POLÍTICA DE CONTINUIDAD DE NEGOCIO

POLÍTICA DE CONTINUIDAD DE NEGOCIO

1 Introducción

El Consejo de Administración de MAPFRE, S.A. (la "**Sociedad**") es el órgano competente para definir la estrategia general y establecer las bases para una adecuada y eficiente coordinación entre la Sociedad y las demás compañías integradas en el grupo de sociedades del que MAPFRE, S.A. es la entidad dominante en el sentido establecido en el artículo 42 del Código de Comercio (el "**Grupo**" o el "**Grupo MAPFRE**").

En ejercicio de estas competencias, aprueba y actualiza las políticas corporativas que rigen la actuación de la Sociedad y establece las pautas y los principios básicos que inspiran, presiden o son la base de obligada observancia de las normas que las demás compañías del Grupo aprueban en el ámbito propio de la capacidad de decisión y responsabilidad de cada una de ellas.

Asimismo, de conformidad con la normativa vigente que resulta de aplicación a la Sociedad en materia de resiliencia operativa y digital y con las exigencias derivadas de la normativa de Solvencia II, el Consejo de Administración debe aprobar una política de continuidad de negocio.

En este sentido, el Consejo de Administración de la Sociedad ha aprobado la presente *Política de continuidad de negocio* (la "***Política***"), que forma parte del sistema de gobierno corporativo del Grupo MAPFRE.

2 Calificación

La presente norma es una política de ámbito corporativo de acuerdo con la clasificación recogida en la *Política corporativa sobre la elaboración y la organización de las normas que integran el sistema de gobierno corporativo del Grupo MAPFRE*.

3 Finalidad

La presente *Política* establece el marco global para el desarrollo, documentación, implantación, prueba, revisión y mejora continua de los planes de continuidad de negocio del Grupo MAPFRE y de sus sistemas de gestión, incluyendo los elementos vinculados con la continuidad de la actividad en materia TIC y siguiendo un enfoque basado en riesgos.

4 Ámbito de aplicación

La presente *Política* es de aplicación a todas las sociedades que integran el Grupo MAPFRE. También resulta aplicable, en la medida en que proceda y atendiendo a los pactos de accionistas correspondientes, a las distintas alianzas y sociedades compartidas en las que participen sociedades del Grupo.

Sin perjuicio de lo anterior, los órganos de administración de las entidades aseguradoras y reaseguradoras del Grupo deberán aprobar una política similar a la presente *Política*, con las adaptaciones que, en su caso, sean estrictamente imprescindibles a fin de (i) hacerla compatible con las particularidades del negocio de dichas entidades y (ii) cumplir con cualesquiera normas de carácter sectorial o derivadas de la legislación aplicable o de los requerimientos de los supervisores en los países en los que desarrollen su actividad.

Dichas adaptaciones estarán sujetas a la revisión previa del Área de Resiliencia Operativa y GRC de la Dirección Corporativa de Seguridad.

5 Principios generales

La *Política* se sustenta en el conjunto de principios y compromisos que a continuación se exponen:

i. La protección y seguridad de las personas es la primera premisa y el objetivo prioritario, tanto en situaciones normales como de crisis.

ii. Los propietarios de los planes de continuidad de negocio deberán designar representantes de las distintas áreas con experiencia y conocimientos suficientes, para que participen activamente en el desarrollo, documentación, implantación, prueba, revisión, actualización y mejora continua de los planes de continuidad de negocio y de sus sistemas de gestión.

iii. El desarrollo e implantación de planes de continuidad de negocio por las empresas del Grupo tendrá en cuenta las áreas y departamentos internos y los proveedores y servicios, empleando sistemas, recursos y procedimientos adecuados y proporcionados. Los planes de continuidad de negocio incluirán disposiciones, planes, procedimientos y mecanismos específicos, adecuados y documentados, destinados a garantizar la continuidad de la actividad en materia TIC, articulados a través de las estrategias de recuperación asociadas a la indisponibilidad de la tecnología.

iv. El aprovechamiento de las sinergias generadas y las lecciones aprendidas en el desarrollo e implantación de los planes de continuidad de negocio y cualesquiera otros planes en el ámbito de la seguridad en las entidades del Grupo, teniendo en cuenta los medios y recursos comunes de los que disponen.

v. La adopción de medidas razonables para la continuidad operativa de los procesos y actividades, incluyendo la resiliencia operativa digital, en función de la criticidad establecida por el Grupo.

vi. La inclusión de criterios de seguridad, privacidad y fiabilidad que garanticen de forma razonable la continuidad de los servicios críticos proporcionados por terceros.

vii. La incorporación de procedimientos adecuados de comunicación de crisis en los planes de continuidad de negocio, que garanticen la transmisión de información relevante y oportuna. Estos procedimientos tendrán en cuenta y deberán cumplir lo dispuesto en la *Política de comunicación corporativa* y deben cubrir:

- La comunicación interna a todo el personal, diferenciando los mensajes dirigidos a las personas involucradas en la respuesta y recuperación, de los mensajes para el resto del personal.

- La comunicación externa, así como el suministro oportuno de información a las partes interesadas pertinentes (las cuales incluyen, entre otros, a accionistas, empleados, intermediarios, clientes, proveedores, supervisores y autoridades regulatorias, así como a otros actores clave para la continuidad del negocio).

viii. La comunicación de las responsabilidades y de los procedimientos que conciernen al personal del Grupo con competencias en el ámbito de la continuidad de negocio, mediante labores de concienciación y formación. Los contenidos a divulgar incluirán los procedimientos de escalado de los incidentes que pudieran producirse, teniendo en consideración tanto su naturaleza, como el escenario de indisponibilidad que estos pudieran ocasionar. Igualmente, se divulgará esta *Política* al personal del Grupo.

ix. Bajo la coordinación del Área de Resiliencia Operativa y GRC de la Dirección Corporativa de Seguridad, se establecerá un marco de referencia que sirva para fijar objetivos de continuidad de negocio dentro de un sistema de gestión que, cumpliendo con los requisitos legislativos, reglamentarios y los principales estándares aplicables, incluya revisiones, pruebas y actualizaciones periódicas de los planes de continuidad de negocio. Estas revisiones y actualizaciones tendrán en cuenta las lecciones aprendidas de las crisis e incidentes acontecidos y se realizarán (i) ante cambios significativos en la infraestructura tecnológica, (ii) como consecuencia de los resultados obtenidos tras la ejecución de pruebas o (iii) tras la aparición de nuevas amenazas. Todo ello, como parte de un proceso que permita evaluar regularmente la eficacia de las medidas de continuidad implementadas y garantizar la mejora continua de las capacidades de resiliencia operativa del Grupo.

x. La permanente disposición a colaborar con las autoridades en caso de desastre o necesidad, como parte del espíritu de servicio que impregna todas las actuaciones del Grupo y de la responsabilidad para con las sociedades en las que desarrolla su actividad.

6 Objetivos específicos en materia de continuidad de negocio

Los planes de continuidad de negocio y los sistemas de gestión asociados a los mismos serán desarrollados conforme a lo establecido en esta *Política*, de tal modo que*:*

a) Permitan, a través de la realización de análisis de impacto en el negocio ("**BIA**", por sus siglas en inglés), estimar con carácter preliminar las posibles repercusiones, daños y pérdidas que pueda suponer un incidente disruptivo que afecte a los procesos de negocio de la compañía. El BIA permitirá evaluar el impacto potencial de dichos incidentes mediante criterios cuantitativos y cualitativos, teniendo en cuenta las funciones identificadas como críticas y los recursos que las soportan.

b) Posibiliten una respuesta adecuada y oportuna ante la materialización de un riesgo de seguridad de características catastróficas, que provoque un escenario de falta de disponibilidad de alguno de los componentes básicos de la actividad del Grupo (personas, edificios y oficinas, tecnología, información y proveedores).

c) Aminoren la repercusión de las posibles catástrofes sobre las actividades de negocio, garantizando que se preservan los datos y funciones esenciales o, de no ser posible, que tales datos o funciones se recuperen, oportuna y progresivamente, hasta la vuelta a la normalidad.

d) Permitan, después de la ocurrencia de un incidente disruptivo, la recuperación de las funciones identificadas como críticas y el restablecimiento del resto de las actividades normales de negocio, cumpliendo con los objetivos de tiempos y puntos de recuperación identificados en el BIA. Estos objetivos podrán variar dependiendo de la naturaleza del incidente y la criticidad de las operaciones afectadas.

e) Garanticen que, ante un incidente de las características descritas, las actividades pueden ser operadas adecuadamente durante un período de tiempo suficiente, de acuerdo con las necesidades del negocio y hasta que el funcionamiento normal haya sido restaurado.

f) Contribuyan a la mejora continua de las capacidades de resiliencia operativa del Grupo MAPFRE, mediante la realización de pruebas anuales que permitan comprobar el correcto funcionamiento de las estrategias implantadas y que ayuden a la identificación de áreas de mejora.

7 Responsabilidades

El Comité de Seguridad, Crisis y Resiliencia del Grupo es el órgano responsable de impulsar y coordinar el desarrollo, la implantación, la evolución y la mejora continua de los planes de continuidad de negocio en las entidades del Grupo, así como de decidir y coordinar las actividades de implantación, mantenimiento y mejora del sistema de gestión de continuidad de negocio asociado a cada plan

de continuidad de negocio. Dichas actuaciones proporcionan protección, reducen la probabilidad de ocurrencia y el impacto de eventos de desastre o catástrofe y facilitan la preparación, respuesta y recuperación ante disrupciones, incluidas aquellas con afectación al entorno TIC.

Según el impacto potencial estimado por el Comité de Seguridad, Crisis y Resiliencia tras evaluar el incidente, éste decidirá la conveniencia o no de activar sin demora los planes de continuidad y otros planes de acción complementarios que corresponda, incluidos los planes de comunicación de crisis. Todo ello, con el fin de proporcionar una respuesta centralizada, oportuna y eficaz a los incidentes y limitar sus posibles efectos adversos.

Asimismo, dicho comité asumirá el liderazgo y el control de la gestión de las crisis que involucren a varias entidades del Grupo o que, por sus características, superen el alcance contemplado en los planes de continuidad de negocio de las diversas entidades, ya sea por afectar a varias sociedades del Grupo o a más de una región, requerir inversiones económicas extraordinarias que excedan el ámbito de las entidades o de las unidades de negocio, o tener el potencial de afectar de manera relevante a la posición competitiva y/o a la reputación del Grupo MAPFRE.

Además, el Comité de Seguridad, Crisis y Resiliencia determinará el momento en que se da por finalizada la situación de crisis y se retorna a la normalidad, que podrá realizarse de forma progresiva, dependiendo del impacto y de la eficacia de las medidas adoptadas.

El Comité de Seguridad, Crisis y Resiliencia dará cuenta de sus actividades al Comité Ejecutivo de la Sociedad y le informará de las actuaciones llevadas a cabo y de las medidas adoptadas en situaciones de crisis que requieran la activación de planes de continuidad de negocio.

El resto de los roles y las responsabilidades asociadas a la gestión de la continuidad de negocio se detallan en el *Marco de gobierno de gestión de crisis y continuidad de negocio de MAPFRE* aprobado por el Comité Corporativo de Seguridad, Crisis y Resiliencia.

8 Supervisión, difusión y seguimiento de esta *Política*

La Dirección Corporativa de Seguridad es el Promotor de esta *Política*, según este término se define en la *Política corporativa sobre la elaboración y la organización de las normas que integran el sistema de gobierno corporativo del Grupo MAPFRE*.

Por su parte, el Comité de Seguridad, Crisis y Resiliencia del Grupo es el órgano responsable de impulsar el desarrollo e implantación de esta *Política*.

Sin perjuicio de lo anterior, los órganos de administración y de dirección de las compañías del Grupo, tanto los corporativos como los regionales y locales, son los responsables de la difusión y el cumplimiento de esta *Política* en sus

respectivas sociedades. A dicho efecto, deberán adoptar las medidas necesarias para ello, así como comunicar, en su caso, por los cauces establecidos, los aspectos que no cumplan o cumplan parcialmente.

La revisión de esta *Política* se llevará a cabo, al menos, anualmente, pudiendo ser modificada en cualquier momento por el Consejo de Administración de MAPFRE, S.A., previo informe de la Comisión de Riesgos, Sostenibilidad y Cumplimiento, para su adaptación a cualquier cambio significativo que afecte a alguno de sus contenidos. A tal efecto, tendrán en cuenta la información proporcionada por el Comité de Seguridad, Crisis y Resiliencia y por el Promotor de esta *Política* en relación con los resultados de las pruebas realizadas, las recomendaciones derivadas de los controles de auditoría o las revisiones que pudieran producirse por parte de los órganos supervisores.

En el marco del compromiso de la Sociedad con sus grupos de interés, esta *Política* se publicará en la página web corporativa.

9 Aprobación y entrada en vigor de esta *Política*

Esta *Política* fue aprobada inicialmente por el Consejo de Administración de la Sociedad el 20 de diciembre de 2021 y modificada por última vez el 22 de diciembre de 2025, derogando y sustituyendo a la versión anteriormente vigente.