v 1.9 Febrero 2024

Seguridad

Respaldando tu confianza

MAPFRE

ÍNDICE

Guillermo Llorente,
Director Corporativo de Seguridad de MAPFRE,

"Para MAPFRE las personas son el bien más importante y, por ello, nuestra principal misión es protegerlas, tanto a ellas mismas como a los datos que nos confían, garantizando el servicio que les prestamos y la confianza que depositan en nosotros.

Para lograrlo, se constituye la Función de Seguridad Corporativa, a fin de proteger los activos tangibles e intangibles de MAPFRE. Esta misión está recogida en el Plan Director de Seguridad que, con un enfoque basado en la gestión de riesgos, opera como Marco Estratégico y se constituye como punto de partida para la elaboración de las Políticas de Seguridad y Privacidad; y Continuidad de Negocio, así como para el desarrollo de la Normativa Interna asociada a las mismas. Todo ello dentro del más estricto respeto a la legalidad vigente y al Código Ético y de Conducta de MAPFRE.

La seguridad es parte integral de toda la organización y de su cultura y la visión de MAPFRE es que toda iniciativa nazca con la seguridad embebida. Por ello, para mantener la continuidad del servicio que prestamos y la privacidad de la información que se nos confía, la seguridad se integra desde el principio en el diseño de cualquier aplicación, servicio, dispositivo o nuevo edificio; en resumen, en todo nuevo proyecto que ponemos en marcha.

Para supervisar el normal desarrollo de nuestra actividad, MAPFRE dispone de un Centro de Operaciones de Seguridad (Global SOC), que forma parte de la red FIRST (Forum of Incident Response and Security Teams), desde donde se vigila y analiza la seguridad de las Redes y Sistemas de Información de MAPFRE en todo el mundo, y desde donde se coordina y lleva a cabo la respuesta a los incidentes de seguridad que pueda sufrir la compañía.

Para cuando todo ello no basta y se materializan ataques, aparecen graves crisis o catástrofes naturales, MAPFRE tiene desarrollados e implantados Planes de Gestión de Crisis y Continuidad de Negocio en sus entidades que son probados anualmente, y que tienen por objeto posibilitar la continuidad del servicio a nuestros clientes aún en las peores circunstancias.

En conclusión, la seguridad y la privacidad de nuestros clientes constituye un eje fundamental de la Política y de la vocación de servicio de MAPFRE. Es un Compromiso personal y colectivo.

Guillermo Llorente
Director Corporativo de Seguridad de MAPFRE

Visión y modelo de Seguridad

La aspiración de **liderazgo** de MAPFRE y su **carácter global** inspiran, como en el resto de las actividades del Grupo, las actuaciones en materia de Seguridad, ámbito en el que también pretende ser una referencia.

01

1.1

Visión de la Función de Seguridad en MAPFRE

La Función de Seguridad en MAPFRE es la encargada de proteger, dentro del más estricto respeto a la legalidad y a los principios éticos de MAPFRE, los activos tangibles e intangibles del Grupo, velando especialmente por el cumplimiento normativo y por la buena reputación de la compañía. **Contempla 5 principios fundamentales:**

Se define como Global e Integral,
protegiendo cualquier tipo de activo del Grupo en cualquier país del mundo frente a todas las amenazas de seguridad susceptibles de comprometer el mismo.

Tiene carácter Permanente y Sostenible, formando parte de la cultura y procesos corporativos y con el firme compromiso de ser medioambientalmente responsables.

Está orientada al Servicio, considerándolo un deber ineludible, en respuesta a la confianza depositada por nuestros clientes internos y externos.

Es Independiente de cualquier otra área de MAPFRE con la que pueda haber conflicto de interés, a fin de mantener el principio de segregación de funciones.

Debe aportar Valor, evolucionando en función de las estrategias y necesidades del Grupo y de sus clientes.

1.2

Modelo Integral de Seguridad

MAPFRE aplica un enfoque **holístico a la Seguridad,** integrando la gestión de todos los aspectos relacionados con la Seguridad de las personas y de sus activos, en una única Dirección Corporativa con presencia y ámbito de actuación global.

Las responsabilidades de la Dirección Corporativa de Seguridad (DCS) incluyen:

- **Seguridad de las Personas.**
- **Seguridad de las Instalaciones.**
- **Seguridad de los Sistemas de Información.**
- **Privacidad y Protección de datos personales.**
- **Gestión de Crisis y Continuidad del Negocio.**
- **Lucha contra el fraude.**
- **Cumplimiento Regulatorio en materia de Seguridad y Privacidad.**

Sobre este enfoque se ha construido el modelo para el desarrollo de la **Función de Seguridad.**

Dicho modelo está regido por el código ético de MAPFRE y basado en los estándares y mejores prácticas de la industria, como son, entre otros:

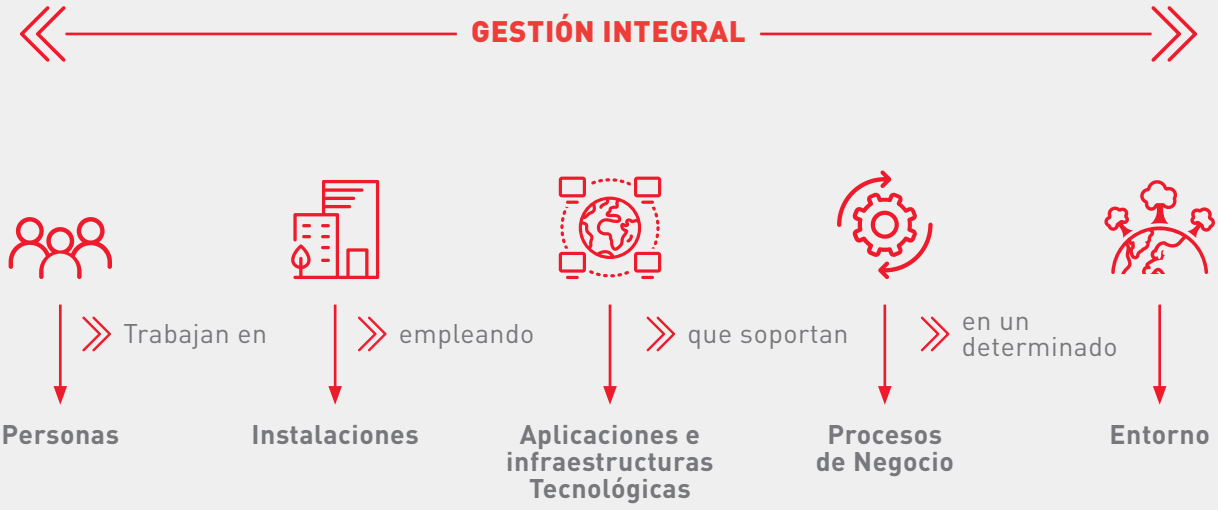
ISO 27001 y 27002 en Seguridad de Sistemas de Información

ISO 22301 de Continuidad de Negocio

ISO 14001, 14064, ISO 50001 y Reglamento Residuo Cero relacionados con la protección del Medio Ambiente

ISO 9001 de gestión de la calidad

ISO 29100 relativa a la protección de la privacidad



1.3

Marco de Gestión de la función de Seguridad

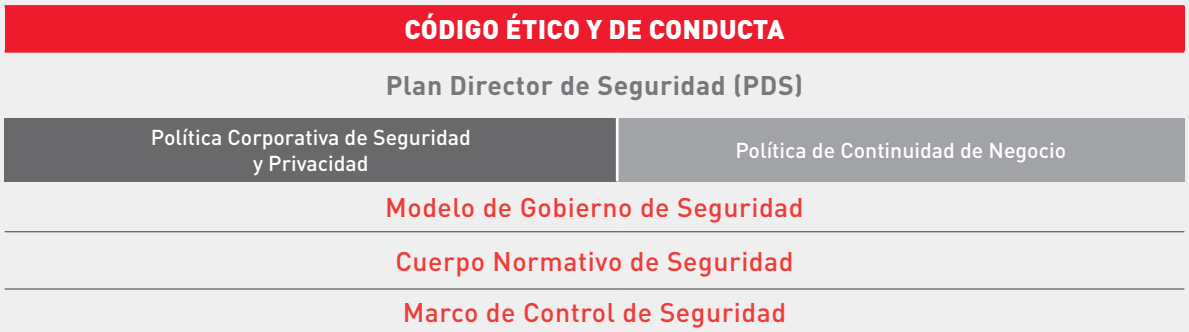
Reflejando los principios anteriormente citados, MAPFRE cuenta con un **Plan Director de Seguridad** que opera como Marco Estratégico, establece la misión y el modelo de gestión de la **Función de Seguridad** y, con una visión holística y un enfoque basado en la gestión de riesgos y en el código ético de MAPFRE, se constituye en punto de partida del que emanan las políticas y la normativa interna:

Política Corporativa de Seguridad y Privacidad y Política de Continuidad de Negocio, aprobadas por el Consejo de Administración de MAPFRE y de aplicación en todo el Grupo MAPFRE.

Modelo de Gobierno de Seguridad, que permite a MAPFRE dotarse de una Función de seguridad eficaz y eficiente.

El cuerpo normativo de Seguridad, desarrollado en más de 100 normas, estándares y procedimientos internos.

Marco de Control de Seguridad, que traduce, a nivel de controles, los diferentes requerimientos establecidos en el Marco de Gestión, que deben cumplir las Entidades y Unidades de Negocio de MAPFRE.



En los siguientes enlaces puede consultar el código ético y de conducta, así como las políticas corporativas en materia de Seguridad:

- **Código Ético y de Conducta**
  https://www.mapfre.com/media/sostenibilidad/2019/codigo-etico-2019.pdf
- **Política Corporativa de Seguridad y Privacidad**
  https://www.mapfre.com/media/accionistas/2015/politica-corporativa-seguridad-privada.pdf
- **Política de Continuidad de Negocio**
  https://www.mapfre.com/media/accionistas/2020/politica-de-continuidad-de-negocio-2019-12-13.pdf

1.4

Proceso de Mejora Continua de Seguridad

Para llevar a cabo su misión, la Seguridad en MAPFRE sigue un **proceso de mejora continua** que permite además alinear los planes y proyectos en este ámbito, con la Estrategia del Grupo y las necesidades de nuestros clientes.

Organización de Seguridad

El Gobierno de la Seguridad requiere una **Organización** que articule adecuadamente la Función y que esté alineada con la **dimensión global y la estructura organizativa** del Grupo MAPFRE.

02

2.1

Alcance Global

Nuestra concepción de la Seguridad como **ÚNICA** para todo MAPFRE y de carácter **INTEGRAL** frente a todos los tipos de amenazas en una entidad global como nuestro Grupo, implica contar con una **estructura de carácter bidimensional,** que permita dar una respuesta homogénea y coherente a los riesgos, tanto globales como locales.

Dimensión Global

- Protección contra amenazas globales.
- Cumplimiento regulatorio Global.
- Búsqueda y maximización de sinergias.
- Alineada a la Estrategia Global de MAPFRE.

Dimensión Específica

- Protección frente a amenazas locales.
- Cumplimiento regulatorio local.
- Comunicación con Cuerpos y Fuerzas de Seguridad locales.
- Capturando y adaptándose a las necesidades y hábitos/costumbres en cada entidad, país y mercado.

2.2

Comité Corporativo de Seguridad, Crisis y Resiliencia

En la cúspide de la organización de Seguridad en MAPFRE se encuentra el **Comité Corporativo de Seguridad, Crisis y Resiliencia.** Está compuesto por consejeros ejecutivos y altos directivos de la compañía y constituye el máximo órgano ejecutivo de la Fúnción de Seguridad.

Este Comité vela porque la actividad de la Función de Seguridad esté plenamente alineada e integrada en la estrategia corporativa y contribuya a la consecución de los objetivos de negocio. Al mismo tiempo, garantiza que la seguridad es contemplada como un elemento constituyente de los procesos de negocio y soporte corporativos.

De igual forma, en situación de Crisis, es el encargado de gestionar una respuesta adecuada que permita mantener el servicio a los clientes, aminorando las posibles consecuencias y velando por que se preservan los datos y las funciones esenciales en un proceso de mejora continua de las capacidades de resiliencia operativa de la compañía.

2.3

Equipo humano altamente cualificado

MAPFRE, a través del equipo de expertos altamente cualificados de la **Dirección Corporativa de Seguridad (DCS),** ha logrado dotarse de las mejores capacidades para cumplir su misión y atender un entorno cada vez más globalizado, complejo y exigente.

La **alta especialización y cualificación técnica** de nuestro personal destaca como parte fundamental de la contribución de valor a la compañía y a nuestros clientes, y ha sido motivo de reconocimiento por parte de autoridades públicas y privadas en numerosas ocasiones.

Esta alta especialización está acreditada por las más de **300 certificaciones** individuales en todas las disciplinas de Seguridad, Privacidad y Continuidad de Negocio, que posee el personal de la DCS, entre ellas, están las siguientes:

	DS: Director de Seguridad por Ministerio del Interior Español.
	CISA: Certified Information Systems Auditor es una certificación para auditores.
	CISM: Certified Information Security Manager es una certificación para el gobierno de la seguridad de la información que define las competencias necesarias para que un director de seguridad pueda dirigir, diseñar, revisar y asesorar un programa de seguridad de la información.
	CISSP: Certified Information Systems Security Professional es una certificación de alto nivel profesional con el objetivo de ayudar a las empresas a reconocer a los profesionales con formación en el área de seguridad de la información.
	CRISC: Certified in Risk and Information Systems Control, certificación de gestores de control de riesgos en sistemas de información.
	DPO: Delegado de Protección de Datos (Según RGPD)
	COBIT: Control Objectives for Information and Related Technology define un conjunto de procesos genéricos para la gestión de TI. El marco define cada proceso junto con los inputs y outputs del proceso, las actividades clave del proceso, los objetivos del proceso, las medidas de rendimiento y un modelo de madurez elemental.
	CSX: Fundamentals: Conceptos y funciones clave de la ciberseguridad.
	CSSLP: Certified Secure Software Lifecycle Professional reconoce las habilidades líderes en seguridad de aplicaciones. Muestra las habilidades técnicas avanzadas y el conocimiento necesario para la autenticación, autorización y auditoría utilizando las mejores prácticas, políticas y procedimientos.
	SSCP: Systems Security Certified Practitioner muestra las habilidades y conocimientos técnicos avanzados para implementar, supervisar y administrar la infraestructura de TI utilizando las mejores prácticas, políticas y procedimientos de seguridad.
	PMP: Project Management Professional certifica que se han alcanzado unos conocimientos y una experiencia relativa a la gestión de proyectos.

CHFI: Computer Hacking Forensic Investigator valida el conocimiento y las habilidades para detectar ataques de hacking, para obtener apropiadamente la evidencia necesaria para reportar el crimen y procesar al cibercriminal, y para conducir un análisis que le permita prevenir futuros ataques.

Certificaciones de CISCO: CCNP ,CCDP, CCNA, CCSA, CCENT, CCDA.

Certificaciones de MICROSOFT: MCP, MCSE, MCSA, MCSI.

CEH: Certified Ethical Hacker es una cualificación obtenida demostrando conocimientos de evaluación de la seguridad de los sistemas informáticos mediante la búsqueda de debilidades y vulnerabilidades en los sistemas de destino, utilizando los mismos conocimientos y herramientas que un hacker malicioso, pero de forma legal y legítima para evaluar la postura de seguridad de un sistema de destino.

Certificaciones de ITIL: 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 es la primera certificación española dirigida a los profesionales de la Privacidad. La obtención de esta certificación acredita un alto nivel de especialización en la normativa española en materia de Protección de Datos de carácter personal, tanto en un contexto local, como en un contexto europeo e internacional, así como un dominio de los fundamentos que rigen la Seguridad de la Información.

OSA: Operational Support and Analysis es una de las certificaciones en el flujo de trabajo de ITIL® Service Capability. El módulo se centra en la aplicación práctica para permitir la gestión de eventos, incidencias, peticiones, problemas, accesos, operaciones técnicas, TI y aplicaciones.

CND: Certified Network Defender Certification, es un programa de certificación que se centra en la creación de administradores de red capacitados para proteger, detectar y responder a las amenazas en la red.

CNDA: Certified Network Defense Architect está especialmente diseñado para Agencias Gubernamentales o Agencias Militares alrededor del mundo.

CSA: Certified Security Analyst: es un programa totalmente práctico con laboratorios y ejercicios que cubren escenarios del mundo real.

CSP: Certified Secure Programmer, un programador seguro es un profesional con habilidades esenciales y fundamentales para desarrollar aplicaciones seguras y robustas.

ISO 27001	**ISO** 27001 Foundations, **ISO** 27001 Lead Implementer, **ISO** 27001 Lead Auditor
Certified SCADA Security Architect	**SCADA:** Security Architect enseña cómo defender el Control de Supervisión y Adquisición de Datos (SCADA) y los Sistemas de Control Industrial (ICS) que administran las infraestructura críticas.
Certified Penetration Tester	**CWAPT:** Certified Web App Penetration Tester está diseñada para certificar que los candidatos tienen conocimientos y habilidades de trabajo en relación con el campo de las pruebas de penetración de aplicaciones web.
GIAC Certifications	**Certificaciones de GIAC:** GCIH, GSEC, GCFE, GCED
PCI DSS Certified	**PCI-DSS ISA:** Payment Card Industry Data Security Standard Internal Security Assessor enseña cómo realizar evaluaciones internas para su empresa y le recomienda soluciones para remediar problemas relacionados con el cumplimiento de PCI DSS.
PCI Security Standards Council	**PCIP:** Proporciona una cualificación individual para los profesionales del sector que deseen demostrar su experiencia profesional y su comprensión del Estándar de Seguridad de Datos PCI (PCI DSS).
Offensive Security OSCP	**OSCP:** Offensive Security Certified Professional es una certificación de hacking ético que enseña metodologías de pruebas de penetración y el uso de las herramientas incluidas en la distribución Kali Linux
Check Point Certified Security Expert CCSE	**CCSE:** Checkpoint Certified Security Expert, las competencias incluyen la configuración y gestión de VPN-1/FireWall-1 como solución de seguridad de Internet y red privada virtual (VPN), el uso de tecnologías de cifrado para implementar VPNs de acceso remoto y de sitio a sitio, y la configuración de la seguridad del contenido al permitir el bloqueo de Java y la comprobación antivirus.
Certified ISO 22301 Certified	**ISO** 22301 Foundations, **ISO** 22301 Lead Implementer, **ISO** 22301 Lead Auditor
BS25999 Lead Auditor	**BS** 25999 Lead Auditor

CRCM: Corporate Risk and Crisis Management ha sido diseñado para gerentes de seguridad, riesgos y crisis experimentados a los que se les ha encomendado la planificación y gestión de escenarios cada vez más complejos.

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: Técnico Superior en Prevención de Riesgos Laborales; TIPRL Técnico Intermedio en Prevención de Riesgos Laborales (experto).

PRINCE2: Practitioner: Projects IN Controlled Environments es un método estructurado de gestión de proyectos y un programa de certificación de profesionales.

CICA: Certified Internal Controls Auditor, revisión o evaluación de los controles y de los sistemas de control interno.

ICS-100 Incident Command System 100; **ICS**-200 Incident Command System 200; **ICS**-700 Incident Command System 700

LPIC-1 validará la capacidad para realizar tareas de mantenimiento en la línea de comandos, instalar y configurar un ordenador con Linux y configurar una red básica.

CFE Certified Fraud EXaminer: sus actividades incluyen la producción de información, herramientas y capacitación en materia de fraude.

CHS-II Certified in Homeland Security Level II: en el nivel II se ofrece un panorama general de las armas de destrucción en masa, el terrorismo propiamente dicho y las posibles armas que pueden utilizarse en caso de ataque.

OSHA: Occupational Safety and Health Administration

FES: Fire Extinguisher Safety

Bloodborne Pathogens: Certificación donde enseña a los profesionales qué hacer en caso de exposición a patógenos transmitidos por la sangre.

CFPS: Certified Fire Protection Specialist tiene el propósito de documentar la competencia y ofrecer reconocimiento profesional a las personas involucradas en la reducción de la pérdida por incendio, tanto física como financiera.

PSM: Professional Scrum Master I; PSPO Professional Scrum Product Owner I

EXIN Agile: Scrum Foundation ofrece a los profesionales una certificación única que combina principios ágiles y prácticas de scrum.

ISO 14001 Lead Auditor: permite desarrollar la experiencia necesaria para llevar a cabo una auditoría de Sistemas de Gestión Medioambiental (SGA) mediante la aplicación de principios, procedimientos y técnicas de auditoría ampliamente reconocidos.

ISO 50001 Lead Auditor: permite desarrollar la experiencia necesaria para llevar a cabo una auditoría de un Sistema de Gestión de Energía (SGMA) aplicando principios, procedimientos y técnicas de auditoría ampliamente reconocidos.

ATHE Level5: Award in Corporate Risk and Crisis Management.

CDPSE: Certified Data Privacy Solutions Engineer permite a los tecnólogos de la privacidad demostrar que comprenden los aspectos técnicos de la creación y gestión de programas de privacidad para garantizar el cumplimiento y mitigar el riesgo.

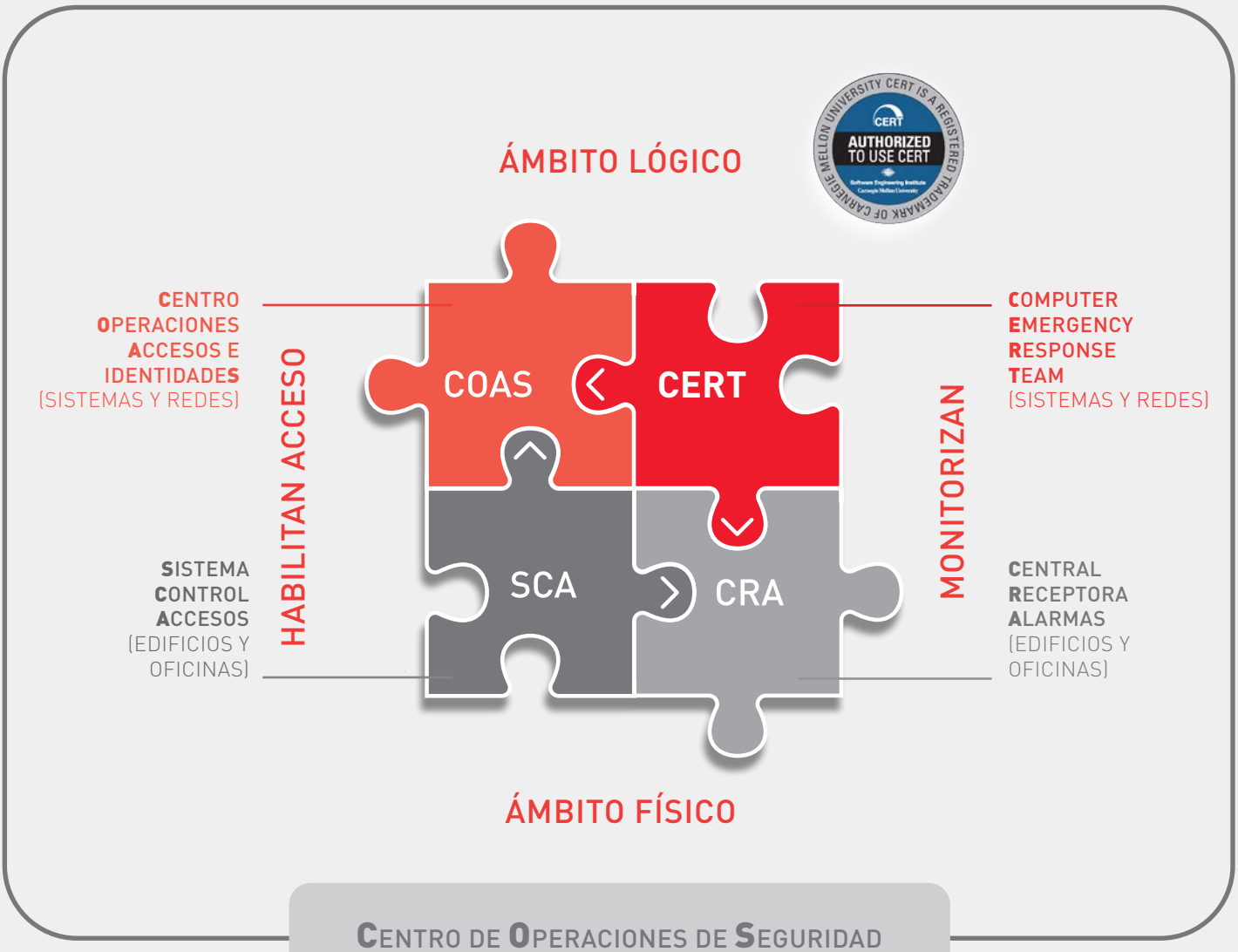
2.4

Centro de Operaciones de Seguridad Global (Global SOC)

El **Centro de Operaciones de Seguridad Global (Global SOC)** de MAPFRE es el órgano, certificado como **"Computer Emergency Response Team" (CERT),** que proporciona al Grupo capacidades de monitorización, gestión de identidades y control de acceso, y respuesta a incidentes a nivel Global.

En este órgano se plasma el modelo de seguridad integral de MAPFRE, controlándose el acceso a los Sistemas de Información y a las instalaciones de MAPFRE, monitorizándose los diferentes eventos tanto físicos como lógicos y respondiendo a incidentes de Seguridad de cualquier naturaleza.

El SOC está integrado en la red **"Forum of Incident Response and Security Teams" (FIRST)** y está en contacto permanente con los principales CERT privados y gubernamentales del mundo, así como en la Red Nacional de SOC's del CNN-CERT español, y forma parte de la red CSIRT.es, lo que facilita la colaboración y el intercambio de información entre centros de operaciones de ciberseguridad públicos de cara a la identificación de las amenazas y la respuesta temprana frente a eventuales incidentes.



Centro de Operaciones de Seguridad

(Operación de Sistemas y Herramientas de Seguridad)

El **SOC** está certificado en la **ISO 27001 y en la ISO 22301**, fue **el primer CERT español en obtener la certificación ISO 9001,** y ha sido reconocido por **Gartner Group como un caso de éxito** en el diseño, implantación y operación de un modelo de seguridad integral.

La certificación ISO 9001:

- Certifica una gestión eficaz de los procesos del SOC.
- Ayuda a identificar ineficiencias y actividades de mejora en un proceso de mejora continua.
- Permite valorar la satisfacción de las áreas cliente.

La certificación ISO 27001 en Seguridad de la Información acredita:

- Disponer de un modelo de gestión de riesgos.
- Disponer de unos controles acordes a los niveles de riesgo.
- Que se evalúa periódicamente:
  - La posición de riesgo de la organización.
  - La idoneidad y efectividad de los controles implantados.

La certificación ISO 22301 en Continuidad de Negocio muestra la capacidad de:

- Identificar posibles escenarios de riesgo presentes y futuros.
- Determinar las funciones críticas y reforzar su protección ante posibles situaciones de emergencia.
- Reaccionar para que la materialización de alguno de los escenarios de riesgo afecte lo menos posible al desarrollo de esas funciones críticas.
- Posibilitar la continuidad del servicio ante situaciones imprevistas, mejorando la ciber resiliencia de la organización y de los servicios que presta a sus clientes.

El **Global SOC** es el órgano donde se centraliza la gestión de incidentes de seguridad, mediante su identificación, análisis, evaluación, contención, resolución, comunicación y registro.

Desde el Global SOC se monitorizan:

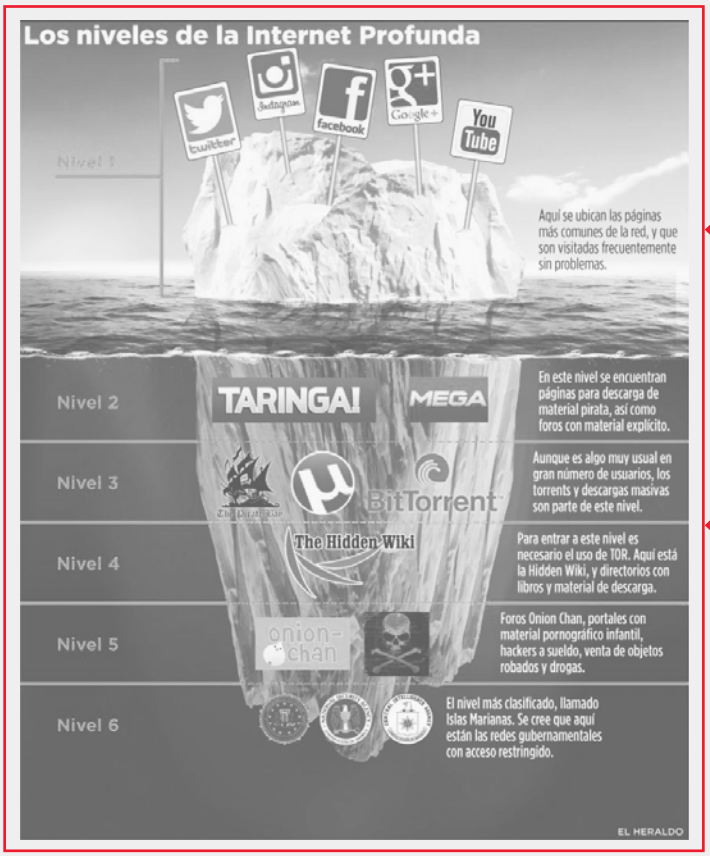
1 **Universo MAPFRE**

EDIFICIOS Y OFICINAS

REDES, SISTEMAS Y USUARIOS

2 **Redes Sociales Web Accesible**

3 **Deep Web Dark Web**



PERFILES CORPORATIVOS, OPINIONES Y TOPICS

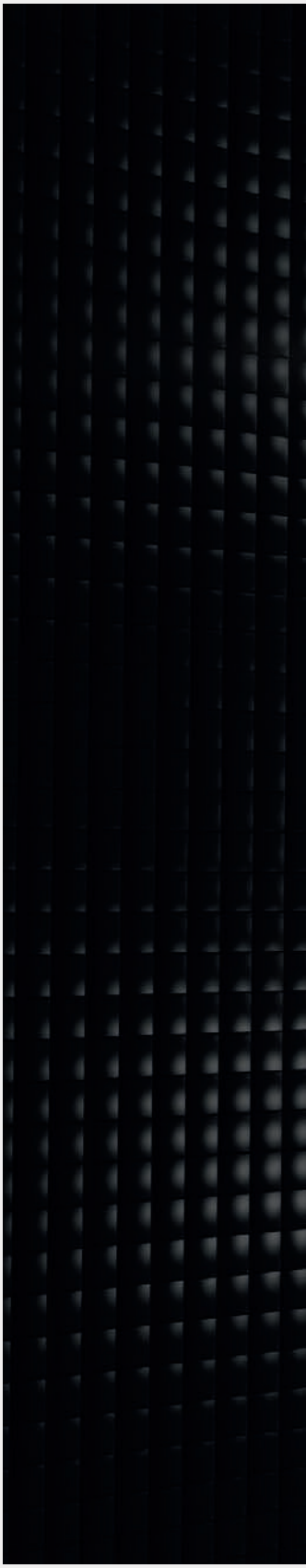
BLACK MARKETS

Red Nacional de SOC

- En Q1 de 2023 MAPFRE fue la primera entidad privada (no proveedora de servicios TIC a la Administración) en incorporarse a la RNSOC del CCN-CERT.
- La RNSOC agrupa 150 entidades clasificadas en 2 niveles de acceso, Gold e Informado, en base al grado de participación, valorando la cantidad y la calidad de información compartida.
- El nivel de acceso determina el decalaje con el que los participantes acceden a la información que el resto de participantes de la RNSOC pone en la red.

MAPFRE ha sido incluida como GOLD, siendo de nuevo la primera compañía privada no tecnológica en conseguirlo.

Cumplimiento en Materia de Seguridad y Privacidad



Los órganos de gobierno de MAPFRE han sentido desde siempre una especial preocupación por el buen gobierno corporativo, por lo que han ido adoptando un conjunto de principios y normas que rigen su actuación, entre los que se encuentra el cumplimiento estricto de las leyes y de sus obligaciones, así como de los buenos usos y prácticas de los sectores y territorios en que se desarrollan nuestras actividades.

03

MAPFRE se ha dotado de un Cuerpo Normativo de Seguridad, basado en las normas ISO 27002, ISO 22301 e ISO 29100 y que también se enriquece de otros estándares ampliamente reconocidos en la industria, como el Marco de Ciberseguridad NIST CSF o la normativa PCI-DSS. Este Cuerpo Normativo, es de obligada aplicación a todos los procesos y actividades en los que participan las entidades del Grupo.

Este Cuerpo Normativo, compuesto por más de 100 documentos, se va adaptando permanentemente, al igual que MAPFRE, a las distintas legislaciones que van apareciendo en los países donde opera.

MAPFRE colabora con instituciones públicas y en los foros sectoriales, a fin de posibilitar tanto el más correcto desarrollo, como la más eficiente implantación de las distintas legislaciones en la materia, así como el más adecuado cumplimiento.

Mención especial merece el **Reglamento General de Protección de Datos de la Unión Europea,** norma de referencia para MAPFRE en materia de privacidad, cuyo estricto cumplimiento constituye la garantía ofrecida a nuestros clientes de que haremos el adecuado uso de los datos personales que nos confían, garantizando su privacidad y confidencialidad.

MAPFRE está trabajando de manera proactiva para la adopción de los requisitos del **Reglamento sobre la Resiliencia Operativa Digital de la Unión Europea (DORA)**, de forma que se garantice que puede resistir y responder a cualquier tipo de perturbación y amenaza relacionada con las TIC y recuperarse de ellas.

Otra de las referencias fundamentales, son las **Guías editadas por la Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA)**, que recogen directrices sobre la Seguridad y el Gobierno de TIC y sobre la Gestión de la Externalización de Servicios Cloud.

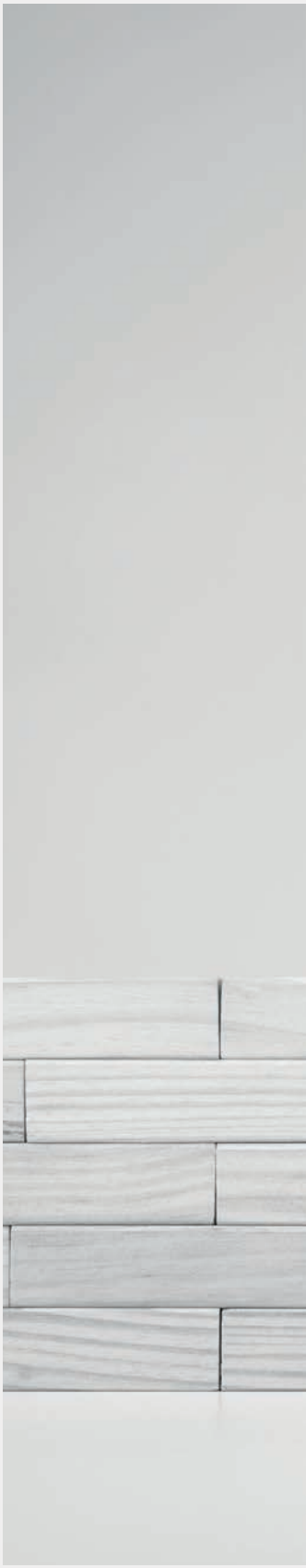
MAPFRE incorpora a todos sus contratos con terceros **cláusulas de seguridad y protección de datos,** exigiendo su cumplimiento a todos sus colaboradores, a fin de asegurar un comportamiento prudente y diligente en la gestión de su seguridad y de los datos personales.

MAPFRE dispone de un observatorio normativo y de análisis de los múltiples pronunciamientos por parte de los reguladores, de los países en que está presente, con el objetivo de garantizar que, desde el diseño, todos los procesos cumplen en todo momento con las normativas de privacidad y protección de datos que son de aplicación.

Por todo ello, podemos garantizar que MAPFRE cuenta con la normativa, procedimientos internos y **medidas de control necesarias para satisfacer los requisitos regulatorios y de nuestros clientes**, que le son de aplicación en materia de seguridad y privacidad, vigilando y monitorizando su cumplimiento en todos los niveles de la empresa mediante la implantación de los mecanismos exigidos por su propio cuerpo normativo.

Todas las consideraciones anteriores permiten poder transmitir firmemente la voluntad y capacidad de MAPFRE de **cumplir con los requisitos de seguridad y privacidad** exigidos por las legislaciones de todos los países donde opera.

Seguridad de personas e instalaciones



MAPFRE considera prioritario y objetivo irrenunciable, **la seguridad de todas las personas que se encuentran en sus instalaciones, ya sean empleados, clientes, proveedores o visitas**. En consecuencia, ha definido directrices e implantado procedimientos y herramientas para protegerlos.

04

Análisis de Riesgos:
Los principales establecimientos o instalaciones de MAPFRE cuentan con análisis periódicos de riesgos de seguridad que contemplan la totalidad de las amenazas que pueden materializarse en dichos espacios: de la naturaleza, medioambientales, de incendio, los originados por accesos no controlados, la sustracción o degradación de la información almacenada en diferentes soportes, los riesgos provocados, etc. En base a ellos se consideran y establecen las medidas de protección.

Protección contra Incendios:
La normativa interna de MAPFRE establece unos requisitos en cuanto a la protección contra incendios de las instalaciones que ocupa, sean o no de su propiedad, que suponen, como mínimo, el cumplimiento con suficiencia de la reglamentación aplicable, con especial atención a aquellas zonas críticas para la seguridad de las personas y el desarrollo del negocio. Destacar que MAPFRE, en su compromiso con la sostenibilidad, utiliza en sus sistemas de extinción agentes limpios respetuosos con el Medio Ambiente.

Planes de Autoprotección y Emergencia:
implantados y actualizados en todas las instalaciones donde MAPFRE lleva a cabo su actividad; adaptados a las exigencias normativas establecidas en cada ámbito, incluyendo la realización de simulacros con la periodicidad que la normativa establece y, al menos, una (1) vez al año.

Seguridad en Viajes y Eventos:
El compromiso de MAPFRE con la seguridad de sus empleados y colaboradores abarca también sus desplazamientos. Los empleados disponen de una Guía de Autoprotección, con consejos de seguridad para los viajes, así como de Guías específicas de Seguridad para viajes a aquellos países considerados de riesgo medio o alto, donde además su viaje es monitorizado desde el Global SOC. Dichas guías contienen información sobre las distintas zonas del país, contactos útiles, entre ellos el teléfono de atención permanente del SOC, así como consejos de seguridad sobre los riesgos del país.

Sistemas de Seguridad y Control de Accesos: como respuesta a los riesgos identificados, tanto en edificios como en oficinas, MAPFRE dispone de sistemas de control de acceso físico y donde procede, en función de ese análisis de riesgo previo, video-vigilancia, sistemas de alarma y/o personal de seguridad. Aquellos espacios cuya integridad tiene mayor incidencia en el desarrollo de las actividades y negocio de MAPFRE, disponen de medidas reforzadas de seguridad, diseñadas según un modelo de defensa escalonada y en profundidad.

El Global SOC de MAPFRE monitoriza y supervisa de forma continua estos sistemas, lo que aporta rapidez y efectividad de respuesta en la gestión de incidentes. La mayor parte de los sistemas de seguridad instalados están basados en tecnología IP, sobre redes de comunicación propias de uso exclusivo de MAPFRE.

Estas medidas son, además, reforzadas por simulacros y actividades de formación y sensibilización, que se realizan de forma periódica y sistemática.

CiberSeguridad

MAPFRE ha establecido un modelo de prevención y protección en materia de **CiberSeguridad** articulado sobre los siguientes pilares:

La arquitectura de seguridad tecnológica, a través de la cual se crean los cimientos de la ciberseguridad en la empresa, mediante la selección de las mejores soluciones para cada uno de los ámbitos.

La integración de la seguridad desde el inicio en todas las nuevas iniciativas: la construcción de nuevas soluciones, la contratación de nuevos servicios, etc. En otras palabras, integrar la Ciberseguridad en el negocio constituye un requisito básico de calidad de todos los procesos de MAPFRE.

Una gestión proactiva del riesgo de terceros, aplicando metodologías específicas para comprobar que tienen el adecuado nivel de seguridad y verificar que los riesgos derivados del servicio que prestan están controlados

La sensibilización a todo el personal de MAPFRE en materia de Seguridad y la capacitación específica del personal crítico, así como de aquellos que pueden tener acceso a información de terceros, a los que se brinda un servicio (clientes) o que lo proporciona (proveedores).

05

TECNOLOGÍA

- Definición línea base Seguridad Cyber.
- Herramientas específicas: lo mejor del Mercado.
- Búsqueda del valor añadido.

CIBERSEGURIDAD Y PRIVACIDAD
"desde la cuna hasta la tumba"

- Integradas desde el diseño y por defecto en todas las iniciativas de negocio.
- Incluidas en la construcción y adquisición de soluciones y servicios, así como en el establecimiento de acuerdos con terceros.
- Evaluando el impacto en la privacidad de los nuevos tratamientos e implantando controles y medidas al respecto

RIESGO DE SEGURIDAD DE TERCEROS

- Abarcando el ciclo de vida de nuestra relación con terceros: homologación, licitación/contratación, ejecución del contrato y finalización.
- Nivel de exigencia asociado al riesgo para MAPFRE que supone la actividad prestada.
- Uso de Sellos de Confianza (LEET Security) y herramientas de calificación para evaluar el nivel de seguridad del tercero.

CULTURA

- Concienciación para empleados, clientes y grupos de interés.
- Formación específica para el personal crítico.
- Entrenamiento para personal de Seguridad y ejercicios de gestión de Crisis.

5.1

Gestión de Identidades

MAPFRE considera crítico gestionar de una forma segura los accesos sobre los distintos activos de la organización, estableciendo procesos de Gestión de Identidades y Accesos para cada colectivo de usuarios (empleados, colaboradores, mediadores...) que permitan identificar quién ha accedido a qué y con qué permisos.

Los principios que rigen estos procesos de Gestión de Identidades son los siguientes:

- **Establecimiento de un identificador único e inmutable** para cada usuario que requiera de acceso a los sistemas de información de la compañía.
- **Definición de un identificador de usuario específico** para aquellas cuentas que requieren de elevación de permisos (administradores, automatismos, etc.).
- **Control de accesos gestionado y controlado por seguridad**, en base a matrices de autorización y una adecuada segregación de funciones.
- **Utilización de Múltiple Factor de Autenticación (MFA)** para accesos especialmente sensibles y, en especial, para cualquier tipo de acceso remoto.
- **Definición de una política de contraseñas robusta.**
- **Protección avanzada de accesos basada en analítica de comportamiento.**
- **Incorporación de la Gestión de Identidades y Accesos** en el ciclo de vida de desarrollo de las aplicaciones.
- **Restricción entre entornos productivos y no productivos** respecto al uso de las identidades y los accesos.
- **Revisiones periódicas de seguridad** de las cuentas y permisos asignados a los usuarios.
- **Control exhaustivo y revisión continua de las actividades de usuarios especialmente privilegiados en entornos críticos.**

Los procesos de Gestión de Identidades gobernados por la DCS están engarzados con el resto de controles de seguridad, siendo operados tanto de manera automática a través de los Sistemas de Gestión de Identidades Corporativos, como desde los Centros de Operación manual, integrados en el SOC.

5.2

Seguridad en redes

MAPFRE basa la **protección de las redes** en un modelo de segregación y localización de recursos en diferentes capas. Al mismo tiempo, se aplican diferentes soluciones de seguridad en red, por ejemplo:

- **Doble nivel de Firewall.**
- **IDS/IPS para la detección y bloqueo de patrones de ataque.**
- **Segregación de VLANs.**
- **Aislamiento físico y/o lógico entre entidades.**
- **Utilización de Múltiple Factor de Autenticación (MFA) para accesos externos.**
- **Conexión a terceros aislada.**
- **Diferentes Proveedores de Servicios.**
- **Protección anti ataques de denegación de servicio distribuidos (DDoS)**
- **Tecnologías WAF y balanceadores de carga.**
- **Secure Web Gateway y DLP en la conexión a internet Secure Web Gateway y DLP en el correo electrónico, etc.**
- **Seguridad a nivel de DNS.**

5.3

Seguridad en dispositivos (puestos informáticos, servidores y móviles)

Al igual que en caso anterior, MAPFRE utiliza distintos procedimientos y soluciones de seguridad para proteger los dispositivos utilizados, así como la información que contienen, como son:

- **Protección antimalware avanzada: Antivirus & EDR.**
- **Sistema procedimentado e implantado de gestión de vulnerabilidades y parches asociados.**
- **Cifrado de la información.**
- **Bastionados del dispositivo.**
- **Inventario, gestión y monitorización de la seguridad del dispositivo.**
- **Mobile Device Management para dispositivos móviles y tablets, etc.**
- **Restricción de acceso a los puertos USB en los equipos de los usuarios.**

5.4

Seguridad en la Nube

MAPFRE no es ajena a la transformación digital y, de forma análoga a lo que están haciendo otras compañías, está incluyendo las tecnologías de nube en sus proyectos tecnológicos. MAPFRE únicamente utiliza proveedores de nube que cumplen con los más altos estándares, normativas y certificaciones de seguridad (entre otros: ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, PCI-DSS o GDPR).

De manera adicional, las distintas iniciativas en nube deben tener como mínimo los mismos controles de seguridad que los existentes en los centros de proceso de datos corporativos, no debiendo suponer en modo alguno una disminución del nivel de seguridad previamente existente.

Muestra de los controles de seguridad utilizados para conseguir lo descrito anteriormente son:

- **Arquitecturas de Seguridad para los principales proveedores de IaaS.**
- **Adaptación de los controles de seguridad actuales.**
- **Cloud Access Security Broker (CASB).**
- **Cloud Security Posture Management (CSPM).**
- **Cloud Workload Protection Platform (CWPP).**
- **Control del Shadow IT, etc.**

5.5

Revisiones técnicas de seguridad

Con el objetivo de que todas las entidades que conforman el Grupo MAPFRE puedan beneficiarse del conocimiento, experiencia, recursos, infraestructura y herramientas existentes a nivel corporativo en materia de hacking ético y análisis de seguridad, se ha constituido el **Centro de Referencia de Revisiones Técnicas de Seguridad, formado por personal**, servicios y herramientas de una muy alta especialización.

CENTRO DE REFERENCIA DE REVISIONES TÉCNICAS DE SEGURIDAD

Información	Recursos	Personas
Marco Documental y de Gobierno	Laboratorio de Revisiones Técnicas	Equipo de Revisiones Técnicas

A través de los servicios prestados por dicho Centro, tanto la DCS como las diferentes entidades del Grupo MAPFRE disponen de información constante sobre su nivel de seguridad y vulnerabilidad, tanto desde el punto de vista de un atacante interno como externo. Con ello se logra una visión global de la situación de seguridad del Grupo en este aspecto.

Del mismo modo, este centro realiza las revisiones de seguridad de la capa tecnológica de las nuevas iniciativas de la compañía, previamente a su puesta en producción.

Consecuencia de ello, MAPFRE es capaz de aplicar un amplio catálogo de revisiones técnicas de seguridad, que velan por la protección de la información corporativa y de nuestros clientes. Como, por ejemplo:

TIPOS DE REVISIÓN	
A las Nuevas Iniciativas	Revisiones de Código Fuente
	Pruebas de Seguridad
	Pruebas de Cumplimiento
A la Infraestructura Externa (Publicada en Internet)	Pruebas de Intrusión Externas
	Escaneo Externo de Vulnerabilidades / ASV
A la Infraestructura Interna	Pruebas de Intrusión Internas (Incluyendo pruebas de segmentación y controles de reducción del ámbito)
	Escaneo Interno de Vulnerabilidades
	Revisión de Aplicaciones de especial relevancia
	Revisiones de Infraestructura Corporativa

Este catálogo de revisiones incluye el proceso de **revisión continua y automatizada de los sistemas expuestos a internet así como los sistemas internos de carácter crítico,** de todas las entidades de la compañía, y permite detectar cualquier nueva vulnerabilidad en dichos sistemas.

Indicar también que a través de este Centro de Referencia se articulan las revisiones de tipo **Red Team** llevadas a cabo contra los Sistemas de Información ubicados en nuestros Data Centers, así como el resto de **CiberEjercicios** destinados a evaluar tanto nuestras capacidades de protección, detección y respuesta, como la sensibilización en materia de Seguridad de nuestros empleados.

Los resultados de este conjunto de revisiones se integran en el Sistema de gestión de vulnerabilidades y parches antes mencionado y motivan el desarrollo de unos planes de "remediación" sujetos a plazos concretos, realizándose a su vez un seguimiento continuo de la corrección de las vulnerabilidades previamente detectadas y del cumplimiento de los plazos de resolución establecidos.

5.6

Gestión de vulnerabilidades y parches

Uno de los procesos de seguridad clave para garantizar un nivel adecuado de protección de cualquier sistema de información, tiene que ver con el parcheado de sistemas y la resolución de vulnerabilidades de manera efectiva y en los plazos apropiados.

MAPFRE dispone de un proceso de gestión de vulnerabilidades y parches, formalizado, implantado y maduro, que abarca desde la identificación temprana de las mismas hasta la certificación de su resolución por parte de equipos especializados. Este proceso asegura que los sistemas de información se actualizan de forma periódica y sistemática con los últimos parches liberados por los fabricantes de software.

MAPFRE dispone de acuerdos de soporte con los principales fabricantes de tecnología para la notificación temprana de vulnerabilidades y realiza un seguimiento continuo de cualquier vulnerabilidad que pueda afectar a la tecnología utilizada en nuestros sistemas de información. Asimismo MAPFRE participa en las principales asociaciones de CERT/SOC, donde se intercambia información sobre vulnerabilidades, en particular de Zero Day.

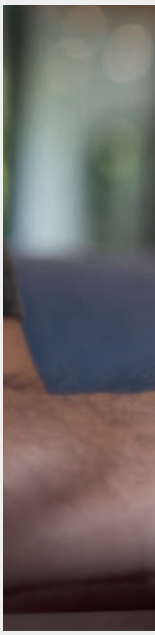
Cada vez que se publica una nueva vulnerabilidad, el equipo de ciberseguridad realiza una evaluación atendiendo a la criticidad e impacto en los sistemas de MAPFRE, dando como resultado una clasificación la misma. Para las vulnerabilidades de la más alta criticidad, se activa un procedimiento urgente con el fin de resolverlas, a nivel global, en menos de 24 horas en todos los sistemas de información que puedan estar afectados.

5.7

Monitorización y respuesta a incidentes

Como se ha indicado anteriormente en este documento, MAPFRE aglutina en el GLobal SOC las capacidades de monitorización y respuesta a incidentes de **CiberSeguridad,** operando como:

- SOC con personal dedicado en las instalaciones de MAPFRE, con disponibilidad permanente (en formato 24x7x365).
- SOC global de seguridad estratificado en 3 niveles de actuación con capacidad y autonomía para la respuesta inmediata frente a las amenazas.
- Sistema de recolección automática de amenazas basado en MISP.
- Sistema de Orquestación y automatización de operación de seguridad.
- Sistemas de monitorización de seguridad con ingesta de más de 3.000 millones de eventos diarios monitorizados.
- Escenarios específicos de monitorización para entornos críticos.
- Conectado a diferentes grupos y redes de colaboración de ámbito nacional e internacional (First, CSIRT, FS-ISAC, Red Nacional de SOC's).
- Participa de manera habitual en CyberEx, ciberejercicios organizados por el Instituto Nacional de Ciberseguridad de España (INCIBE), en coordinación con la Oficina de Diberseguridad (OCC).
- Laboratorio aislado para el análisis forense.



La alta capacitación de las personas, las herramientas y procedimientos implantados, así como la red de contactos con organizaciones de similar naturaleza en el ámbito público y privado, posibilitan a MAPFRE llevar a cabo la detección y respuesta temprana a cualquier incidente de ciberseguridad.

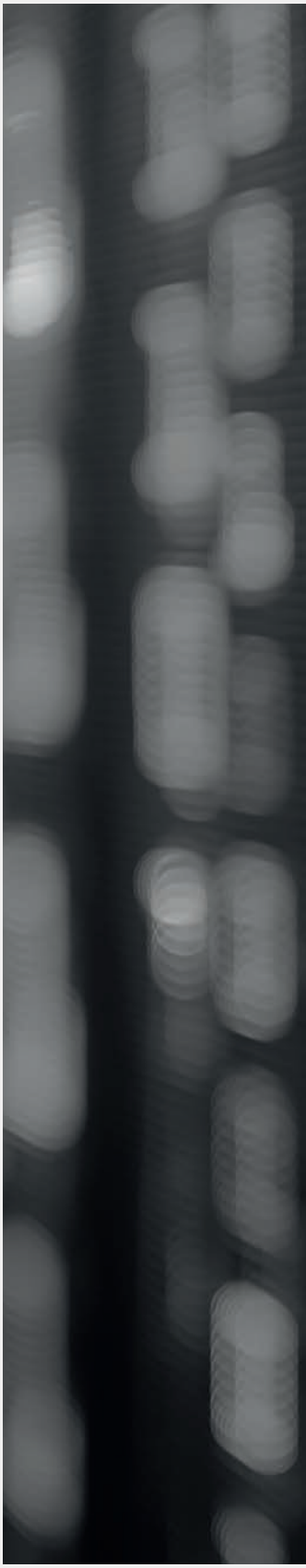
5.8

CiberSeguros

Las entidades del Grupo MAPFRE disponen de aseguramiento específico en materia de **CiberRiesgos,** que incluye tanto los daños propios como las eventuales responsabilidades frente a terceros en el caso de materializarse este tipo de eventos. En términos de coberturas y límites asegurados, la protección contratada es coherente y adecuada al riesgo, la actividad y el tamaño de una compañía como la nuestra.

Datacenters corporativos

MAPFRE cuenta con **Centros de Proceso de Datos (CPD)** corporativos de primer nivel que cumplen con los más altos estándares de la industria, tanto en la capacidad y funcionalidad de la infraestructura como en la calidad de su operación. En este sentido, a continuación se enumeran algunas de las certificaciones con las que cuentan los DataCenters corporativos de MAPFRE.



06

TIER III en diseño y operación
Un datacenter Tier III ofrece una disponibilidad del 99,98%. Esta configuración permite programar periodos de mantenimiento en los servidores sin que afecten a la continuidad del servicio.

CPD Alcalá de Henares (Madrid): Diseño y Construcción
CPD Miami: Diseño
CPD Tamboré (Sao Paulo): Diseño, Construcción y Operación

SSAE 18 (Statement on Standards for Attestation Engagements).

ISAE 3402 (International Standard for Assurance Engagements), Permiten asegurar que los controles relativos a preservar la seguridad y confidencialidad de la información son adecuados.

CPD Miami: SOC 1 tipo 2 y SOC 2 tipo 2
CPD Tamboré (Sao Paulo): SOC 1 Tipo 2

ISO 27001: Gestión de la Seguridad de la Información
Se garantiza que en los datacenters se cumplen los requisitos necesarios para establecer, implantar, mantener y realimentar un sistema de gestión basado en un ciclo de mejora continua.

CPD Alcalá de Henares (Madrid): Sistemas para Control de Accesos a Instalaciones y redes, Monitorización de Redes y Sistemas de Alarma
CPD Miami
CPD Tamboré (Sao Paulo)

PCI-DSS Collocation
Los datacenter cumplen con los requisitos asociados a la seguridad de acceso físico, así como al mantenimiento de una política de seguridad de la información, lo que proporciona un entorno PCI compliant.

CPD Alcalá de Henares (Madrid)

HIPAA-HITECH
Garantiza la protección de la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida (ePHI). (USA)

CDP Miami

Certificación PCI DSS e-commerce. Recientemente MAPFRE España ha conseguido dicha certificación para todos sus e-commerce.

La certificación PCI DSS acredita que cumplimos con las medidas establecidas por el PCI SSC (Payment Card Industry Security Standards Council), que definen los requisitos necesarios para garantizar que los datos de tarjetas son procesados con las máximas garantías de seguridad.

Esta certificación acredita que todos los portales web de MAPFRE España que permiten compras online, cumplen con todas las medidas de seguridad necesarias para garantizar el adecuado nivel de seguridad cuando se procesan los datos de tarjeta de nuestros clientes.

Gestión de Crisis y Continuidad de Negocio

La misión de la Función de Seguridad Corporativa es posibilitar el normal desarrollo del negocio, facilitando un entorno seguro en el que MAPFRE pueda desarrollar sus actividades. Para preservar el servicio proporcionado a nuestros clientes durante una situación de crisis o contingencia, MAPFRE cuenta con un **Modelo corporativo de Continuidad de Negocio,** integrado en su enfoque global de la Seguridad.

07

Este modelo está basado en la **ISO 22301,** responde a la dimensión internacional del Grupo MAPFRE y se ha desplegado en todas las entidades del mismo, atendiendo a las necesidades de negocio y a los requisitos particulares de cada Filial.

El modelo corporativo está compuesto por **tres grandes bloques:**

Modelo de Continuidad de Negocio del Grupo MAPFRE

Es en su Política de Continuidad de Negocio Corporativa, donde MAPFRE se compromete con esta función y define el marco para el desarrollo, implantación, revisión y mejora de Planes de Continuidad de Negocio, de manera que éstos:

- Posibiliten una respuesta adecuada y oportuna ante la materialización de un riesgo de seguridad (o de cualquier otra naturaleza) de características catastróficas, que provoquen un escenario de falta de disponibilidad de alguno de los componentes básicos de nuestra actividad: personas, instalaciones, tecnología, información y proveedores.
- Minimicen la repercusión de las posibles catástrofes sobre las actividades de negocio: preservando los datos y garantizando el uso de las funciones esenciales. Si no fuese posible, faciliten que se recuperen progresivamente hasta la vuelta a la normalidad.

Como segundo elemento, MAPFRE cuenta con **PERSONAL altamente cualificado** en esta materia y un **MARCO DE GOBIERNO** donde se determinan los diferentes órganos y funciones asociados con la continuidad dentro del Grupo (Unidades, Entidades, Centros).

Asimismo, dispone de una **METODOLOGÍA** que permite definir y desarrollar de manera homogénea y eficiente en forma de Planes de Continuidad de Negocio, mecanismos, procedimientos y estrategias para restaurar recursos y servicios.

Estos **Planes de Continuidad de Negocio están desarrollados, implantados y se prueban al menos una vez al año,** en todas las entidades de MAPFRE, habiéndose demostrado de forma reiterada su correcto funcionamiento en las catástrofes naturales y situaciones de indisponibilidad que han padecido las distintas entidades de MAPFRE por todo el mundo, como huracanes, grandes nevadas, incendios, caídas de comunicaciones, etc.

Especial atención requieren en este contexto, pues son pilar básico de los Planes de Continuidad Negocio, los **Planes de Recuperación ante Desastre (PRD,s)** o de Contingencia Informática que están implantados en los Data Center corporativos, a fin de garantizar la permanente disponibilidad de los servicios que desde ellos se prestan. Estos PRD,s son probados de forma sistemática, al menos anualmente, en todas las entidades, incorporando, en cada ocasión, un mayor nivel de exigencia a dichas pruebas.

Adicionalmente, MAPFRE ha optado por un proceso progresivo de certificación de estos planes en sus diferentes entidades, habiendo logrado que, en la actualidad, muchas de sus entidades: **MAPFRE ESPAÑA, MAPFRE VIDA, MAPFRE PORTUGAL, MAPFRE MEXICO, MAPFRE PUERTO RICO, MAPFRE BHD, MAPFRE RE, MAPFRE GLOBAL RISK, MAPFRE INVERSION, MAPFRE TURQUÍA, MAPFRE PANAMÁ, MAPFRE COSTA RICA, MAPFRE HONDURAS, MAPFRE INVESTIMENTOS y MAPFRE TECH.** están certificadas en la ISO 22301 garantizando la actualización y mejora continua de estos planes.


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.

Privacidad y Protección de datos personales

MAPFRE tiene como prioridad absoluta la privacidad y la protección de los datos de carácter personal a los que tiene acceso en el ejercicio de su actividad, entendiendo esto como un elemento esencial que debe perseguirse de manera proactiva, no sólo con el objetivo de lograr el cumplimiento de las normativas de aplicación, sino como justa correspondencia a la confianza depositada por clientes, proveedores, colaboradores, empleados y resto de grupos de interés.

08

8.1 Data Protection Officer

MAPFRE dispone de un **Data Protection Officer Corporativo y un área específica** dentro de la Dirección Corporativa de Seguridad encargada de velar por el cumplimiento de las regulaciones existentes en materia de **privacidad y protección de datos** de carácter personal.

Dentro de esta área y como apoyo al Data Protection Officer Corporativo, se constituye la **Oficina Corporativa de Privacidad y Protección de Datos (OCPPD)**, cuya misión es ser el punto de referencia de todas las actividades relacionadas con la privacidad y la protección de datos en MAPFRE, aportando una visión única y global de la materia, y fomentando la homogeneidad de todos los procesos y criterios relacionados con esta.

Adicionalmente, MAPFRE cuenta con un **Comité Corporativo de Privacidad y Protección de Datos**, para la dirección y control de los distintos proyectos relacionados con la privacidad y protección de datos de carácter personal, con el fin de apoyar al DPO en el desarrollo de sus funciones. Adicionalmente, este comité ejercerá sus funciones de apoyo al Comité Corporativo de Seguridad, Crisis y Resiliencia en lo relativo a la gestión de incidentes y violaciones de seguridad de datos personales, incluyendo la coordinación, el seguimiento y toma de decisiones, y la notificación a la Autoridad de Control y/o Afectados.

En los distintos países donde están presentes las entidades de seguros del Grupo y donde la legislación requiere de dicha figura, dispone de Data Protection Officer Locales, y de Comités de Privacidad y Protección de Datos Locales, con dependencia funcional del corporativo. En aquellos países donde, por el tamaño de la entidad o negocio, no se nombre un DPO específico, existe una figura responsable de privacidad y protección de datos, que se relaciona con su DPO correspondiente.

MAPFRE mantiene una relación transparente con las Autoridades de Control, facilitando una estrecha colaboración, cooperación y comunicación, con el fin de garantizar una protección efectiva de los derechos fundamentales y libertades de las personas físicas en relación con el tratamiento de sus datos de carácter personal.

8.2

Marco de Referencia de Privacidad

MAPFRE ha asumido **el Reglamento General de Protección de Datos de la Unión Europea** (RGPD) como marco de referencia en materia de Privacidad y Protección de Datos.

Para su implantación y gestión, este modelo de referencia, se articula en una serie de líneas estratégicas:

- Adecuación temprana a la regulación de aplicación en materia de privacidad en las diferentes geografías en las que opera.
- Integración de la Privacidad en el ciclo de vida de cualquier nueva iniciativa que gestione datos personales garantizando su protección desde el diseño y por defecto, incluyendo la realización de análisis de impacto en la privacidad de los nuevos tratamientos.
- Implantación de controles destinados a preservar la confidencialidad, integridad y disponibilidad de la información que se maneja y de los sistemas de que la soportan.

- Evaluación de privacidad en los procesos de compra de soluciones tecnológicas y en la contratación de servicios tecnológicos.

- Inclusión de las cláusulas informativas y gestión de los consentimientos en la recogida de datos personales.

- Inclusión de Cláusulas de Privacidad y Protección de datos en los Contratos de Prestación de Servicios, con aquellos proveedores que manejen o accedan a información, para garantizar el cumplimiento de las obligaciones de seguridad y privacidad.

- Atención en plazo y forma al ejercicio de los derechos de los interesados, como las consultas y/o reclamaciones dirigidas al Delegado de Protección de Datos.

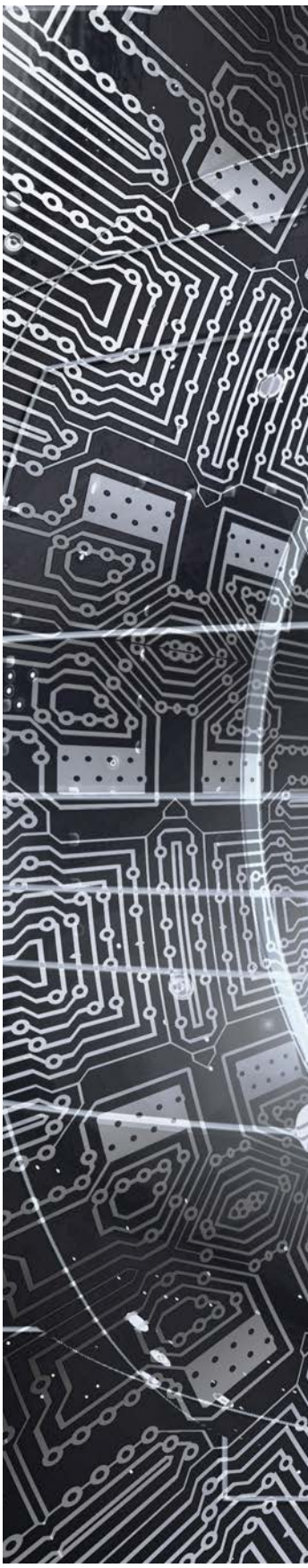
- Planes de Formación y concienciación específica en materia de Privacidad y Protección de Datos.

Mediante este modelo de referencia, el Grupo MAPFRE logra asegurar el cumplimiento de un estándar de protección común y homogéneo en todo el Grupo, que se complementará con la adhesión de las distintas entidades del grupo a las Normas Corporativas Vinculantes (BCR) que se han desarrollado y presentado a la Agencia Española de Protección de Datos.

Decálogo MAPFRE para el tratamiento de los Datos Personales, donde se establece los principios de privacidad que todos los empleados, agentes y delegados deben respetar dondequiera que se encuentren en el mundo:

Inteligencia Artificial y Ética del Dato

MAPFRE valora el desarrollo de la tecnología y el aumento del volumen y uso de los datos como un factor fundamental y se esfuerza por posicionarse en la vanguardia de la innovación en el aprovechamiento de los datos de la manera más ética.



09

MAPFRE cuenta con un **Marco Ético de Gobernanza Digital**, en el que se definen la oportunidades y riesgos que traen las nuevas tecnologías como la inteligencia artificial y los principios a seguir por wl Grupo MAPFRE para que su actuación en el ámbito digital se ajuste a la legalidad vigente.

Se han definido directrices y establecidos protocolos de actuación, para implementar un modelo de gobierno que permita tener un mayor control sobre los sistemas de Inteligencia Artificial utilizados, así como los mecanismos necesarios para determinar el nivel de riesgo existente en función del uso que se va a dar a los mismos.

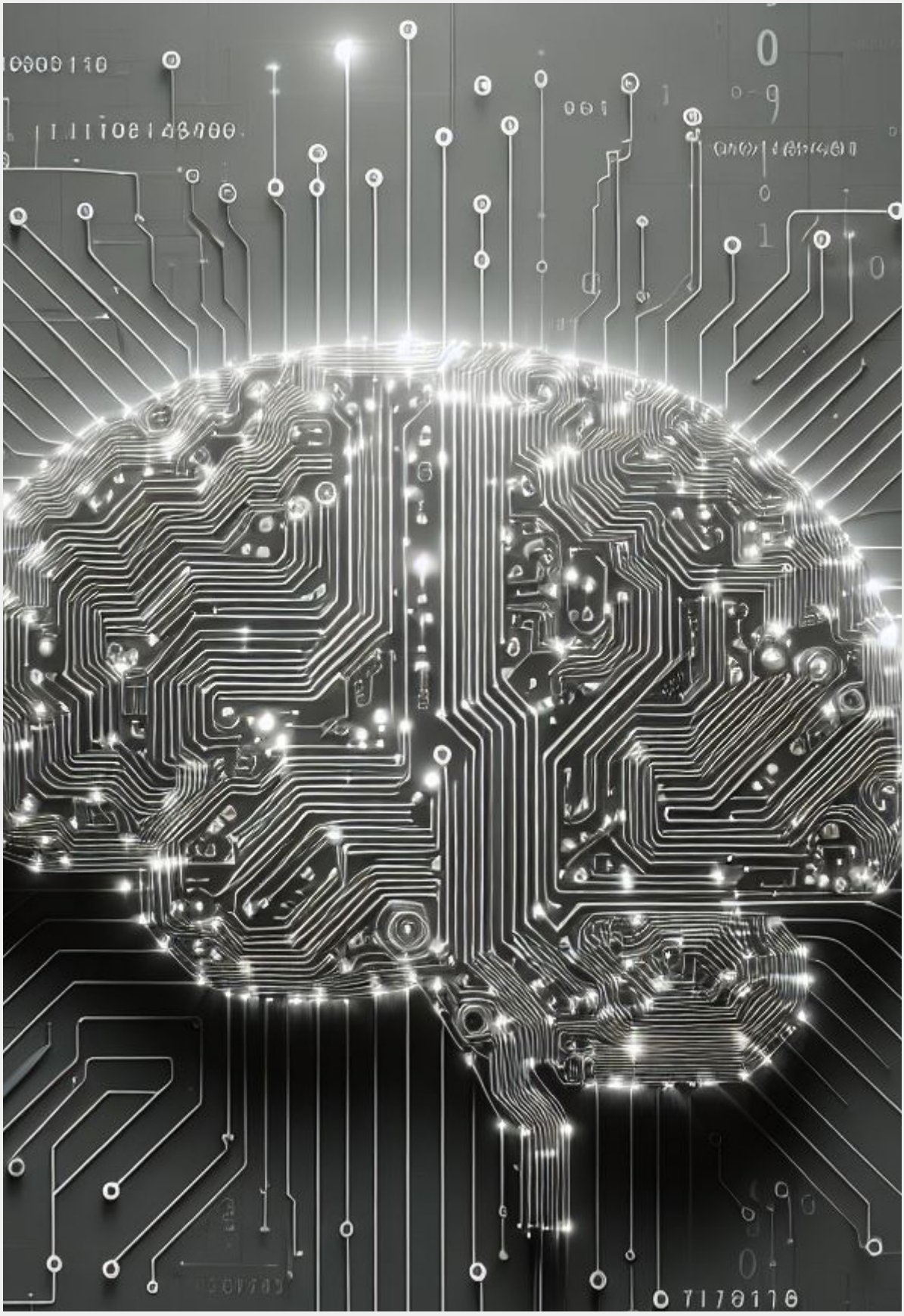
MAPFRE está adaptando sus requisitos de seguridad y privacidad para tener un mayor control sobre el uso que se está haciendo de esta tecnología, protegiendo no sólo los datos personales utilizados, sino toda aquella información relevante para la compañía, para alcanzar niveles óptimos de calidad, seguridad, trazabilidad, privacidad, equidad, explicabilidad y transparencia sobre los datos.

Adicionalmente, se ha definido un **Grupo de Trabajo sobre Inteligencia Artificial**, cuya misión es la de elevar los temas relacionados con la ética y la protección de datos, la agilización de los procesos, la automatización de decisiones y la mejora en la experiencia de los clientes, con el objetivo de realizar un uso ético y efectivo de los datos.

Fruto de la creación de este Grupo de Trabajo, se ha desarrollado una **'Guía de Uso de Sistemas de Inteligencia Artificial'** con el objetivo de establecer las directrices y medidas necesarias para mitigar los riesgos asociados que surgen por el uso de este tipo de tecnologías y que a su vez permite realizar una adecuación temprana a la regulación de aplicación en esta materia.

Por último, mencionar la adhesión de MAPFRE a los **'Compromisos para la Privacidad y la Ética Digital'** de la Fundación Cotec. Compromiso que nace para dar respuesta al desafío que supone el tratamiento de los datos en un contexto de transformación digital, en el que adquieren una importancia creciente la aplicación de principios éticos en la gestión de la privacidad, y especialmente en el desarrollo y uso de aplicaciones basadas en datos.

La adhesión a este decálogo es una demostración del compromiso y preocupación de MAPFRE por la gestión de la privacidad desde la perspectiva de la gestión ética de los datos que nuestros clientes, colaboradores, mediadores y empleados nos proporcionan.



Cultura de Seguridad: Sensibilización, Concienciación y formación

MAPFRE es consciente de que las personas son el eslabón más importante y, en ocasiones, el más débil de la cadena de seguridad. Por ello, la creación de una cultura de seguridad constituye un requisito estratégico para la compañía.

10

MAPFRE ha creado un Grupo de Trabajo multidisciplinar, con la participación de las Áreas Corporativas de Personas y Organización, Relaciones Externas y Comunicación y Seguridad, encargado de definir, desarrollar y mantener el Plan Corporativo de Sensibilización, Concienciación y Formación de Seguridad, que se actualiza anualmente, y se adapta de forma continua a las necesidades del entorno.

En línea con la visión global e integral que MAPFRE tiene de la seguridad, dicho plan contempla la seguridad de las TIC, privacidad y protección de los datos, resiliencia operativa digital, así como la seguridad de las personas y las instalaciones.

Las acciones incluidas en el Plan están dirigidas no solo a empleados de MAPFRE, sino también a terceros, como proveedores críticos, clientes y otros grupos de interés.

Incluyen campañas de sensibilización, que persiguen conseguir un impacto emocional, actividades de concienciación, para que las personas conozcan las amenazas y las buenas prácticas, así como programas de formación técnica, adaptados a distintos colectivos de acuerdo con su nivel de criticidad y atribuciones.

Algunos ejemplos de estas actuaciones son:

- Publicación periódica de noticias de seguridad, consejos, vídeos, infografías, podcast y otros recursos de comunicación.
- Campañas específicas de sensibilización y concienciación para empleados, mediante gamificación.
- Píldoras formativas en la Universidad Corporativa de MAPFRE, a disposición de todos los empleados.
- Cursos de formación para colectivos específicos (Alta Dirección, personal TIC, equipos de ciberseguridad, Contact Center, etc.)
- Ciberejercicios con campañas dirigidas a todos los empleados.

De todas ellas se realiza una medición sistemática, obteniendo estadísticas e indicadores que permiten evaluar su eficacia y la mejora continua del proceso.


Training

Auditorías y Revisiones

Dentro del proceso de mejora continua de la Seguridad y como tercera línea de defensa del sistema de control interno, MAPFRE realiza de manera sistemática y periódica Revisiones y Auditorías de seguridad.

11

MAPFRE realiza **Revisiones** y **Auditorías** específicas, relacionadas con el cumplimiento de la Política de Seguridad y Privacidad, la Política de Continuidad de Negocio y la normativa de protección de datos, que, en la mayor parte de las entidades, son contratadas con auditores expertos.

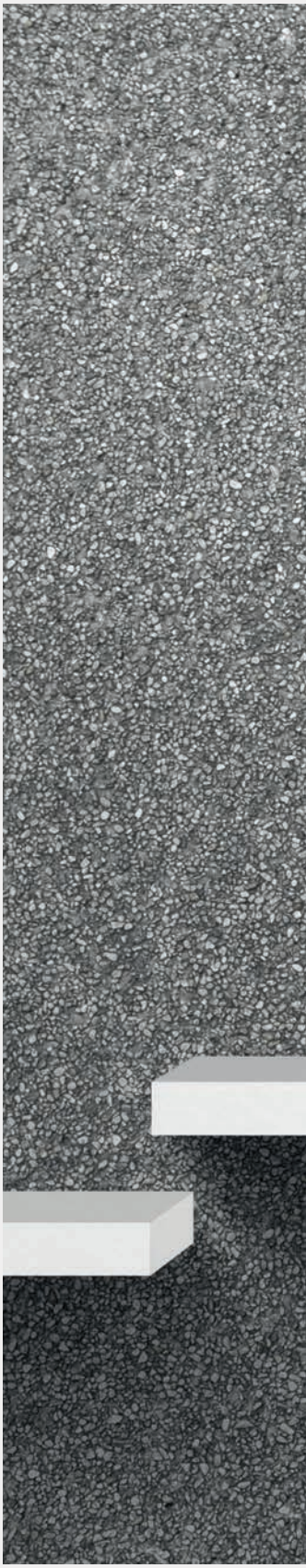
Adicionalmente, dentro de la Metodología de Auditoría de Control Interno de Tecnología y Seguridad desarrollada en MAPFRE, siempre se incluye un apartado en el Área de Control del Entorno TIC sobre el cumplimiento del Cuerpo Normativo de Seguridad y de la legislación que afecta a estas materias, incluida la protección de datos.

Por último, las auditorías de los procesos de negocio también incluyen aspectos específicos de seguridad y privacidad, con el fin de identificar posibles debilidades, vulnerabilidades y riesgos e implementar acciones de mejora preventivas y correctivas que garanticen el cumplimiento normativo y permitan elevar el nivel de seguridad y resiliencia operativa.

Consecuencia de ello, a lo largo del 2023 se han realizado más de 50 trabajos de auditoria sobre gobierno de la seguridad, sistemas de la información y seguridad, continuidad de negocio, así como privacidad y protección de datos.

Reconocimientos y Benchmark de terceros

El modelo de **seguridad integral y global** adoptado por MAPFRE es referencia para analistas internacionales y otras organizaciones de seguridad corporativas de grandes empresas, lo que se ha traducido en numerosos premios y reconocimientos, entre los que destacan:



12

GartnerGroup

Definición de un Caso de Estudio relativo al SOC Global (antiguo Centro de Control General de MAPFRE, CCG-CERT), realizado por el prestigioso analista internacional **Gartner Group.**


Gartner Research

Publication Date: 23 September 2010 ID Number: G00206504

Case Study: Mapfre Implements an Integrated Security Control Center

Primer Premio a la Excelencia en Seguridad Corporativa Duque de Ahumada otorgado por el Ministerio del Interior del Reino de España a MAPFRE por contar con un modelo de seguridad integral, referencia para las organizaciones de seguridad corporativas.

REVISTA SIC

Premio de Seguridad de la Revista SIC en su XIV edición, a la Subdirección General de Seguridad y Medio Ambiente de MAPFRE "**en reconocimiento a su pionero** enfoque, multidisciplinar e integrado, de los frentes de la protección corporativa, incluidos los asociados con la gestión de la seguridad de la información y la ciberseguridad".

BORRMART, S.A.

Trofeo Internacional de Seguridad a la Actividad Investigadora (I+D), en la XXVI Edición del Certamen Internacional de Premios a la Seguridad, en su modalidad de los Trofeos al mejor proyecto de seguridad convocado por la **editorial Borrmart.**

redseguridad.com

Premio extraordinario del Jurado de los premios de RED SEGURIDAD.

Mención honorífica de la Dirección General del Cuerpo Nacional de Policía Española.

IDC
ANALYZE THE FUTURE

Mapfre ha sido galardonada en 2019 por la consultora IDC Research España **"Proyecto de estrategia de ciberseguridad adaptado al nuevo escenario digital"**

De manera adicional, el modelo de seguridad de MAPFRE ha sido seleccionado por el IE Business School, considerada por los principales Rankings internacionales como una de las cinco mejores escuelas europeas por sus programas MBA y de formación ejecutiva, como caso práctico dentro de su Máster en CiberSeguridad, formando parte de los contenidos del mismo desde 2017.

A continuación, vemos la evaluación de benchmarks de terceros correspondientes al año 2023 en relación con la situación de seguridad en MAPFRE:

Dow Jones Sustainability Indexes	**96 (sobre 100). Information Security/Cybersecurity & System availability.** • +14 puntos respecto al 2022.
CNPIC incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD	**4,7 (sobre 5). Indicadores mejora CiberResiliencia - IMC.** • +0,4 puntos media sector financiero. • +0,1 puntos respecto al año anterior.
DSN isms forum	**9,13 (sobre 10). Gestión de crisis cibernéticas 2023.** • Madurez "Excelente". • Primera posición de las 26 empresas participantes.

MAPFRE