v 1.6 July 2023

Security

Keeping your trust

MAPFRE

TABLE OF CONTENTS

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, it constitutes the Corporate Security and Environment function, in order to protect the tangible and intangible assets of MAPFRE. This mission is included in the Security and Environment Master Plan which, from a risk management standpoint, operates as a Strategic Framework and is a starting point for the creation of Policies on Security and Privacy, Business and Environmental Continuity as well as for the development of the Internal Regulations relating to these policies. All this strictly complies with current legislation and the MAPFRE Code of Ethics and Conduct.

Security is an integral part throughout the entire organization and its culture, 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 General Control Center (CCG-CERT), which is part of the FIRST network (Forum of Incident Response and Security Teams), where the security of the MAPFRE Networks and Information Systems worldwide, and where the response to security incidents that the company may encounter 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.

At the same time, MAPFRE is firmly committed to the Environment, coordinating its action via three fundamental axes, the integration of the Environment into the business, the development of environmental management actions and the promotion of environmental responsibility within the Company."

Guillermo Llorente
Group Head of Security at MAPFRE

Vision and Model of Security and the Environment

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 and the Environment, an area in which it also seeks to be a benchmark.

01

1.1

Vision of the Function of Security and the Environment 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 and the Environment

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

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

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

The model for the development of **Function of Security and the Environment** was built on this approach.

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

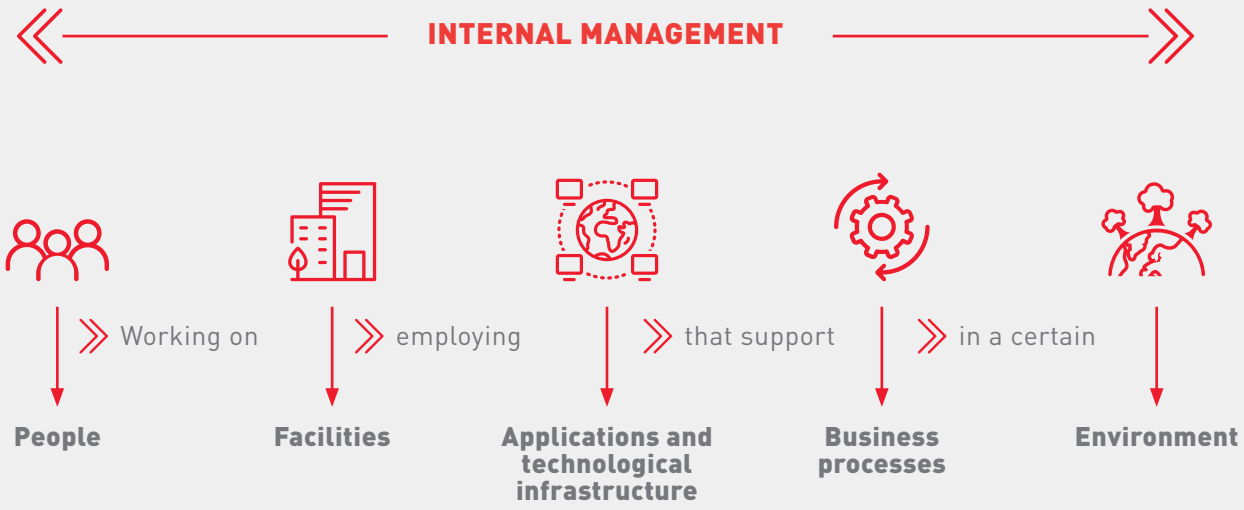
ISO 27001 abnd 27002 in Information Systems Security

ISO 22301 in Business Continuity

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

ISO 9001 for qualify management

ISO 29100 regarding privacy protection



1.3

Management Framework for Security and the Environment Function

Reflecting the above principles, MAPFRE has a **Security and Environment Master Plan** which operates as a Strategic Framework, establishes the mission of **the Function of Security and the Environment** and, with an holistic vision and an approach based on risk management and MAPFRE's Code of Ethics, is a starting point for the creation of policies and internal regulations:

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

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

Finally, the regulatory body for Security and the Environment, developed in more than 100 norms, standards, regulations and internal procedures.

CODE OF ETHICS AND CONDUCT		
Security and Environment Master Plan (SEMP)		
Security and Privacy Corporate Policy	Business Continuity Policy	Environment Policy
Security and Environment Governance Model		
Regulatory Body for Security and the Environment		

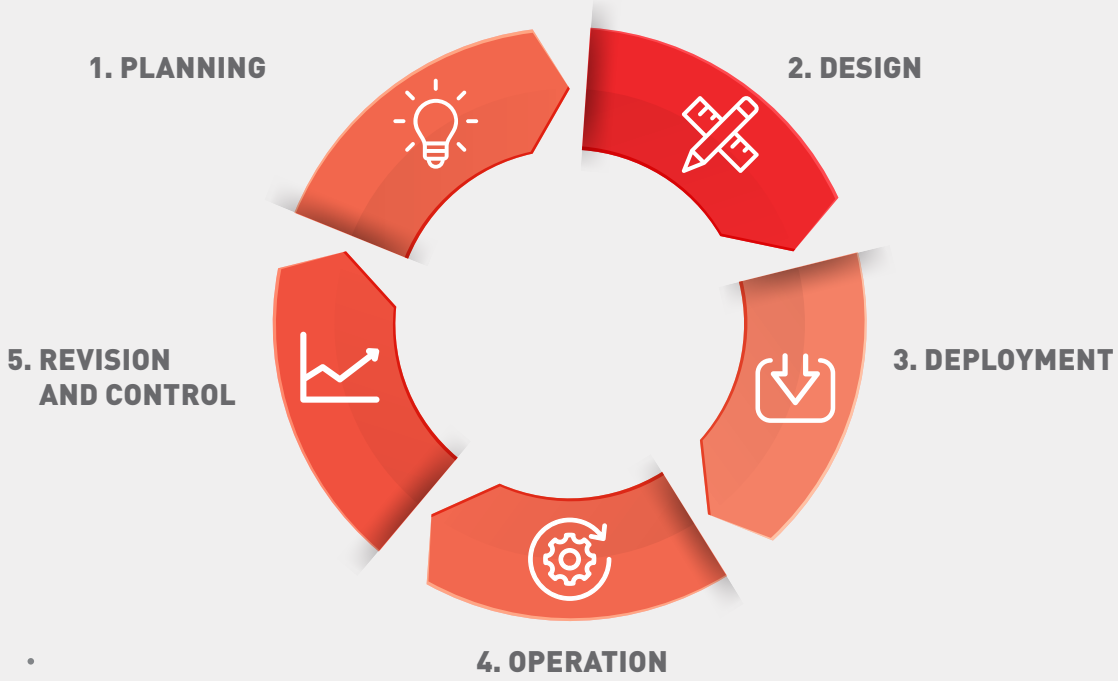
In the following links you can consult the Code of Ethics and Conduct, as well as for corporate policies on Security and the Environment:

- **Code of Ethics and Conduct**
  https://www.mapfre.com/media/sostenibilidad/2019/codigo-etico-2019.pdf
- **Security and Privacy Policy**
  https://www.mapfre.com/media/accionistas/2015/politica-corporativa-seguridad-privada.pdf
- **Business Continuity Policy**
  https://www.mapfre.com/media/accionistas/2020/politica-de-continuidad-de-negocio-2019-12-13.pdf
- **Environment Policy**
  https://www.mapfre.com/media/acionistas-investidores/politica-de-medio-ambiente.pdf

1.4

Process of Continuous Improvement of Security and Environmental Management

To carry out its mission, Security and Environmental management 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 and the Environment

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

02

2.1

Global Approach

Our conception of Security as being UNIQUE for everything as a whole in a Global company such as MAPFRE and of an INTEGRAL nature in the event of all types of threats in a global entity such as our Group, involves a **two-dimensional structure**, which provides a consistent 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, entity and market.

2.2

Corporate Security Committee

At the top of the MAPFRE Security Organization is the **Corporate Security and Environment Committee,** the most senior management body of the organization.

This committee, composed of executive board directors and senior managers of MAPFRE, ensures that business objectives and requirements govern the activity of the Security and the Environment Function. At the same time **it guarantees that Security** is considered as an essential element of corporate business and support processes.

The main functions of this committee are to:

- To promote the development and implementation of the Security and Privacy Policy and the Business Privacy Policy and the Business Continuity Policy, ensuring compliance, dissemination and periodic review of the same.
- Approve the specific body of regulations on Security, Privacy and Business Continuity that Business Continuity that develops the Policies mentioned in the previous point.
- Approving the strategy and high-level objectives. Dictating criteria in relation to Security, Privacy and Business Continuity, and their alignment with the Business. Business.
- Promoting the implementation of plans, programmes and projects in relation to Security, Privacy and Business Continuity. Security, Privacy and Business Continuity, guaranteeing the appropriate alignment with the Security with MAPFRE's Security Master Plan (PDS).
- Supervise the global evolution of Security initiatives and metrics, Privacy and Business Continuity initiatives and metrics.

- Ensuring that the necessary human, material and financial resources are assigned and provided to meet the financial resources are allocated and provided to meet the established objectives and functions.
- Ensure compliance with the regulations and legislation in force in these matters, as well as the commitments entered into with third parties in this area.
- Controlling Security, Privacy and Business Continuity risks, being informed of the exceeding of the defined risk thresholds and informed of the exceeding of the defined risk thresholds and making decisions in this respect.
- Ensure the performance of periodic tests and trials aimed at assessing the Group's Security the Group's Security capabilities, including those specific to CyberSecurity, Business Cyber Security, Business Continuity and IT Contingency.
- Be aware of the most relevant Security and Privacy incidents that have occurred, as well as the main results of the security, business continuity and IT contingency tests carried out and ensure that they are reviewed in order to identify and incorporate the relevant lessons learned.
- Promote the implementation and dissemination of a "Culture of Security, Privacy and Business Continuity" in the entity, communicating the importance of complying with the established policy and standards, as well as the individual responsibilities of all employees in the protection of information security.
- Determine the entity's security risk tolerance, aligned with the Group's risk appetite, communicating the importance of complying with the established policy and standards, as well as the individual Group's risk appetite, proposing it for approval by the competent bodies.

2.3

Human team

highly qualified

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 **400** i**ndividual 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	**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.
GIAC CERTIFICATIONS	**Certifications of GIAC:** GCIH, GSEC, GCFE, GCED
	IBM QRadar®: Helps security teams accurately detect and prioritize threats throughout the organization. QRadar can be deployed in hybrid or SaaS facilities.
PCI DSS Certified	**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.
PCI Security Standards Council	**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).
OFFENSIVE security OSCP	**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.
CHECK POINT CERTIFIED SECURITY EXPERT CCSE	**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.
CERTIFIED ISO 22301 CERTIFIED	**ISO** 22301 Foundations, **ISO** 22301 Lead Implementer, **ISO** 22301 Lead Auditor
BS25999 Lead Auditor	**BS** 25999 Lead Auditor

CRCM	**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	**CompTIA** Linux+; **CompTIA** A+; **CompTIA** Systems Support Specialist; **CompTIA** Network+; **CompTIA** IT Operations Specialist; **CompTIA** Linux Network Professional; **CompTIA** Security+
splunk>	**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 FOUNDATION CPD	**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.
FEMA	**ICS**-100 Incident Command System 100; **ICS**-200 Incident Command System 200; **ICS**-700 Incident Command System 700
LPIC-1 LINUX ADMINISTRATOR	**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.
CERTIFIED FRAUD EXAMINER	**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	**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 50001 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

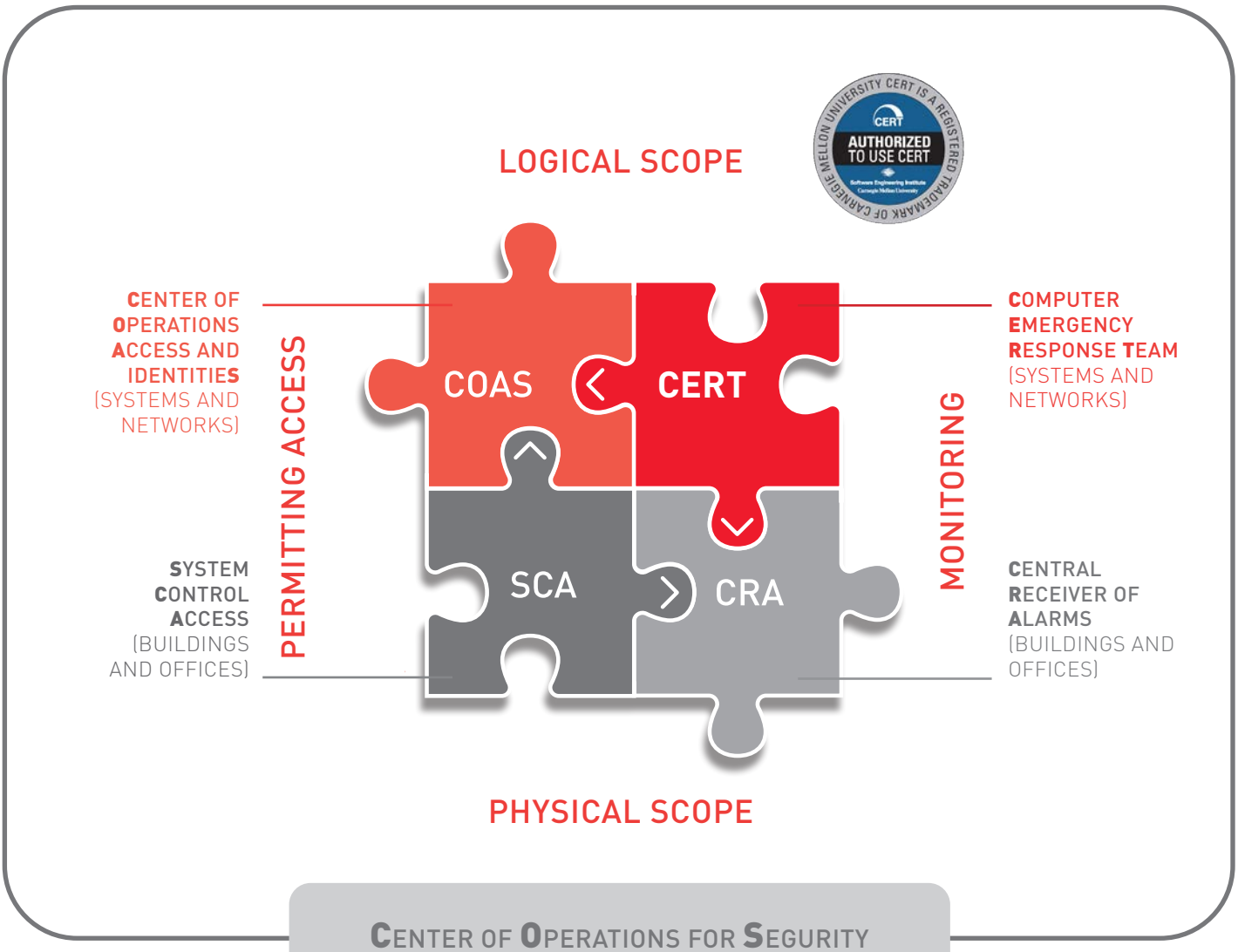
2.4

General Control Center (CCG-CERT)

The **General Control Center (CCG)** 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 reflects MAPFRE's comprehensive security model, controlling access to MAPFRE's information systems and facilities, monitoring the different physical and logical events and responding to security incidents of any nature.

The CCG-CERT is integrated in the following network: **"Forum of Incident Response and Security Teams" (FIRST).** It is in permanent contact with the main private and governmental CERTs in the world, as well as in the National Network of SOCs of the spanish CNN-CERT, which facilitates collaboration and the exchange of information between public cybersecurity operations centers with a view to identifying threats and early response to eventual incidents.



CENTER OF OPERATIONS FOR SEGURITY

(Operation of Systems and Security Tools)

The **CCG-CERT** is **ISO 27001 and ISO 22301**-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 in Information Security 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.

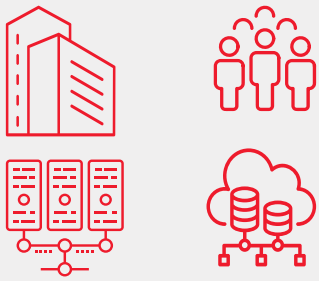
ISO 22301 certification in Business Continuity shows the ability to:

- Determine possible present and future risk situations.
- React so that such a situation affects as little as possible the performance of duties.
- Identify critical functions and reinforce them in the event of an emergency situation.
- To ensure resilience to unexpected situations, improving the cyber resilience of the organization and the services it provides to its clients.

The **CCG-CERT** 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 CCG-CERT:

1 MAPFRE Universe

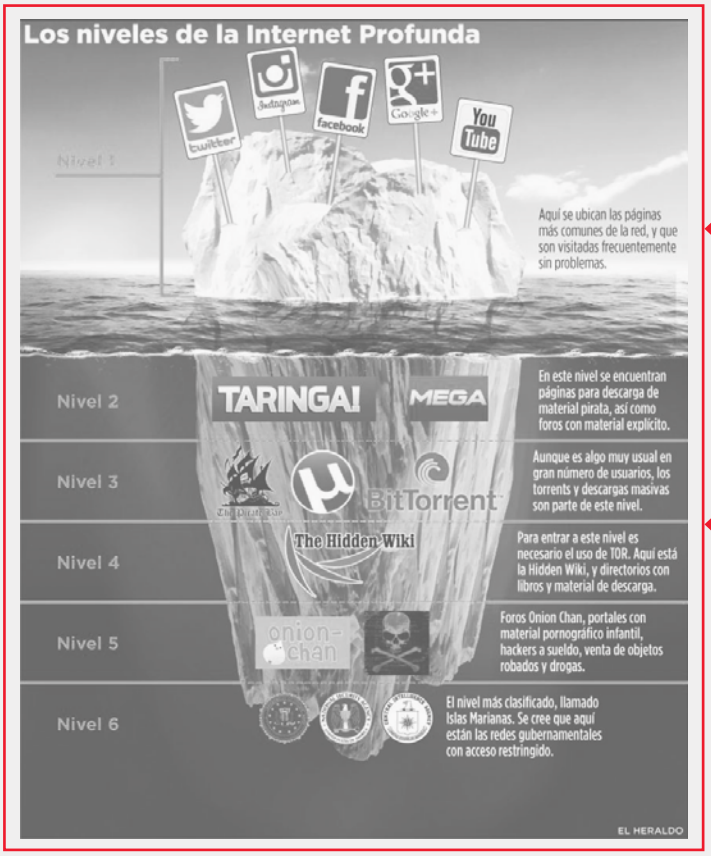


BUILDINGS AND OFFICES

NETWORKS, SYSTEMS AND USERS

2 Social Networks Web Accessible

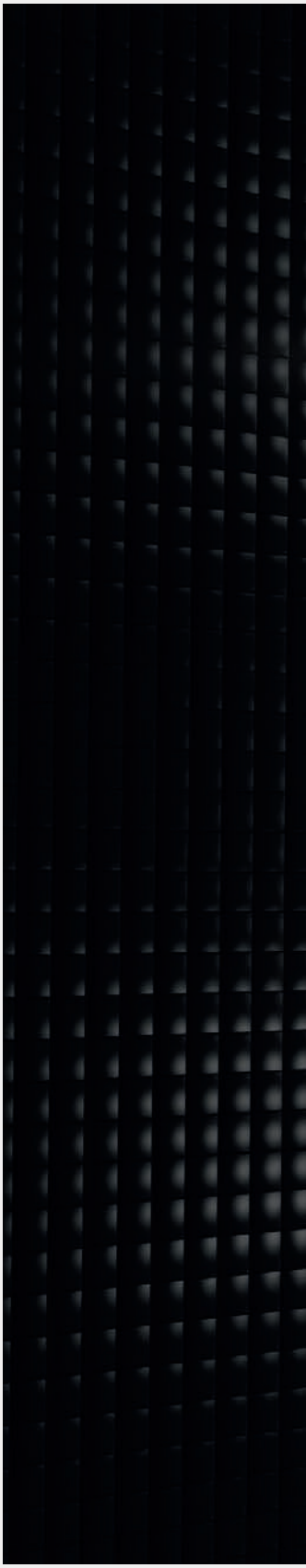
3 Deep Web Dark Web



CORPORATE PROFILES, OPINIONS AND TOPICS

BLACK MARKETS

Compliance in the Area of Security and privacy



MAPFRE's governing bodies have always been particularly concerned about good corporate governance, so they have adopted a set of principles and standards that govern its performance, among which is strict compliance with the laws, and their obligations, as well as the correct uses and good practices of the sectors and territories in which our activities are carried out.

03

MAPFRE has established a Security Standards Body, based on the ISO 27002, ISO 22301 and ISO 29100 standards. 22301 and ISO 29100, and which is also enriched by other widely other widely recognised industry standards, such as the industry, such as the NIST CSF Cybersecurity Framework or the PCI-DSS or the PCI-DSS. This body of standards is mandatory application to all processes and activities in which the Group's entities participate.

This body of regulations, comprising more than 100 documents, is constantly being documents, is constantly being adapted, as is MAPFRE, to the 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 legislations on the subject, as well as the most adequeate compliance.

Special mention should be made of the **General Data Protection Regulation Data Protection Regulation** of the European Union, a standard of reference for MAPFRE in the field of privacy, the strict compliance constitutes the guarantee offered to our clients that we will make appropriate use of the personal data entrusted to us, guaranteeing their privacy and confidentiality.

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

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

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

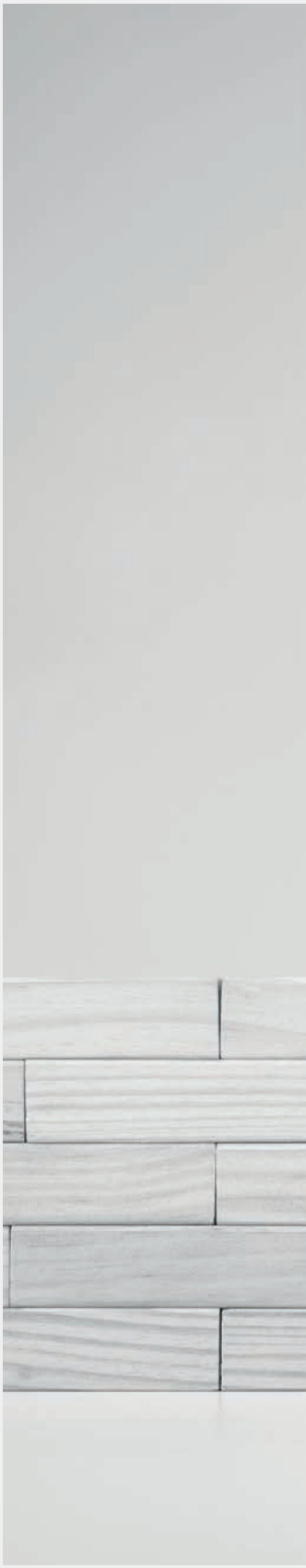
MAPFRE has a regulatory observatory and analysis of the multiple pronouncements made by regulators in the countries in which it operates, with the aim of ensuring that, from the design stage, all processes comply at all times with the applicable privacy and data protection regulations.

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

All of the above considerations enable us to firmly convey MAPFRE's willingness and ability to **comply with the security and privacy requirements** demanded by the legislation of all the countries in which 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

Risk analysis:
MAPFRE's main establishments or installations rely on periodic safety 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 considered and established.

Fire Protection:
The MAPFRE internal regulations 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 for the safety of people and business development. Highlights that MAPFRE, in its commitment to sustainability, uses clean extinguishing systems that respect the environment.

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 at least, once (1) a year.

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 (CCG CERT). These guides contain information on the different areas of the country, useful contacts, including the CCG's 24-hour hotline, as well as Security advice focused on the risks of the country.

Security and Access Control Systems:
In response to the identified risks, both in buildings and in offices, MAPFRE has physical access control systems, and, where appropriate per a risk analysis, video-surveillance, alarm systems and/or security guards. Spaces whose integrity has the greatest impact on the development of MAPFRE's activities and business, have reinforced security measures, designed according to a model of staggered defense in depth.

MAPFRE's General Control Center (CCG) continuosly 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:

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.

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.

A proactive risk management of third parties, applying specific methodologies to ensure that they have the appropriate level of security and guarantee that the risks derived from the service they provide are controlled.

The awareness 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 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.
- Assessing the privacy impact of new treatments and implementing controls and measures to address it.

MANAGEMENT OF THIRD PARTY SECURITY RISK

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

CULTURE

- Awareness of employees, customers and stakeholders.
- Training for employees and agents.
- 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 appropiate segregation os duties.
- Use a Multiple Factor Authentication (MFA) for particularly 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.
- Continuous review of the activities of particularly 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 CCG-CERT.

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 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:

- **Advanced Anti-malware protection: Antivirus & EDR.**
- **Proceeded and implemented system for vulnerability management and associated patches.**
- **Data encryption.**
- **Device fortification.**
- **Device security inventory, management and monitoring.**
- **Mobile Device Management for mobile devices and tablets, etc.**
- **Restriction USB ports access ports on user computers.**

5.4

Cloud Security

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

In addition, the different cloud initiatives must have at least the same security controls as those existing in the corporate data processing centres, and must in no way imply a reduction in the previously existing level of security.

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).**
- **Control del Shadow IT, 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, the **Technical Security Inspection Reference Center has been created**, composed of hihgly specialized personnel, services and tools.

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, both DCS and 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. This provides an overall view of the Group's security situation in this regard.

Similarly, this center carries out 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 catalog of technical security reviews, which ensure corporate information and our customers are protected. Such as, for example:

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

This catalogue of reviews includes the process of **continuous and automated review of the systems exposed to the internet, as well as the critical internal systems of all the company's entities**, and makes it possible to detect any new vulnerability in these systems.

It should also be noted that this Reference Centre is used to coordinate the **Red Team** type reviews carried out on the Information Systems located in our Data Centres, as well as the other **CyberExercises** aimed at assessing both our protection, detection and response capabilities and the security awareness of our employees.

The results of this set of reviews are integrated into the aforementioned Vulnerability and Patch Management System and lead to the development of "remediation" plans subject to specific deadlines, with continuous monitoring of the correction of previously detected vulnerabilities and compliance with the established resolution deadlines.

5.6

Vulnerability and patch management

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

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

MAPFRE has support agreements with the main technology manufacturers for the 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, in particular Zero Day.

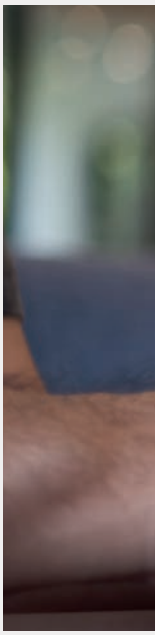
Each time a new vulnerability is published, the cybersecurity team carries out an assessment based on the criticality and impact on MAPFRE's systems, resulting in a classification of the vulnerability. For vulnerabilities of the highest criticality, an urgent procedure is activated in order to resolve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

5.7

Monitoring and incident response

As indicated earlier in this document, MAPFRE brings together the monitoring and response capabilities of cybersecurity incidents in the **CCG CERT,** which assumes the functions of **Global Cybersecurity SOC** and operates as:

- SOC with dedicated personnel in a 24x7x365 format.
- Global security SOC stratified in 3 action levels.
- MISP-based automated threat collection system.
- Security operation automation and orchestration system.
- Security monitoring systems with ingestion of more than 3 billion monitored events daily.
- Specific monitoring scenarios for critical environments.
- Connected to different national and international collaboration groups and networks (First, CSIRT, FS-ISAC, SOC's National Network).
- Participates in CyberEx, cyber exercises organized by the National Institute of Cybersecurity of Spain (INCIBE), in coordination with the Office of Cybersecurity (OCC).The high level training of people, tools and procedures implemented, as well as
- Isolated laboratory for forensic analysis.



the network of contacts with organizations of similar nature in the public and private sphere, enable MAPFRE to implement early detection and response to any cybersecurity incident.

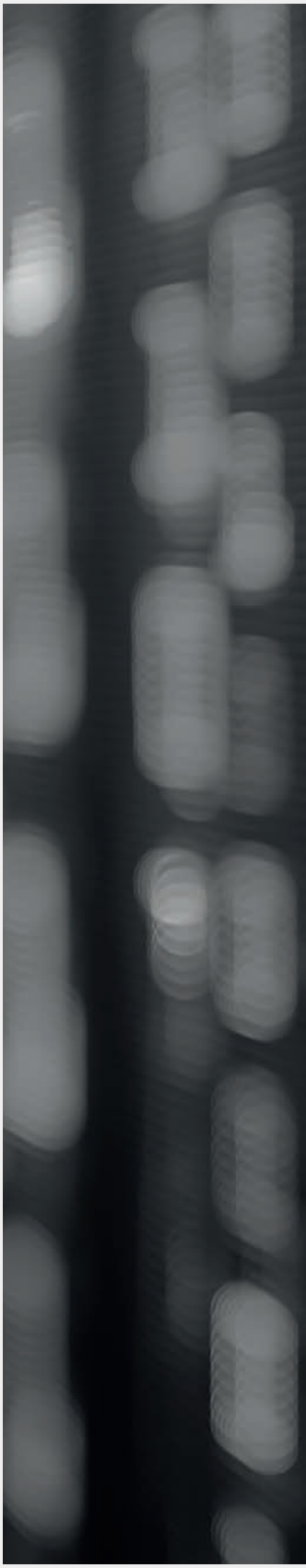
5.8

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
.
DPC Alcalá de Henares (Madrid): Design & Construction
DPC Miami: Design
DPC Tamboré (Sao Paulo): Design, Construction & Operation

SSAE 18 (Statement on Standards for Attestation Engagements)**.**

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

DPC Miami: SOC 1 type 2 & SOC 2 type 2
DPC Tamboré (Sao Paulo): SOC 1 type 2

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.

DPC Alcalá de Henares (Madrid): Systems for Access Control to Facilities and Networks, Network Monitoring and Alarm Systems
DPC Miami
DPC Tamboré (Sao Paulo)

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.

DPC Alcalá de Henares (Madrid)

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

DPC Miami

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 situation, MAPFRE has a **corporate model of Business Continuity**, included in its global approach to Security.

07

This model is based on **ISO 22301,** responds to the international dimension of the MAPFRE Group and has been been 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:**

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 business 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 is required in this context, as the **Disaster Recovery Plans (DRPs)** or IT Contingency Plans implemented in the corporate Data Centres are a basic pillar of the Business Continuity Plans, in order to guarantee the permanent availability of the services provided from them. These DRPs are systematically tested, at least annually, in all the entities, incorporating, on each occasion, a higher level of stringency to these tests.

Additionally, MAPFRE has opted for a progressive certification process of these plans across its different companies, resulting in, at present, 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 y MAPFRE INVESTIMENTOS**. being certified in ISO 22301 guaranteeing the updating and continuous improvement of these plans.


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
Anexo al Certificado


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

MAPFRE's absolute priority is the privacy and protection of personal data we have access in the exercise of its activity, understanding this as an essential element that must be proactively pursued, not only with the aim of achieving compliance of the applicable regulations, but also as a 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 Division that is in charge of ensuring compliance with existing privacy and personal data protection regulations.

Within this area, in support of the **Corporate Data Protection Officer, the Corporate Office for Privacy and Data Protection (CODP) was established with the mission of acting as the point of reference** for all activities related to privacy and data protection at MAPFRE, providing a single comprehensive view of the issue, and encouraging uniformity in all processes and criteria related to it.

MAPFRE also has a **Corporate Privacy and Data Protection Committee** that manages and controls different projects related to privacy and personal data protection, in support of the DPO in the performance of their functions. In addition, this committee will perform support functions for the Corporate Crisis Committee by managing security incidents and personal data breaches, including coordination, monitoring and decision-making, and notifying the Control Authority and/or Data Subjects.

In the different countries where the Group's insurance entities are present and where the legislation requires this figure, it has Local Data Protection Officers and Local Privacy and Data Protection Committees, with functional dependence on the head office. In those countries where, due to the size of the entity or business, a specific DPO is not appointed, there is a figure responsible for privacy and data protection, who is related to 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 individuals in relation to the processing of their personal data.

8.2

Privacy Framework

MAPFRE integrates the **European Union's General Data Protection Regulation (GDPR)** as a framework in everything related to Privacy and Data Protection.

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

- Timely adaptation to privacy regulations applicable in the different geographical areas where we operate.
- Integrating Privacy in the life cycle of any new initiative that handles personal data, to ensure protection by design and default, including the privacy impact assessment of new.
- Establishing controls that maintain the confidentiality, integrity, and availability of the information that is handled and the systems that support that information.
- Evaluating privacy in processes covering the purchase of technology solutions and contracting technology services.

- Including informative clauses and consent management when collecting personal data.
- Including Privacy and Data Protection Clauses in contracts for the provision of services, with providers that handle or have access to information, to guarantee compliance with security and privacy obligations.
- Timely and appropriate assistance to data subjects when exercising their rights, such as with enquiries or complaints sent to the Data Protection Delegate.
- Training Programs and awareness-raising in issues specifically related to Privacy and Data Protection.

By means of this reference model, the MAPFRE Group manages to ensure compliance with a common and homogeneous standard of protection throughout the Group, which will be complemented by the adherence of the various group entities to the Binding Corporate Rules (BCR) that have been developed and submitted to the Spanish Data Protection Agency.

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

8.3 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 manner, adapting its security and privacy requirements in order to have greater control over the use and protection of data.

In addition, a Working Group on Artificial Intelligence has been defined, whose mission is to raise issues related to data ethics and protection, the streamlining of processes, the automation of decisions and the improvement of 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 aim of establishing the necessary guidelines and measures to mitigate the associated risks arising from the use of this type of technology, which in turn allows for early adaptation to the applicable regulations in this area.

Finally, mention should be made of MAPFRE's adherence to the Cotec Foundation's **'Commitments to Privacy and Digital Ethics'.** This commitment was created in response to the challenge posed by the processing of data in a context of digital transformation, in which the application of ethical principles in the management of privacy, and especially in the development and use of applications and services, is becoming increasingly important and especially in the development and use of data-driven applications.

Adherence 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 with.

8.4

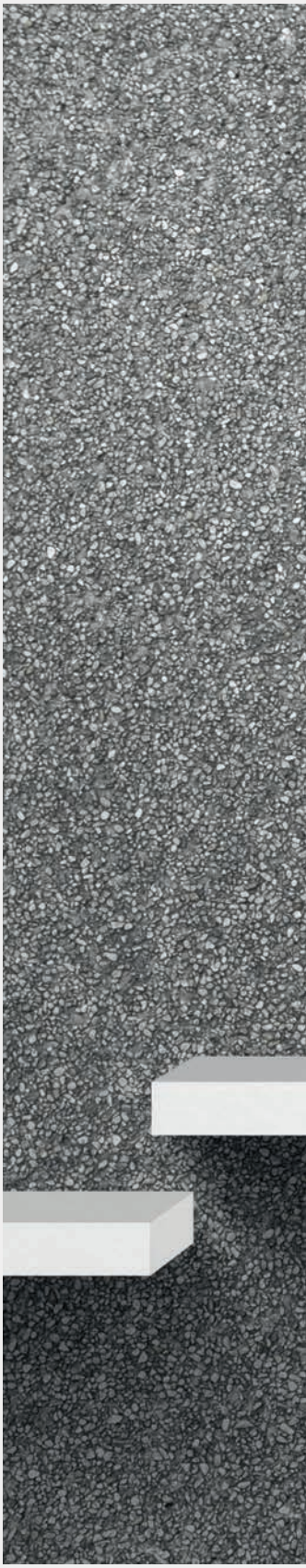
Audits and Reviews

MAPFRE systematically and periodically carries out specific **reviews and audits** related to compliance with data protection regulations, which, in most entities, are contracted with expert auditors.

In addition, within the Internal Control of Technology and Security Audit Methodology developed at MAPFRE, a section is always included in the IT Environment Control Area on compliance with the legislation affecting these matters, including data protection. Finally, audits of business processes also include specific aspects of privacy and data protection in order to ensure compliance with regulations and anticipate any problems that may exist.

Recognition

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:



09

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


Gartner Research

Case Study: Mapfre Implements an Integrated Security Control Center

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 Borrmart.

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 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 case study within its Masters on CyberSecurity, and has formed part of its syllabus since 2017.

MAPFRE