE CENTER FOR TECHNICAL SAFETY INSPECTIONS

Information	Resources	People
Documentary and Government Framework	Technical Review Lab	Technical Review Team

Through the services provided by this Center, both the Corporate Security Directorate and the various entities within the Mapfre Group have access to constant information about their security and vulnerability levels, from both the perspective of an internal and external attacker. This provides a comprehensive view of the Group's security posture in this area, enabling the rapid detection and correction of any vulnerabilities.

Similarly, this center performs security reviews of the technological layer of the company's new initiatives, prior to their implementation.

As a result, Mapfre is able to apply a wide range of technical security reviews, which ensure the protection of corporate information and our clients.

This catalog of reviews includes the automated **continuous review process of systems exposed to the internet, as well as systems deployed in the Corporate and local Data Centers** of all company entities, and allows the detection of any new vulnerability in these systems.

For example:

TYPES OF REVIEW	
New Initiatives	Source Code Reviews
	Safety Tests
	Compliance Tests
External Infrastructure (Published on the Internet)	External Intrusion Testing
	External Vulnerability Scanning / ASV
Internal Infrastructure	Internal Penetration Testing (including segmentation testing and scope reduction controls)
	Internal Vulnerability Scanning
	Review of particularly relevant applications
	Corporate Infrastructure Reviews

Through this Reference Center, the execution of **Red Team exercises is led,** through which **the security posture of the organization is evaluated by simulating real and controlled attacks, emulating common hacking techniques to identify technical, physical and human vulnerabilities, also seeking to strengthen the detection and response capacity of our Global SOC.**

Similarly, other types of **Cyber Exercises are carried out** to evaluate both our protection, detection and response capabilities, as well as the security awareness of our employees.

The results of this set of reviews are integrated into the aforementioned **vulnerability and patch management system** and motivate the development of "remediation" plans subject to specific deadlines, in turn carrying out continuous monitoring of the correction of the previously mentioned vulnerabilities. detected and compliance with the established resolution deadlines.

Corporate DataCenters

07

Mapfre has four top-level **Corporate Data Processing Centers (CPD)** that meet the highest industry standards, both in the capacity and functionality of the infrastructure and in the quality of their operation. In this regard, some of the certifications that Mapfre's corporate Data Centers have are listed below.

	**TIER III in design and operation** A Tier III Data Center offers 99.98% availability. This configuration allows for scheduling. server maintenance periods without affecting service continuity. ➢ Data Center Alcalá de Henares (Madrid): Design, Facility ➢ CPD Miami: Design, Facility ➢ CPD Tamboré (Sao Paulo): Design, Facility and Operation
	**SSAE 16** (Statement on Standards for Attestation Engagements). **ISAE 3402** (International Standard for Assurance Engagements), They help ensure that the controls related to preserving the security and confidentiality of information are adequate. ➢ CPD Miami: SOC 1 type 2 and SOC 2 type 2 ➢ CPD Tamboré (Sao Paulo): SOC 1 Type 2
	**ISO 27001: Information Security Management** It is guaranteed that the data centers meet the necessary requirements to establish, implement, maintain and provide feedback on a management system based on a continuous improvement cycle. ➢ CPD Alcalá de Henares (Madrid) ➢ CPD Miami ➢ CPD Tamboré (Sao Paulo)
	**Certification of Conformity in the National Security Scheme (ENS), HIGH category, according to RD 311/2022** This certification means that the data center meets the strictest security requirements established by the Spanish National Security Scheme, guaranteeing adequate protection of the information processed and the services provided. ➢ CPD Alcalá de Henares (Madrid)
	**PCI-DSS Compliance - Service Provider** This certification guarantees that the data center complies with the requirements of the PCI-DSS (Payment Card Industry Data Security Standard) regulations, to ensure the protection of payment card data. ➢ CPD Alcalá de Henares (Madrid)

ISO 50001 ENERGY MANAGEMENT	**ISO 50001:2018 - Energy management systems** This certification guarantees that the data center meets the highest standards of energy management and efficiency, optimizing energy use, reducing costs and improving sustainability. ➢ CPD Alcalá de Henares (Madrid)
HIPAA HITECH Compliant	**HIPAA-HITECH** It guarantees the protection of confidentiality, integrity, and availability of protected electronic health information (ePHI). (USA) ➢ CDP Miami
STAR LEVEL ONE: SELF-ASSESSMENT STAR LEVEL ONE SECURITY TRUST ASSURANCE & RISK	**CSA (Cloud Security Alliance) – STAR Level 1 (Managed Cloud Services)** This certification guarantees that cloud solutions are based on cutting-edge technologies capable of providing a comprehensive response with the highest security guarantees and low latency. ➢ CDP Miami

Operational Resilience: Crisis and Business Continuity Management

08

The mission of the Security Function is to enable the normal development of the business, providing a safe environment in which Mapfre can carry out its activities. To preserve the service provided to our clients during a crisis or contingency situation, Mapfre has a **Corporate Crisis Management and Business Continuity Model**, integrated into its global approach to Security.

This model is based on **ISO 22301,** responds to the international dimension of the Mapfre Group and has been deployed in all its entities, taking into account the business needs and the particular requirements of each subsidiary.

The corporate model is based on **three main pillars:**

Its Corporate Business Continuity Policy, where Mapfre commits to this function and defines the framework for the development, implementation, review and improvement of Business Continuity Plans, so that these:

- Enable an appropriate and timely response to the materialization of a security risk (or any other type of risk) of catastrophic characteristics, which causes a scenario of unavailability of any of the basic components of our activity: people, facilities, technology, information and suppliers.
- Minimize the impact of potential disasters on business activities by preserving data and ensuring the use of essential functions. If this is not possible, facilitate a gradual recovery until normal operations are restored.

As a second pillar, Mapfre has **highly qualified PERSONNEL** in this area and a **GOVERNANCE FRAMEWORK** that determines the different bodies and functions associated with continuity within the Group (Units, Entities, Centers).

It also has a **METHODOLOGY** that allows for the homogeneous and efficient definition and development of Business Continuity Plans, mechanisms, procedures and strategies to restore resources and services.

These **Business Continuity Plans are developed, implemented and tested at least once a year** in all Mapfre entities, having repeatedly demonstrated their correct functioning in natural disasters and situations of unavailability that the different Mapfre entities have suffered throughout the world, such as pandemics, hurricanes, heavy snowfalls, fires, communication outages, etc.

In this context, **Disaster Recovery Plans (DRPs)** or IT Contingency Plans implemented in corporate data centers require special attention, as they are a fundamental pillar of Business Continuity Plans, in order to guarantee the continuous availability of the services provided from them. These DRPs are systematically tested, at least annually, in all organizations, with increasingly rigorous testing each time.

Additionally, Mapfre has opted for a progressive certification process for these plans across its various entities. Currently, many of its entities— **Mapfre Spain (including Mapfre VIDA), Mapfre RE, MAWDY, Mapfre USA, Mapfre Brazil, Mapfre Global Risks , Mapfre Investment, Mapfre Mexico, Mapfre Peru, Mapfre Turkey, Mapfre TECH, Mapfre BHD (Dominican Republic), Mapfre Puerto Rico, Mapfre Malta, Mapfre Panama, Mapfre Portugal, Mapfre Honduras, Mapfre Costa Rica, Mapfre Investimentos (Brazil),** and the Mapfre Group's Global SOC—are certified under ISO 22301, ensuring the continuous updating and improvement of these plans.

The countries/business units with Business Continuity Plans **certified under ISO 22301 represent 92% of the total premiums** issued by the Mapfre Group. This international standard certifies that the certified entities have properly implemented Business Continuity Management Systems (BCMS) designed to protect them from potential disruptions, guaranteeing their recovery with reasonable expectations of success in the face of different types of disasters and ensuring the continuity of their operations. Furthermore, it guarantees the continuous updating and improvement of these systems.


AENOR
Certificado del Sistema de Gestión de la Continuidad del Negocio


AENOR
Certificado del Sistema de Gestión de la Continuidad del Negocio
MAPFRE ESPAÑA, S.A.


AENOR
Certificado del Sistema de Gestión de la Continuidad del Negocio
MAPFRE RE, COMPAÑIA DE REASEGUROS, S.A.


AENOR
Certificado del Sistema de Gestión de la Continuidad del Negocio
MAPFRE GLOBAL RISKS, S.A.

Privacy and Personal Data Protection

09

Mapfre has as an absolute priority the privacy and protection of personal data to which it has access in the exercise of its activity, understanding this as an essential element that must be pursued proactively, not only with the objective of achieving compliance. of the applicable regulations, but as fair correspondence to the trust placed by clients, suppliers, collaborators, employees and other interest groups.

9.1

Data and Artificial Intelligence Protection Officer

Mapfre has a **Data and Artificial Intelligence Corporate Protection Officer and a specific area** within the Corporate Security Directorate responsible for ensuring compliance with existing regulations on **privacy,** personal **data protection and artificial intelligence.**

Within this area and in support of the Corporate Data Protection Officer, the **Corporate Office of Privacy and Data Protection (OCPPD) is established** , whose mission is to be the point of reference for all activities related to privacy and data protection at Mapfre, providing a unique and global vision of the matter, and promoting the homogeneity of all processes and criteria related to it.

The DAIPO corresponds to the figure of the data protection officer (DPO) established in the privacy and/or data protection regulation, who, in addition to the functions established in said regulation, assumes the responsibility to ensure responsible and ethical use of data and artificial intelligence systems.

Additionally, Mapfre has a responsible **Corporate Committee on Privacy, Data Protection and Artificial Intelligence** to support the DAIPO in carrying out its functions.

In the various countries where the Group's insurance entities operate and where legislation requires such a role, it has **Local Data Protection Officers** and **Local Privacy and Data Protection Committees,** which report functionally to the corporate office. In those countries where, due to the size of the entity or business, a specific DPO is not appointed, there is a person responsible for privacy and data protection who works in conjunction with the corresponding DPO.

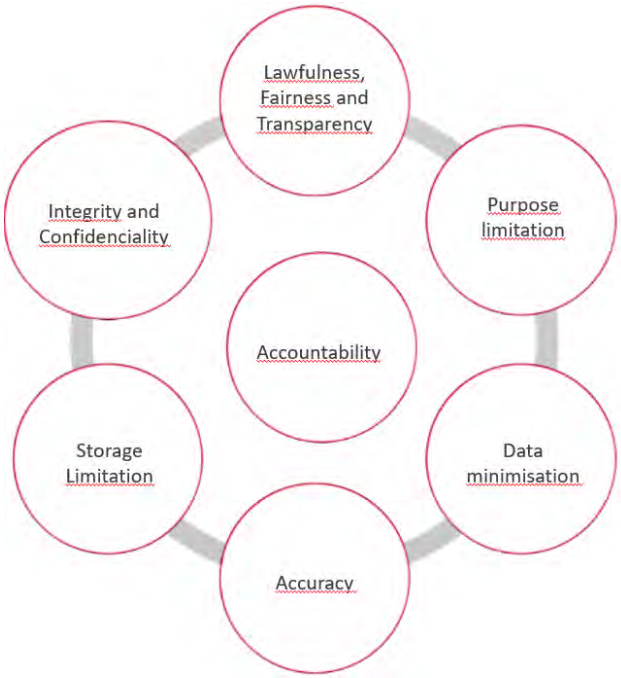
Mapfre maintains a **transparent relationship with the Supervisory Authorities,** facilitating close collaboration, cooperation and communication, in order to guarantee effective protection of the fundamental rights and freedoms of natural people in relation to the processing of their personal data.

9.2

Privacy Framework

Mapfre has adopted **the European Union's General Data Protection Regulation** (GDPR) as its framework for Privacy and Data Protection.

Through this reference model, the Mapfre Group ensures compliance with a **common and homogeneous protection standard** throughout the Group, and guarantees compliance with the principles relating to the processing of personal data.

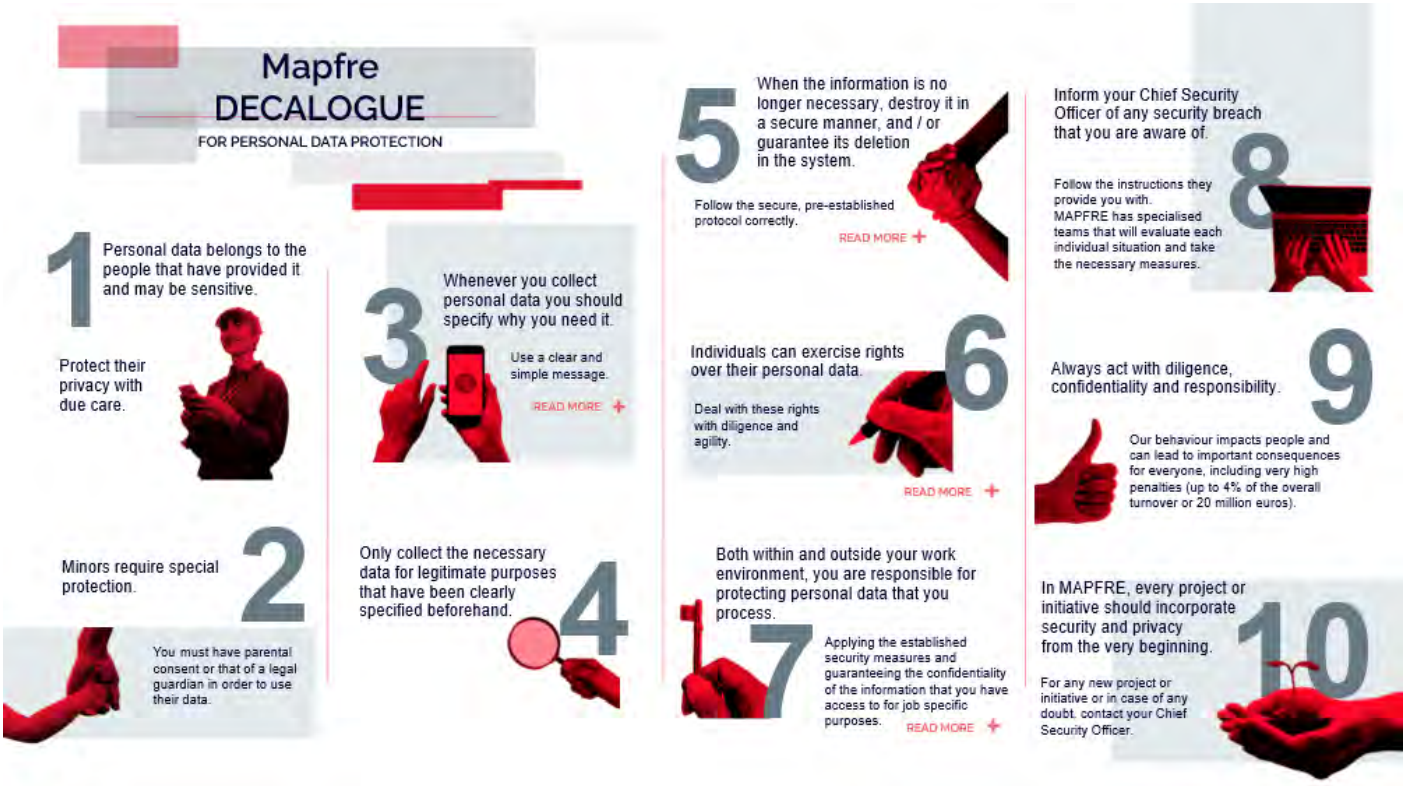


For its implementation and management, this reference model is structured around a series of **strategic lines:**

- **Proactive Responsibility:**
  - **Early adaptation** to applicable privacy regulations in the different geographies in which it operates.
  - **Implementation of appropriate technical and organizational measures in the company's processes**, not only to ensure protection and compliance with applicable regulations but also to demonstrate compliance to supervisory authorities and interested parties.

- **Protection by design and by default: Integrating privacy into the life cycle of any new initiative** that manages personal data, respecting the rules for the protection of fundamental rights and freedoms and implementing controls and measures designed to preserve the confidentiality, integrity and availability of the information handled and the systems that support it.
- **Risk Management.** Privacy impact assessment of new processing activities. As well as in the event of substantial changes that affect the processing environment (its requirements and/or risks) or the security and privacy measures in place.
- **Privacy assessment** in the processes of purchasing technological solutions and in the contracting of technological services.
- Inclusion of **Information Clauses** and management of consents (or other legal bases) in the collection of personal data.
- Inclusion of **Privacy and Data Protection Clauses** in Service Provision Contracts, with those providers who handle or access information, to guarantee compliance with security and privacy obligations.
- Timely and proper attention to the exercise of the **Rights of Interested Parties,** such as queries and/or complaints addressed to the Data Protection Officer.
- **Privacy Culture:** Specific Training and Awareness Plans on Privacy and Data Protection.
- **Promoting public-private collaboration.** Participating in associations that promote privacy and in sectoral and institutional initiatives aimed at clarifying the application of the GDPR, such as the DPO Forum or the DPO Community.

Decalogue for the Processing of Personal Data, which establishes the principles of privacy that all employees, agents and delegates must respect wherever they are in the world:



9.3

Binding Corporate Rules (BCR)

As an evolution of the model, and in order to comply with more demanding standards, Mapfre has adopted **Binding Corporate Rules of Controllership (BCR-C)** , a personal data protection policy assumed by a business group, which enables international data transfers between its different entities by guaranteeing in all of them, regardless of their location, a level of protection equivalent to that offered by the EU General Data Protection Regulation (GDPR).

favorable opinion of the European Data Protection Board (EDPB), the BCR-Cs have been **approved by the Spanish Data Protection Agency (AEPD),** which led the formal review and approval process, with the collaboration of the Co-Reviewing Supervisory Authorities and other EU supervisory authorities for their assessment.

- https://www.aepd.es/documento/ti-00002-2024-resolucion-aprobacion-bcr-r-Mapfre.pdf

The Binding Corporate Rules demonstrate Mapfre's commitment to Privacy (customers, suppliers, collaborators, employees and stakeholders), proving to third parties compliance with the General Data Protection Regulation (GDPR) even in **Mapfre entities located outside the EEA,** and a homogeneous level of protection over their data regardless of the country in which they are hosted and the obligations required by local regulations in carrying out **international data transfers** between the entities of the Mapfre Group.

The full text of the BCR can be found at the following links:

- Spanish: BCR of the Mapfre Group
- English: Mapfre Group's BCR
- Portuguese: BCR of Grupo Mapfre

Artificial Intelligence and Data Ethics

10

Mapfre values the development of technology and the increase in the volume and use of data as a fundamental factor and strives to position itself at the forefront of innovation in the use of data in the most ethical way.

Mapfre is committed to the **responsible and ethical use of Artificial Intelligence,** taking advantage of the opportunities of new technologies and complying with current legislation in the digital field, as set out in the Digital Governance Ethics Framework and the Principles on the responsible and ethical use of Artificial Intelligence.

Furthermore, Mapfre has a **Framework of Reference** to implement a **governance model for the responsible use of AI,** with a human-centered approach, which allows for the definition of new responsibilities in the field of AI, and which have been reflected in the **Manifesto for a humanistic, ethical and responsible artificial intelligence.**

- Manifesto-AI-interactive-EN.pdf

Mapfre adapts its security, privacy, and responsible use requirements from the outset and by default in all its initiatives and projects to **ensure adequate control** over the use of this technology, protecting both the personal data used and the information relevant to the company, and achieving optimal levels of quality, security, reliability, robustness, traceability, privacy, fairness, explainability , and transparency for each use case. Mapfre also has defined contractual clauses to be included in contracts with service providers related to Artificial Intelligence.

Additionally, Mapfre has a **multidisciplinary Working Group on the responsible use of Artificial Intelligence,** as well as a Corporate Committee on Privacy and Data Protection and responsible Artificial Intelligence, to manage issues related to ethics and data protection, streamlining processes, raising employee awareness, automating decisions and improving customer experience, with the aim of ensuring ethical and responsible use of data.

Mapfre has a “Guide **to the Use of Artificial Intelligence Systems”** which establishes the guidelines and mechanisms necessary to determine the level of risk based on the use that will be given to them, as well as the necessary measures to mitigate the associated risks that arise from the use of this type of technology.

Mapfre has been working for some time on **early adaptation to the** applicable regulations in this area of Artificial Intelligence and is currently implementing a **Plan for Adaptation to the European Union's regulations on Artificial Intelligence** , which brings together a series of projects and lines of work, whose objective is to comply with the obligations required by the regulators within the established deadlines.

Finally, it is worth mentioning Mapfre's adherence to the **'Commitments to Privacy and Digital Ethics'** of the Cotec Foundation. This commitment was created to address the challenge of data processing in a context of digital transformation, where the application of ethical principles in privacy management, and especially in the development and use of data-driven applications, is becoming increasingly important.

- https://cotec.es/proyectos-cpt/compromisos-para-la-privacidad-y-etica-digital/

Adherence to this ten-point plan demonstrates Mapfre's commitment and concern for privacy management from the perspective of the **ethical and responsible handling of data** provided to us by our clients, partners, intermediaries and employees.

Security Culture: Awareness, Sensitization and Training

11

Mapfre is aware that people are the most important and, sometimes, the weakest link in the security chain. Therefore, the creation of a Security culture constitutes a strategic requirement for the company.

Mapfre has a multidisciplinary **Working Group** called **"Security Culture"**. with the participation of the Corporate Areas of People and Organization, External Relations and Communication and Security, responsible for defining, developing and maintaining the **Global Security Awareness and Training Plan,** which is updated annually, and is continuously adapted to the needs of the environment.

This Plan is approved by the Corporate Security, Crisis and Resilience Committee, the highest executive body of the Security Organization, thus materializing the commitment of Senior Management to the promotion of security culture in the organization.

In line with Mapfre's global and comprehensive vision of security, this plan includes **ICT security, privacy and data protection, artificial** intelligence**, digital operational resilience,** and the **safety of people and facilities.**

The actions included in the Plan are aimed not only at Mapfre **employees, but also at third parties,** such as **intermediaries, critical suppliers, customers** and other **stakeholders.**

Awareness campaigns, which aim to achieve an emotional impact, through **awareness-raising activities,** so that people know about the threats and good practices, as well as technical **training programs,** adapted to different groups according to their level of criticality and responsibilities.

99,697 hours have been dedicated to security training over the last three fiscal years. The number of Mapfre employees trained between 2023 and 2025 reached **23,709.** By the end of the fiscal year, **86% of the workforce** had received training in this area.

All of them are systematically measured, obtaining statistics and indicators that allow for the evaluation of their effectiveness and the continuous improvement of the process.

Some examples of these actions are:

- **Regular publication of** security news, tips, videos, infographics, podcasts, interactive mini-games, and other communication resources. During 2025, over 100 security-related pieces of content were published in various corporate languages.

- **Specific awareness-rising campaigns** for employees, using gamification and storytelling techniques. Throughout 2025, the cybersecurity training program "The Firewall Mindset" continued, launching a new season of content that was completed by the end of the year by a total of 8,832 employees globally.

- **Training modules** at the Mapfre Corporate University, available to all employees.

- **During the period 2023-2024, an ambitious training plan was carried out for all ICT staff,** through 10 monographic courses, with more than 1,800 professionals trained and around 15,000 hours of training carried out in this field.

- Specific awareness sessions aimed at **Senior Management and External Advisors** of the Group.

- Security personnel **training and crisis management exercises.**

- **Cyber exercises** with campaigns targeting all employees were designed to test the effectiveness of training and awareness initiatives, as well as to evaluate employee behavior in the face of the most common cyberattacks. In 2025, employees demonstrated appropriate behavior in **93%** of the exercises.

- **Cyberincident management drills,** executed by the Management Committees of the different Entities, constituted as Crisis Committees of the different entities of the Group.

Audits

12

Within the process of continuous Security improvement and as the third line of defense of the internal control system, Mapfre systematically and periodically carries out Security Audits.

Mapfre conducts specific **audits** related to compliance with the Security and Privacy Policy, the Business Continuity Policy and the Data Protection regulations, which are carried out by expert auditors.

Additionally, within the **Internal Control Audit Methodology for Technology and Security** developed at Mapfre, a section is always included in the ICT Environment Control Area regarding compliance with the Security Regulations and legislation affecting these matters, including data protection.

Finally, **business process audits** also **include specific security and privacy aspects,** in order to identify potential weaknesses, vulnerabilities and risks and implement preventive and corrective improvement actions that guarantee regulatory compliance and allow raising the level of security and operational resilience.

As a result, throughout 2025, external and internal auditors have carried out **141 audits** on information systems and security, cybersecurity, business continuity, cloud systems, artificial intelligence, as well as privacy and data protection.

The Mapfre Group Executive Committee carries out a systematic and protocolized monitoring of the results of the audits and the implementation of the action plans derived from its recommendations.

The year 2025, like the preceding years, **closed with no overdue audit recommendations.** The recommendations planned for subsequent years have been implemented or are in the process of being resolved, in accordance with the established action plans.

Third-Party Acknowledgement and Benchmarking

13

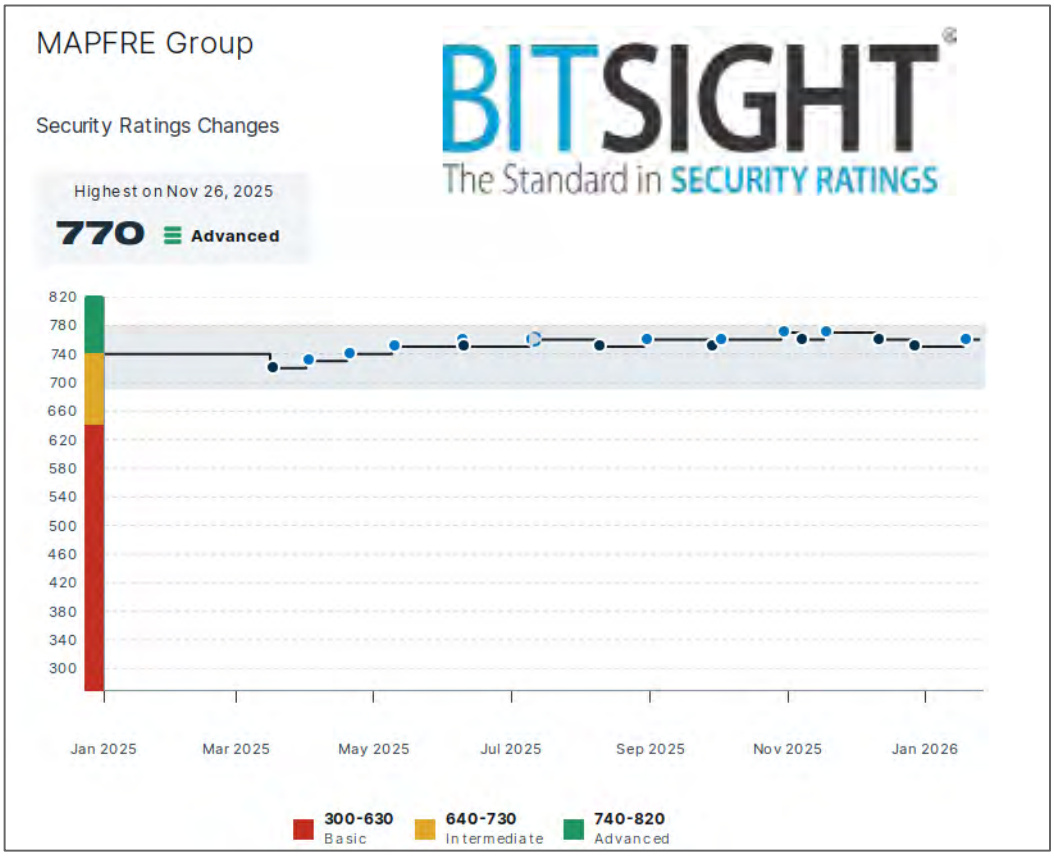
The **integrated and global security** model adopted by Mapfre is a benchmark for international analysts and other corporate security organizations of large companies, which has resulted in numerous awards and recognitions, including:

Forbes	Fourth Edition of the Forbes Innovation Awards Kyndryl Mapfre has been awarded the **first prize** in the **Cybersecurity and Resilience category,** for its project “Cryptographic risk in a post-quantum world”.
GartnerGroup	Definition of a Case Study relating to the Global SOC (formerly Mapfre General Control Center, CCG-CERT), carried out by the prestigious international analyst **Gartner Group.** 
	First Prize for Excellence in Corporate Security Duke of Ahumada awarded by the Ministry of the Interior of the Kingdom of Spain to Mapfre for having a comprehensive security model, a reference for corporate security organizations.
REVISTA SIC	**The SIC Magazine Security Award** in its 14th edition was given to Mapfre “in recognition of its pioneering, multidisciplinary and integrated approach to the fronts of corporate protection, including those associated with information security management and cybersecurity.”
BORRMART, S.A.	**International Security Trophy for Research and Development (R&D) Activity,** in the XXVI Edition of the International Security Awards Competition, in its category of Trophies for the best security project convened by the Borrmart publishing house.
redseguridad.com	**Extraordinary Jury Prize from the RED SEGURIDAD awards.**

	Honorable Mention from the General Directorate of the Spanish National Police Corps.
IDC ANALYZE THE FUTURE	Mapfre was awarded in 2019 by the consulting firm IDC Research Spain **for "Cybersecurity strategy project adapted to the new digital scenario"**

Additionally, Mapfre's security model was selected by IE Business School, considered by the main international rankings as one of the five best European schools for its MBA and executive training programs, as a practical case within its Master in Cybersecurity.

Below, we see the evaluation of third-party benchmarks for the year 2025 in relation to the security situation at Mapfre:



The cybersecurity rating (BitSight) maintains a sustained upward trajectory and consistently ranks above the average for the insurance sector, consolidating Mapfre's position at the **ADVANCED level.** This progress reflects the effectiveness of the implemented management and control model and the ongoing commitment to continuous improvement.

Dow Jones Sustainability Indexes	**100 points** (out of 100) in the section **Privacy Protection** (2025)
CNPIC incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD	**4.7 points** (out of 5). IMC Cyber Resilience Improvement Indicators (2024) ➢ +0.4 points above the average for the financial sector. ➢ +1.7 points above the average of participants
DSN isms forum	**Cyber crisis management 2025** ➢ Mapfre obtained **1st Position** ➢ Nearly 30 participating companies.
cyberex_ incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD	**Cyber exercises 2025,** organized by INCIBE and aimed at digital service providers and entities of strategic interest. ➢ Mapfre is comfortably **above the average of the participating entities,** also exceeding the average recorded in the financial sector.

- **CNPIC:** National Center for the Protection of Critical Infrastructures (CNPIC) of Spain
- **DSN:** Spanish National Security Department. Advisory body to the President of the Government of Spain on matters of national security.
- **INCIBE:** National Cybersecurity Institute, officially SME National Cybersecurity Institute of Spain MP, SA
- **ISMS FORUM:** Spanish Association for the Promotion of Information Security.

Annexes

A.1

DCS Team Certifications

	DS: Director of Security for the Spanish Ministry of the Interior.
	CISA: Certified Information Systems Auditor is a certification for auditors.
	CISM: Certified Information Security Manager is a certification for information security governance that defines the competencies necessary for a security director to lead, design, review, and advise on an information security program.
	CISSP: Certified Information Systems Security Professional is a high-level professional certification with the aim of helping companies recognize professionals trained in the area of information security.
	CRISC: Certified in Risk and Information Systems Control, certification risk management managers in information systems.
	DPO: Data Protection Officer (According to GDPR)
	COBIT: Control Objectives for Information and Related Technology defines a set of generic processes for IT management. The framework defines each process along with the process inputs and outputs, key process activities, process objectives, performance measures, and an elementary maturity model.
	CSX: Fundamentals: Key concepts and functions of cybersecurity.

CSSLP	**CSSLP:** Certified Secure Software Lifecycle Professional recognizes leading skills in application security. It demonstrates the advanced technical skills and knowledge necessary for authentication, authorization, and auditing using best practices, policies, and procedures.
SSCP	**SSCP:** Systems Security Certified Practitioner demonstrates advanced technical skills and knowledge to implement, monitor, and manage IT infrastructure using best security practices, policies, and procedures.
PMI Project Management Institute	**PMP:** Project Management Professional certifies that knowledge and experience related to project management have been achieved.
CHFI Computer Hacking Forensic INVESTIGATOR	**CHFI:** Computer Hacking Forensic Investigator validates the knowledge and skills to detect hacking attacks, to properly obtain the evidence needed to report the crime and prosecute the cybercriminal, and to conduct an analysis that allows you to prevent future attacks.
CISCO	**CISCO Certifications:** CCNP, CCDP, CCNA, CCSA, CCENT, CCDA.
Microsoft	**Microsoft Certifications:** MCP, MCSE, MCSA, MCSI.
CEH Certified Ethical Hacker	**CEH:** Certified Ethical Hacker is a qualification obtained by demonstrating knowledge of evaluating the security of computer systems by searching for weaknesses and vulnerabilities in target systems, using the same knowledge and tools as a malicious hacker, but in a legal and legitimate way to assess the security posture of a target system.
ITIL	**ITIL Certifications:** ITIL Foundation v2; ITIL Foundation v3; ITIL Intermediate v3; ITIL Bridge v3; ITIL Operational, Support and Analysis; ITIL Release, Control and Validation; ITIL Service, Offers and Agreements; ITIL Planning, Protection and Optimization; ITIL Managing Across the Life Cycle; ITIL Expert.
CDPP Certified Data Privacy Professional	**CDPP:** Certified Data Privacy Professional is the first Spanish certification aimed at privacy professionals. Obtaining this certification demonstrates a high level of specialization in Spanish regulations regarding the protection of personal data, both in a local, European, and international context, as well as a mastery of the fundamentals of information security.
OSA	**OSA:** Operational Support and Analysis is one of the certifications in the ITIL® Service Capability workflow. The module focuses on practical application to enable the management of events, incidents, requests, problems, access, technical operations, IT, and applications.
CND Certified Network Defender	**CND:** Certified Network Defender Certification, is a certification program that focuses on creating network administrators trained to protect, detect and respond to threats on the network.

	CNDA: Certified Network Defense Architect is specially designed for Government Agencies or Military Agencies around the world.
	CSA: Certified Security Analyst: is a fully practical program with labs and exercises that cover real-world scenarios.
	CSP: Certified Secure A programmer, a secure programmer, is a professional with essential and fundamental skills to develop secure and robust applications.
	ISO 27001 Foundations, **ISO** 27001 Lead Implementer, **ISO** 27001 Lead Auditor
	SCADA: Security Architect teaches how to defend Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) that manage critical infrastructure.
	CWAPT: Certified Web App Penetration Tester is designed to certify that candidates have knowledge and working skills related to the field of web application penetration testing.
	GIAC Certifications: GCIH, GSEC, GCFE, GCED
	PCI-DSS ISA: Payment Card Industry Data Security Standard Internal Security Assessor teaches you how to conduct internal assessments for your company and recommends solutions to remedy issues related to PCI DSS compliance.
	PCIP: Provides an individual qualification for industry professionals who wish to demonstrate their professional experience and understanding of the PCI Data Security Standard (PCI DSS).
	OSCP: Offensive Security Certified Professional is an ethical hacking certification that teaches penetration testing methodologies and the use of tools included in the Kali Linux distribution.
	CCSE: Checkpoint Certified Security Expert, competencies include configuring and managing VPN-1/FireWall-1 as an Internet security and virtual private network (VPN) solution, using encryption technologies to implement remote access and site-to-site VPNs , and configuring content security by enabling Java blocking and antivirus checking.

	ISO 22301 Foundations, **ISO** 22301 Lead Implementer, **ISO** 22301 Lead Auditor
	BS 25999 Lead Auditor.
	TSI PROFESSIONAL: Evaluation and certification of high availability data center infrastructures according to the EN50600 standard and the Trusted Site Infrastructure (TSI) method.
	CRCM: Corporate Risk and Crisis Management has been designed for experienced security, risk and crisis managers who have been tasked with planning and managing increasingly complex scenarios.
	CompTIA Linux+; **CompTIA** A+; **CompTIA** Systems Support Specialist; **CompTIA** Network+; **CompTIA** IT Operations Specialist; **CompTIA** Linux Network Professional; **CompTIA** Security+
	Splunk CU Splunk Certified User; **Splunk** CPU Splunk Certified Power User
	TSPRL: Senior Technician in Occupational Risk Prevention; TIPRL: Intermediate Technician in Occupational Risk Prevention (expert).
	PRINCE2: Practitioner: Projects IN Controlled Environments is a structured project management method and a professional certification program.
	CICA: Certified Internal Controls Auditor, review or evaluation of controls and internal control systems.
	ICS- 100 Incident Command System 100; **ICS-** 200 Incident Command System 200; **ICS-** 700 Incident Command System 700
	LPIC-1 will validate the ability to perform maintenance tasks on the command line, install and configure a computer with Linux, and configure a basic network.

	CFE Certified Fraud Examiner: its activities include the production of information, tools and training on fraud.
	CHS-II Certified in Homeland Security Level II: Level II provides an overview of weapons of mass destruction, terrorism itself, and the possible weapons that may be used in the event of an attack.
	OSHA: Occupational Safety and Health Administration
	FES: Fire Extinguisher Safety
	Bloodborne Pathogens: Certification that teaches professionals what to do in case of exposure to bloodborne pathogens.
	CFPS: Certified Fire Protection Specialist aims to document competence and provide professional recognition to individuals involved in reducing fire loss, both physical and financial.
	PSM: Professional Scrum Master I; PSPO Professional Scrum Product Owner I
	EXIN Agile: Scrum Foundation offers professionals a unique certification that combines agile principles and scrum practices.
	ISO 14001 Lead Auditor: enables you to develop the necessary experience to carry out an Environmental Management System (EMS) audit by applying widely recognized auditing principles, procedures and techniques.
	ISO 50001 Lead Auditor: enables you to develop the necessary experience to carry out an audit of an Energy Management System (EMS) applying widely recognized auditing principles, procedures and techniques.
	ATHE Level5: Award in Corporate Risk and Crisis Management.

	CDPSE: Certified Data Privacy Solutions Engineer enables privacy technologists to demonstrate that they understand the technical aspects of creating and managing privacy programs to ensure compliance and mitigate risk.
	CPCC: Certified Professional Cyber Compliance, from the ISMS Forum, which certifies a high level of specialization in Spanish regulations on cybersecurity compliance.
	CIPP/E: Certified Information Privacy Professional, a globally recognized certification developed by the International Association of Privacy Professionals (IAPP), which accredits global knowledge of data protection laws and regulations
	CAIP: Certified Artificial Intelligence and Information Security Professional, which certifies solid knowledge and experience in AI related to cybersecurity and privacy.

mapfre