

v 1.9 February 2024



Security

Keeping your trust

TABLE OF CONTENTS

1	VISION AND MODEL OF SECURITY	4
1.1.	Vision of the MAPFRE Security Function	6
1.2.	Security Integrated Model	8
1.3.	Guidelines framework for Security	10
1.4.	Process of Continuous Improvement of Security	12
2	ORGANIZATION OF SECURITY	14
2.1.	Global approach	16
2.2.	Corporate Security, Cisis and Resilience Committee	17
2.3.	Highly qualified Security	18
2.4.	Global Security Operations Center (Global SOC)	24
3	SECURITY AND PRIVACY COMPLIANCE	30
4	SECURITY FOR PEOPLE AND FACILITIES	34
5	CYBERSECURITY	38
5.1.	Identity management	41
5.2.	Network security	42
5.3.	Device security (computing, server, and cellphone stations)	43
5.4.	Cloud Security	44
5.5.	Technical Security reviews	45
5.6.	Vulnerability and patch management	47
5.7.	Monitoring and response to incidents	48
5.8.	Cyber Insurance	49
6	CORPORATE DATA CENTERS	50
7	CRISIS MANAGEMENT AND BUSINESS CONTINUITY	54
8	PRIVACY AND PERSONAL DATA PROTECTION	58
8.1.	Data Protection Officer	60
8.2.	Privacy Reference Framework	61
9	ARTIFICIAL INTELLIGENCE AND DATA ETHICS	64
10	Security Culture: Sensitization, Awareness and Training	68
11	AUDITS AND REVIEWS	72
12	ACKNOWLEDGMENTS	76

**Guillermo Llorente,
Group Head 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 Corporate Security Function is established, in order to protect the tangible and intangible assets of MAPFRE. This mission is included in the Security Master Plan which, with an approach based on risk management, operates as a Strategic Framework and constitutes a starting point for the development of Security and Privacy Policies; and Business Continuity, as well as for the development of the Internal Regulations associated with them. All of this within the strictest respect for current legislation and the MAPFRE Code of Ethics and Conduct.

Security is an integral part throughout the entire organization, and MAPFRE’s vision guarantees that all initiatives are developed with embedded security. Therefore, to maintain the continuity of the service we provide and the privacy of the information entrusted to us, security is integrated from the very beginning at the design stage of any application, device or new facility; in short, in every new project that we start.

To monitor 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), where the security of the companies is monitored and analyzed. MAPFRE Networks and Information Systems around the world, and from where the response to security incidents that the company may suffer is coordinated and carried out.

For when all this is not enough, and attacks materialize, serious crisis or natural disasters appear, MAPFRE has developed and implemented Crisis Management and Business Continuity Plans in its companies, which are tested annually, and which aim to provide continuity of service to our clients even in the worst circumstances.

In conclusion, the security and privacy of our clients constitutes a fundamental axis of MAPFRE’s Policy and vocation for service. It is a personal and collective Commitment.”

A stylized, handwritten signature in black ink, appearing to read 'Guillermo Llorente'.

Guillermo Llorente
Group Head of Security at MAPFRE





Vision and Model of Security

The aspiration of **leadership** at MAPFRE and its **global nature** inspire, as at the rest of the Group's activities, the actions related to Security, an area in which it also seeks to be a benchmark





01





1.1

Vision of the Function of Security at MAPFRE

The Security and the Environment function at MAPFRE is responsible for protecting, while strictly complying with the legality and ethical principles of MAPFRE, the tangible and intangible assets of the Group, especially ensuring regulatory compliance and protecting the company's good reputation.

This includes 5 fundamental principles:



It is defined as Global and Integral,

protecting any type of Group assets in any country in the world against all security threats that may jeopardize them.



It has a permanent and sustainable character, forming part of corporate culture and processes and with the firm commitment of being environmentally responsible.



It is Service-oriented, considering it an inescapable duty, which maintains the trust of our internal and external clients.



It is independent of any other area of MAPFRE with which there may be a conflict of interest, in order to maintain the principle of segregation of duties.



It must add Value, evolving based on the strategies and needs of the Group and its clients.

1.2

Integrated Model of Security

MAPFRE applies a **holistic approach to Security**, integrating all aspects related to the Security of people and their assets, into a single Corporate Division with a global presence and scope of action.

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

- » **Personal Security.**
- » **Security of Facilities.**
- » **Security of Information Systems.**
- » **Personal Data Protection and Privacy.**
- » **Crisis and Business Continuity Committee.**
- » **Anti-fraud measures.**
- » **Regulatory compliance in the area of Security and Privacy.**

The model for the development of function of **Security** was built on this approach.

This model is governed by MAPFRE's Code of Ethics and based on industry standards and best practices, such as:

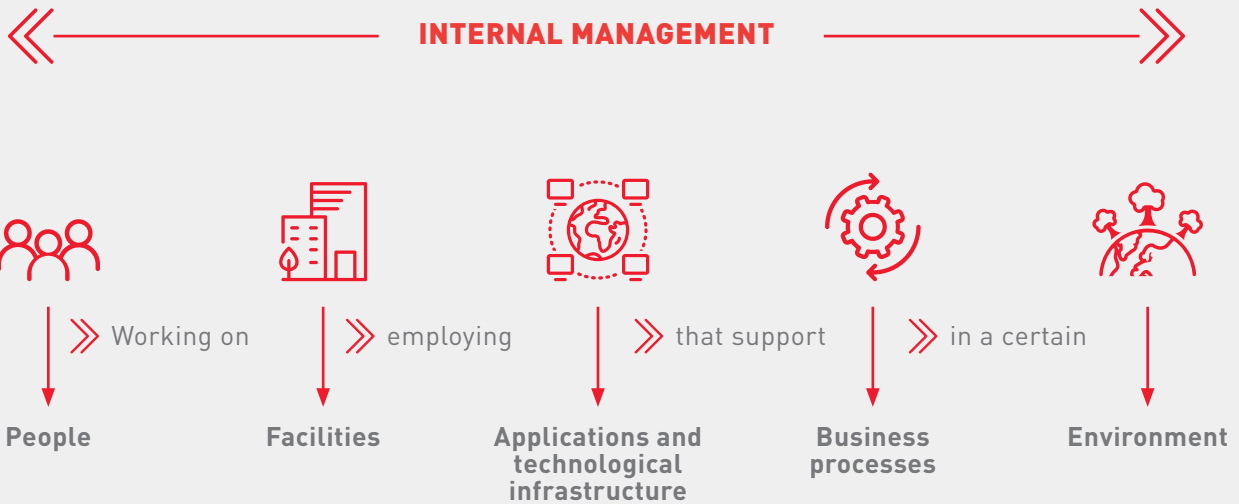
ISO 27001 and 27002 in Information Systems Security

ISO 22301 Business Continuity

ISO 14001, 14064 and ISO 50001 relating to the protection of the Environment

ISO 9001 for quality management

ISO 29100 regarding privacy protection



1.3

Guidelines Framework for Security

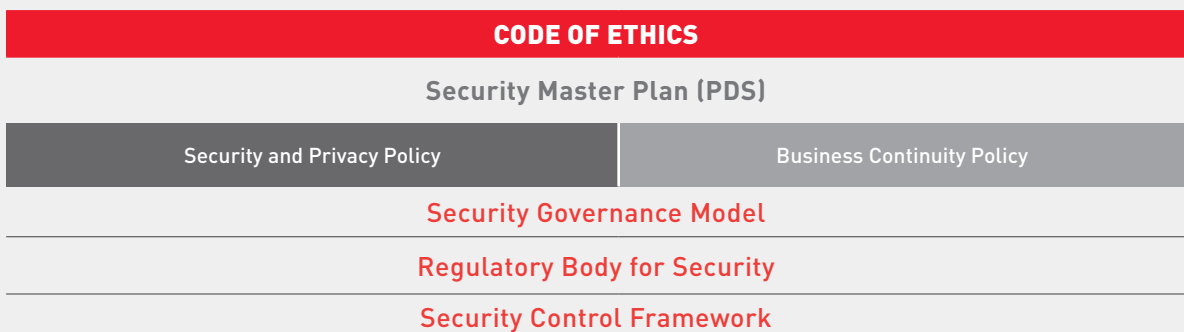
Reflecting the above principles, MAPFRE has a **Security Master Plan** which operates as a Strategic Framework, establishes the mission of **the Function of Security** and, with a holistic vision and an approach based on risk management and MAPFRE's code of ethics, it constitutes the starting point from which policies and internal regulations emanate:

Corporate Policy on Security and Privacy and Business Continuity, approved by the MAPFRE Board of Directors and applicable throughout the MAPFRE Group.

Government Model for Security, which allows MAPFRE to have an effective and efficient Security function.

The regulatory body for Security, developed in different internal policies, standards, regulations and procedures.

Security Control Framework, which translates, at the level of controls, the different requirements established in the Management Framework, which MAPFRE's companies and Business Units must comply with.



In the following links you can consult the Code of Ethics for corporate policies on Security and the Environment:

» **Code of Ethics**

<https://www.mapfre.com/media/shareholders/2019/internal-code-of-conduct-relating-to-listed-securities.pdf>

» **Security and Privacy Policy**

<https://www.mapfre.com/media/shareholders/2015/mapfre-group-corporate-security-and-privacy-policy.pdf>

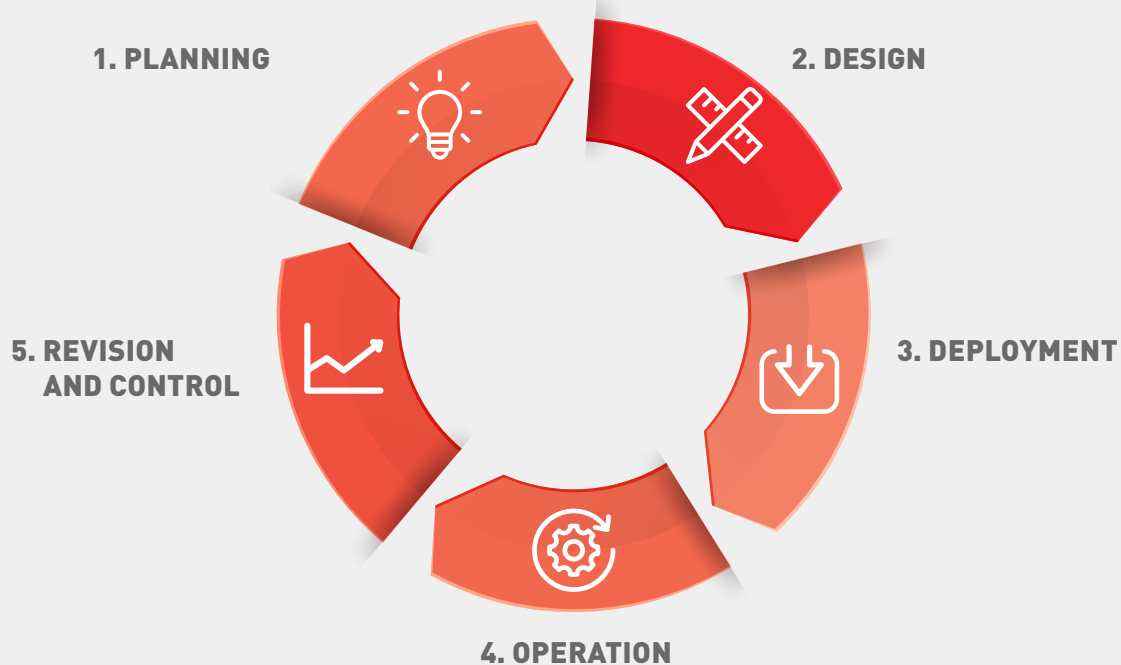
» **Business Continuity Policy**

<https://www.mapfre.com/media/shareholders/2020/politica-de-continuidad-de-negocio-2019-12-13-en.pdf>

1.4

Process of Continuous Improvement of Security

To carry out its mission, Security at MAPFRE follow a process of continuous improvement that also allows the alignment of plans and projects in this area with the needs of the Business and the Group Strategy.





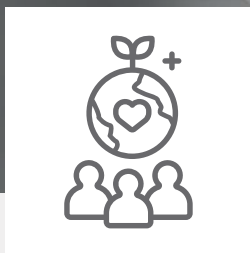
Organization of Security

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





02



2.1

Global Approach

This concept of Security as **UNIQUE** for all of MAPFRE and of a **COMPREHENSIVE** nature against all types of threats in a global entity like our Group, implies having a **two-dimensional structure**, which allows for a homogeneous and coherent response to risks, both global and local.



Global Dimension

- » Protection against global threats.
- » Global Regulatory Compliance.
- » Search for maximization of synergies.
- » Aligned with the MAPFRE Global Strategy.



Specific Dimension

- » Protection against local threats.
- » Local regulatory compliance.
- » Communication with Local Security Forces and Bodies.
- » Taking into account the needs and habits/customs in each country and market.

2.2

Corporate Security, Crisis and Resilience Committee

At the top of the MAPFRE Security Organization is the **Corporate Security, Crisis and Resilience**. It is made up of executive directors and senior managers of the company and constitutes the highest executive body of the Security Function.

This Committee ensures that the activity of the Security Function is fully aligned and integrated into the corporate strategy and contributes to the achievement of business objectives. At the same time, it guarantees that security is considered as a constituent element of corporate business and support processes.

Likewise, in a Crisis situation, it is in charge of managing an appropriate response that allows maintaining the service to customers, reducing possible consequences and ensuring that data and essential functions are preserved in a process of continuous improvement of the services. operational resilience capabilities of the company.

2.3

highly qualified **Human** **Team**

MAPFRE, via the team of highly qualified experts in the **Corporate Security Division (DCS)**, has managed to equip itself with the best capabilities to fulfill its mission and meet the needs of an increasingly globalized, complex and demanding climate.

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

This high level of specialization is accredited by more than **300** individual certifications in all disciplines of Security, Privacy and Business Continuity, which DCS personnel, among them, has, which are as follows:



DS: Director of Security for the Spanish Ministry of Interior.



CISA: The Certified Information Systems Auditor is a certification for auditors.



CISM: The Certified Information Security Manager is a data security government certification that defines the competences required for a security manager to conduct, design, review and provide advice on a data security program.



CISSP: Certified Information Systems Security Professional is a high-level professional certification to help companies recognize trained professionals in the area of data security.



CRISC: Certified in Risk and Information Systems Control, certification of risk control 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 together with the inputs and outputs of the process, the key activities of the process, the objectives of the process, the performance measures and a model of elementary maturity.



CSX: Fundamentals: Key concepts and functions of cybersecurity.



CSSLP: Certified Secure Software Lifecycle Professional recognizes the leading application security skills. Displays advanced technical skills and knowledge required for authentication, authorization, and auditing using best practices, policies, and procedures.



SSCP: Systems Security Certified Practitioner demonstrates the advanced skills and expertise to implement, monitor, and manage IT infrastructure using best practices, policies, and security procedures.



PMP: Project Management Professional certifies that knowledge and experience regarding project management are held.



CHFI: Computer Hacking Forensic Investigator validates the knowledge and skills to detect hacking attacks, to properly obtain the necessary evidence to report the crime and prosecute the cybercriminal, and to conduct an analysis that allows it to prevent future attacks.



Certifications of CISCO: CCNP ,CCDP, CCNA, CCSA, CCENT, CCDA.



Certifications of MICROSOFT: MCP, MCSE, MCSA, MCSI.



CEH: Certified Ethical Hacker is a qualification obtained by demonstrating knowledge of evaluation of the security of computer systems by searching of weaknesses and vulnerabilities in the 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 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, Offerins and Agreements; ITIL Planning, Protection and Optimization; ITIL Managing Across the Life Cycle; ITIL Expert.



CDPP: Certified Data Privacy Professional is the first Spanish certification for Privacy professionals. Obtaining this certification accredits a high level of specialization in Spanish regulations on the Protection of Personal Data, both in a local context, and in a European and international context, as well as a mastery of the fundamental principles that govern Data Security.



OSA: Operational Support and Analysis is one of the certifications in the ITIL® Service Capability workflow. The module focuses on practical application enabling the management of events, incidents, requests, issues, access, technical operations, IT and applications.



CND: Certified Network Defender Certification, is a certification program that focuses on the creation of 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: this is a purely practical program with laboratories and exercises that cover real-life scenarios.



CSP: Certified Secure 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 the Supervision and Data Acquisition Control (SCADA) and Industrial Control Systems (ICS) that manage critical infrastructure.



CWAPT: Certified Web App Penetration Tester is designed to certify that candidates have working knowledge and skills in relation to the field of web application penetration testing.



Certifications of GIAC: GCIH, GSEC, GCFE, GCED



PCI-DSS ISA: Payment Card Industry Data Security Standard Internal Security Assessor teaches how to conduct internal assessments for your company and recommends solutions to remedy problems related to PCI DSS compliance.



PCIP: Provides an individual qualification for professionals in the sector who wish to demonstrate their professional experience and their 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 the tools included in the Kali Linux distribution.



CCSE: Checkpoint Certified Security Expert, the competences include the configuration and management of VPN-1/FireWall-1 as an Internet and virtual private network (VPN) security solution, the use of encryption technologies to implement remote access and site-to-site VPNs, and the configuration of content security to allow Java blocking and antivirus checking.



ISO 22301 Foundations, ISO 22301 Lead Implementer, ISO 22301 Lead Auditor



BS 25999 Lead Auditor

- • •
- • •
- • •
- • •
- • •
- • •
- • •
- • •
- • •
- • •



CRCM: Corporate Risk and Crisis Management has been designed for experienced security, risk and crisis managers who are 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: Superior technician in prevention of labor risks; TIPRL intermediate technician in prevention of labor risks (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 This will validate the ability to perform maintenance tasks on the command line, install and configure a Linux computer and configure a basic network.



CFE Certified Fraud Examiner: their activities include the production of information, tools and training on fraud.



CHS-II Certified in Homeland Security Level II: a general overview of weapons of mass destruction, terrorism itself and possible weapons that can be used in the event of an attack are offered at level II.



OSHA: Occupational Security and Health Administration



FES: Fire Extinguisher Security



Bloodborne Pathogens: Certification where professionals are taught what to do in case of exposure to bloodborne pathogens.



CFPS: Certified Fire Protection Specialist has the purpose of documenting the competence and offering professional recognition to the people 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: Allows development of the necessary experience to carry out an audit of Environmental Management Systems through the application of widely recognized audit principles, procedures and techniques.



ISO 5001 Lead Auditor: Allows development of the experience required carry out an audit of an Energy Management System applying widely recognized audit principles, procedures and techniques.



ATHE Level5: Award in Corporate Risk and Crisis Management



CDPSE: CCertified 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.



2.4

Global Security Operations Center (Global SOC)

The **Global Security Operations Center (Global SOC)** of MAPFRE is the body certified as “**Computer Emergency Response Team**” (**CERT**), which provides the Group with monitoring, identity management and access control and incident response capabilities globally.

This body uses MAPFRE’s internal security model, controlling access to Information Systems and MAPFRE facilities, monitoring different physical and logical events and responding to security incidents of any nature.

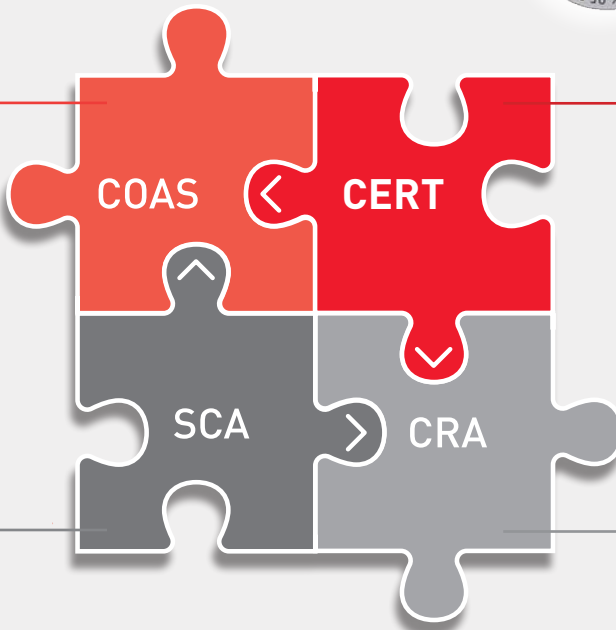
The SOC is integrated into the “Forum of Incident Response and Security Teams” (FIRST) network and is in permanent contact with the main private and government CERTs in the world, as well as in the National Network of SOC’s of the Spanish CNN-CERT, and forms part of the CSIRT.es network, which facilitates collaboration and exchange of information between public cybersecurity operations centers for the identification of threats and early response to possible incidents.



LOGICAL SCOPE

CENTER OF OPERATIONS ACCESS AND IDENTITIES
(SYSTEMS AND NETWORKS)

PERMITTING ACCESS



COMPUTER EMERGENCY RESPONSE TEAM
(SYSTEMS AND NETWORKS)

MONITORING

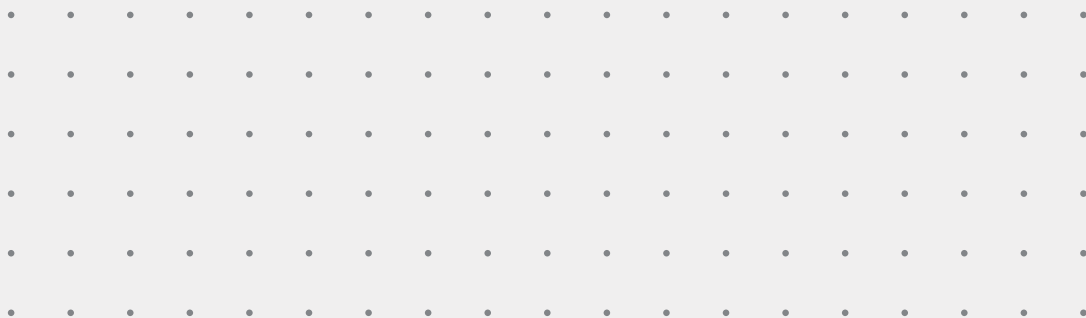
SYSTEM CONTROL ACCESS
(BUILDINGS AND OFFICES)

CENTRAL RECEIVER OF ALARMS
(BUILDINGS AND OFFICES)

PHYSICAL SCOPE

CENTER OF OPERATIONS FOR SECURITY

(Operation of Systems and Security Tools)



The **SOC** is **ISO 27001**-certified; it was the **first Spanish CERT** to obtain **ISO 9001 certification**, and has been recognized by the Gartner Group as a success story in the design, implementation and operation of a comprehensive security model.



ISO 9001 certification:

- » Certifies an effective management of the CCG-CERT processes.
- » Helps to identify inefficiencies and improvement activities in a process of continuous improvement.
- » Allows the satisfaction of the client areas to be assessed.

ISO 27001 certification leads to:

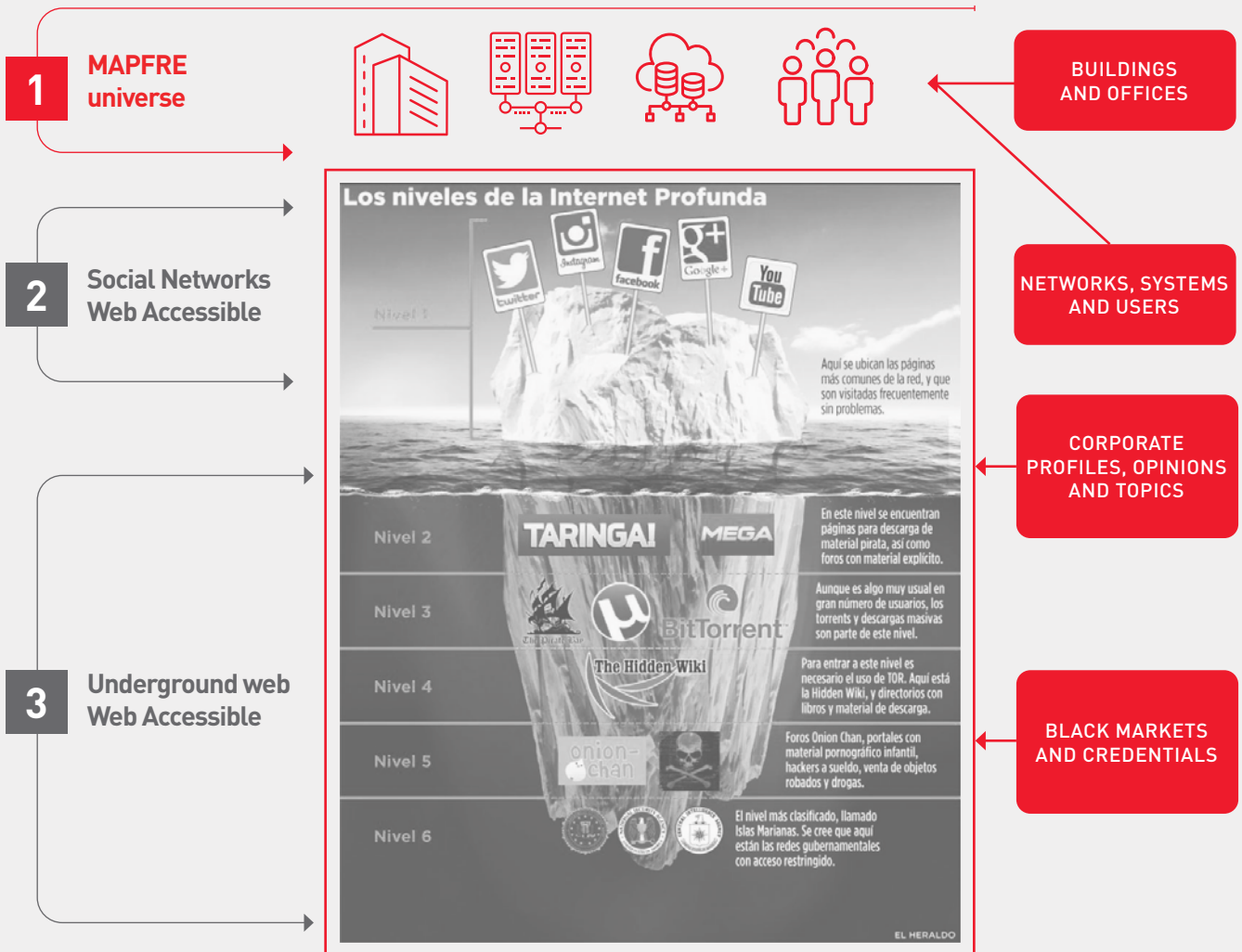
- » The availability of a risk management model.
- » The availability of controls according to risk levels.
- » The periodic evaluation of:
 - The risk position of the organization.
 - The suitability and effectiveness of the installed controls.

The ISO 22301 certification in Business Continuity shows the ability to:

- » Identify possible present and future risk scenarios.
- » Determine critical functions and reinforce their protection in the event of possible emergency situations.
- » React so that the materialization of any of the risk scenarios affects the development of these critical functions as little as possible.
- » Enable service continuity in the face of unforeseen situations, improving the cyber resilience of the organization and the services it provides to its clients.

The **Global SOC** is the body where security incident management is centralized, through identification, analysis, evaluation, containment, resolution, communication to recipients and registration.

The following are monitored by the Global SOC:



National Net of SOC

- » In Q1 2023 MAPFRE was the first private entity (not a provider of ICT services to the Administration) to join the RNSOC of the CCN-CERT.
- » In Q1 2023 MAPFRE was the first private entity (not a provider of ICT services to the Administration) to join the RNSOC of the CCN-CERT.
- » The access level determines the delay with which participants access the information that the rest of the RNSOC participants put on the network.

MAPFRE has been included as GOLD, once again being the first non-technological private company to achieve this.



- • • •
- • • •
- • • •
- • • •
- • • •
- • • •
- • • •
- • • •
- • • •
- • • •
- • • •
- • • •



Security and Privacy Compliance



MAPFRE's governing bodies have always felt a special concern for good corporate governance, which is why they have been adopting a set of principles and rules that govern their actions, among which is strict compliance with the laws and their regulations. obligations, as well as the good uses and practices of the sectors and territories in which our activities are carried out.



03





MAPFRE has provided itself with a Security Regulatory Body, based on the ISO 27002, ISO 22301 and ISO 29100 standards and which is also enriched by other standards widely recognized in the industry, such as the NIST CSF Cybersecurity Framework or the PCI-DSS regulations. . This Regulatory Body is mandatory for all processes and activities in which the Group entities participate. This Regulatory Body, made up of more than 100 documents, is constantly adapting, like MAPFRE, to the different legislations that appear in the countries where it operates.



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 different legislation on the matter, as well as the most adequate compliance.



Special mention deserves the **General Data Protection Regulation of the European Union**, a reference standard for MAPFRE in terms of privacy, whose strict compliance constitutes the guarantee offered to our clients that we will make appropriate use of the personal data they entrust to us, guaranteeing your privacy and confidentiality.

MAPFRE is working proactively to adopt the requirements of the **European Union's Digital Operational Resilience Regulation (DORA)**, to ensure that it can resist and respond to any type of ICT-related disruption and threat and recover. of them.

Another fundamental reference is the **Guides published by the European Insurance and Occupational Pensions Authority (EIOPA)**, which include guidelines on ICT Security and Governance and on the Management of the Outsourcing of Cloud Services.



MAPFRE **incorporates security and data protection clauses** into all its contracts with third parties, requiring compliance from all its collaborators, in order to ensure prudent and diligent behavior in the management of their security and personal data.

MAPFRE has a regulatory observatory and analysis of the multiple pronouncements by regulators, in the countries in which it is present, with the aim of guaranteeing that, from the design, all processes comply at all times with privacy regulations. and data protection that are applicable.



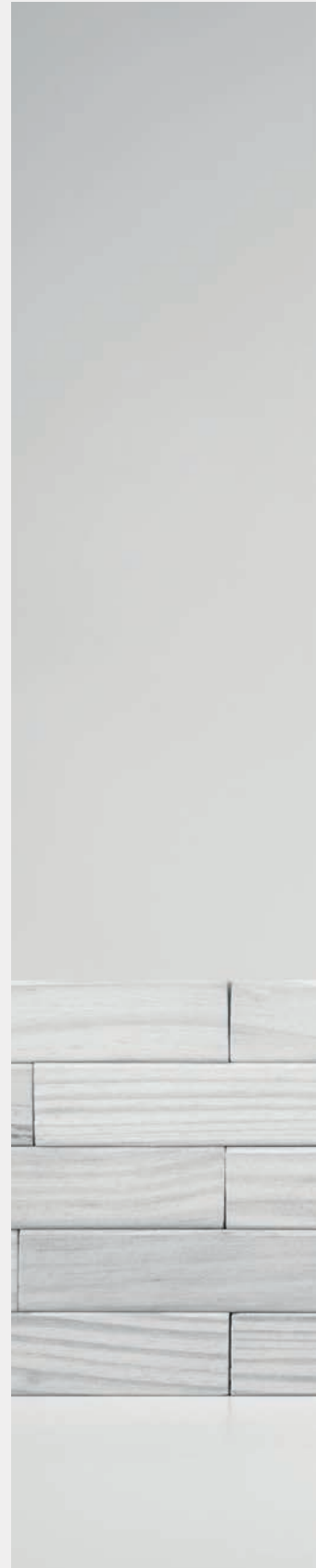
For all this, we can guarantee that MAPFRE has the regulations, internal procedures and control measures necessary to satisfy the regulatory requirements and those of our clients, which apply to it in terms of security and privacy, monitoring and monitoring compliance in all areas. levels of the company through the implementation of the mechanisms required by its own regulatory body.

All of the above considerations allow us to firmly transmit MAPFRE's will and capacity to **comply with the security and privacy requirements** demanded by the legislation of all the countries where it operates.



Security of people and facilities

MAPFRE considers **the security of everyone in its facilities, whether employees, customers, suppliers or visitors**, as a priority and an indispensable objective. As a consequence, guidelines have been defined and procedures have been installed to protect them.





04



Self-protection and Emergency Plans,

implemented and updated in all facilities where MAPFRE carries out its activity; adapted to the regulatory requirements established in each area, which includes conducting drills with the frequency established by regulations.

Fire Protection:

The MAPFRE guidelines establish requirements regarding the fire protection of the facilities it occupies, whether or not they are its own, which entails, at a minimum, compliance with sufficient applicable regulations, with special attention to those critical areas of the Security of people and business development. Highlights that MAPFRE, in its commitment to sustainability, uses inert extinguishing systems that respect the environment.

Travel and Event Security:

MAPFRE's commitment to the Security of its employees and collaborators also covers travel. Employees have a Self-Protection Guide, with travel security tips, as well as specific Security Guides for trips to those countries considered medium or high risk, where their trip is monitored from the General Control Center. These guides contain information on the different areas of the country, useful contacts in MAPFRE and diplomatic centers, as well as Security advice focused on the main risks of the country.

Risk analysis:

MAPFRE's main establishments rely on analyses that contemplate all the risks that may materialize in the following areas: nature, environment, fire, those caused by uncontrolled access, subtraction or degradation of data stored on different media, risks, etc. Based on these, protection measures are established and considered.





Security and Access Control Systems:

In response to these risks, both in buildings and in offices, MAPFRE has physical access control systems, CCTV surveillance, alarm systems and, where appropriate, surveillance services. Spaces whose integrity has the greatest impact on the development of MAPFRE’s activities and business have reinforced security measures.

MAPFRE’s General Control Center (CCG) monitors and supervises these systems, providing rapid and effective response in incident management. Most of the installed security systems are based on IP technology, on proprietary communication networks used exclusively by MAPFRE.

These measures are also reinforced by drills and training and awareness-raising activities, which are carried out on a regular and systematic basis.



CyberSecurity

MAPFRE has established a **Cybersecurity** prevention model based on the following pillars:



On the one hand, **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.



On the other hand, a fundamental element for the Cybersecurity strategy is **the integration of security from the very beginning** in all new initiatives: the construction of new solutions, the hiring of new services, etc. In other words, integrating cybersecurity into the business 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 controlled.



Finally, **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).





05



TECHNOLOGY



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

CYBERSECURITY AND PRIVACY “from the cradle to the grave”



- » 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

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.

CULTURE



- » Educating employees, customers and stakeholders.
- » Specific training for critical personnel.
- » Training for Security personnel and Crisis management exercises.

5.1

Identity Management

MAPFRE considers the secure management of access to the different assets of the organization critical, establishing Identity and Access Management processes for each group of users (employees, collaborators, intermediaries, etc.) to identify who has accessed what and with what permissions.

The principles that govern these Identity Management processes are the following:

- » **Creation of a unique and immutable** identifier for each user that requires access to the company's information systems.
- » **Definition of a specific user identifier for accounts that require the** lifting of permissions (administrators, automatisms, etc.).
- » **Access control managed and controlled by security**, based on authorization matrices and adequate segregation of functions.
- » **Use of Multiple Factor Authentication (MFA)** for especially sensitive access and, especially, for any type of remote access.
- » **Definition of a robust password policy.**
- » **Incorporation of Identity and Access** Management in the application development life cycle.
- » **Restriction between productive and non-productive environments** regarding the use of identities and access.
- » **Periodic reviews** of account security and permissions assigned to users.
- » **Comprehensive control and continuous review of the activities** of especially privileged users in critical environments.

The Identity Management processes governed by DCS are linked to the rest of the security controls, being operated both automatically through the Corporate Identity Management Systems, as well as from the Manual Operation Centers, integrated in the Global SOC.

5.2

Network security

MAPFRE bases the **network protection** on a model of segregation and location of resources in different layers. At the same time, different network security solutions are applied, for example:

- » **Double Firewall level.**
- » **IDS/IPS for the detection and blocking of attack patterns.**
- » **Segregation of VLANs.**
- » **Physical and/or logical isolation between companies.**
- » **Use of Multiple 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 Internet connection Secure Web Gateway and DLP in email, etc.**
- » **Security at the DNS level**

5.3

Security on devices (computer, server and cellphone stations)

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

- » **Anti-malware protection.**
- » **Vulnerability management and associated patches.**
- » **Data encryption.**
- » **Device fortification.**
- » **Device security inventory, management and monitoring.**
- » **Mobile Device Management for mobile devices and tablets, etc.**
- » **Restricting access to USB ports on user computers.**

5.4

Cloud Security

MAPFRE is no stranger to digital transformation and, analogous to what other companies are doing, it is including cloud technologies in its technological projects. MAPFRE only uses cloud providers that comply with the highest standards, regulations and security certifications (among others: ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, PCI-DSS or GDPR).

Consequently, MAPFRE has established, together with the main Cloud Computing Service Providers, the Cybersecurity foundation that encompasses the architecture and basic security controls on which all technological projects are built.

Sample of the security controls used to achieve the objectives described above are:

- » **Security Architectures for 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.**

5.5

Technical security reviews

With the objective that all the companies that make up the MAPFRE Group can benefit from the knowledge, experience, resources, infrastructure and tools existing at the corporate level in terms of ethical hacking and security analysis, **Security Technical Review Reference Center has been created.**

SECURITY TECHNICAL REVIEW REFERENCE CENTER

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

Through the services provided by this Center, the different companies of the MAPFRE Group get regular information on their level of security and vulnerability both from the point of view of an internal and external attacker. Similarly, this center carries out security reviews of the company's new initiatives, before they are put into production.

Likewise, this center carries out security reviews of the technological layer of the company's new initiatives, prior to their launch into production.

In this way, MAPFRE is able to apply a wide catalog of technical security reviews, which ensure corporate information and our customers are protected. Such as, for example:

TYPES OF REVIEWS	
New Initiatives	Source Code Revisions
	Security Tests
	Evidence of Compliance
External	External Intrusion Tests
	External vulnerability scanning/ASV
Internal	Internal Intrusion Tests (Including segmentation tests and scope reduction controls)
	Internal Vulnerability Scanning
	Review of critical Applications
	Corporate Infrastructure Reviews

This catalog of reviews includes the process of **the continuous and automated review** of the systems exposed to the Internet across all the companies of the company, and allows any new vulnerability in said systems to be detected.

Also indicate that through this Reference Center the **Red Team** type reviews carried out against the Information Systems located in our Data Centers are articulated, as well as the rest of the **Cyber Exercises** intended to evaluate both our protection, detection and response capabilities. , such as security awareness among our employees.

As a result of this set of reviews, "remediation" plans are established subject to specific deadlines and, in turn, continuous monitoring of the correction of previously detected vulnerabilities is carried out.

5.6

Vulnerability and patch management

One of the key security processes to guarantee an adequate level of protection for any information system has to do with patching systems and resolving vulnerabilities effectively and within appropriate deadlines.

MAPFRE has a formalized, implemented and mature vulnerability and patch management process, which ranges from their early identification to the certification of their resolution by specialized teams. This process ensures that information systems are periodically and systematically updated with the latest patches released by software manufacturers.

MAPFRE has support agreements with the main technology manufacturers for early notification of vulnerabilities and continuously monitors any vulnerability that may affect the technology used in our information systems. MAPFRE also participates in the main CERT/SOC associations, where information on vulnerabilities is exchanged, particularly Zero Day.

Every time a new vulnerability is published, the cybersecurity team carries out an evaluation based on its criticality and impact on MAPFRE's systems, resulting in a classification. For vulnerabilities of the highest criticality, an urgent procedure is activated in order to resolve them, at a global level, in less than 24 hours in all information systems that may be affected.

5.7

Monitoring and response to incidents

As previously indicated in this document, MAPFRE brings together the monitoring and response capabilities for Cybersecurity incidents in the GLocal SOC, operating as:

- » SOC with dedicated personnel at MAPFRE facilities, with permanent availability (24x7x365 format).
- » Global security SOC stratified into 3 levels of action with capacity and autonomy for immediate response to threats.
- » Automatic threat collection system based on MISP.
- » Security operation orchestration and automation system.
- » Security monitoring systems with ingestion of more than 3,000 million daily monitored events.
- » Specific monitoring scenarios for critical environments.
- » Connected to different national and international collaboration groups and networks (First, CSIRT, FS-ISAC, National Network of SOC's).
- » He regularly participates 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 training of people, the tools and procedures implemented, as well as the network of contacts with organizations of a similar nature in the public and private spheres, enable MAPFRE to carry out early detection and response to any cybersecurity incident.

5.8

Cyber-insurance

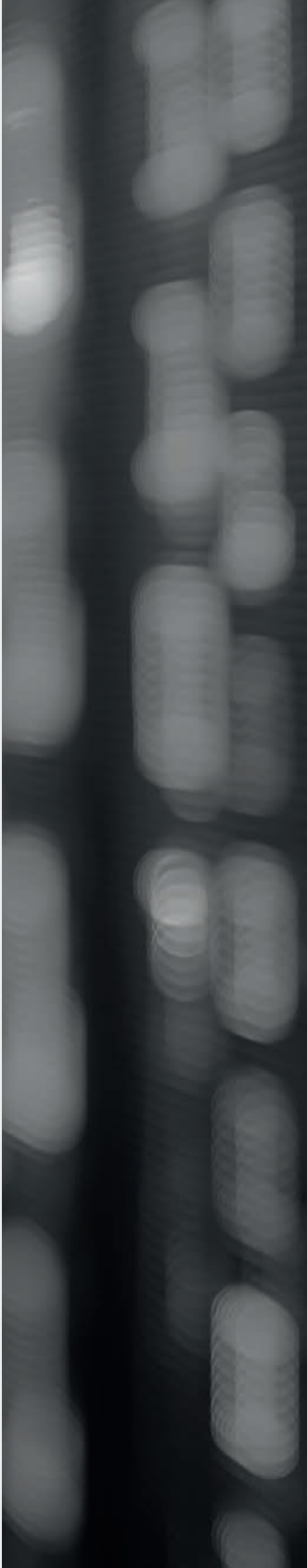
The MAPFRE Group companies have specific assurance regarding **CyberRisks**, which includes both their own damages and possible liabilities to third parties in the event of this type of event materializing. In terms of coverage and limits insured, the contracted protection is consistent with the activity and size of a company like ours.





Corporate DataCenters

MAPFRE has first-rate corporate **Data Processing Centers**, which comply with the highest industry standards, both in terms of the capacity and functionality of the infrastructure and the quality of its operation. In this sense, some of the certifications that the MAPFRE corporate DataCenters have are listed below.





06





TIER III in design and operation

A Tier III DataCenter offers 99.98 percent availability. This configuration allows you to schedule maintenance periods on the servers without affecting the continuity of the service.



SAE 16 Tipo 2 (Statement on Standards for Attestation Engagements).

SAE 3402 (International Standard for Assurance Engagements) These ensure that the controls related to preserving the security and confidentiality of data are adequate.



ISO 27001: Management of Data security

This guarantees that the DataCenters meet the necessary requirements to establish, implement, maintain and update a management system based on a cycle of continuous improvement.



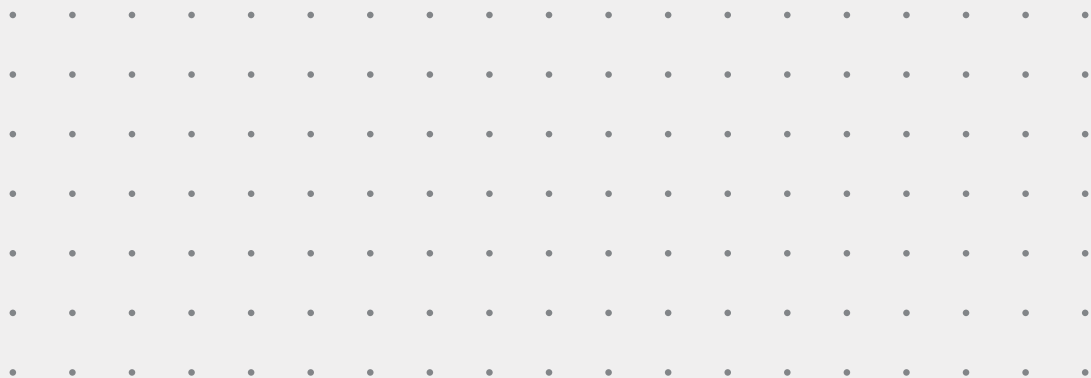
PCI-DSS Collocation

The DataCenters meet the requirements associated with physical access security, as well as the maintenance of a data security policy, which provides a compliant PCI environment.



HIPAA-HITECH

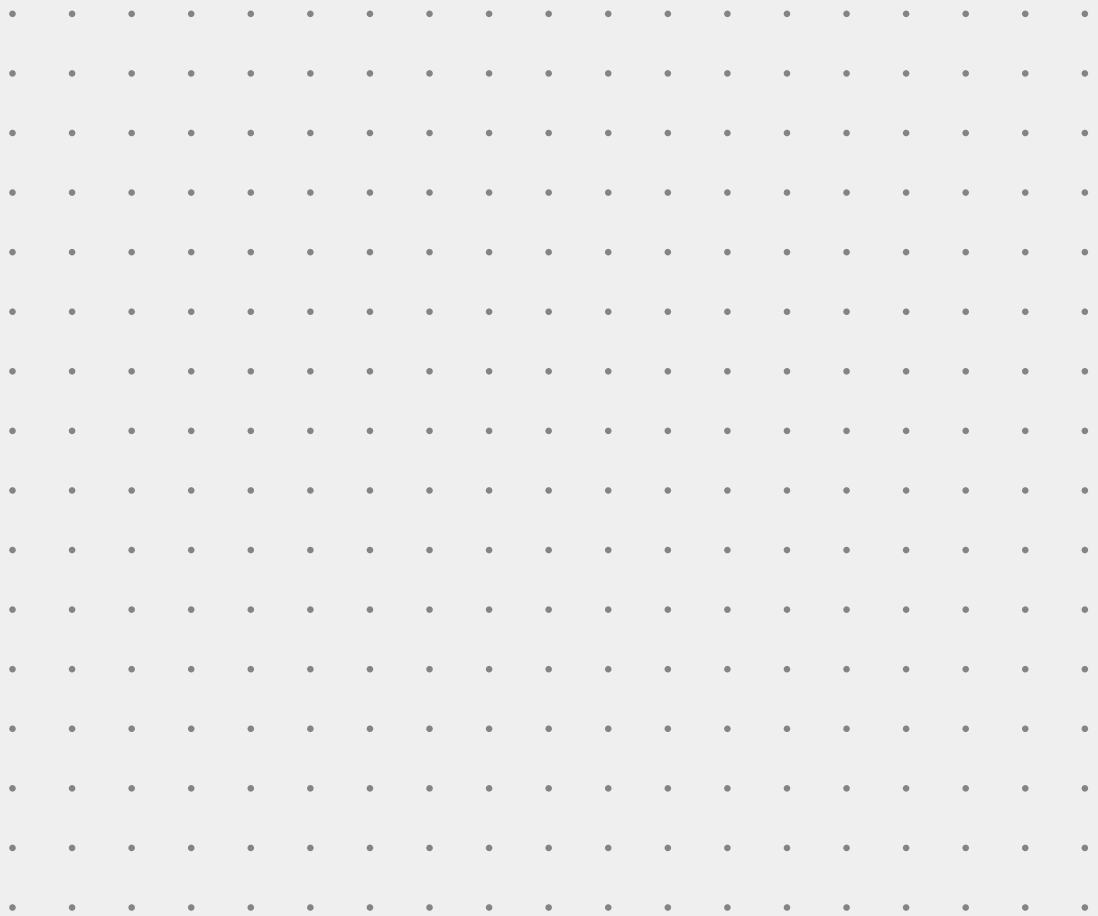
This guarantees the protection of the confidentiality, integrity and availability of protected electronic medical information (ePHI). USA



PCI DSS e-commerce certification. MAPFRE Spain has recently achieved this certification for all its e-commerce.

The PCI DSS certification certifies that we comply with the measures established by the PCI SSC (Payment Card Industry Security Standards Council), which define the necessary requirements to guarantee that card data is processed with the maximum security guarantees.

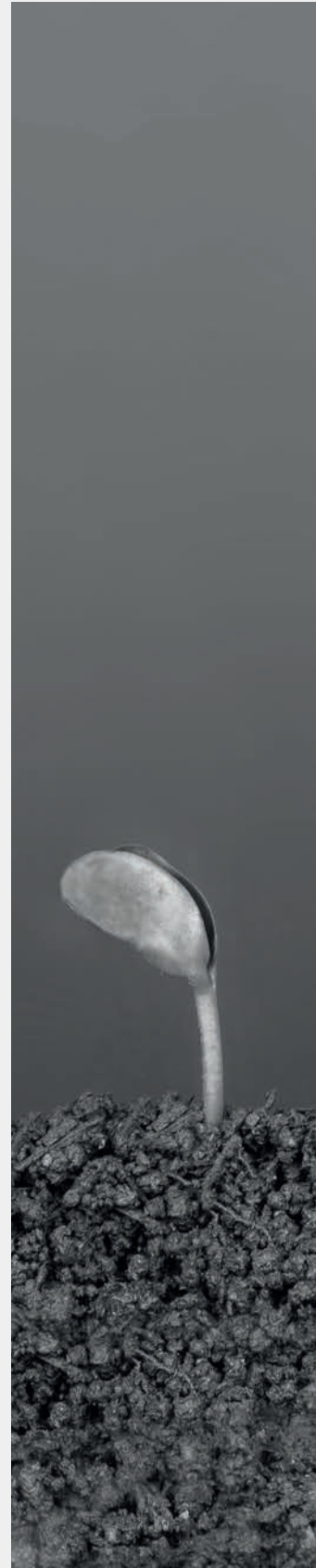
This certification certifies that all MAPFRE Spain web portals that allow online purchases comply with all the necessary security measures to guarantee the appropriate level of security when our customers' card data are processed.





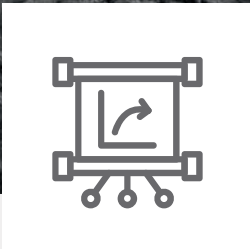
Crisis and Business Continuity Management

The mission of the Corporate Security and Environment Function is to enable the normal development of business, promoting a safe environment in which MAPFRE can develop its activities. To preserve the service provided to our clients during a contingency, MAPFRE has a **corporate model of Business Continuity**, included in its global approach to Security, business needs and to the particular requirements of each Subsidiary.





07



This model is based on **ISO 22301**, which responds to the international dimension of the MAPFRE Group and which is being deployed in all its companies, taking into account the business requirements and the particular requirements of each Subsidiary.

The corporate model is composed of **three large blocks**:



MAPFRE group business Continuity Model



It is demonstrated in its Corporate Business Continuity Policy that MAPFRE is committed to this function and defines the framework for the development, implementation, review and improvement of Business Continuity Plans, so that these:

- » Allow for an adequate and timely response to the materialization of a security or environmental risk (or of any other nature) with catastrophic characteristics, which cause a scenario where there is a lack of availability of any of the basic elements of our activity: people, facilities, technology, information and providers.
- » Minimize the impact of possible catastrophes on business activities: preserving data and ensuring the use of essential functions. If this is not possible, they aim to recover them progressively until a return to normal.

As a second element, MAPFRE has **highly qualified personnel** in this area and a Government Framework where the different bodies and functions associated with continuity within the Group (Units, Companies, Centers) are determined.

It also has a **methodology** that allows the homogeneous and efficient definition and development in the form of Business Continuity Plans, of 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 companies, and their successful functioning has been repeatedly demonstrated in natural disasters and unavailability situations suffered by the various companies of MAPFRE worldwide, such as hurricanes, heavy snowfalls, fires, communications drops, etc.

Special attention should be given, since they are a basic pillar of Business Continuity Plans, to the **Disaster Recovery Plans** or Computer Contingency Plans that are implemented in corporate Data Centers, in order to guarantee the permanent availability of the services that are provided from those centers. These Data Recovery Plans are systematically tested at least annually in all companies, a higher level of demand for such tests being incorporated on each occasion.

Additionally, MAPFRE has opted for a progressive process of certification of these plans in its different entities, having achieved that, currently, many of its entities: **MAPFRE ESPAÑA, MAPFRE VIDA, MAPFRE PORTUGAL, MAPFRE MEXICO, MAPFRE PUERTO RICO, MAPFRE BHD , MAPFRE RE, MAPFRE GLOBAL RISK, MAPFRE INVERSION, MAPFRE TURQUÍA, MAPFRE PANAMÁ, MAPFRE COSTA RICA, MAPFRE HONDURAS, MAPFRE INVERSIONES and MAPFRE TECH**. They are certified in ISO 22301, guaranteeing the updating and continuous improvement of these plans.





Privacy and Personal Data Protection

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.





08



8.1

Data Protection Officer

MAPFRE has a **Corporate Data Protection Officer and a specific area** within the Corporate Security Department in charge of ensuring compliance with existing regulations regarding **privacy and protection of personal data**.

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

Additionally, MAPFRE has a **Corporate Privacy and Data Protection Committee**, for the direction and control of the different projects related to privacy and protection of personal data, in order to support the DPO in the development of its functions. Additionally, this committee will exercise its support functions to the Corporate Security, Crisis and Resilience Committee in relation to the management of incidents and security breaches of personal data, including coordination, monitoring and decision-making, and notification to the Control Authority and/or Affected Parties.

In the different countries where the Group's insurance entities are present and where legislation requires such a figure, it has Local Data Protection Officers, and Local Data Protection and Privacy Committees, with functional dependence on the corporate. In those countries where, due to the size of the entity or business, a specific DPO is not named, there is a figure responsible for privacy and data protection, which is related to its corresponding DPO.

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

8.2

Privacy Reference Framework

MAPFRE has adopted the **General Data Protection Regulation of the European Union** (GDPR) as a reference framework in matters of Privacy and Data Protection



For its implementation and management, this reference model is articulated in a series of strategic lines:

- » Early adaptation to applicable privacy regulations in the different geographies in which it operates.
- » Integration of Privacy in the life cycle of any new initiative that manages personal data, guaranteeing its protection from design and by default, including carrying out privacy impact analysis of new treatments.
- » Implementation of controls aimed at preserving the confidentiality, integrity and availability of the information handled and the systems that support it.

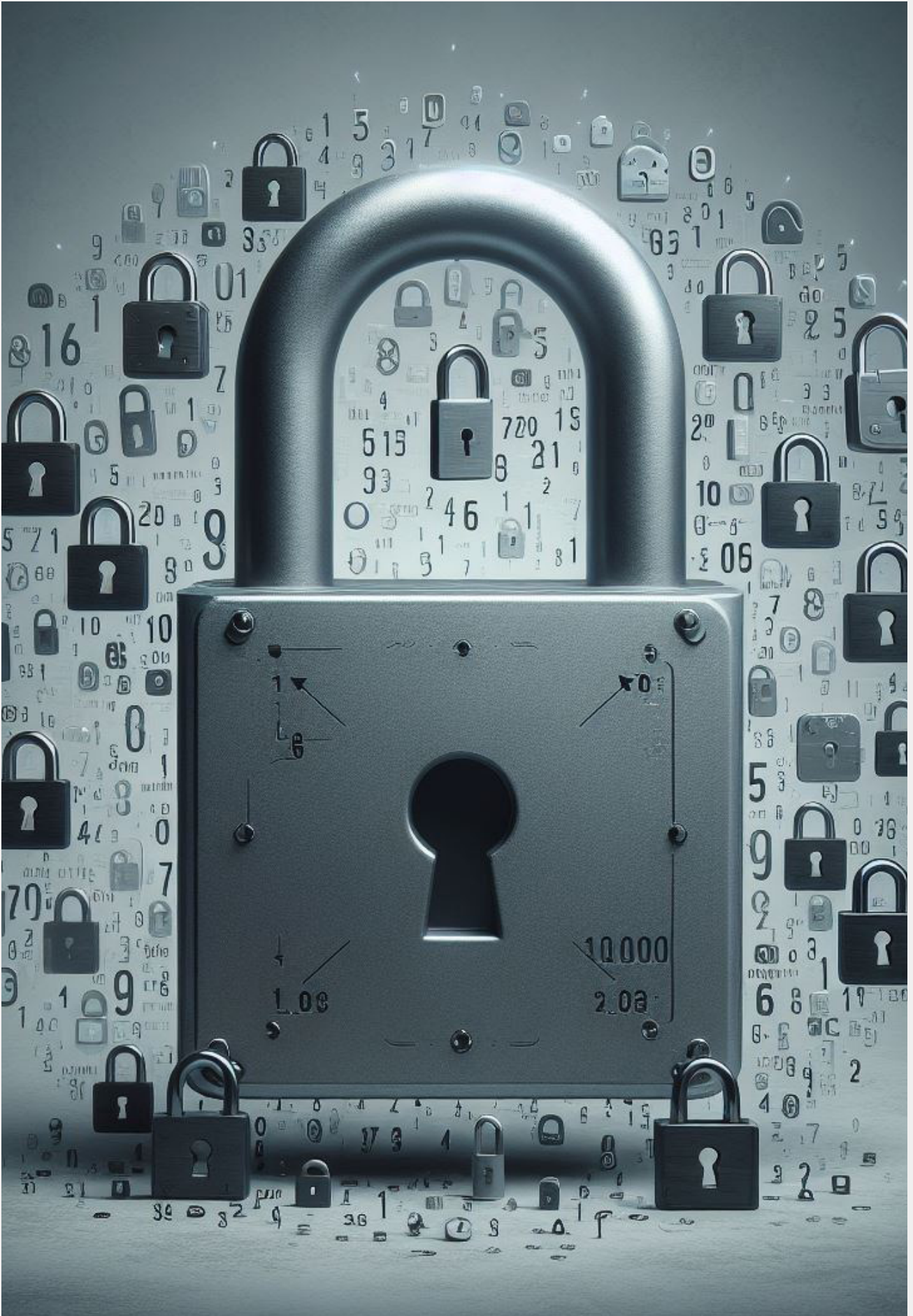
- » Privacy evaluation in the purchasing processes of technological solutions and in the contracting of technological services.
- » Inclusion of information clauses and management of consents in the collection of personal data.
- » Inclusion of Privacy and Data Protection Clauses in Service Provision Contracts, with those suppliers that manage or access information, to guarantee compliance with security and privacy obligations.
- » Attention in time and manner to the exercise of the rights of the interested parties, such as queries and/or complaints addressed to the Data Protection Officer.
- » Training plans and specific awareness regarding Privacy and Data Protection.

Through this reference model, the MAPFRE Group manages to ensure compliance with a common and homogeneous protection standard throughout the Group, which will be complemented by the adherence of the different entities of the group to the Binding Corporate Rules (BCR) that have been developed. and presented to the Spanish Data Protection Agency. MAPFRE Decalogue for the processing of Personal Data, which establishes the privacy principles that all employees, agents and delegates must respect wherever they are in the world:

DECÁLOGO MAPFRE
PARA EL TRATAMIENTO DE LOS DATOS PERSONALES

- 1** Los datos personales son de las personas que nos los han facilitado y forman parte de su privacidad e intimidad, protégelos.
Úsalos debidamente.
- 2** Los menores requieren una especial protección.
Para poder usar sus datos debes tener siempre el consentimiento de sus padres o tutores legales.
- 3** Siempre que recabes datos debes informar para qué los necesitas.
Usa un mensaje claro y sencillo.
- 4** Recaba únicamente los datos que sean necesarios para las finalidades, legítimas y válidas, de las que has informado previamente.
- 5** Cuando la información deje de ser necesaria asegúrate de destruirla de forma segura y/o garantizar su supresión en los sistemas.
Sigue los procedimientos y mecanismos seguros establecidos para ello.
- 6** Las personas pueden ejercer derechos sobre sus datos personales.
Atiende el ejercicio de esos derechos con diligencia y agilidad.
- 7** En tu trabajo, y en tu día a día, te corresponde proteger los datos personales que tratas.
Aplicando para ello las medidas de seguridad establecidas y garantizando la confidencialidad de la información a la que accedas por razón de tu puesto de trabajo.
- 8** Informa a tu responsable de seguridad de cualquier incidente de seguridad del que tengas conocimiento.
Sigue las instrucciones que te faciliten. MAPFRE cuenta con equipos especializados que evaluarán cada situación y tomarán las medidas adecuadas.
- 9** Actúa siempre con diligencia, confidencialidad y responsabilidad.
Nuestro comportamiento impacta en las personas y puede derivar en responsabilidades importantes para todos y sanciones muy elevadas (hasta el 4% de la facturación mundial, o 20 millones de euros).
- 10** En MAPFRE, todo proyecto o iniciativa debe incorporar la seguridad y privacidad desde el origen.
Para todo nuevo proyecto o iniciativa o ante cualquier duda, contacta con tu responsable de seguridad.

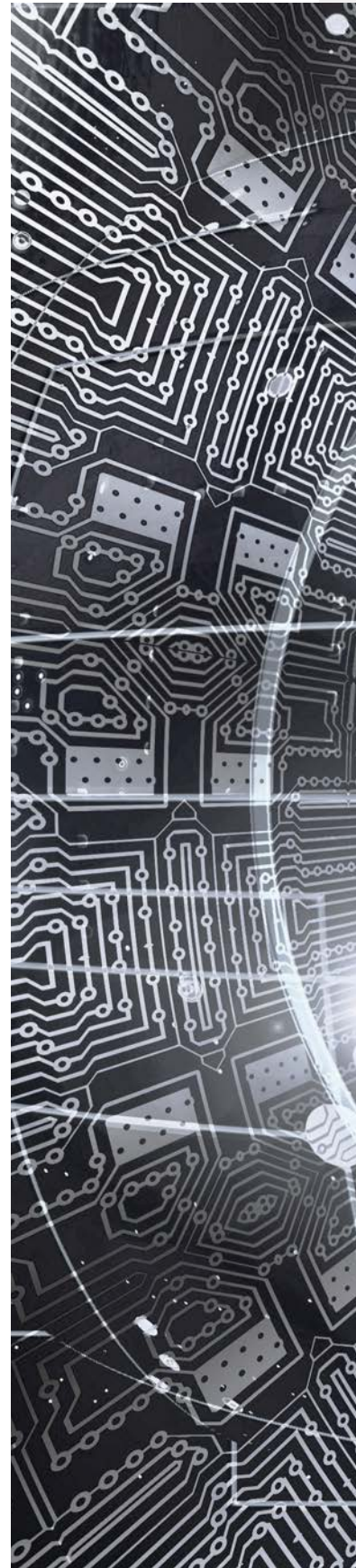
© MAPFRE





Artificial Intelligence and Data Ethics

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.





09



MAPFRE has a **Digital Governance Ethical Framework**, which defines the opportunities and risks brought by new technologies such as artificial intelligence and the principles to be followed by the MAPFRE Group so that its actions in the digital field comply with the law. current.

Guidelines and action protocols have been defined to implement a government model that allows greater control over the Artificial Intelligence systems used, as well as the necessary mechanisms to determine the level of risk that exists based on the use that will be made. give to them.

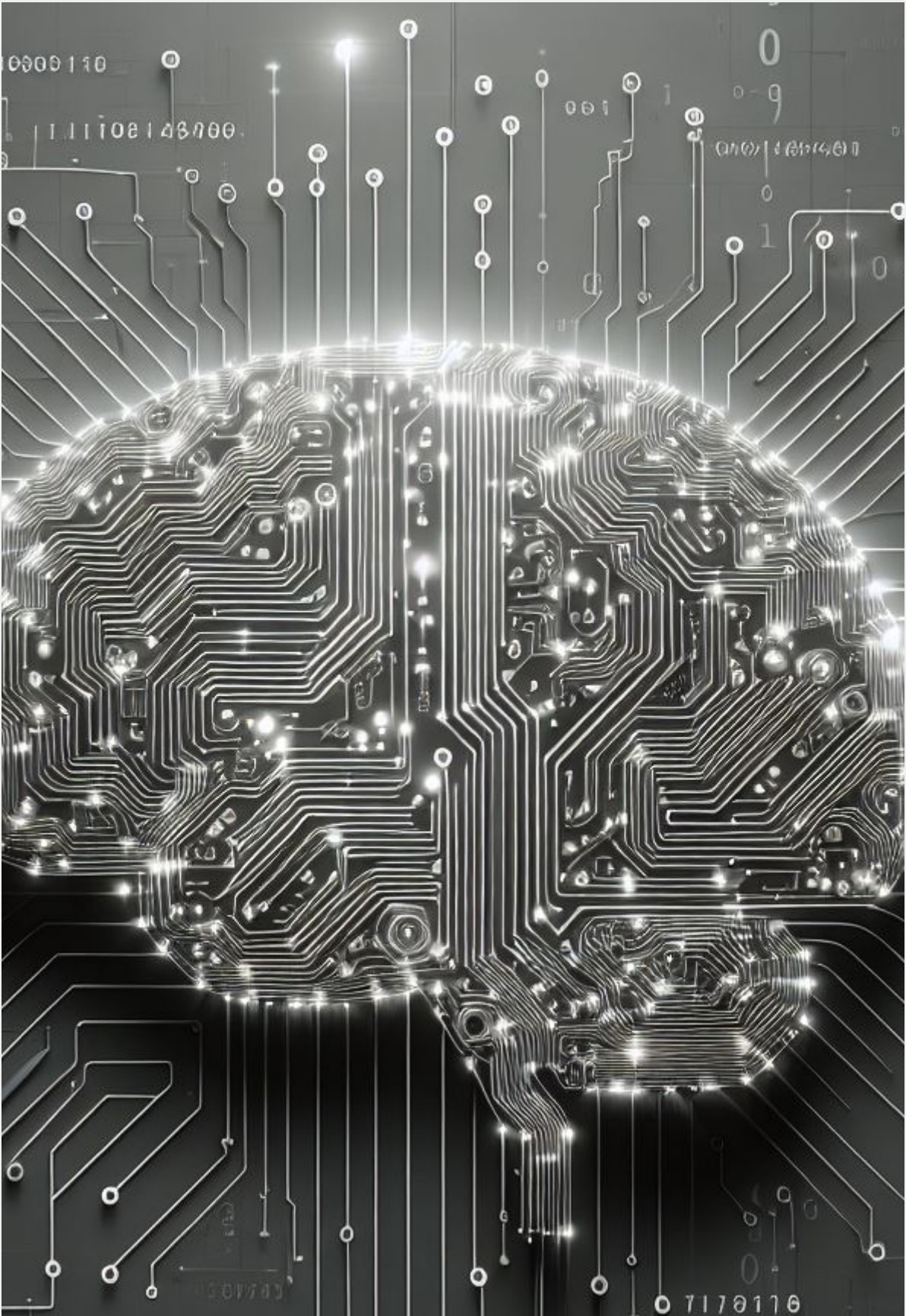
MAPFRE is adapting its security and privacy requirements to have greater control over the use that is being made of this technology, protecting not only the personal data used, but all information relevant to the company, to achieve optimal levels of quality, security , traceability, privacy, fairness, explainability and transparency of data.

Additionally, a **Working Group on Artificial Intelligence** has been defined, whose mission is to raise issues related to ethics and data protection, streamlining processes, automating decisions and improving customer experience. , with the aim of making ethical and effective use of data.

As a result of the creation of this Working Group, a **'Guide for the Use of Artificial Intelligence Systems'** has been developed with the objective of establishing the necessary guidelines and measures to mitigate the associated risks that arise from the use of this type of technologies and which in turn allows for early adaptation to the applicable regulations in this matter.

Finally, we should mention MAPFRE's adherence to the **'Commitments to Privacy and Digital Ethics'** of the Cotec Foundation. Commitment that was born to respond to the challenge posed by data processing in a context of digital transformation, in which the application of ethical principles in privacy management, and especially in the development and use of applications, acquires growing importance. based on data.

Adhering to this decalogue is a demonstration of MAPFRE's commitment and concern for privacy management from the perspective of the ethical management of the data that our clients, collaborators, mediators and employees provide us.





Security Culture: Sensitization, Awareness and Training

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





10



MAPFRE has created a multidisciplinary Working Group, with the participation of the Corporate Areas of People and Organization, External Relations and Communication and Security, in charge of defining, developing and maintaining the Corporate Security Awareness, Awareness and Training Plan, which is updated annually, and continuously adapts to the needs of the environment.

In line with MAPFRE's global and comprehensive vision of security, this plan contemplates ICT security, data privacy and protection, digital operational resilience, as well as the security of people and facilities.

The actions included in the Plan are aimed not only at MAPFRE employees, but also at third parties, such as critical suppliers, customers and other interest groups.

They include awareness campaigns, which seek to achieve an emotional impact, awareness activities, so that people are aware of threats and good practices, as well as technical training programs, adapted to different groups according to their level of criticality and attributions.

Some examples of these actions are:

- » Regular publication of security news, tips, videos, infographics, podcasts and other communication resources.
- » Specific awareness-raising campaigns for employees, through gamification.
- » Training pills at the MAPFRE Corporate University, available to all employees.
- » Training courses for specific groups (Senior Management, ICT staff, cybersecurity teams, Contact Center, etc.)
- » Cyber exercises with campaigns aimed at all employees.





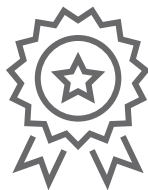
Audits and Reviews


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 Safety Reviews and Audits.





11





MAPFRE carries out specific **Reviews** and **Audits**, related to compliance with the Security and Privacy Policy, the Business Continuity Policy and data protection regulations, which, in most entities, are contracted with expert auditors.

Additionally, within the Technology and Security Internal Control Audit Methodology developed at MAPFRE, a section is always included in the ICT Environment Control Area on compliance with the Security Regulatory Body and the legislation that affects these matters. including data protection.

Finally, business process audits also include specific security and privacy aspects, in order to identify possible 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.

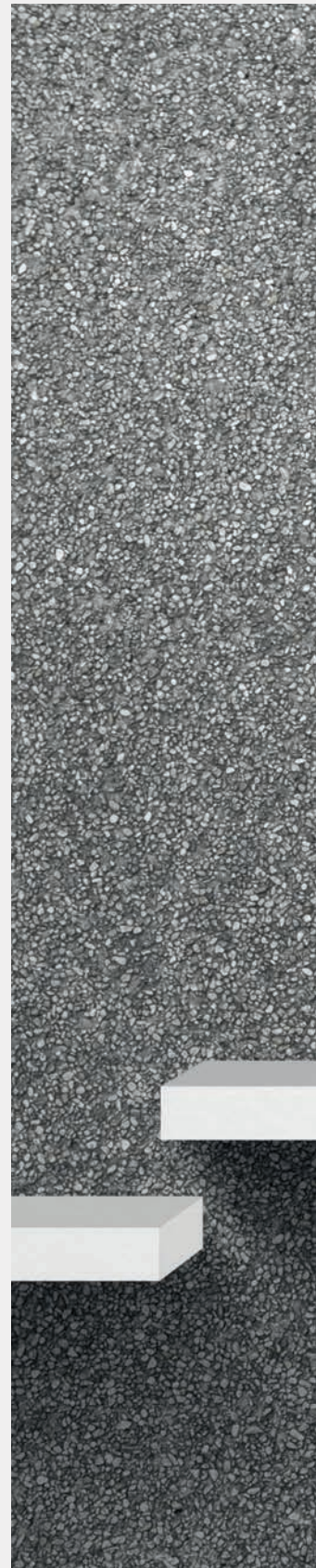
As a result, throughout 2023, more than 50 audit projects have been carried out on security governance, information systems and security, business continuity, as well as privacy and data protection.



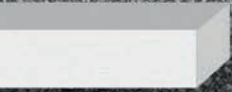
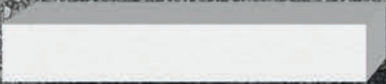


Recognition and Bench- mark from Thrid Parties

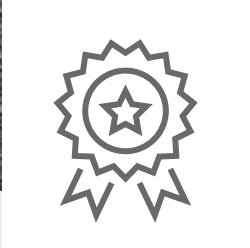
The **integrated and global security** model adopted by MAPFRE is a benchmark for international analysts and other corporate security organizations of large companies, which has resulted in numerous awards and recognitions, including:



 **MAPFRE**



12





Defining a Case Study relating to the MAPFRE General Control Center (CCG-CERT), performed by the prestigious international analyst **Gartner Group**.



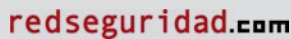
Security Award from Revista SIC in its XIV edition, to the Assistant General Management of Security and Environment of MAPFRE "in recognition of its pioneering, multidisciplinary and integrated approach to corporate protection fronts, including those associated with the management of data security and cybersecurity."



International Security Trophy for Research and Development Activity (R&D), in the XXVI Edition of the International Security Awards Contest, in the form of Trophies for the best security project convened by the publisher Borrmarkt.



First Prize for Excellence in Corporate Security - Duque de Ahumada awarded by the Spanish Ministry of Interior to MAPFRE for having a comprehensive security model, which is a benchmark for corporate security organizations.



Extraordinary prize from the awards juries at **RED SEGURIDAD**.



Honorable mention from the **General Directorate of the Spanish Police Force**.



In 2019, MAPFRE was awarded by IDC Research Spain for its **"Cybersecurity strategy project adapted to the new digital scenario"**

Additionally, the MAPFRE security model has been selected by the **INSTITUTO DE EMPRESA (IE)**, one of the most prestigious international business schools, as a case study within its Masters on CyberSecurity, and has formed part of its syllabus since 2017.



Below, we see the evaluation of third-party benchmarks corresponding to the year 2023 in relation to the security situation at MAPFRE:

 <p>Dow Jones Sustainability Indexes</p>	<p>96 (out of 100). Information Security/Cybersecurity & System availability.</p> <ul style="list-style-type: none">+14 points compared to 2022.
 <p>CNPIC incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD</p>	<p>4,7 (out of 5). Cyber Resilience improvement indicators - BMI.</p> <ul style="list-style-type: none">+0,4 financial sector half points.+0,1 points compared to the previous year.
 <p>DSN isms FORUM</p>	<p>9,13 (out of 10). Cyber crisis management 2023.</p> <ul style="list-style-type: none">“Excellent” maturity.First position of the 26 participating companies.

