v 2.2 March 2025

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

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

To oversee the normal development of our activity, MAPFRE has a Security Operations Center (Global SOC), which is part of the FIRST network (Forum of Incident Response and Security Teams) and the Spanish National SOC Network, from where the security of MAPFRE's Networks and Information Systems worldwide is monitored and analyzed and from where the response to security incidents that any entity of the Group may suffer is coordinated and carried out.

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

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

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

Guillermo Llorente
Group Head of Security at MAPFRE

PHISHING
SPAM
MALWARE
US

Strategic Approach

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

Characteristics of the Function of Security at MAPFRE

The Security Function at MAPFRE is responsible for protecting, in strict compliance with the law and MAPFRE's ethical principles, the Group's tangible and intangible assets, ensuring regulatory compliance, the company's good reputation and operational resilience.

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

It is GLOBAL for the entire Company.
It affects all personnel, all resources and facilities, all technological assets and all processes and activities of the various Entities, Bodies and Areas of MAPFRE, regardless of their geographic location and corporate structure.

Ensures the Group's RESILIENCE.
Enabling the normal development of the business and providing detection, response and recovery capabilities in the event that risks that affect the operational reliability and integrity of the company materialize.

It is SERVICE oriented.
The Security Function has a vocation of service to the organization, considering it as its client, satisfying the needs that may be demanded from it and accompanying it in its transformation process.

Must PROVIDE VALUE.
Providing differentiation, reliability and competitive advantage to the company. It will evolve according to the needs of the Group in order to remain permanently integrated in the business, adapting, aligning and contributing at all times to the corporate strategy and image of MAPFRE, reinforcing the trust placed in it by its clients and other stakeholders.

1.2

Mission of the Security Function

The Security Function's mission is to prevent the emergence and mitigate the impact of security risks that may cause damage to MAPFRE, its reputation or its personnel, as well as disrupt or limit its operational and/or financial capacity.

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

- **Protect people and other MAPFRE assets,** including data owned by third parties to which MAPFRE has access, ensuring regulatory compliance, ethical and responsible conduct and the preservation of the company's good reputation.

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

1.3

Corporate Security Function Vision

To ensure adequate and sustainable protection in a challenging environment, security, privacy, and operational resilience must be essential and inherent elements of the company's very activity, integrated into its business processes and in line with MAPFRE's responsibility to its employees, clients, shareholders, suppliers, collaborators, and the society in which it operates.

The Security Function also contributes to MAPFRE's leadership in security, privacy, and operational resilience through innovative, effective, and efficient solutions, governed by parameters of strict proportionality, establishing protection mechanisms commensurate with the risk and value of assets, and improving the quality of processes, products, and services.

Additionally, the Security Function ensures legal and regulatory compliance in terms of protection of people, facilities, information, privacy, operational resilience, AI and prevention of antisocial or illicit acts.

The Security Function is governed by the MAPFRE Group's governance standards and the Strategic Security Framework, based on international best practices and standards, and implemented through a standardized and systematic risk management process.

1.4

Principles of the Security Function

The MAPFRE Group's Security Function is governed by the following Principles:

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

2. Comprehensive approach, considering the asset to be protected as the center of its activity and protecting it against all types of threats and risks within the scope of security, privacy and operational resilience, regardless of their mode of materialization.

3. Proportionality, defining and implementing security measures in line with the risk and value of the assets, optimizing available resources for the purpose of continuous improvement in efficiency.

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

5. Preventive action, anticipating damage to avoid it or reduce its consequences, within the concept of due diligence.

6. Security in Depth and Tiered, applying a strategic approach that employs multiple layers of defense to protect assets and mitigate risks, so that if one measure fails, the following ones continue to provide protection, combining different physical, technical and organizational controls

7. Response capacity, acting promptly and proactively to any threat and responding quickly to ensure operational resilience.

8. Centralized Management, Ensuring consistency in the planning of the Security Function, decision-making, and implementation of measures to achieve a consistent level of Security across the Group.

9. Security, privacy, and resilience culture: relevant training and information on these topics for board members, employees, clients, suppliers, and partners, integrating them into the Corporate Culture.

10. Co-responsibility, ensuring that all levels of the organization (Management, employees, suppliers, etc.) share the commitment to protecting MAPFRE's people and other assets.

1.5

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:

- **Security of People.**
- **Security of Facilities.**
- **Security of Information Systems (Cibersecurity).**
- **Personal Data Protection and Privacy.**
- **Operational Resiliencie: Crisis and Business Continuity Committee.**
- **Anti-fraud measures.**
- **Security Intelligence**
- **Regulatory compliance in the area of Security and Privacy and Operational Resiliencie.**
- **Third-party and supplier security risks.**

Security actions are based on a risk management model, ensuring the appropriate protection of MAPFRE's corporate assets.

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

The model for the development of the Security Function at MAPFRE has been built on this approach, governed by the Code of Ethics and Conduct and based on industry standards and best practices, such as, among others:

ISO 27001 and 27002 in Information Systems Security

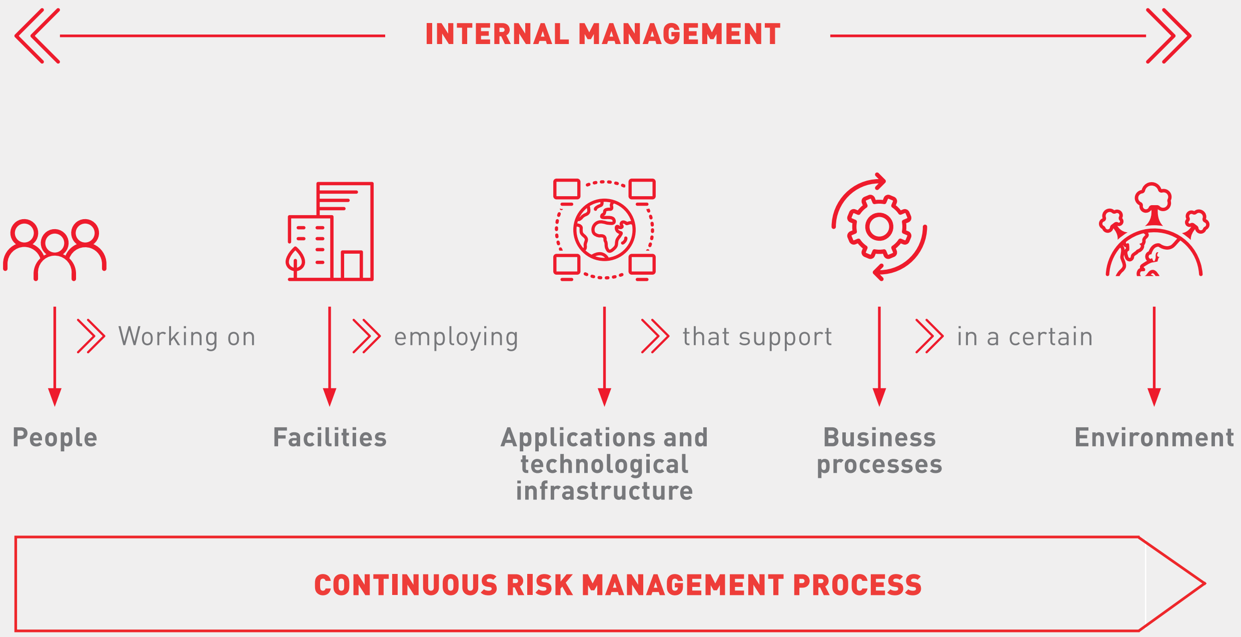
ISO 22301 Business Continuity

ISO 9001 for qualify management

ISO 29100 regarding privacy protection

PCI DSS. On payment card data security.

ISO 31030 on travel risk management.



INTERNAL MANAGEMENT

» Working on

» employing

» that support

» in a certain

People

Facilities

Applications and technological infrastructure

Business processes

Environment

CONTINUOUS RISK MANAGEMENT PROCESS

1.6

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 Regulators, Authorities and Local Security Forces and Bodies.
- Capturing and adapting to the needs, threats and habits/customs in each entity, country and market..

1.7

Security Document System

Reflecting the principles mentioned above and in accordance with the Institutional and Business Principles and the Code of Ethics and Conduct, MAPFRE has a Security Document System, the highest-level element of which is the set of Corporate Policies, which set out MAPFRE's commitment to guarantee the protection of MAPFRE's assets, also ensuring regulatory compliance in terms of security and privacy, the operational resilience of the services provided to third parties, the preservation of the company's good reputation and image and its sustainability. These policies have been approved by the Board of Directors of MAPFRE, SA and are mandatory throughout the Group..

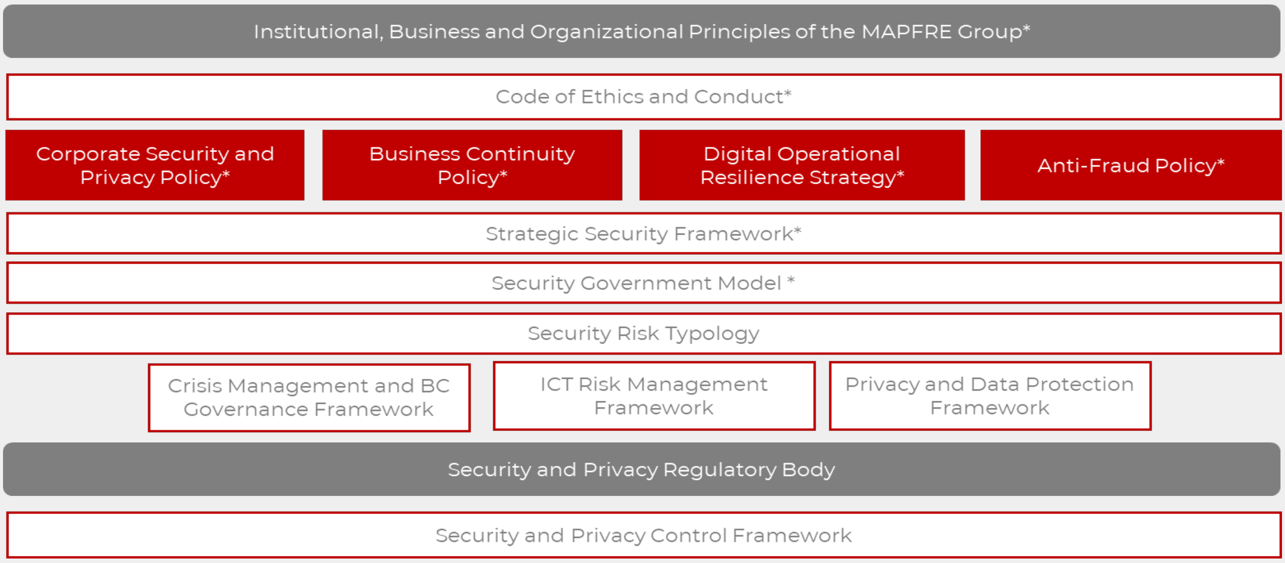
Corporate Security and Privacy Policy, which establishes MAPFRE's guidelines and commitments in terms of security and privacy.

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

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

Anti-Fraud Policy, which establishes the guidelines, procedures and responsibilities to prevent, detect, investigate and prosecute fraud in all its forms.

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



Institutional, Business and Organizational Principles of the MAPFRE Group*

Code of Ethics and Conduct*

Corporate Security and Privacy Policy*

Business Continuity Policy*

Digital Operational Resilience Strategy*

Anti-Fraud Policy*

Strategic Security Framework*

Security Government Model *

Security Risk Typology

Crisis Management and BC Governance Framework

ICT Risk Management Framework

Privacy and Data Protection Framework

Security and Privacy Regulatory Body

Security and Privacy Control Framework

* Aprobados por el comité de Administración de Grupo MAPFRE.

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/Codigo-Etico_ENU-1.pdf

Security and Privacy Policy

https://www.mapfre.com/media/shareholders/2024/mapfre-group-corporate-security-and-privacy-policy.pdf

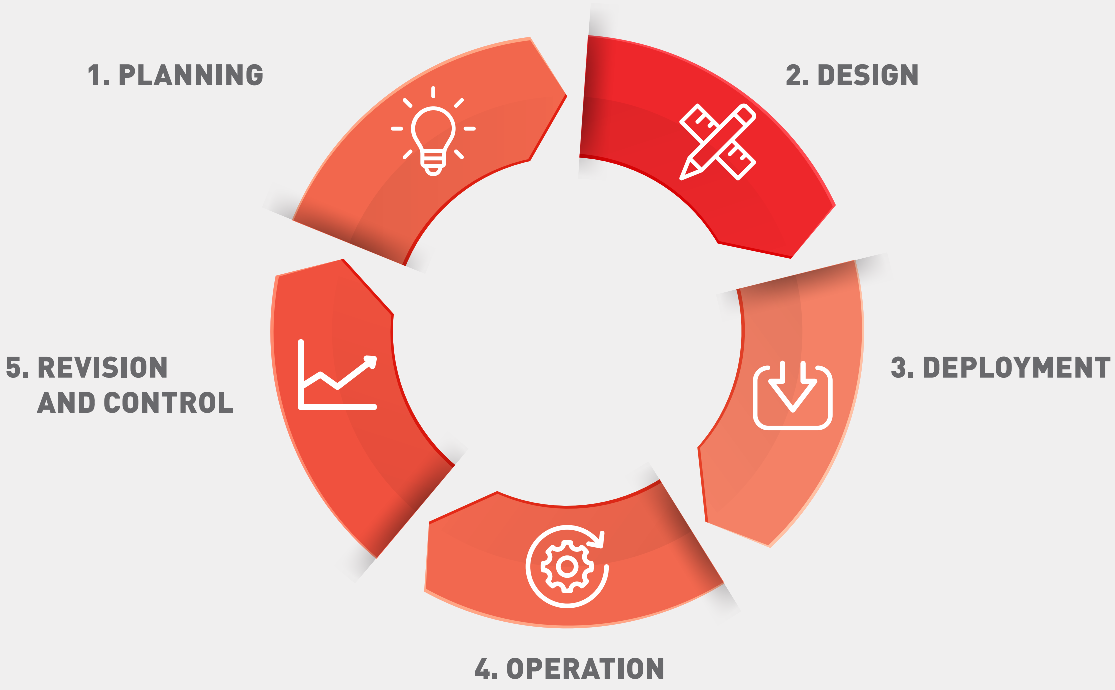
Business Continuity Policy

https://www.mapfre.com/media/politica-de-continuidad-del-negocio-en.pdf

1.8

Process of Continuous Improvement of Security

To carry out its mission, Security at MAPFRE follows 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

Security Organization Structure

MAPFRE's Security Organisation integrates the human teams, means and resources of all kinds intended for the protection of the Group's tangible and intangible assets, aimed at preserving the company's operational resilience.

It is structured into different levels of responsibility aligned with the Group's corporate structure, as indicated below:

ORGANIZATIONAL STRUCTURE
MAPFRE Board of Directors
MAPFRE Executive Committee
Corporate Security, Crisis and Resilience Committee
Corporate Privacy and Data Protection Committee
Corporate Security Department

2.2

Board of Directors of MAPFRE SA

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

2.3

MAPFRE Executive Committee

MAFPRE's Executive Committee, mandated by the Board of Directors, exercises direct oversight of Security management, embodying Senior Management's commitment to and support of the Security Function. This responsibility is exercised, within their respective spheres, by the Management Committees of the Group's various entities.

2.4

Corporate Security, Crisis and Resilience Committee

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

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

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

The composition of the Committee at the date of writing this document is as follows: its Chairman is the First Vice Chairman of the Board of Directors of MAPFRE SA* and the members are the top managers of the Territories/Regions (IBERIA*, INTERNATIONAL* and NORAM*), as well as those of the Corporate Areas of General Secretariat and Legal Affairs*, Finance and Media (Deputy CFO**), Operational Transformation**, People, Strategy and Sustainability**, External Relations and Communication**, Business**, Technology and Security, and the Director of Operational Resilience and GRC acts as its secretary.

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

** Member of the Executive Committee of MAPFRE SA.

2.5

Corporate Privacy and Data Protection Committee

A specific operational committee subordinate to the Corporate Security, Crisis, and Resilience Committee, for the management and control of privacy and personal data protection situations, in order to support the DPO in the performance of his or her duties.

2.6

Corporate Security Department

MAFPRE's Corporate Security Directorate (DCS) is the global body for the direction, planning and execution of the Corporate Security Function, in its different areas of action:

- **Security of People.**
- **Security of Facilities.**
- **Security of Information Systems (Cibersecurity).**
- **Personal Data Protection and Privacy.**
- **Operational Resiliencie: Crisis and Business Continuity Committee.**
- **Anti-fraud measures.**
- **Security Intelligence**
- **Regulatory compliance in the area of Security and Privacy and Operational Resiliencie.**
- **Third-party and supplier security risks.**

The DCS, in addition to being responsible for ensuring the security of the entire Group, provides service, operates common security systems and manages the demand of all MAPFRE Entities and Business Units.

2.7

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

TSI PROFESSIONAL: assessment and certification of high-availability data center infrastructures in accordance with the standard EN50600 and the Trusted Site Infrastructure (TSI) method.

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 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

CDPSE: Certified Data Privacy Solutions Engineer enables privacy technologists to demonstrate that they understand the technical aspects of creating and managing privacy programs to ensure compliance and mitigate risk.

CPCC: Certified Professional Cyber Compliance, del ISMS Forum, which accredits a high level of specialization in Spanish regulations regarding cybersecurity compliance.

CIPP:/E Certified Information Privacy Professional, recognized worldwide, developed by the International Association of Privacy Professionals (IAPP), which accredits global knowledge of data protection laws and regulations.

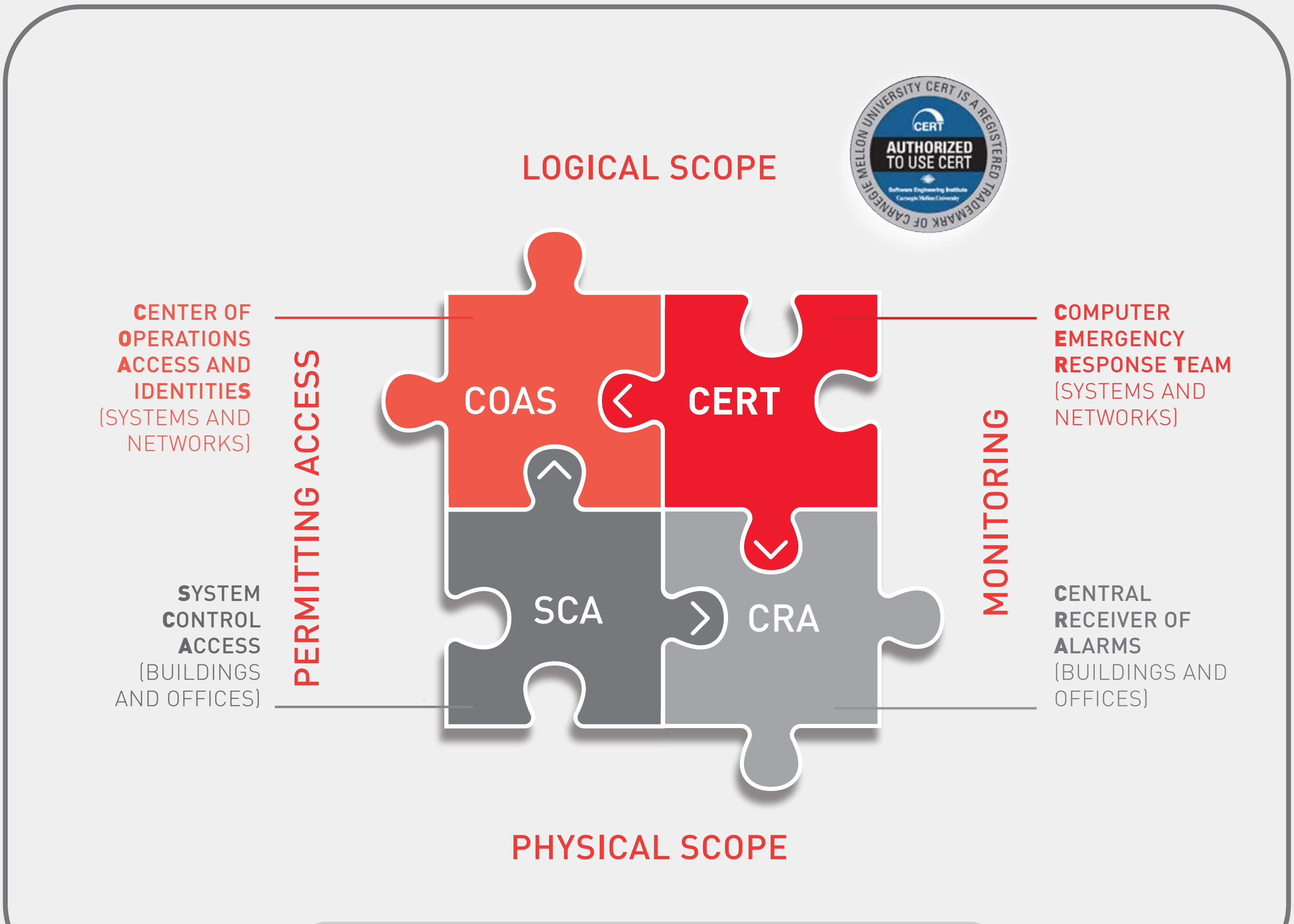
2.8

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 embodies MAPFRE's comprehensive security model, which is at its heart. It controls access to MAPFRE's Information Systems and facilities, monitors various physical and logical events and responds to security incidents of any kind.

The Global SOC is integrated into the **"Forum of Incident Response and Security Teams" (FIRST)** 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
CARNEGIE MELLON UNIVERSITY CERT IS A REGISTERED TRADEMARK OF CARNEGIE MELLON UNIVERSITY
CERT
AUTHORIZED TO USE CERT
Software Engineering Institute
Carnegie Mellon University
CENTER OF OPERATIONS ACCESS AND IDENTITIES (SYSTEMS AND NETWORKS)
PERMITTING ACCESS
COAS
CERT
COMPUTER EMERGENCY RESPONSE TEAM (SYSTEMS AND NETWORKS)
MONITORING
SYSTEM CONTROL ACCESS (BUILDINGS AND OFFICES)
SCA
CRA
CENTRAL RECEIVER OF ALARMS (BUILDINGS AND OFFICES)
PHYSICAL SCOPE

SEGURITY PLATFORMS OPERATIONS CENTER

(Operation of Systems and Security Tools)

The Global SOC is certified **in ISO 27001, ISO 22301,** and was the **first Spanish CERT to obtain ISO 9001 certification,** recognized by Gartner Group as a success story in the design, implementation and operation of a comprehensive security model.

ISO 9001 certification: Certifies effective management of SOC processes Helps to identify inefficiencies and improvement activities in a continuous improvement process and allows the satisfaction of client areas to be assessed.

ISO 27001 certification in Information Security accredits: Having a risk management model, controls in accordance with risk levels. The risk position of the organization and the suitability and effectiveness of the implemented controls are periodically evaluated.

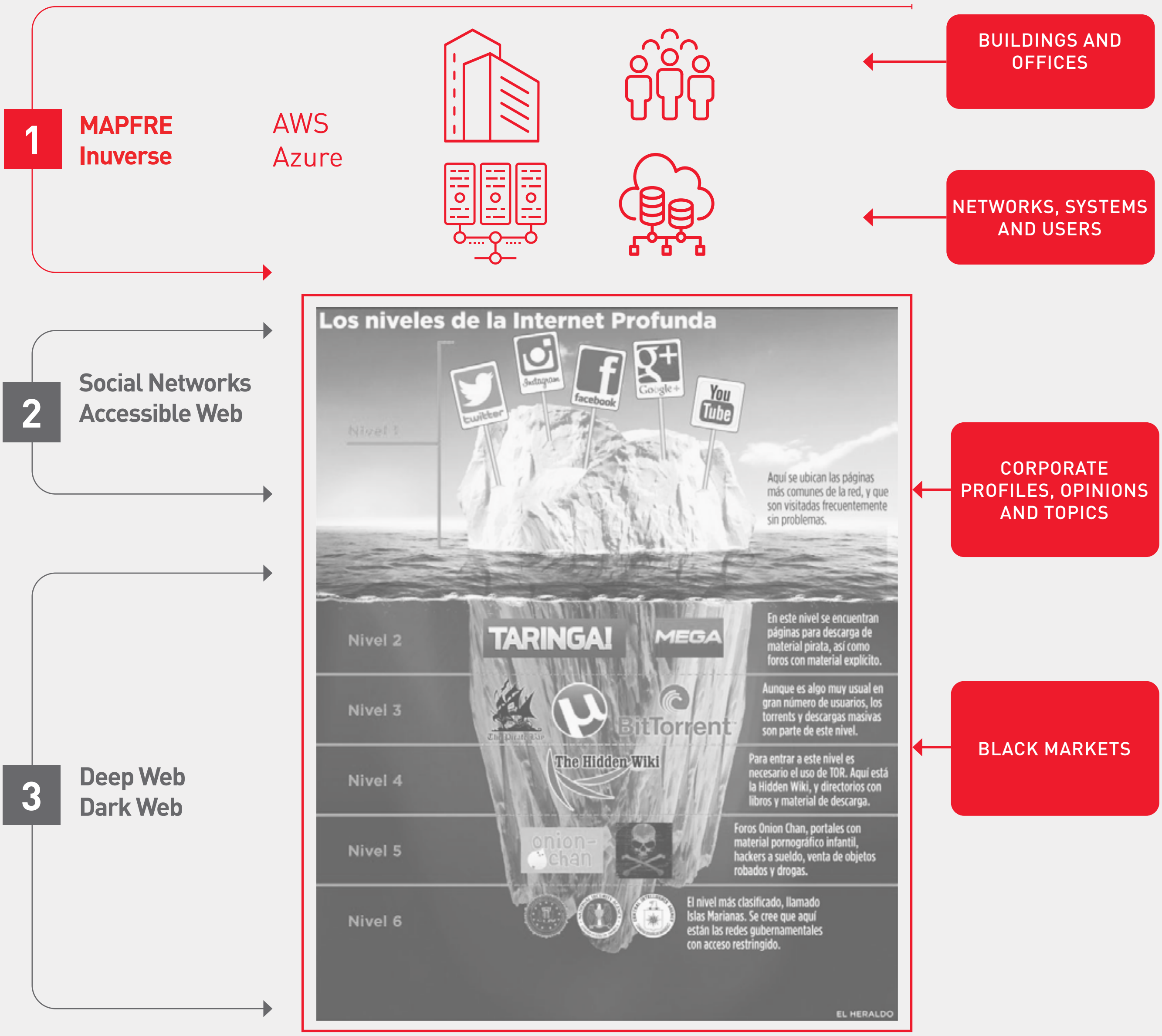
ISO 22301 certification in Business Continuity shows the ability to: Identify possible present and future risk scenarios Determine critical functions and reinforce their protection against possible emergency situations Enable service continuity in the event of unforeseen situations.

National SOC Network (RNSOC): In Q1 2023, MAPFRE was the first private entity (not a provider of ICT services to the Administration) to join the CCN-CERT's RNSOC. The RNSOC groups together 244 entities classified in two access levels, Gold and Silver. MAPFRE has been included as GOLD, once again being the first non-technological private company to achieve this.

The **Global SOC** monitors all network, system and user activity events generated in the technological areas in which MAPFRE is present. More than 4 billion events are managed daily and analysed by applying intelligence rules to generate alerts in the event of potential anomalous events.

The alerts generated are managed globally by specialised teams, in a 24x7x365 mode, in wich a rigorous process is applied for identification, analysis, evaluation, containment, resolution, escalated and registration of alerts.

The Global SOC monitors:



1 MAPFRE Inuverse

AWS
Azure

BUILDINGS AND OFFICES

NETWORKS, SYSTEMS AND USERS

2 Social Networks Accessible Web

3 Deep Web Dark Web

CORPORATE PROFILES, OPINIONS AND TOPICS

BLACK MARKETS

Los niveles de la Internet Profunda

Aquí se ubican las páginas más comunes de la red, y que son visitadas frecuentemente sin problemas.

En este nivel se encuentran páginas para descarga de material pirata, así como foros con material explícito.

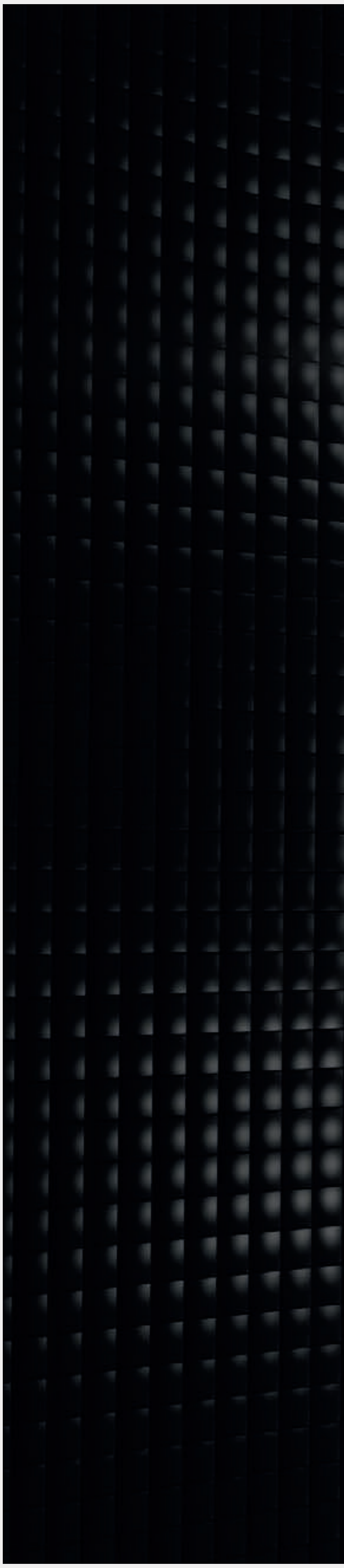
Aunque es algo muy usual en gran número de usuarios, los torrents y descargas masivas son parte de este nivel.

Para entrar a este nivel es necesario el uso de TOR. Aquí está la Hidden Wiki, y directorios con libros y material de descarga.

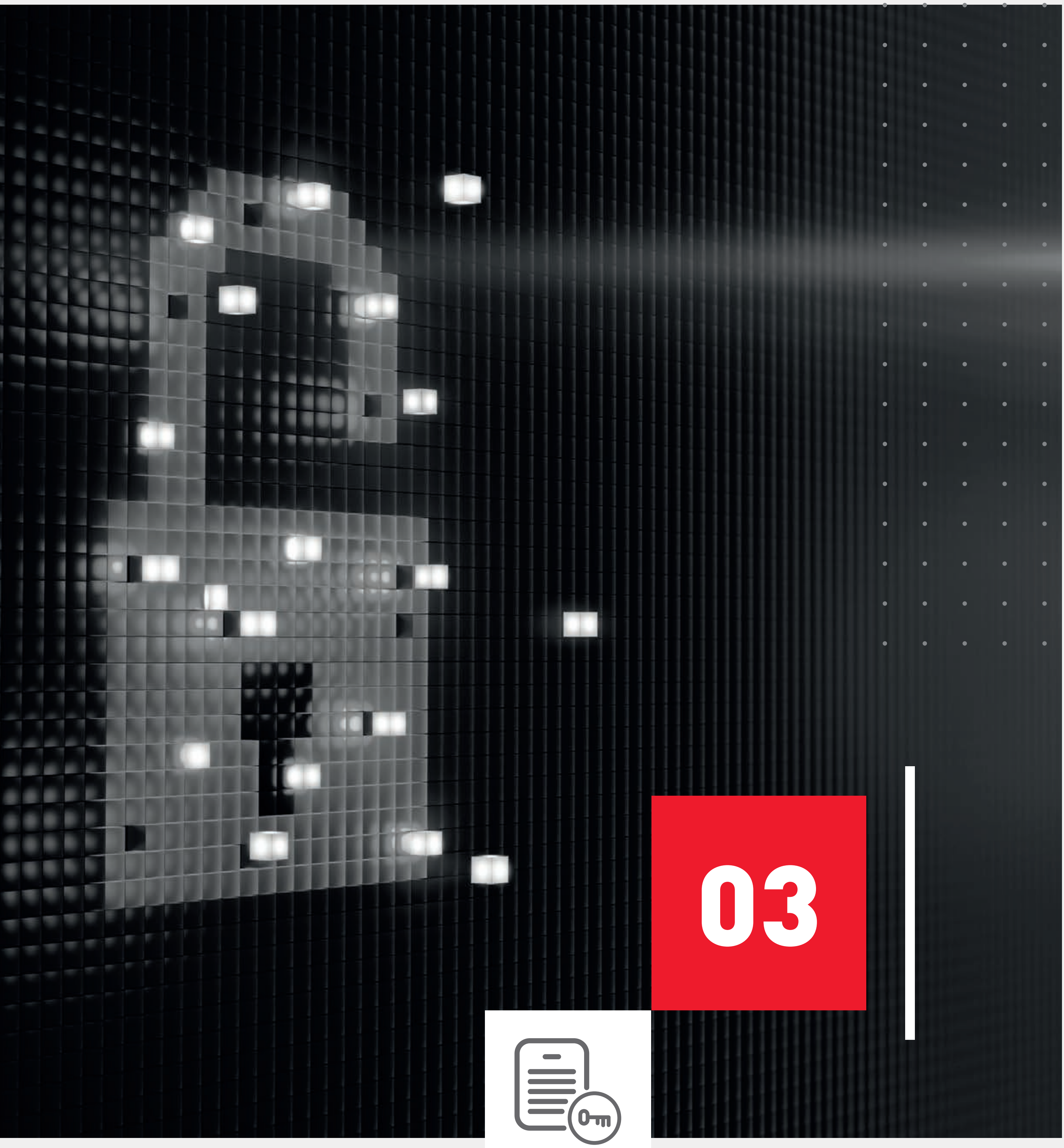
Foros Onion Chan, portales con material pornográfico infantil, hackers a sueldo, venta de objetos robados y drogas.

El nivel más clasificado, llamado Islas Marianas. Se cree que aquí están las redes gubernamentales con acceso restringido.

Security and Privacy Compilance



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



03

MAPFRE has created a Security Regulatory Body, based on ISO 27002, ISO 22301 and ISO 29100 standards and also enriched by other widely recognised industry standards, 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's entities participate.

The Regulatory Body, made up of more than 100 documents, is constantly adapting, as is MAPFRE, to the different legislations that appear in the countries where it operates.

With regard to compliance, special mention should be made of the applicable European Union Regulations, which MAPFRE assumes as reference standards for the entire Group:

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

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

- **Artificial Intelligence Regulation (RIA),** the project to adapt the Regulation is currently underway to ensure not only compliance with this legislation, but also to ensure the ethical and responsible use of AI Systems.

MAPFRE collaborates with public institutions and in sectoral forums, to enable both the most correct development and the most efficient implementation of the various legislations in this area, as well as the most appropriate compliance.

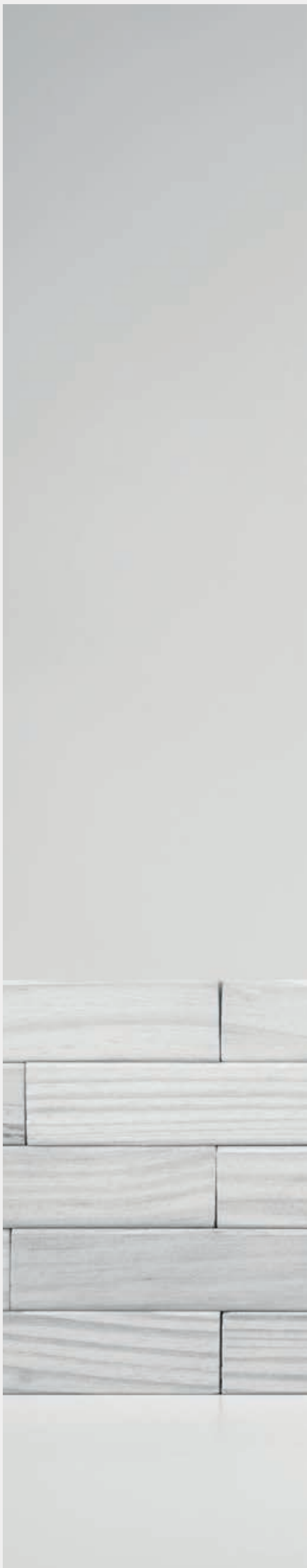
MAPFRE has a regulatory observatory and analyses the multiple pronouncements made by regulators in the countries in which it operates, with the aim of ensuring that, from the design stage, all processes comply at all times with the applicable security, privacy and data protection regulations..

As part of its third-party security risk management process, MAPFRE includes cybersecurity, privacy and operational resilience criteria in its purchasing processes for technological solutions and services, incorporating **security, data protection and operational resilience clauses** demanding compliance from all its collaborators, in order to ensure prudent and diligent behavior in the management of their security and the personal data entrusted to them.

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, privacy and operational resilience, 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

Risk Analysis:

MAPFRE's main establishments and facilities carry out regular security risk analyses that take into account all the threats that may occur in these spaces: natural risks, fire, those caused by uncontrolled access, theft or degradation of information stored on different media, the risks caused, etc. The appropriate protection measures are considered and established based on these.

Fire Protection:

MAPFRE's internal regulations establish requirements for fire protection in the facilities it occupies, whether or not they are its property, which entail, at a minimum, sufficient compliance with the applicable regulations, with special attention to those areas that are critical to the safety of people and the development of the business.
It is worth noting that MAPFRE, in its commitment to sustainability, uses clean, environmentally friendly agents in its extinguishing systems.

Self-Protection and Emergency Plans:

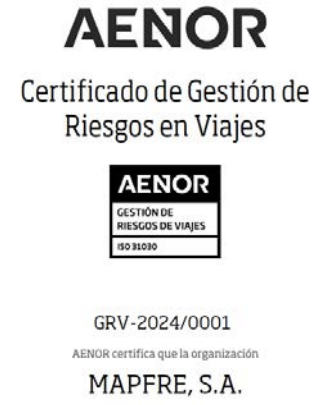
implemented and updated in all facilities where MAPFRE carries out its activity; adapted to the regulatory requirements established in each area, including the performance of drills with the frequency established by the regulations and, at least, once (1) a year. During 2024, more than 450 emergency drills were carried out at MAPFRE facilities.

Security in Travel and Events:

MAPFRE's commitment to the safety of its employees and collaborators also covers their travels. Employees have a complete system that protects them on trips abroad. This system analyzes future trips, identifies and evaluates the risks associated with them and contacts those travelers who assume greater risks in their travels, being monitored at all times from the Global SOC. In addition, travelers have a Self-Protection Guide, with safety advice for travel, as well as specific Safety Guides for trips to those destinations considered to be of medium or high risk. These guides contain information about the different areas of the country, useful contacts, including the SOC's permanent helpline, as well as safety advice on the country's risks.

In this regard, MAPFRE has obtained Travel Risk Management certification in accordance with the ISO 31030 standard "Travel risk management. Guidance for organizations" for the management of international travel originating in Spain for Group employees.

La certificación ISO 31030 es un ISO 31030 certification is a recognition of MAPFRE's advanced practices in managing travel-related risks, ensuring that Group employees have the best protection, security and support measures when travelling internationally.



AENOR

Certificado de Gestión de Riesgos en Viajes

AENOR
GESTIÓN DE RIESGOS DE VIAJES
ISO 31030

GRV-2024/0001

AENOR certifica que la organización

MAPFRE, S.A.

Security and Access Control Systems:

MAPFRE has physical access control systems, based on this prior risk analysis, video surveillance, alarm systems and/or security personnel for surveillance and monitoring of these systems. Those spaces whose integrity has a greater impact on the development of MAPFRE's activities and business have reinforced security measures, designed according to a model of tiered and in-depth defence.

MAPFRE's Global SOC continuously monitors and supervises these systems, which provides a fast and effective response in incident management. Most of the security systems installed are based on IP technology, on MAPFRE's own communication networks for exclusive use.

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

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.

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

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

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

*See chapter 11

0100010110 1
1000101011
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, for the management of the entities.
- Training and Awareness Plan, approved by the Corporate Security, Crisis and Resilience Committee.
- Crisis management drills and exercises for management committees and key personnel of the entities.

5.1

Identity Management

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

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

- Incorporation of Identity and Access Management in the application development life cycle.
- 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 that is reinforced by protection mechanisms against stolen identities and weak passwords.
- Advanced access protection based on behavioral analytics.
- Restriction between productive and non-productive environments regarding the use of identities and access.
- Periodic reviews of 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:

- Advanced anti-malware protection: Antivirus & EDR.
- Procedural and implemented vulnerability management system 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.
- Security breach simulation tool.

5.4

Cloud Security

MAPFRE is no stranger to digital transformation and, similar to what other companies are doing, has been including cloud technologies in its technological projects for years. MAPFRE only uses cloud providers that comply with the highest security standards, regulations, and certifications (including ISO 27001, ISO 27018, SOC 1, SOC 2, SOC 3, PCI-DSS, and GDPR).

MAPFRE's priority suppliers are:

Azure aws Google Cloud

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.
- Monitoring and response to incidents.

Cloud activity monitoring is one of MAPFRE's priority tasks. More than 500 million events generated in these clouds are monitored daily and analyzed using advanced information processing filters. All alerts and potential anomalies are managed by the Global SOC as one of its areas of action.

5.5

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.

In addition to the capabilities associated with the Technical Safety Review Reference Center, 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.

Each time a new vulnerability is identified or published, the cybersecurity team conducts an assessment based on its criticality and potential impact on MAPFRE systems, resulting in a classification. For the most critical vulnerabilities, an urgent procedure is activated to resolve them globally within 24 hours for all potentially affected information systems.

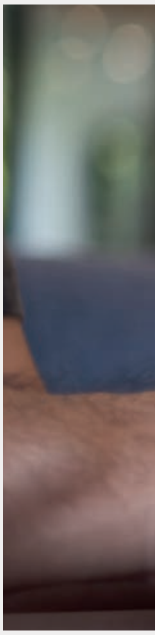
5.6

Monitoring and response to incidents

As previously indicated in this document, MAPFRE brings together the monitoring and response capabilities for Cybersecurity incidents in the GLobal 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).
- Regularly participation in CyberEx, cyber exercises organized by the National Cybersecurity Institute of Spain (INCIBE), in coordination with the Cybersecurity Office (OCC).
- Isolated laboratory for forensic analysis.

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



5.7

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.

Technical Security Reviews

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

06

6.1

Technical security reviews

With the objective that all the entities that make up the MAPFRE Group can benefit from the knowledge, experience, resources, infrastructure and tools that exist at the corporate level in terms of ethical hacking and security analysis, the Reference **Center for Technical Reviews of Security, made up of highly 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 said Center, both the DCS and the different entities of the MAPFRE Group have constant information on their level of security and vulnerability, both from the point of view of an internal and external attacker. This provides a global vision of the Group's security situation in this regard, allowing any vulnerability to be quickly detected and corrected.

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

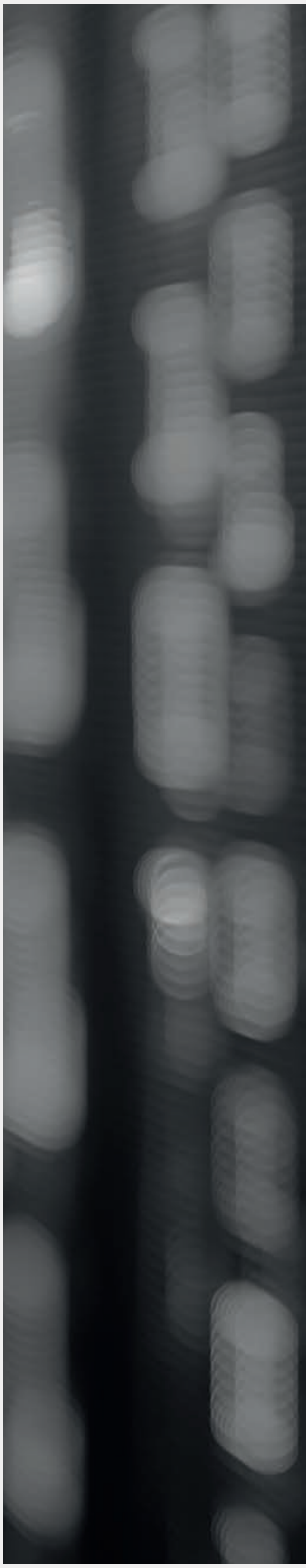
This review catalogue includes the **AUTOMATED CONTINUOUS REVIEW** process of the systems exposed to the Internet as well as the critical internal systems of all the company's entities, and allows for the detection of any new vulnerability in said systems.

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.

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

Corporate DataCenters

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



07

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.

CPD Alcalá de Henares (Madrid): Design, Facility
CPD Miami: Design, Facility
CPD Tamboré (Sao Paulo): Design, Facility and Operation

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.

CPD Miami
CPD Tamboré (Sao Paulo)

Certification of Conformity in the National Security Scheme (ENS), HIGH category, according to RD 311/2022

This certification implies that the data center meets the strictest security requirements established by the National Security Scheme of Spain, guaranteeing adequate protection of the information processed and the services provided.

CPD Alcalá de Henares (Madrid)

ISO 50001:2018 - Energy Management Systems
This certification ensures that the data center meets the highest standards of energy management and efficiency, optimizing energy use, reducing costs, and improving sustainability.

CPD Alcalá de Henares (Madrid)

HIPAA-HITECH
Ensures the protection of the confidentiality, integrity, and availability of electronic protected health information (ePHI). (USA)

CDP Miami

Operational Resiliencie: Crisis and Business Continuity Management

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

08

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:**

Business Continuity Policy

Governance and Specialized Organization Framework

Methodology

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 pandemics, 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 certification process for these plans in its different entities, and has now achieved that many of its entities: **MAPFRE España (incluida, MAPFRE VIDA), MAPFRE RE, MAPFRE USA, MAPFRE Global Risks, MAPFRE Inversión, MAPFRE México, MAPFRE Perú, MAPFRE Turquía, MAPFRE TECH, MAPFRE BHD (República Dominicana), MAPFRE Puerto Rico, MAPFRE Malta, MAPFRE Panamá, MAPFRE Portugal, MAPFRE Honduras, MAPFRE Costa Rica, MAPFRE Investimentos (Brasil), MAPFRE TECH and the MAPFRE Group's Global SOC**. are certified under ISO 22301, guaranteeing the continuous updating and improvement of these plans.

The Countries/Business Units that have Business Continuity Plans **certified under the ISO 22301** standard represent **77% of the total premiums** issued by the MAPFRE Group. This international standard certifies that certified entities have correctly implemented Business Continuity Management Systems (BCMS) designed to protect them from possible interruptions, guaranteeing their recovery with reasonable expectations of success in the face of different types of disasters and managing to maintain the continuity of their operations. Certified Businesses, guaranteeing their continuous updating and improvement.

AENOR

Certificado del Sistema de Gestión de la Continuidad del Negocio

SCN-2017/0006

MAPFRE ESPAÑA, S.A.

AENOR

Certificado del Sistema de Gestión de la Continuidad del Negocio

SCN-2017/0006

Anexo al Certificado

AENOR

Certificado del Sistema de Gestión de la Continuidad del Negocio

SCN-2018/0010

MAPFRE RE, COMPAÑÍA DE REASEGUROS, S.A.

AENOR

Certificado del Sistema de Gestión de la Continuidad del Negocio

SCN-2018/0007

MAPFRE GLOBAL RISKS, S.A.

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.

09

9.1 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** to support the DPO in the performance of his or her duties.

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.

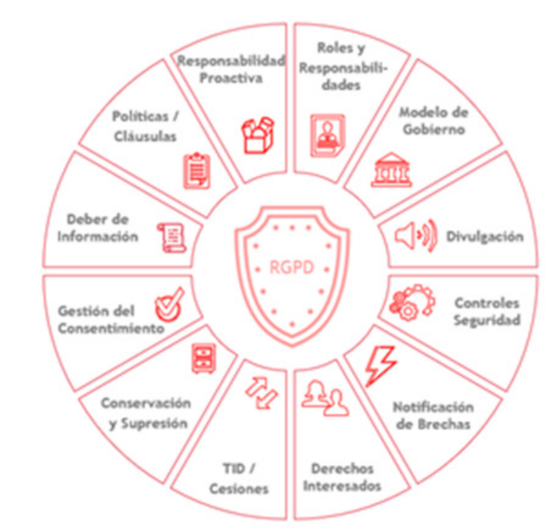
MAPFRE maintains a **transparent relationship with the Control Authorities,** facilitating close collaboration, cooperation and communication, in order to guarantee effective protection of the fundamental rights and freedoms of natural persons in relation to the processing of their personal data.

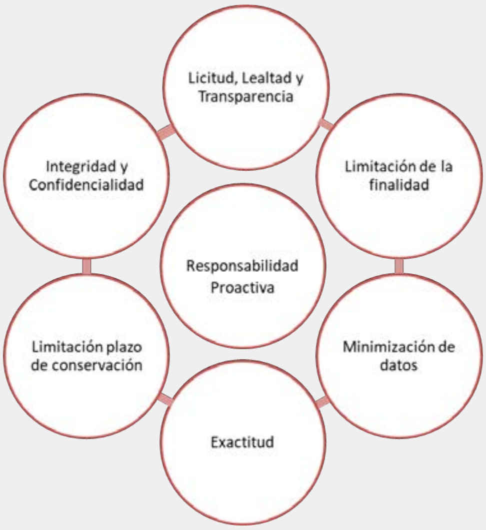
9.2

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.

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




Licitud, Lealtad y Transparencia
Integridad y Confidencialidad
Limitación de la finalidad
Responsabilidad Proactiva
Limitación plazo de conservación
Minimización de datos
Exactitud

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

» **Responsabilidad Proactiva:**

- **Early adaptation** to applicable privacy regulations in the different geographies in which it operates.

- **Implementation of appropriate technical and organizational measures in the company's processes,** not only to guarantee protection and compliance with applicable regulations, but also to demonstrate compliance to supervisory authorities and stakeholders.

- **Protection by design and by default: Integrating privacy into the lifecycle of any new initiative** that manages personal data, respecting the rules for the protection of fundamental rights and freedoms and implementing controls and measures designed to preserve the confidentiality, integrity and availability of the information handled and the systems that support it.

- **Risk Management.** Privacy impact assessment of new treatments. As well as, in the event of substantial changes that affect the treatment environment (their requirements and/or risks) or the security and privacy measures in place.

- **Privacy assessment in the purchasing processes** for 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 **Information Clauses** and management of consents in the collection of personal data.

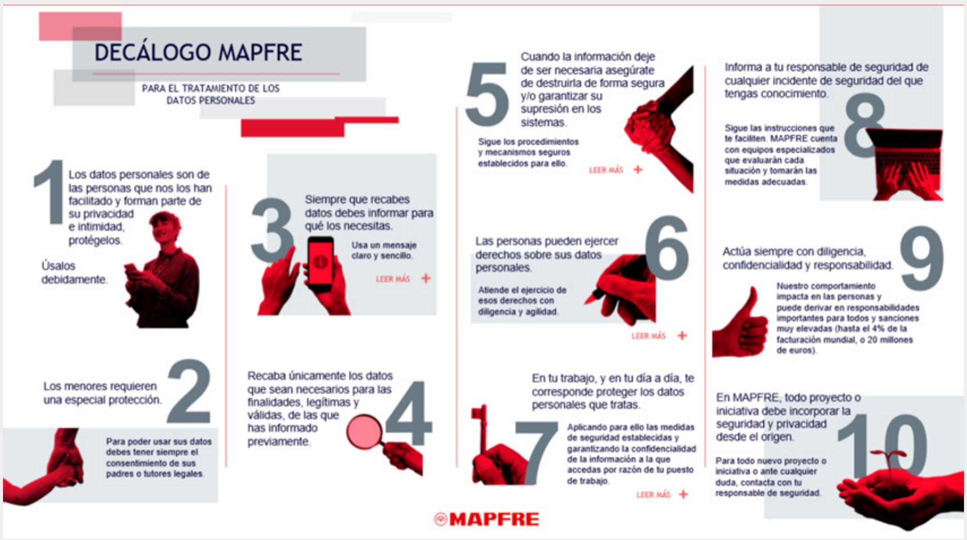
- **Inclusion of Privacy and Data Protection Clauses** in Service Provision Contracts, with those providers that handle or access information, to guarantee compliance with security and privacy obligations.

- Attention in a timely and appropriate manner to the exercise of the **Rights of Interested** parties, such as queries and/or complaints addressed to the Data Protection Officer.

- **Privacy Culture:** Specific Training and Awareness Plans on Privacy and Data Protection.

- **Promoting public-private collaboration.** Participation in associations that promote privacy and in sectoral and institutional initiatives aimed at clarifying the application of the GDPR, such as the DPO Forum or the DPO Community.

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.

LEER MÁS +

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.

LEER MÁS +

6 Las personas pueden ejercer derechos sobre sus datos personales.

Atiende el ejercicio de esos derechos con diligencia y agilidad.

LEER MÁS +

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.

LEER MÁS +

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

9.3

Binding Corporate Rules (BCR)

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

The BCR-C, after the **favorable opinion of the European Data Protection Committee (CEPD),** have been **approved by the Spanish Data Protection Agency (AEPD),** who has led the formal review and approval process, with the collaboration of the Correvisory Control Authorities and other EU control authorities for their assessment.

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

The Binding Corporate Rules demonstrate MAPFRE's commitment to Privacy (customers, suppliers, collaborators, employees and interest groups), accrediting to third parties compliance with the General Data Protection Regulation (GDPR) even in **MAPFRE entities located outside the EEA.** , and a homogeneous level of protection for your data regardless of the country in which it is hosted and the obligations required by local regulations when carrying out **international data transfers** between the entities of the MAPFRE Group.

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

» Spanish

https://www.mapfre.com/statics/bcrs-mapfre/Normas_Corporativas_Vinculantes.pdf

» English

https://www.mapfre.com/statics/bcrs-mapfre/Binding_Corporate_Rules_ENU.pdf

» Portuguese

https://www.mapfre.com/statics/bcrs-mapfre/Normas_Corporativas_Vinculantes_PTB.pdf

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.

10

MAPFRE is committed to making **Responsible and Ethical Use of Artificial Intelligence**, taking advantage of the opportunities offered by new technologies and complying with current legislation in the digital field, as set out in the Digital Governance Ethics Framework and in the Principles on the Responsible and Ethical Use of Artificial Intelligence established.

In addition, MAPFRE has a **Reference Framework** to implement a **governance model for the responsible use of AI,** with a human-centred approach, which allows for the definition of new responsibilities in the field of AI, and which have been reflected in the MAPFRE AI Manifesto.

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

Additionally, MAPFRE has a **multidisciplinary Working Group on the responsible use of Artificial Intelligence,** to manage issues related to ethics and data protection, streamlining processes, employee awareness and decision automation, and improving customer experience, with the aim of ensuring ethical and responsible use of data.

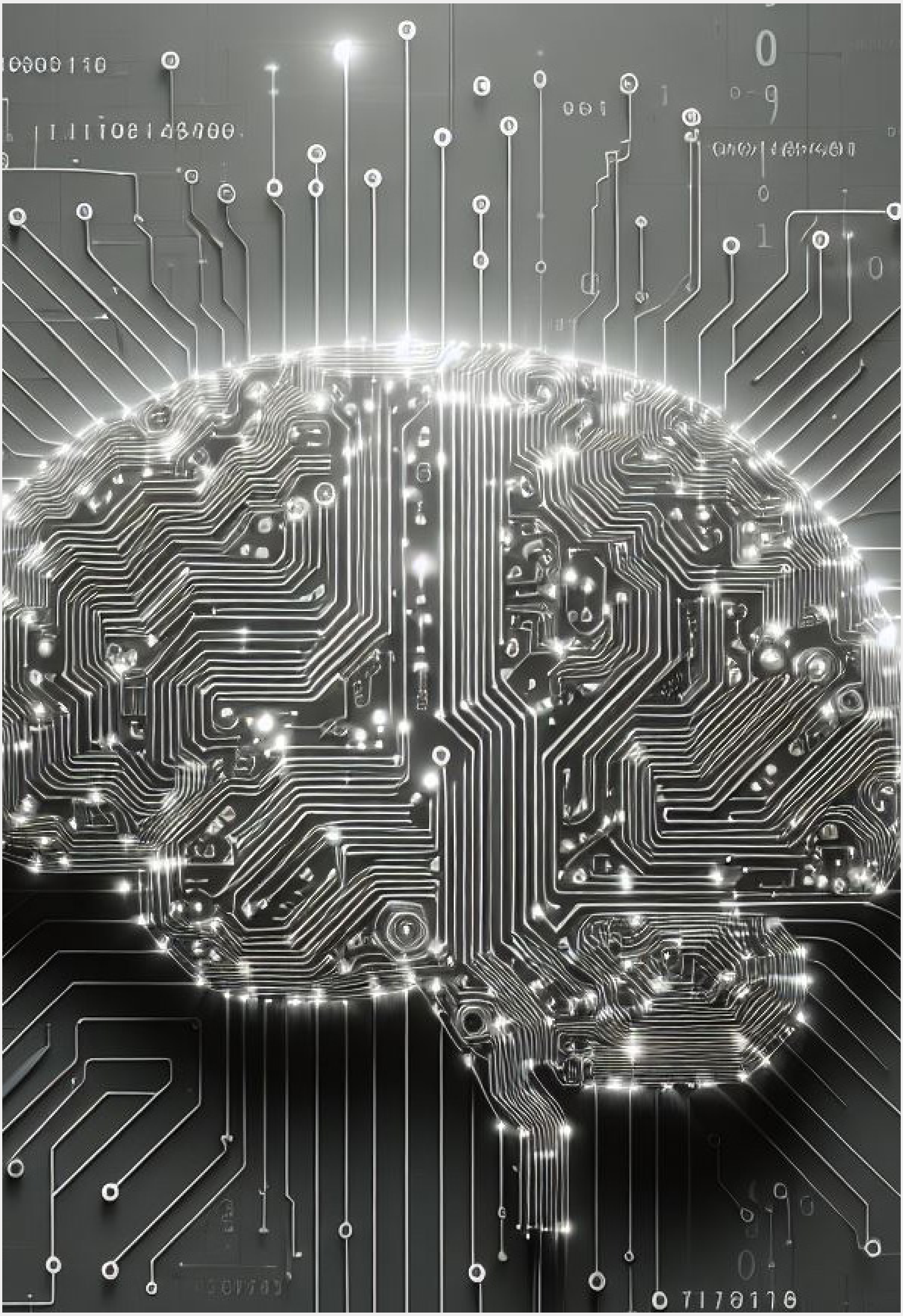
The result of this Working Group is the **'Guide to the Use of Artificial Intelligence Systems',** which establishes the guidelines and mechanisms necessary to determine the level of risk existing based on the use that will be given to them, as well as the measures necessary to mitigate the associated risks that arise from the use of this type of technology.

MAPFRE has been working for **some time on early adaptation to the applicable regulations** in this area of Artificial Intelligence and has **defined an Adaptation Plan** that brings together a series of projects and lines of work, the objective of which is to comply with the obligations required by regulators over the coming years.

Finally, it is worth mentioning MAPFRE's adherence to the **'Commitments to Privacy and Digital Ethics'** of the Cotec Foundation. This commitment 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 data-based applications, is becoming increasingly important.

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

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 Security culture constitutes a strategic requirement for the company.

11

MAPFRE has a **multidisciplinary Work 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 and Training Plan**, which is updated annually, and continuously adapts to the needs of the environment.

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

In line with MAPFRE's global and comprehensive vision of security, this plan contemplates **ICT security, privacy and data 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 **sensitization** 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.

In this sense, in the last three years, a total of **95,785 hours** have been allocated to security training. The number of MAPFRE workers trained between 2022 and 2024 amounts to **28,103**. At the end of the year, **92% of the staff** had received training in this area.

A systematic measurement is carried out on all of them, obtaining statistics and indicators that allow evaluating their effectiveness and the continuous improvement of the process.

Some examples of these actions are:

- **Regular publication of security news,** tips, videos, infographics, podcasts and other communication resources. During 2024, more than 38 security-related contents have been published.

- **Specific awareness-raising campaigns** for employees, using the "gamification" and "storytelling" technique.

- **Training pills** at the MAPFRE Corporate University, available to all employees.

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

- Specific awareness sessions aimed at **Senior Management and Independent Borad Members** of the Group.

- **Training** for Security personnel and Crisis management exercises.

- **Cyber exercises** with campaigns aimed at all employees, aimed at checking the effectiveness of training and awareness actions, as well as evaluating employee behavior in the face of the most common cyber attacks. In 2024, employees behaved appropriately in the exercises carried out in more than 94% of cases.

- **Cyberincident Management Drills,** implemented gradually with the Management Committees of the different Entities, constituted as Crisis Committees of the different entities of the Group.

Audits

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

12

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

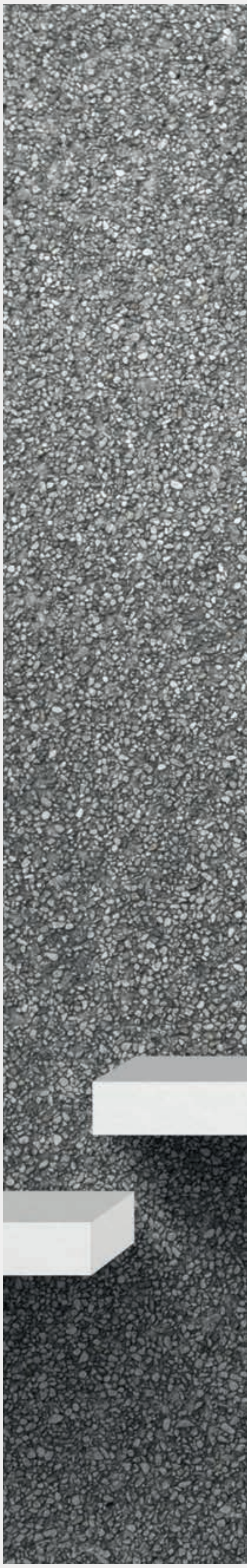
Additionally, within the **Technology and Security Internal Control Audit** Methodology developed at MAPFRE, a section is always included in the ICT Environment Control Area on compliance with the Security Regulatory Body and the legislation that affects these matters. including data protection.

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 2024, external and internal auditors have carried out **more than 124 audits** on, information systems and security, business continuity, cloud systems and artificial intelligence as well as privacy and data protection.

The year 2024, like previous years, closed without any overdue audit recommendations. The recommendations planned for the following years have been implemented or are in the process of being resolved, in accordance with the established action plans.

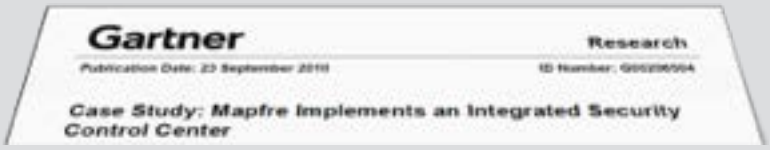
Acknowledgement and Benchmark from Thrid Parties



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:

13

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



Gartner Research

Publication Date: 23 September 2010 ID Number: G00206504

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.

Dirección General de la Guardia Civil

[illegible]

MAPFRE

PREMIO DUQUE DE AHUMADA a la EXCELENCIA en SEGURIDAD CORPORATIVA

[illegible]

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, MAPFRE's security model was 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 practical case within its Master in Cybersecurity.

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

BITSIGHT The Standard in SECURITY RATINGS	**MAPFRE Group Rating: 740 (Advanced Level):**
Dow Jones Sustainability Indexes	**100 points (out of 100) in Privacy Protection section.**
CNPIC incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD	**4.7 points (out of 5). Cyber Resilience Improvement Indicators - IMC. 2024.** • +0.4 points average financial sector.
DSN isms forum	**Cyber Crisis Management 2024.** • "Very Good" Maturity. • Above the average of the participating companies.

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

MAPFRE