Ibermática

Política General de la Continuidad de Negocio

SGQ-SGCN-POLCN (01)

Control de la documentación

La última versión de este documento está disponible en la Intranet. Si utiliza el documento impreso (documento no controlado) ***asegúrese que es la versión vigente y que está completo*** *consultando la lista de documentos vigentes del Sistema de Gestión de la Calidad integrado publicada en la Intranet*

Participantes

Responsabilidad	Nombre / función
Propietario:	Ibermática S.A.
Desarrollado por:	Jesús Martín González / Responsable de Calidad y Privacidad. Delegado de Protección de Datos
Revisado por:	M. Jesús Crespo Fernández / Seguridad Juan Carlos Chamizo Aragón / Chief Information Security Officer
Aprobado por:	Jesús Martín González / Responsable de Calidad y Privacidad. Delegado de Protección de Datos

Memoria

Versión	Fecha aprobación	Cambio producido
01	15/07/2020	Primera versión.

Contenidos

1. Política General de la Continuidad de Negocio

La Dirección, como política general, garantiza la adecuada gestión de la Continuidad de Negocio de los servicios prestados desde el Centro de Servicios Madrid (CSM), contemplados en el alcance del SGCN.

El objetivo global de la Continuidad de Negocio de Ibermática, es realizar los preparativos necesarios y planificar un conjunto suficiente de procedimientos para responder de forma adecuada ante un incidente, desde el momento en que se declare el desastre hasta la vuelta a la normalidad, de forma que se reduzca al mínimo su impacto sobre el negocio.

La Política de Continuidad establece un marco apropiado a las características de CSM (naturaleza, complejidad, criticidad de las actividades, etc.) que repercute directamente en el entorno operativo, centro de trabajo y cultura de empresa con el que identificar, desarrollar, implantar, operar, mantener, revisar y probar las medidas necesarias para garantizar el correcto funcionamiento del Plan de Continuidad de Negocio (PCN) de CSM, ante la materialización de un incidente.

La Política de Continuidad se sustenta en un conjunto de principios que han sido formulados basándose en las necesidades del negocio y el entendimiento de los riesgos asociados.

Dichos principios son:

- La primera premisa y el objetivo prioritario es la protección y seguridad del personal, tanto en situación normal como en situación de contingencia.
- La Dirección se responsabiliza de la gestión de los riesgos clave y el análisis de impacto de negocio para la continuidad operativa de los procesos considerados críticos para Ibermática.
- La Dirección garantiza que el PCN se desarrolla e implanta de forma adecuada, teniendo en cuenta todas las áreas, proveedores y servicios críticos.
- La Dirección garantiza que el PCN se mantiene actualizado, se revisa, se prueba y, en su caso, se mejora de forma periódica o ante cambios significativos en premisas, personas, procesos, mercados, tecnología o estructura organizativa; para lo cual participarán activamente en dicha revisión las distintas Áreas de Negocio y/o de Soporte con procesos identificados como críticos.
- Las distintas Áreas de Negocio y/o de Soporte nombran representantes con la debida experiencia para que formen parte de los Comités y Equipos de Continuidad de Negocio y participen en el PCN.
- La Dirección garantiza que todo el personal de las distintas Áreas de Negocio y/o de Soporte está informado de las responsabilidades que le competen en el marco de la Continuidad de Negocio, mediante labores periódicas de formación, divulgación y prueba del PCN.
- La Dirección garantiza que los procesos críticos son recuperados dentro de los márgenes de tiempo requeridos en el PCN.
- La Dirección garantizará la promoción y divulgación de la capacidad de Continuidad de Negocio dentro de la cultura de empresa, al igual que el impacto del PCN en nuevos desarrollos de Ibermática.
- La Dirección garantiza la elaboración de planes de comunicación apropiados, tanto internos como externos, que son revisados y actualizados de forma periódica.
- Aunque cada unidad y servicio de CSM disponga de su propio PCN, se aprovechan las sinergias generadas.

La Dirección establece los procedimientos y formas de actuación necesarios para garantizar el correcto desarrollo de esta política, que se plasman en un SGCN, documentado y conocido por todo el personal de los servicios del alcance, y que cumple los requisitos establecidos en la norma ISO·22301.

Todo usuario tendrá la obligación de reportar los incidentes en materia de continuidad utilizando las directrices establecidas por Ibermática.

La Dirección de Ibermática tiene potestad de modificar la Política General o las Políticas Específicas de Continuidad del Negocio de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

Esta política debe ser revisada al menos una vez al año, debiendo actualizarse al efecto; al igual que la documentación que pueda formar parte o referenciada por ésta.

La presente política se pone en su conocimiento y es comunicada a todas las partes interesadas.

1.1. Alcance

Esta política es de aplicación a Ibermática S.A. y a todas las sociedades del Grupo Ibermática (en adelante Ibermática).

La presente política es de obligado cumplimiento para todas las sociedades de Ibermática, los departamentos que las componen y sus empleados en el ámbito del Sistema de Gestión de Continuidad del Negocio (SGCN) implantado.

1.2. Documentos relacionados

- Listado de Requisitos legales y reglamentarios
- UNE-EN ISO 22301:2020. Seguridad y resiliencia. Sistema de Gestión de la Continuidad del Negocio. Requisitos.
- UNE-EN ISO 22313:2020. Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para la utilización de la norma ISO 22301.
- UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información
- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- Manual del Sistema de Gestión de Seguridad de la Información
- Manual de Análisis de Riesgos
- Manual del Sistema de Gestión de Continuidad del Negocio