v 2.2 Marzo 2025

Seguridad

Respaldando tu confianza

MAPFRE

ÍNDICE

1 PLANTEAMIENTO ESTRATÉGICO 6

1.1. Características de la Función de Seguridad en MAPFRE 8
1.2. Misión de la Función de Seguridad 10
1.3. Visión de la Función Corporativa de Seguridad 11
1.4. Principios de la Función de Seguridad 12
1.5. Modelo Integral de Seguridad 13
1.6. Alcance Global 15
1.7. Sistema documental de Seguridad 16
1.8. Proceso de Mejora Continua de Seguridad 18

2 ORGANIZACIÓN DE SEGURIDAD 20

2.1. Estructura de la Organización de Seguridad 22
2.2. Consejo de Administración de MAPFRE SA 23
2.3. Comité Ejecutivo de MAPFRE 23
2.4. Comité Corporativo de Seguridad, Crisis y Resiliencia 24
2.5. Comité Corporativo de Privacidad y Protección de Datos 25
2.6. Dirección Corporativa de Seguridad 25
2.7. Equipo Humano Altamente Cualificado 26
2.8. Centro de Operaciones de Seguridad Global (Global SOC) 32

3 CUMPLIMIENTO EN MATERIA DE SEGURIDAD Y PRIVACIDAD 36

4 SEGURIDAD DE PERSONAS E INSTALACIONES 40

5 CIBERSEGURIDAD 44

5.1. Gestión de Identidades 47
5.2. Seguridad en redes 48
5.3. Seguridad en dispositivos (puestos informáticos, servidores y móviles) 49
5.4. Seguridad en la Nube 50
5.5. Gestión de vulnerabilidaes y parches 51
5.6. Monitorización y respuesta a incidentes 52
5.7. CiberSeguros 53

6 REVISIONES TÉCNICAS DE SEGURIDAD 54

7 DATACENTERS CORPORATIVOS 58

8 RESILIENCIA OPERATIVA: GESTIÓN DE CRISIS Y CONTINUIDAD DE NEGOCIO 62

9 PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES 66

9.1. Data Protection Officer 68

9.2. Marco de Referencia de Privacidad 69

9.3. Normas Corporativas Vinculantes (BCR) 71

10 INTELIGENCIA ARTIFICIAL Y ÉTICA DEL DATO 72

11 CULTURA DE SEGURIDAD: Sensibilización, Concienciación y Formación 76

12 AUDITORÍAS 80

13 RECONOCIMIENTOS Y BENCHMARK DE TERCEROS 82

Guillermo Llorente,
Director Corporativo de Seguridad de MAPFRE,

Para MAPFRE las personas son lo 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, contribuyendo a cuidar lo que les importa.

Para lograrlo, se constituye la Función de Seguridad, a fin de proteger los activos tangibles e intangibles de MAPFRE y garantizar su resiliencia operativa. Esta misión está recogida en el Marco Estratégico de Seguridad que, con un enfoque basado en la gestión de riesgos, opera como elemento vertebrador de las Políticas Corporativas de Seguridad y Privacidad, de la Continuidad de Negocio, así como de la Normativa Interna asociada a las mismas. Todo ello enmarcado siempre en el 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 incorpore la seguridad como atributo fundamental. Por ello, para mantener la continuidad del servicio que prestamos y la privacidad de la información que se nos confía, los requisitos de seguridad se integran, por defecto y desde el diseño, en cualquier aplicación, servicio, dispositivo o instalación; en resumen, en todo 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) y de la Red Nacional de SOC española, 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 cualquier entidad del Grupo.

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.

Todo ello ha permitido detectar y responder a las necesidades de un entorno cada vez más desafiante en materia de seguridad, haciendo posible que en 2024 MAPFRE no haya tenido que reportar ningún ciberincidente grave a las autoridades de control de los países en los que opera.

En conclusión, la continuidad del servicio que les prestamos, así como la seguridad y la privacidad de nuestros clientes son elementos fundamentales e imprescindibles de la naturaleza y de la vocación de servicio de nuestra compañía, constituyendo un Compromiso personal e ineludible de todos cuantos formamos parte de MAPFRE.

Guillermo Llorente
Director Corporativo de Seguridad de MAPFRE


PHISHING
SPAM
MALWARE

Planteamineto Estratégico

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

Características 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, por la buena reputación de la compañía y por la resiliencia operativa. **Los 4 pilares fundamentales que se basa son los siguientes:**

Es GLOBAL para el conjunto de la Compañía.
Afecta a todo el personal, a todos los medios e instalaciones, a todos los activos tecnológicos y a todos los procesos y actividades de las diversas Entidades, Órganos y Áreas de MAPFRE, con independencia de su ubicación geográfica y estructura societaria.

Vela por garantizar la RESILIENCIA del Grupo.
Posibilitando el normal desarrollo del negocio y proporcionando capacidades de detección, respuesta y recuperación en caso de materializarse riesgos que afecten a la fiabilidad operativa y a la integridad de la compañía.

Está orientada al SERVICIO.
La Función de Seguridad tiene una vocación de servicio a la organización, considerando a ésta como su cliente, satisfaciendo las necesidades que desde la misma puedan ser demandadas y acompañándola en su proceso de transformación

Debe APORTAR VALOR.
Proporcionando diferenciación, fiabilidad y ventaja competitiva a la compañía. Evolucionará en función de las necesidades del Grupo a fin de mantenerse permanentemente integrada en el negocio, adaptándose, alineándose y contribuyendo en todo momento a la estrategia corporativa y a la imagen de MAPFRE, reforzando la confianza en ella depositada por sus clientes y resto de grupos de interés.

1.2

Misión de la Función de Seguridad

La Función de Seguridad tiene como misión prevenir la aparición y mitigar el impacto de los riesgos de seguridad que puedan provocar daños a MAPFRE, a su reputación o a su personal, así como perturbar o limitar su capacidad operativa y/o financiera.

Así, además de posibilitar el normal desarrollo de la actividad de las distintas Unidades de Negocio y entidades del Grupo, la Función de Seguridad tiene como misiones específicas:

» **Proteger a las personas y resto de activos de MAPFRE,** incluyendo los datos propiedad de terceros a los que MAPFRE tiene acceso, velando por el cumplimiento normativo, la actuación ética y responsable y la preservación de la buena reputación de la compañía.

» **Posibilitar la resiliencia operativa de los procesos de negocio y soporte,** priorizando aquellos identificados como críticos y que afecten a las obligaciones del Grupo frente a terceros.

1.3

Visión de la Función Corporativa de Seguridad

Para garantizar una protección adecuada y sostenible en un entorno desafiante, la seguridad, privacidad y resiliencia operativa deben ser elementos imprescindibles e inherentes a la propia actividad de la compañía, integrados en sus procesos de negocio y en línea con la responsabilidad de MAPFRE hacia sus empleados, clientes, accionistas, proveedores, colaboradores y la sociedad en la que desarrollan su actividad.

La Función de Seguridad contribuye al liderazgo de MAPFRE también en materia de seguridad, privacidad y resiliencia operativa mediante soluciones innovadoras, eficaces y eficientes, rigiéndose por parámetros de estricta proporcionalidad, estableciendo mecanismos de protección acordes con el riesgo y valor de los activos, mejorando por ello la calidad de procesos, productos y servicios.

De manera adicional, la Función de Seguridad vela por el cumplimiento legal y normativo en materia de protección de personas, instalaciones, información, privacidad, resiliencia operativa, IA y prevención de actos antisociales o ilícitos.

La Función de Seguridad se rige por las normas de gobernanza del Grupo MAPFRE y el Marco Estratégico de Seguridad, basado en las mejores prácticas y estándares internacionales, articulándose mediante un proceso de gestión de riesgos normalizado y sistemático.

1.4

Principios de la Función de Seguridad

La Función de Seguridad del Grupo MAPFRE se rige por los siguientes Principios:

1. Actuación ética y responsable, garantizando el cumplimiento riguroso de la legislación aplicable y del Código Ético y de Conducta del Grupo en todas las actuaciones.

2. Enfoque Integral, considerando el activo a proteger como el centro de su actividad y protegiéndolo frente a todo tipo de amenazas y riesgos dentro el ámbito de la seguridad, la privacidad y la resiliencia operativa, con independencia de su modo de materialización.

3. Proporcionalidad, definiendo e implantando medidas de seguridad acordes con el riesgo y valor de los activos, optimizando los recursos disponibles en aras de una mejora continua de la eficiencia.

4. Incorporación desde el diseño, entendiendo la SEGURIDAD como un proceso continuo que debe formar parte de todos los procesos y actividades de negocio, incorporando los criterios de seguridad, privacidad y resiliencia operativa desde su concepción y manteniéndolos en todo su ciclo de vida.

5. Actuación preventiva, anticipándose a los daños para evitarlos o reducir sus consecuencias, dentro del concepto de diligencia debida.

6. Seguridad en Profundidad y Escalonada, aplicando un enfoque estratégico con múltiples capas de defensa para proteger los activos y mitigar los riesgos, de forma que si una medida fallase, las siguientes sigan proporcionando protección, combinando diferentes controles físicos, técnicos y organizativos.

7. Capacidad de respuesta, actuando oportuna y proactivamente ante cualquier amenaza y respondiendo con rapidez para asegurar la resiliencia operativa.

8. Dirección Centralizada, asegurando la coherencia en el planeamiento de la Función de Seguridad, toma de decisiones e implementación de medidas para conseguir un nivel homogéneo de Seguridad en el conjunto del Grupo. Corresponsabilidad todos los niveles de la organización (Dirección, empleados, proveedores...) comparten el compromiso de proteger a las personas y resto de activos de MAPFRE.

9. Cultura de seguridad, privacidad y resiliencia, formación e información relevante en estas materias para consejeros, empleados, clientes, proveedores y colaboradores, integrándolas en la Cultura Corporativa.

10. Corresponsabilidad, asegurando que todos los niveles de la organización, (Dirección, empleados, proveedores...) comparten el compromiso de proteger a las personas y resto de activos de MAPFRE.

1.5

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, de sus activos y de su negocio, en una única Dirección Corporativa con presencia y ámbito de actuación global.

Las responsabilidades de Función de Seguridad incluyen los siguientes ámbitos:

- **Seguridad de las Personas.**
- **Seguridad de las Instalaciones.**
- **Seguridad de los Sistemas de Información (Ciberseguridad).**
- **Privacidad y Protección de datos personales.**
- **Resiliencia Operativa: Gestión de Crisis y Continuidad del Negocio.**
- **Lucha contra el fraude.**
- **Inteligencia de Seguridad.**
- **Cumplimiento normativo y regulatorio en materia de Seguridad, Privacidad y Resiliencia Operativa.**
- **Riesgos de seguridad de terceros y proveedores.**

Las actuaciones en materia de seguridad se basan en un modelo de gestión de riesgos, garantizando la adecuada protección de los activos corporativos de MAPFRE.

La gestión de los riesgos de seguridad está asimismo integrada en el sistema de gestión de riesgos del Grupo MAPFRE, formando parte de la información periódicamente reportada al Comité de Riesgos y Sostenibilidad del Grupo.

Sobre este enfoque se ha construido el modelo para el desarrollo de la **Función de Seguridad** en MAPFRE, regido por el Código Ético y de Conducta 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

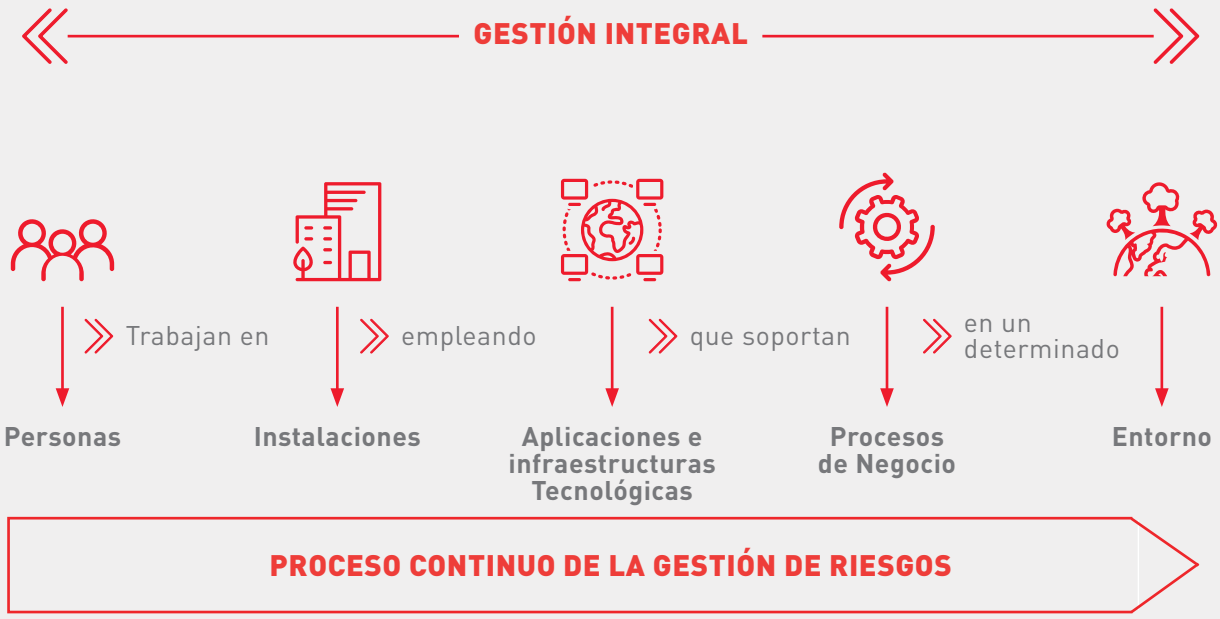
ISO 22301 de Continuidad de Negocio

ISO 9001 de gestión de la calidad

ISO 29100 relativa a la protección de la privacidad

PCI DSS. Sobre seguridad de datos de las tarjetas de pago.

ISO 31030 sobre gestión de riesgos en viajes.



1.6

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 Seguridad Global,** 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 Reguladores, Autoridares y Cuerpos y Fuerzas de Seguridad locales.
- Capturando y adaptándose a las necesidades , amenazas y hábitos/costumbres en cada entidad, país y mercado.

1.7

Sistema documental de Seguridad

Reflejando los principios anteriormente citados y acorde con los Principios Institucionales y Empresariales y con el Código Ético y de conducta, MAPFRE cuenta con un Sistema Documental de Seguridad, cuyo elemento de más alto nivel son el conjunto de Políticas corporativas, en las que se recoge el compromiso de MAPFRE para garantizar la protección de los activos de MAPFRE, velando, además por el cumplimiento normativo en materia de seguridad y privacidad, la resiliencia operativa de los servicios prestados a terceros, la preservación de la buena reputación e imagen de la compañía y la sostenibilidad de la misma. Dichas políticas han sido aprobadas por el Consejo de Administración de MAPFRE, SA y son de obligada aplicación en todo el Grupo.

Política Corporativa de Seguridad y Privacidad, que establece las directrices y compromisos de MAPFRE en materia de seguridad y privacidad.

Política de Continuidad de Negocio, que establece el marco para garantizar la resiliencia operativa y la recuperación de funciones críticas tras incidentes disruptivos, protegiendo a las personas y asegurando la continuidad de los procesos y servicios esenciales.

Estrategia de Resiliencia Operativa Digital, que establece el marco para gestionar los riesgos relacionados con las TIC y asegurar la continuidad de los servicios críticos, protegiendo la información, garantizando la seguridad y la resiliencia operativa.

Política de Lucha Contra el Fraude, que establece las directrices, procedimientos y responsabilidades para prevenir, detectar, investigar y perseguir el fraude en todas sus manifestaciones.

Dichas Políticas constituyen el punto de partida para el desarrollo de del resto de componentes del Sistema Documental de Seguridad, según se muestra en la siguiente figura:

* Aprobados por el comité de Administración de Grupo 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/Codigo-Etico-y-de-Conducta.pdf

Política Corporativa de Seguridad y Privacidad

https://www.mapfre.com/media/accionistas/2024/politica-corporativa-seguridad-privada.pdf

Política de Continuidad de Negocio

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

1.8

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, las amenazas del entorno 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 corporativa** del Grupo MAPFRE.

02

2.1

Estructura de la Organización de Seguridad

La Organización de Seguridad de MAPFRE integra los equipos humanos, medios y recursos de todo tipo destinados a la protección de los activos tangibles e intangibles del Grupo, destinado a preservar la resiliencia operativa de la compañía.

Se estructura en diferentes niveles de responsabilidad alineados con la estructura corporativa del Grupo, del modo que se indica a continuación:

ESTRUCTURA DE LA ORGANIZACIÓN
Consejo de Administración de MAPFRE
Comité Ejecutivo de MAPFRE
Comité Corporativo de Seguridad, Crisis y Resiliencia
Comité Corporativo de Privacidad y Protección de Datos
Dirección Corporativa de Seguridad

2.2

Consejo de Administración de MAPFRE SA

En la cúspide del modelo de gobierno de la Seguridad en MAPFRE se encuentra el Consejo de Administración de MAPFRE S.A, como responsable último de controlar los riesgos del Grupo y, en concreto, los relacionados con las TIC y la Seguridad. Dicha responsabilidad es ejercida, en sus respectvivos ámbitos, por los Consejos de Administración de las distintas entidades del Grupo MAPFRE.

2.3

Comité Ejecutivo de MAPFRE

El Comité Ejecutivo de MAFPRE, por encargo del Consejo de Administración, ejerce la supervisión directa de la gestión en materia de Seguridad, materializando el compromiso y respaldo de la Alta Dirección a la Función de Seguridad. Esta responsabilidad es ejercida, en sus respectivos ámbitos, por parte de los Comités de Dirección de las distintas entidades del Grupo.

2.4

Comité Corporativo de Seguridad, Crisis y Resiliencia

Es el máximo órgano ejecutivo de la Organización de Seguridad, velando porque los objetivos y necesidades empresariales gobiernen la actividad de la Función de Seguridad, al mismo tiempo que garantiza que la seguridad, privacidad y resiliencia operativa son contempladas como un elemento constituyente de los procesos de negocio corporativos.

Cuando la situación lo requiere este Comité se constituye como Comité de Crisis del Grupo, ejerciendo las funciones asignadas en la Política y el Modelo de Gobierno de Continuidad de Negocio.

El Comité está presidido por el Vicepresidente primero del Grupo MAPFRE, y cuenta, entre sus vocales, con losmiembros de la Alta Dirección responsables de sus principales áreas de negocio y funciones corporativas.

La composición del Comité a la fecha de redacción de este documento es la siguiente: su Presidente es el Vicepresidente Primero del Consejo de Administración de MAPFRE SA* y son vocales los máximos responsables de los Territorios/Regiones (IBERIA*, INTERNACIONAL* y NORAM*), así como los de las Áreas Corporativas de Secretaría General y Asuntos Legales*, Financiera y Medios (CFO Adjunto**), de Transformación de la Operación**, Personas, Estrategia y Sostenibilidad**, Relaciones Externas y Comunicación**, Negocio**, Tecnología y Seguridad y actúa como secretario del mismo el Director de Resiliencia Operativa y GRC.

* Miembro del Consejo de Administración y del Comité Ejecutivo de MAPFRE SA.
** Miembro del Comité Ejecutivo de MAPFRE SA.

2.5

Comité Corporativo de Privacidad y Protección de Datos

Comité específico de carácter operativo subordinado al Comité Corporativo de Seguridad, Crisis y Resiliencia, para la dirección y control de las situaciones en materia de privacidad y protección de datos de carácter personal, con el fin de apoyar al DPO en el desarrollo de sus funciones.

2.6

Dirección Corporativa de Seguridad

La Dirección Corporativa de Seguridad de MAFPRE (DCS) es el órgano global de dirección, planeamiento y ejecución de la Función Corporativa de Seguridad, en sus distintos ámbitos de actuación:

- **Seguridad de las Personas.**
- **Seguridad de las Instalaciones.**
- **Seguridad de los Sistemas de Información (Ciberseguridad).**
- **Privacidad y Protección de datos personales.**
- **Resiliencia Operativa: Gestión de Crisis y Continuidad del Negocio.**
- **Lucha contra el fraude.**
- **Inteligencia de Seguridad.**
- **Cumplimiento normativo y regulatorio en materia de Seguridad, Privacidad y Resiliencia Operativa.**
- **Riesgos de seguridad de terceros y proveedores.**

La DCS, además de ser responsable de velar por la Seguridad del conjunto del Grupo, proporciona servicio, opera los sistemas de seguridad comunes y gestiona la demanda del conjunto de las Entidades y Unidades de Negocio de MAPFRE.

2.7

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, con un total de 125 empleados certificados. 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
TSI. PROFESSIONAL TÜVIT TÜV NORD GROUP	**TSI PROFESSIONAL:** Evaluación y certificación de infraestructuras de centros de datos de alta disponibilidad según la norma EN50600 y el método Trusted Site Infrastructure (TSI).

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.

CPCC: Certified Professional Cyber Compliance, del ISMS Forum, por la que se acredita un alto nivel de especialización en la normativa española en materia de cumplimiento en ciberseguridad.

CIPP/E: Certified Information Privacy Professional, reconocida mundialmente, desarrollada por la Asociación Internacional de Profesionales de la Privacidad (IAPP), que acredita conocimiento global de leyes y regulaciones de protección de datos

2.8

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 materializa el modelo de seguridad integral de MAPFRE, constituyéndose en el corazón del mismo. En él se controla 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 Global 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 CCN-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 PLATAFORMAS DE SEGURIDAD

(Operación de Sistemas y Herramientas de Seguridad)

El **Global SOC** está certificado en la **ISO 27001, en la ISO 22301**, fue **el primer CERT español en obtener la certificación ISO 9001,** 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 y 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, controles acordes a los niveles de riesgo. Se evalúa periódicamente la posición de riesgo de la organización y 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. Posibilitar la continuidad del servicio ante situaciones imprevistas.

Red Nacional de SOC (RNSOC): 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 244 entidades clasificadas en 2 niveles de acceso, Gold y Silver. **MAPFRE ha sido incluida como GOLD**, siendo de nuevo la primer compañía privada no tecnológica en conseguirlo.

En el **Global SOC** se monitorizan todos los eventos de actividad de las redes, sistemas y usuarios que se generan en losámbitos tecnológicos en los que MAPFRE está presente. Diariamente se gestionan más de 4.000 millones de eventos que se analizan aplicándoles reglas de inteligencia para la generación de alertas ante potenciales eventos anómalos.

Las alertas generadas son gestionadas de manera global por equipos Especializados, en una modalidad 24x7x365, en el que se aplica un riguroso proceso de identificación, análisis, evaluación, contención, resolución, escalado y registro de las alertas.

Desde el Global SOC se monitorizan:

1 Universo MAPFRE

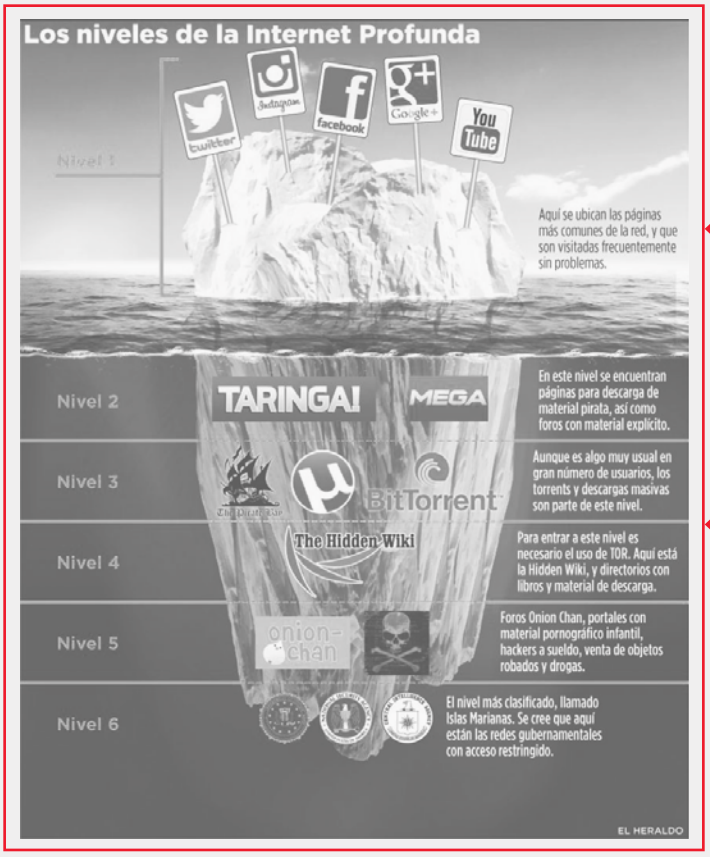
AWS
Azure

EDIFICIOS Y OFICINAS

REDES, SISTEMAS Y USUARIOS

2 Redes Sociales Web Accesible

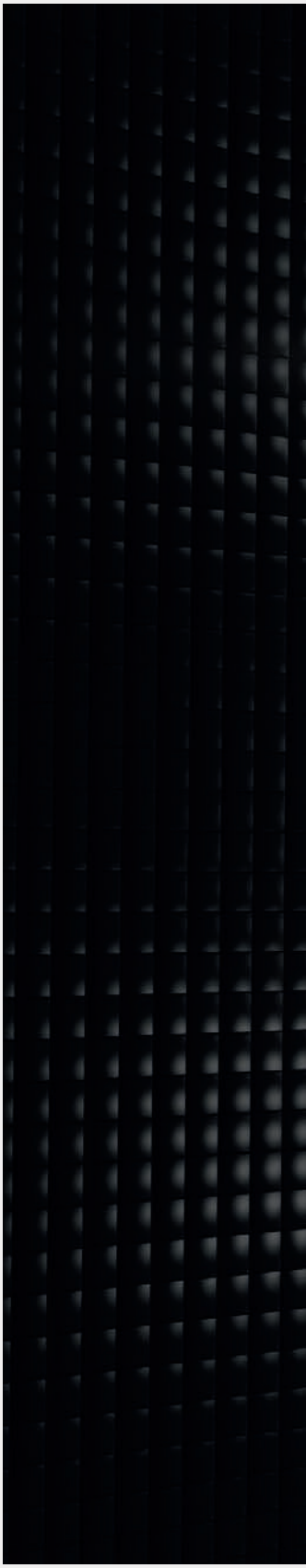
3 Deep Web Dark Web



PERFILES CORPORATIVOS, OPINIONES Y TOPICS

BLACK MARKETS

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, agrupadas en el Código Ético y de Conducta que garantiza 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.

El 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.

En los relativo a observación de su cumplimiento, mención especial merece los Reglamentos de la Unión Europea que son de aplicación, y que MAPFRE asume como normas de referencia para todo el Grupo:

- **Reglamento General de Protección de Datos (RGPD),** norma de referenciaen 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.

- **Reglamento sobre la Resiliencia Operativa Digital (DORA),** el objetivo de MAPFRE es garantizar, no solo el cumplimiento de esta legislación, sino acreditar con suficiencia que puede resistir y responder a cualquier tipo de perturbación y amenaza relacionada con las TIC y recuperarse de ellas en los plazos comprometidos

- **Reglamento sobre Inteligencia Artificial (RIA),** actualmente en ejecución el Proyecto de adecuación del Reglamento de forma que se garantice, no solo el cumplimiento de esta legislación, sino acreditando un uso ético y responsable de los Sistemas de IA.

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.

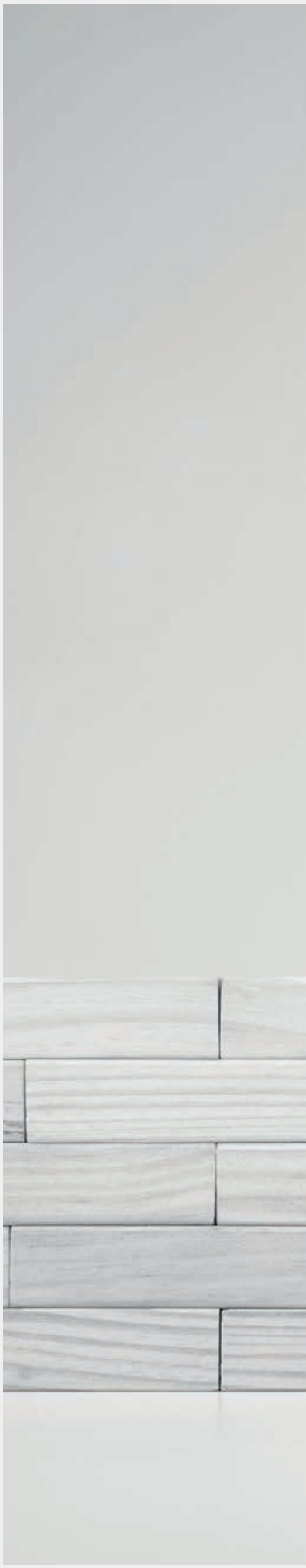
MAPFRE dispone de un observatorio normativo y de análisis de los múltiples pronunciamientos por parte de los reguladores, de los países en que está presente, con el objetivo de garantizar que, desde el diseño, todos los procesos cumplen en todo momento con las normativas de seguridad, privacidad y protección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

MAPFRE, dentro del proceso de gestión del riesgo de seguridad de terceros, incluye criterios de ciberseguridad, privacidad y resiliencia operativa en los procesos de compra de soluciones y servicios tecnológicos, incorporando a todos sus contratos con terceros **cláusulas de seguridad, protección de datos, y resiliencia operativa,** 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 que le son confiados.

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, privacidad y resiliencia operativa digital, 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, 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 oportunas 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. Durante 2024 se realizaron más de 450 simulacros de emergencia en las instalaciones de MAFPRE.

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 todo un sistema que los protege en los viajes que realizan al extranjero. Dicho sistema analiza los futuros viajes, identifica y evalúa los riesgos deasociados a los mismos y contacta con aquellos viajeros que asumen mayores riesgos en sus desplazamientos, estando en todo momento monitorizados desde el Global SOC. Además, los viajeros cuentan con una Guía de Autoprotección, con consejos de seguridad para los viajes, así como con Guías específicas de Seguridad para viajes a aquellos destinos considerados de riesgo medio o alto. 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.

En este sentido, MAPFRE ha obtenido la certificación de Gestión de Riesgos en Viajes conforme a la norma ISO 31030 "Travel risk management. Guidance for organizations" para la gestión de viajes internacionales con origen en España, para empleados del Grupo.

La certificación ISO 31030 es un reconocimiento a las prácticas avanzadas de MAPFRE en la gestión de riesgos asociados a los viajes, asegurando que los empleados del Grupo cuenten con las mejores medidas de protección, seguridad y apoyo en sus desplazamientos internacionales.

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, en función de ese análisis de riesgo previo, video-vigilancia, sistemas de alarma y/o personal de seguridad para funciones de vigilancia y monitorización de estos sistemas. 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 diseño y por defecto en todas las nuevas iniciativas: la construcción de nuevas soluciones, la contratación de nuevos servicios, etc. En otras palabras, integrar la Ciberseguridad desde el diseño 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 adecuadamente 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)*.

*Ver apartado 11

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 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, para los de dirección de las entidades.
- Plan de Formación y Concienciación, aprobado por el Comité Corporativo de Seguridad, Crisis y Resiliencia.
- Simulacros y ejercicios de gestión de Crisis, para los Comités de de dirección y personal clave de las entidades.

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. La concesión de accesos a los usuarios se realiza sobre la base de otorgar el mínimo privilegio posible y solo en caso de que sea necesario para la realización de su función.

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

Incorporación de la Gestión de Identidades y Accesos en el ciclo de vida de desarrollo de las aplicaciones.

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 el área de 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 que se refuerza mediante mecanismos de protección frente a identidades robadas y contraseñas frágiles.

Protección avanzada de accesos basada en analítica de comportamiento.

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 manualmente desde el Centro de Operaciones de Accesos e Identidades (COAS) del Global 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.
- Restricción de acceso a los puertos USB en los equipos de los usuarios.
- Herramienta de simulación de brechas de seguridad.

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, viene incluyendo desde hace años 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).

Los proveedores prioritarios de MAPFRE son:

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.
- Monitorización y respuesta a incidentes.

El control de la actividad en la nube es una de las tareas prioritarias de MAPFRE. Diariamente se monitorizan más de 500 millones de eventos generados en esas nubes, que son analizados mediante avanzados filtros de tratamiento de información. Todas las alertas y potenciales anomalías son gestionadas por el Global SOC como uno más de sus ámbitos de actuación.

5.5

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 su identificación temprana de 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.

Además de las capacidades asociadas al Centro de Referencia de Revisiones Técnicas de Seguridad, 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 identifica o publica una nueva vulnerabilidad, el equipo de ciberseguridad realiza una evaluación atendiendo a su criticidad y potencial 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.

5.6

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).
- Participación 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 y eficaz a cualquier incidente de ciberseguridad.

5.7

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.

Revisiones Técnicas de Seguridad

MAPFRE considera prioritario y un objetivo irrenunciable **garantizar la seguridad a través de rigurosas revisiones técnicas.** En este sentido, ha establecido directrices, procedimientos y herramientas que permiten evaluar, controlar y minimizar los riesgos, asegurando el cumplimiento de los más altos estándares de seguridad en todas sus operaciones.

06

6.1

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, permitiendo detectar y corregir rápidamente cualquier vulnerabilidad.

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

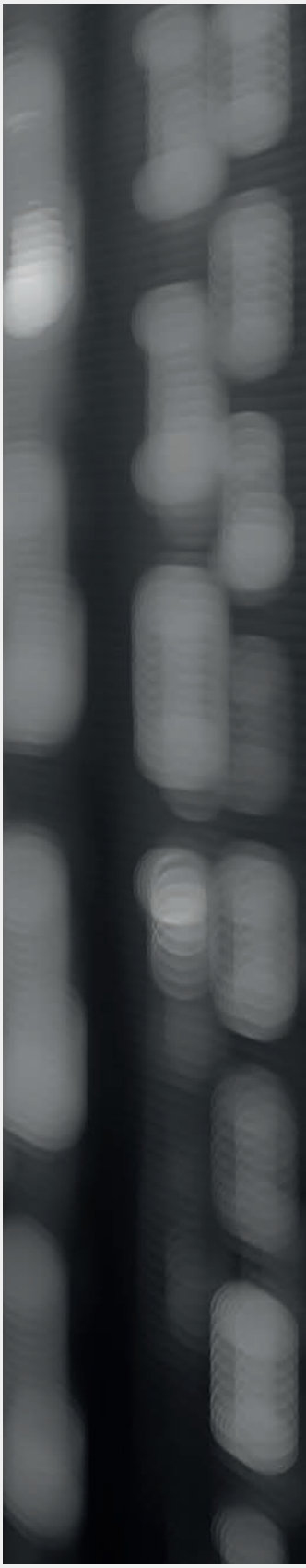
Este catálogo de revisiones incluye el proceso de **revisión continua automatizada de los sistemas expuestos a internet así como los sistemas internos de carácter crítico,** de todas las entidades de la compañía, y permite detectar cualquier nueva vulnerabilidad en dichos sistemas.

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.

Datacenters corporativos

MAPFRE cuenta con **cuatro 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.



07

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): Design, Facility
CPD Miami: Design, Facility
CPD Tamboré (Sao Paulo): Design, Facility and Operation

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 Miami
CPD Tamboré (Sao Paulo)

Certificación de Conformidad en el Esquema Nacional de Seguridad (ENS), categoría ALTA, según RD 311/2022
Esta certificación implica que el centro de datos cumple con los requisitos de seguridad más estrictos establecidos por el Esquena Nacional de Seguridad de España, garantizando una protección adecuada de la información tratada y de los servicios prestados.

CPD Alcalá de Henares (Madrid)

ISO 50001:2018 - Sistemas de gestión de la energía
Esta certificación garantiza que el data center cumple con los más altos estándares de gestión y eficiencia energética, optimizando el uso de la energía, reduciendo costos y mejorando la sostenibilidad.

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

Resiliencia Operativa: Gestión de Crisis y Continuidad de Negocio

La misión de la Función de Seguridad 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 Gestión de Crisis y Continuidad de Negocio,** integrado en su enfoque global de la Seguridad.

08

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 basado en **tres grandes pilares:**

Modelo de Continuidad de Negocio del Grupo MAPFRE

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 pilar, 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 pandemias, 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 (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**, y el SOC Global del Grupo MAPFRE. están certificadas en la ISO 22301 garantizando la actualización y mejora continua de estos planes.

Los Países / Unidades de Negocio que cuentan con Planes de Continuidad de Negocio certificados bajo la norma ISO 22301, representan el 77% de las primas totales emitidas por el Grupo MAPFRE. Este estándar internacional acredita que las entidades certificadas tienen correctamente implantados Sistemas de Gestión de Continuidad de Negocio (SGCN) diseñados para protegerlas de posibles interrupciones, garantizando su recuperación con razonables expectativas de éxito ante diferentes tipos de desastres y logrando mantener la continuidad de sus operaciones. Además, asegura la actualización y mejora continua de dichos sistemas.


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, COMPAÑIA DE REASEGUROS, S.A.


AENOR
Certificado del Sistema de Gestión de la Continuidad del Negocio
SCN-2018/0007
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.

09

9.1

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** con el fin de apoyar al DPO en el desarrollo de sus funciones.

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.

9.2

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.

Mediante este modelo de referencia, el Grupo MAPFRE logra asegurar el cumplimiento de un **estándar de protección común y homogéneo** en todo el Grupo, y garantizar el cumplimiento de los principios relativos al tratamiento de datos personales.

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

- **Responsabilidad Proactiva:**

  - **Adecuación temprana** a la regulación de aplicación en materia de privacidad en las diferentes geografías en las que opera.

  - **Aplicación en los procesos** de la compañía de las medidas técnicas y organizativas adecuadas, no solo para garantizar la protección y cumplir con las normativas de aplicación sino para evidenciar su cumplimiento ante autoridades de control e interesados.

- **Protección desde el diseño y por defecto: Integración de la Privacidad en el ciclo de vida de cualquier nueva iniciativa** que gestione datos personales, respetando las normas de protección de los derechos y libertades fundamentales e implantando los controles y medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información que se maneja y de los sistemas de que la soportan

- **Gestión del Riesgo.** Evaluación de impacto en la privacidad de los nuevos tratamientos. Así como, ante cambios sustanciales que afectan al entorno de los tratamientos (sus requisitos y/o riesgos) o las medidas de seguridad y privacidad dispuestas

- **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.

- **Cultura de la Privacidad: Planes de Formación y Concienciación** específica en materia de Privacidad y Protección de Datos.

- **Fomento de la colaboración público-privada.** Participación en asociaciones que fomenten la privacidad y en iniciativas sectoriales e institucionales orientadas a clarificar la aplicación del RGPD, como el DPO Forum o la DPO Community.

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:

9.3

Normas Corporativas Vinculantes (BCR)

Como evolución al modelo, y de cara a cumplir con estándares más exigentes, MAPFRE se ha dotado de unas **Normas Corporativas Vinculantes de Responsable (BCR-C)**, qpolítica de protección de datos personales asumidas por un grupo empresarial, y que habilitan las transferencias internacionales de datos entre sus distintas entidades al garantizar en todas ellas, con independencia de su ubicación, un nivel de protección equivalente al que ofrece el Reglamento General de Protección de Datos de la U.E. (RGPD).

Las BCR-C tras el **dictamen favorable del Comité Europeo de Protección de Datos (CEPD),** han sido **aprobadas por la Agencia Española de Protección de Datos (AEPD)**, quién ha liderado el proceso formal de revisión y aprobación, con la colaboración de las Autoridades de Control Correvisoras y resto de Autoridades de control de la UE para su valoración.

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

Las Normas Corporativas Vinculantes demuestra el compromiso de MAPFRE por la Privacidad (clientes, proveedores, colaboradores, empleados y grupos de interés), acreditando ante terceros el cumplimiento del Reglamento General de Protección de Datos (RGPD) incluso en las **entidades MAPFRE ubicadas fuera del EEE,** y un nivel homogéneo de protección sobre sus datos independientemente del país en que estos se alojen y de las obligaciones exigidas por la normativa local en la realización de **transferencias internacionales de datos** entre las entidades del Grupo MAPFRE.

En los siguientes enlaces puede consultar el texto completo de las BCR:

» Español

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

» Inglés

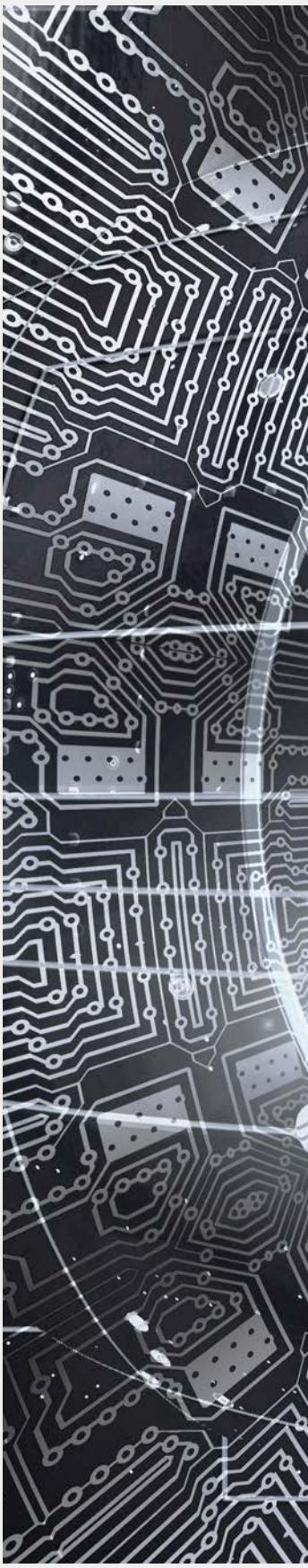
https://www.mapfre.com/statics/bcrs-mapfre/Binding_Corporate_Rules_ENU.pdf

» Portugués

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

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.



10

MAPFRE se compromete a realizar un **Uso Responsable y Ético de la Inteligencia Artificial,** aprovechando las oportunidades de las nuevas tecnologías y ajustándose en el ámbito digital a la legislación vigente, tal y como queda recogido en el Marco de Ético de Gobernanza Digital y en los Principios sobre el uso responsable y ético de la Inteligencia Artificial establecidos.

Además, MAPFRE cuenta con con un **Marco de Referencia**, para implantar un **modelo de gobierno de uso responsable de la IA**, con un enfoque centrado en el ser humano, que permita tener definidas las nuevas responsabilidades en materia de IA, y que han quedado reflejados en el Manifiesto de IA de MAPFRE.

MAPFRE adapta sus requisitos de seguridad y privacidad para desde el inicio y por defecto en todas sus iniciativas y proyectos, **garantizar un control adecuado** sobre el uso que se está haciendo de esta tecnología, protegiendo tanto los datos personales utilizados, como la información relevante para la compañía, y alcanzar niveles óptimos de calidad, seguridad, confiabilidad, robustez, trazabilidad, privacidad, equidad, explicabilidad y transparencia de cada caso de uso, y ha elaborado también las primeras cláusulas contractuales a incluir en los contratos con proveedores de servicios relacionados con materia de Inteligencia Artificial.

Adicionalmente, MAPFRE cuenta con un **Grupo de Trabajo multidisciplinar sobre el uso responsable de la Inteligencia Artificial**, para gestionar los temas relacionados con la ética y la protección de datos, la agilización de los procesos, la concienciación de los empleados y la automatización de decisiones y la mejora en la experiencia de los clientes, con el objetivo de garantizar un uso ético y responsable de los datos.

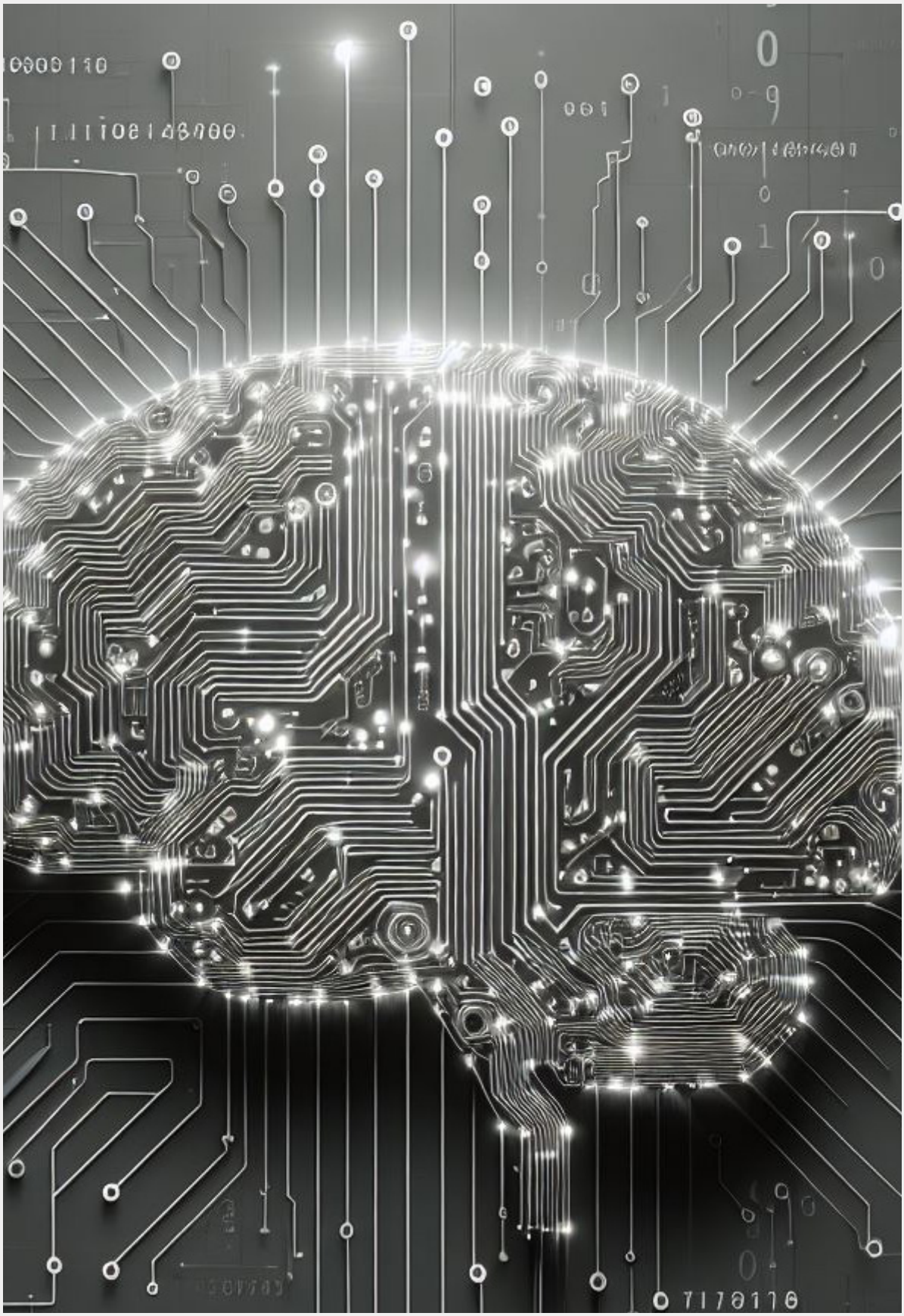
Fruto de ese Grupo de Trabajo, es la **'Guía de Uso de Sistemas de Inteligencia Artificial'** que establece las directrices y mecanismos necesarios para determinar el nivel de riesgo existente en función del uso que se va a dar a los mismos, así como medidas necesarias para mitigar los riesgos asociados que surgen por el uso de este tipo de tecnologías.

MAPFRE lleva tiempo trabajando en la **adecuación temprana a la regulación** de aplicación en esta materia de Inteligencia Artificial y **tiene definido un Plan de Adecuación** que reúne una serie de proyectos y líneas de trabajo, cuyo objetivo es dar cumplimiento a las obligaciones exigidas por los reguladores durante los próximos años.

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.

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

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 y responsable 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.

11

MAPFRE dispone de 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 de Concienciación y Formación de Seguridad**, que se actualiza anualmente, y se adapta de forma continua a las necesidades del entorno.

Dicho Plan es aprobado por el Comité Corporativo de Seguridad, Crisis y Resiliencia, máximo órgano ejecutivo de la Organización de Seguridad, materializando así el compromiso de la Alta Dirección con la promoción de la cultura de seguridad en la organización.

En línea con la visión global e integral que MAPFRE tiene de la seguridad, dicho plan contempla la **seguridad de las TIC**, la **privacidad y protección de los datos** y **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**.

El Plan incluye 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.

En este sentido, en los últimos tres ejercicios, se han destinado un total de **95.785 horas** a la formación en materia de seguridad. El número de empleados en MAPFRE formados entre 2022 y 2024 asciende a **28.103**. Al cierre del ejercicio, el **92 % de la plantilla** ha recibido formación en este ámbito.

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

Algunos ejemplos de estas actuaciones son:

- **Publicación periódica de noticias** de seguridad, consejos, vídeos, infografías, podcast y otros recursos de comunicación. Durante 2024, se han publicado más de 380 contenidos relacionados con la seguridad.
- **Campañas específicas** de sensibilización y concienciación para empleados, mediante la técnica de "gamificación" y "storytelling".
- **Píldoras formativas** en la Universidad Corporativa de MAPFRE, a disposición de todos los empleados.
- **Durante el periodo 2023 – 2024 se ha llevado a cabo un ambicioso plan de formación para todo el personal TIC,** mediante 10 cursos monográficos, habiendo sido formados más de 1.800 profesionales y realizadas en torno a 15.000 horas de formación en este ámbito.
- Sesiones específicas de concienciación destinadas a la **Alta Dirección y a los Consejeros Externos** del Grupo.
- **Entrenamiento** para personal de Seguridad y ejercicios de gestión de Crisis.
- **Ciberejercicios** con campañas dirigidas a todos los empleados, destinados a comprobar la eficacia de las acciones de formación y concienciación, así como a evaluar el comportamiento de los empleados ante los ciberataques más comunes. En 2024, los empleados presentaron un comportamiento adecuado en los ejercicios realizados en más del 94 % de los casos.
- **Simulacros de Gestión de ciberincidentes,** ejecutados de forma gradual con los Comités de Dirección de las diferentes Entidades, constituidos como Comités de Crisis de las diferentes entidades del Grupo.

Auditorías

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 Auditorías de seguridad.

12

MAPFRE realiza **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, son realizadas por auditores expertos.

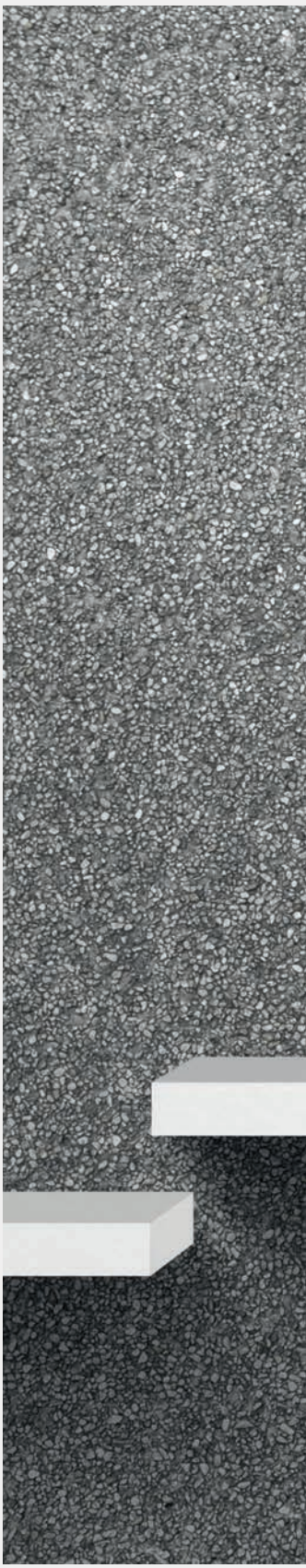
Adicionalmente, dentro de la Metodología de **Auditoría de Control Interno de Tecnología y Seguridad** desarrollada en MAPFRE, siempre se incluye un apartado en el Área de Control del Entorno TIC sobre el cumplimiento del Cuerpo Normativo de Seguridad y de la legislación que afecta a estas materias, 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 2024, auditores externos e internos han realizado **más de 124 trabajos de auditoría** sobre sistemas de la información y seguridad, ciberseguridad, continuidad de negocio, sistemas cloud, inteligencia artificial, así como privacidad y protección de datos.

El año 2024, al igual que los ejecicios precedentes, se cerró sin ninguna recomendación de auditoría vencida. Las recomendaciones planificadas para los siguientes ejercicios han sido implantadas o están en fase de resolución, de acuerdo con los planes de acción establecidos

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:

13

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

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.

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".

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.**

Premio extraordinario del Jurado de los premios de RED SEGURIDAD.

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

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 fue 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.

A continuación, vemos la evaluación de benchmarks de terceros correspondientes al año 2024 en relación con la situación de seguridad en MAPFRE:

BITSIGHT The Standard in SECURITY RATINGS	**Rating Grupo MAPFRE: 740 (Nivel Avanzado)**
Dow Jones Sustainability Indexes	**100 puntos (sobre 100) en el apartado Privacy Protection**
CNPIC incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD	**4,7 puntos (sobre 5). Indicadores mejora CiberResiliencia - IMC. 2024.** • +0,4 puntos media sector financiero.
DSN isms forum	**Gestión de crisis cibernéticas 2024.** • Madurez "Muy Buena". • Por encima de la media de las empresas participantes.

- CNPIC: Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) de España
- DSN: Departamento de Seguridad Nacional de España. Órgano de asesoramiento al Presidente del Gobierno en materia de seguridad nacional.
- INCIBE: Instituto Nacional de Ciberseguridad, oficialmente S.M.E. Instituto Nacional de ciberseguridad de España M.P, S.A.
- ISMS FORUM: Asociación Española para el Fomento de la Seguridad de la Información.

MAPFRE