

CAPÍTULO 10 POLÍTICA DE CONTINUIDAD DE NEGOCIO

10.1 PROPIETARIO DE LA POLÍTICA

La Dirección Corporativa de Seguridad.

10.2 ALCANCE

La presente Política de Continuidad de Negocio es de obligado cumplimiento para todas las entidades del Grupo MAPFRE, con independencia de que estas puedan requerir implantar ajustes en su contenido para satisfacer requisitos específicos adicionales de sus respectivas autoridades o supervisores locales.

10.3 OBJETIVOS

Mediante esta Política se establece el marco global para el desarrollo, documentación, implantación, prueba, revisión y mejora continua de los Planes de Continuidad de Negocio en MAPFRE y de sus Sistemas de Gestión, incluyendo los diferentes elementos vinculados con la continuidad de la actividad en materia TIC y siguiendo un enfoque basado en el riesgo, de tal modo que:

- 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 críticas¹ y los recursos que las soportan.
- 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.
- 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.
- Permitan, después de la ocurrencia de un incidente disruptivo, la recuperación de las funciones identificadas como críticas y el restablecimiento del resto de las normales actividades 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.
- Garanticen que las actividades pueden ser operadas adecuadamente durante un periodo de tiempo suficiente, de acuerdo con las necesidades del negocio y hasta que el funcionamiento normal haya sido restaurado.
- Contribuyan a la mejora continua de las capacidades de resiliencia operativa de la compañía, 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.

10.4 PRINCIPIOS GENERALES

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

1. La protección y seguridad de las personas es la primera premisa y el objetivo prioritario, tanto en situación normal como en situación de crisis derivada de un desastre.

¹ Incluyendo aquellas identificadas como Funciones Esenciales o Importantes por el Reglamento de Resiliencia Operativa Digital (DORA).

2. El nombramiento de representantes de las distintas áreas con la debida experiencia y conocimiento, 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.
3. El desarrollo e implantación de Planes de Continuidad de Negocio por las empresas del Grupo teniendo en cuenta las áreas y departamentos internos, proveedores y servicios y empleando sistemas, recursos y procedimientos adecuados y proporcionados. Los Planes de Continuidad de Negocio incluirán las 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.
4. 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, contemplando los medios y recursos comunes de los que dispone MAPFRE.
5. La adopción de medidas razonables para la continuidad operativa de los procesos y actividades, incluyendo la resiliencia operativa digital, en función de la criticidad de los mismos establecida por la Organización.
6. La inclusión de criterios de seguridad, privacidad y fiabilidad que garanticen de forma razonable la continuidad de los servicios críticos proporcionados por terceros, en caso de su externalización.
7. La elaboración de procedimientos de comunicación de crisis apropiados dentro de los Planes de Continuidad de Negocio, que garanticen la transmisión de información relevante y oportuna. Estos procedimientos 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, de manera que posibiliten su correcta ejecución, así como el suministro oportuno de información a todas las partes interesadas pertinentes.
8. La comunicación de las responsabilidades y de los procedimientos que le conciernen, a todo el personal con competencia en el ámbito de la Continuidad de Negocio, mediante labores de concienciación y formación; así como la divulgación de esta Política al personal de la Organización. 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.
9. Un marco de referencia que sirva para establecer los objetivos de Continuidad de Negocio dentro de un Sistema de Gestión que, cumpliendo con los requisitos legislativos, reglamentarios y de los principales estándares en la materia aplicables, contemple la realización de revisiones, pruebas y actualizaciones de los Planes de Continuidad de Negocio de forma periódica. Estas revisiones y actualizaciones tendrán en consideración las lecciones aprendidas de las crisis e incidentes acontecidos, debiendo realizarse (i) ante cambios significativos en la infraestructura tecnológica, (ii) como consecuencia de los resultados obtenidos tras la ejecución de las pruebas o (iii) derivados de 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 que garantice la mejora continua de las capacidades de resiliencia operativa de la Organización.
10. 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 de MAPFRE y de la responsabilidad para con la sociedad en la que desarrolla su actividad.

10.5 RESPONSABILIDADES

El Comité de Seguridad, Crisis y Resiliencia del Grupo MAPFRE es el órgano responsable de impulsar y dirigir el desarrollo, implantación, evolución y 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. Las actuaciones anteriores permitirán proteger y reducir la probabilidad de ocurrencia e impacto de eventos de desastre o catástrofe, así como prepararse, responder y recuperarse de las disrupciones que pudieran producirse, incluidas aquellas con afectación al entorno TIC.

Según el impacto potencial estimado por el Comité tras evaluar el incidente, éste decidirá la conveniencia o no de la activación sin demora de los Planes de Continuidad y otros planes de acción complementarios que pudiera determinar, 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 asume el liderazgo y control de la Gestión de las Crisis que involucren a varias entidades del Grupo o que por sus características tengan un alcance mayor al contemplado en los Planes de Continuidad de Negocio de las distintas entidades, es decir, que tengan repercusiones multientidad y afecten a más de una región, requieran inversiones económicas extraordinarias que excedan el ámbito de las entidades/unidades, o tengan el potencial de afectar de manera relevante a la posición competitiva y/o a la reputación del Grupo MAPFRE.

Además, establecerá el momento en que se da por finalizada la situación de crisis y se produce el retorno a la normalidad. Esta vuelta a la normalidad podrá realizarse de forma progresiva, dependiendo del impacto y de la eficacia de las medidas adoptadas.

El Comité de Seguridad, Crisis y Resiliencia del Grupo será también el encargado de velar por el cumplimiento, divulgación y revisión periódica de esta Política.

Por otro lado, el Consejo de Administración de MAPFRE S.A será responsable de aprobar, supervisar y revisar periódicamente la aplicación de la presente política.

El resto de roles y responsabilidades asociadas a la gestión de la Continuidad de Negocio se formulan con el detalle necesario en el Marco de Gobierno de Gestión de Crisis y Continuidad de Negocio de MAPFRE.

10.6 ACTUALIZACIÓN

La presente Política de Continuidad de Negocio se revisará anualmente, teniendo en cuenta 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.