



**POLÍTICA CORPORATIVA DE SEGURIDAD Y PRIVACIDAD DEL GRUPO
MAPFRE**

ÍNDICE

I. Definiciones	3
II. Introducción	5
III. Alcance	5
IV. Objetivos	5
V. Compromisos	6
VI. Responsabilidades	7
VII. Aprobación, entrada en vigor y revisiones posteriores	7

I. Definiciones

A los efectos de esta Política, se entiende por:

Activo: conjunto de todas las capacidades, bienes, derechos, medios e intangibles, que son propiedad de una empresa, institución o individuo, o cuya posesión o derecho de explotación ostenta.

CiberRiesgos: siguiendo las definiciones del CRO Forum y del IAIS, son los riesgos asociados al desarrollo de una actividad de negocio, incluyendo la gestión y el control de datos, en un entorno digital o “Cíber”. Estos riesgos emanan del uso, tratamiento y transmisión de datos electrónicos mediante sistemas de información, redes de comunicaciones y la propia Internet, y engloban los daños físicos provocados por CiberIncidentes, así como los fraudes cometidos por el uso inapropiado o indebido de los datos. También se considera dentro de esta categoría la eventual petición de responsabilidades (liabilities) derivadas de la protección de la disponibilidad, integridad y confidencialidad de la información electrónica de individuos, compañías o gobiernos a los que MAPFRE tenga acceso en el ámbito del desarrollo de su actividad.

Riesgo relacionado con las TIC: cualquier circunstancia razonablemente identificable en relación con el uso de redes y sistemas de información que, si se materializa, puede comprometer la seguridad de las redes y sistemas de información, de cualquier herramienta o proceso dependiente de la tecnología, de las operaciones y los procesos o de la prestación de servicios, al provocar efectos adversos en el entorno digital o físico.¹

Control de Acceso: conjunto de medidas de diseño, software, equipos y medios técnicos destinados a regular la entrada o paso a las instalaciones, espacios, sistemas, aplicaciones, dispositivos, información y resto de activos del GRUPO MAPFRE, de forma que posibiliten restringir y conocer con el grado de detalle adecuado a cada uno de ellos, quién, cuándo y cómo, accede a los mismos, a la vez que facilite y agilice el acceso de las personas autorizadas.

Comité de Seguridad, Crisis y Resiliencia: máximo órgano ejecutivo de la Organización de Seguridad. Este Comité velará porque los objetivos y necesidades empresariales gobiernen la actividad de la Función de Seguridad Corporativa al mismo tiempo que garantizará que es contemplada como un elemento constituyente de los procesos de negocio corporativos, conforme a lo establecido en el Plan Director de Seguridad. El Comité de Seguridad, Crisis y Resiliencia asumirá también la dirección y control en el ámbito de la continuidad de negocio y la gestión de crisis.

Comité de Privacidad y Protección de Datos: comité específico subordinado al Comité de Seguridad, Crisis y Resiliencia para la dirección y control en el ámbito de la privacidad y protección de datos de carácter personal, apoyando al DPO en el desarrollo de sus funciones. Este comité ejercerá las funciones de comité de crisis en lo relativo a la gestión de incidentes y violaciones de seguridad de datos personales, incluyendo la coordinación, el seguimiento y

¹ Según definición del Reglamento de Resiliencia Operativa Digital del Parlamento Europeo y del Consejo (DORA)

toma de decisiones y la notificación a la Autoridad de Control y/o Afectados.

Función de Seguridad Corporativa: conjunto de actividades, personas, medios y recursos necesarios para alcanzar el adecuado grado de protección para los activos de una organización empresarial frente a los riesgos establecidos, garantizar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de sus datos personales, así como para dotar a la organización capacidades de resiliencia operativa, conforme a lo establecido en el Plan Director de Seguridad.

MAPFRE, GRUPO MAPFRE o GRUPO: el grupo empresarial integrado por MAPFRE S.A., como entidad matriz, y sus sociedades filiales y dependientes conforme a lo establecido en el artículo 4º de la Ley del Mercado de Valores.

Resiliencia Operativa: la capacidad de una entidad para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente mediante el uso de servicios prestados por proveedores terceros, toda la gama de capacidades necesarias para preservar la seguridad de las redes y los sistemas de información que utiliza la entidad y que sustentan la prestación continuada de sus servicios y la calidad de los mismos, incluso en caso de perturbación.

Plan Director de Seguridad: marco estratégico para el desarrollo de la Función de Seguridad Corporativa.

Privacidad: condición de privado, que garantiza los derechos de las personas físicas en lo que respecta al tratamiento de sus datos personales, incluyendo el respeto del derecho al honor y a la intimidad.

Riesgo: posibilidad de que eventos futuros den lugar a consecuencias adversas para la consecución de los objetivos económicos y de negocio o la situación financiera del GRUPO. El concepto de riesgo se entenderá en un sentido amplio, abarcando eventos o combinaciones de eventos que afecten a uno o varios riesgos que por su importancia o entidad requieran un tratamiento separado.

Riesgos de Seguridad: subconjunto de riesgos cuya gestión ha sido encomendada a la Organización de Seguridad, del total de riesgos que soportan los activos del GRUPO.

Seguridad:

1. Condición conseguida cuando los activos están protegidos contra los riesgos.
2. Calidad de seguro, esto es, exento de todo daño, peligro o riesgo.
3. Conjunto de medidas necesarias para alcanzar la condición anterior. En función de los activos que se protejan y de la naturaleza de las medidas, suele hablarse de diferentes tipos de seguridad, así Seguridad de la Información, Privacidad, Seguridad Laboral, Seguridad de las Personas, Seguridad contra Incendios, etc.

II. Introducción

La razón de ser 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 ello deberá proteger sus activos tangibles e intangibles y procesos de negocio, de forma permanente, frente a los riesgos de seguridad, velando especialmente por la seguridad de las personas, la seguridad de la información, la privacidad, la resiliencia operativa de los servicios prestados a terceros, la preservación de la buena reputación de la compañía, la sostenibilidad de la misma, y el cumplimiento normativo en dichos ámbitos.

En ese sentido, todos los empleados, directivos y colaboradores de MAPFRE son corresponsables de la protección de dichos activos y procesos, por lo que utilizarán los recursos que MAPFRE pone a su disposición de forma profesional y responsable, notificarán cualquier situación que detecten que pueda suponer un riesgo para la compañía y/o las personas que la integran y, con carácter general, aplicarán con debida diligencia las medidas que se establezcan al efecto.

La aspiración de liderazgo de MAPFRE y su vocación global inspiran, como en el resto de las actividades del GRUPO, las actuaciones en materia de seguridad; ámbito en el que también aspira a ser una referencia.

La presente Política está alineada con el Plan Director de Seguridad de MAPFRE, que establece el Marco Estratégico y el modelo para la realización de las diferentes actuaciones en materia de seguridad y gestión medioambiental del GRUPO.

III. Alcance

La presente Política Corporativa de Seguridad y Privacidad es de obligado cumplimiento en todo el GRUPO MAPFRE.

IV. Objetivos

Esta Política formaliza la respuesta del GRUPO MAPFRE frente a un escenario global y cambiante, que le permite dotarse de una Función de seguridad corporativa eficaz y acorde con los Principios Institucionales y Empresariales para llevar a cabo 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.

V. Compromisos

El GRUPO MAPFRE asume los siguientes compromisos de actuación en materia de seguridad y privacidad:

1. La seguridad de las personas, el bien más valioso para MAPFRE, es el primer objetivo y preocupación permanente.
2. El cumplimiento de la normativa de seguridad y privacidad, respetando de forma escrupulosa la legalidad vigente, de forma acorde con el principio del GRUPO de ser ética y socialmente responsable.
3. La integración de la seguridad y la privacidad en los procesos de negocio, como un componente más de los mismos, contribuyendo a su calidad y sostenibilidad.
4. La adopción de un modelo de seguridad integral y global de protección de los activos y procesos de negocio del GRUPO frente a los riesgos de seguridad y privacidad de cualquier naturaleza, con independencia del lugar en el que los mismos sean susceptibles de materializarse, y prestando especial atención a los riesgos relacionados con las TIC y a los CiberRiesgos, con objeto de garantizar la resiliencia operativa. En este sentido, se trasladarán a los proveedores terceros requisitos de seguridad proporcionales al riesgo de los servicios que prestan para el Grupo MAPFRE, con objeto de garantizar una protección homogénea de los activos corporativos y de la resiliencia operativa.
5. El aporte de valor añadido a MAPFRE y a sus procesos de negocio o soporte, a través de la búsqueda y aprovechamiento de sinergias con otras áreas y funciones del GRUPO en el desarrollo de su actividad.
6. La aplicación de principios de optimización de recursos, oportunidad, economía de escala y mejora continua, como manifestación del espíritu innovador y de búsqueda de la excelencia de MAPFRE.
7. La contribución a la confianza de los grupos de interés, posibilitando que éstos puedan desarrollar su labor y/o relacionarse con el GRUPO sin que los riesgos de seguridad perturben su voluntad y capacidad de decidir y actuar libremente.
8. La adecuada protección de la información propiedad de MAPFRE y de la perteneciente a sus clientes, colaboradores, empleados y resto de grupos de interés y a la que MAPFRE tiene acceso en virtud de la relación que mantiene con ellos, garantizando la confidencialidad, autenticidad, privacidad, disponibilidad e integridad de la misma, así como la de los sistemas que la almacenan, transmiten o procesan. Para ello, existirán las medidas y controles necesarios, entre ellos controles de acceso, según un enfoque de gestión de riesgos, que además garantizarán un tratamiento de acuerdo a los principios y criterios de privacidad establecidos en la legislación vigente. En particular, serán objeto de especial protección los centros en los que se procesa y custodia la información y datos mencionados (CPDs – Data Centers).

9. La formación y concienciación de todo su personal en materia de seguridad y privacidad, así como la divulgación de normas, procedimientos y responsabilidades. En este sentido, todos los empleados son conscientes de las obligaciones de garantizar, entre otros aspectos, la confidencialidad de la información y el cumplimiento de las normativas de protección de datos, estableciéndose en el Código Ético y de Conducta de MAPFRE, así como en su Código Telemático, la posibilidad de que, ante un incumplimiento de estos principios, se adopten las sanciones que correspondan según el régimen disciplinario vigente.
10. La permanente disposición a colaborar con las autoridades como parte del espíritu de servicio que impregna todas las actuaciones de MAPFRE y de la responsabilidad para con la sociedad en la que desarrolla su actividad.

VI. Responsabilidades

El Comité de Seguridad, Crisis y Resiliencia del GRUPO es el órgano responsable de impulsar el desarrollo e implantación de esta Política, así como de velar por el cumplimiento, divulgación y revisión periódica de la misma.

El resto de las responsabilidades asociadas a la gestión de la Seguridad y la Privacidad se formulan con el detalle necesario en el Marco de Gobierno de Seguridad de MAPFRE.

VII. Aprobación, entrada en vigor y revisiones posteriores

La presente Política Corporativa de Seguridad y Privacidad ha sido aprobada por el Consejo de Administración de MAPFRE, con fecha 26 de junio de 2024, a partir de la cual entra en vigor. Sustituye a la anterior versión de la misma (Política Corporativa de Seguridad y Privacidad del Grupo MAPFRE) aprobada por el Consejo de Administración de MAPFRE, S.A. con fecha 13 de diciembre de 2018.

Procederá su revisión al menos anualmente, pudiendo ser modificada en cualquier momento a propuesta del Comité Ejecutivo de MAPFRE para su adaptación a cualquier cambio significativo que afecte a alguno de sus contenidos.

Aprobada el 23 de julio de 2015

Última modificación aprobada el 26 de junio de 2024