Política de riesgos de ciberseguridad

SGQ-SGSI-POL-CYBRSK (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:	Oficina Técnica del CISO
Revisado por:	Jesús Martín González / Responsable de Calidad y Privacidad. Delegado de Protección de Datos César Sáiz Sanz / Asesoría Jurídica y Chief Compliance Officer (CCO) Juan Carlos Chamizo Aragon / Chief Information Security Officer (CISO)
Aprobado por:	Juan Carlos Chamizo Aragon / Chief Information Security Officer (CISO)

Memoria

Versión	Fecha aprobación	Cambio producido
01	29/03/2022	Primera versión.

Contenidos

1. Introducción

La Política de riesgos de ciberseguridad establece un marco global para el control y la gestión de los riesgos de ciberseguridad aplicable a todas las sociedades del Grupo Ibermática (en adelante Ibermática). En particular, se refiere a los riesgos derivados de amenazas y vulnerabilidades que afecten a los sistemas de control o sistemas de información y comunicaciones de Ibermática, así como a cualquier otro activo que forme parte de su infraestructura TI y ciberseguridad.

Asimismo, establece las directrices de un modelo de gestión de la ciberseguridad común para todo Ibermática coordinado por un Comité de Seguridad Global (CSG) y basado en el desarrollo de normas y estándares globales de aplicación en todos los negocios y funciones corporativas, que fomenten una sólida cultura de ciberseguridad.

1.1. Objeto

El objeto del presente documento es la definición de las reglas necesarias para un marco global para el control y la gestión de los riesgos de ciberseguridad.

1.2. Alcance

La presente política es de obligado cumplimiento para todos los empleados, fijos o temporales, y terceros que trabajen o actúen en nombre de Ibermática, S.A. (o cualquier empresa del Grupo Ibermática), independientemente de si realizan su función habitual presencialmente en el centro de trabajo, como colaborador tecnológico o trabajando desde casa en el ámbito del Sistema de Gestión de Seguridad de la Información (SGSI).

1.3. Contenido

Además de este capítulo introductorio, el presente documento incluye:

- Política de riesgos de ciberseguridad
- Cumplimiento y revisión

1.4. Documentos relacionados

- Política general de seguridad de la información
- Código de buenas prácticas para la protección de datos personales (en Ibermática) v01
- Código de conducta
- Política de protección de datos
- Política general de calidad
- Política de compliance penal y antisoborno

2. Política de riesgos de ciberseguridad

2.1. Principios básicos

La Política de riesgos de ciberseguridad se fundamenta en los siguientes principios básicos:

- Sensibilizar a todo el personal de Ibermática, a los proveedores y a los colaboradores acerca de los riesgos de ciberseguridad y garantizar que disponen de los conocimientos, habilidades, experiencia y capacidades necesarias para sustentar los objetivos de ciberseguridad de Ibermática.
- Garantizar que los ciberactivos de Ibermática poseen un nivel de ciberseguridad y ciber-resiliencia adecuados y aplicar los estándares más avanzados en aquellos que soporten la operación de ciberinfraestructuras críticas.
- Impulsar la existencia de mecanismos de ciberseguridad y ciber-resiliencia adecuados para los sistemas y operaciones gestionados por terceros que presten servicios a Ibermática.
- Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades de terrorismo y delincuencia en el ciberespacio.
- Dotarse de procedimientos y herramientas que permitan adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y a las nuevas amenazas.
- Colaborar con los organismos reguladores relevantes para contribuir a la mejora de la ciberseguridad en el ámbito nacional e internacional.
- Promover los principios establecidos en la Política general de seguridad en materia de ciberseguridad.
- Proteger la información sobre las ciberinfraestructuras críticas y los sistemas de ciberseguridad de Ibermática.
- Implementar medidas de ciberseguridad basadas en criterios de eficiencia y que contribuyan a la funcionalidad de los sistemas y la continuidad de los servicios clave.
- Actuar de acuerdo a la legislación vigente, el Código de Conducta, los sistemas de gestión implantados y demás normativa interna de Ibermática.

La Política de riesgos de ciberseguridad recoge el compromiso de Ibermática de informar sobre sus riesgos e incidentes en materia de ciberseguridad de forma clara y transparente, de conformidad con lo dispuesto con la ley. Ibermática deberá informar al mercado a través de INCIBE-CERT sobre los riesgos y los incidentes de ciberseguridad no públicos, que se refieran directa o indirectamente a Ibermática y que, de hacerse públicos, puedan influir de manera apreciable sobre cualquier valor que Compliance defina como elemento afectado.

Hasta que dicha información sea pública, las personas que conozcan la existencia del riesgo o incidente de que se trate tendrán la consideración de informados y, entre otras restricciones, no podrán realizar operaciones sobre los elementos afectados y estarán sujetas al deber de confidencialidad.

3. Cumplimiento y revisión

Los incumplimientos de esta política se gestionarán según lo estipulado en el Código de Conducta de Ibermática.

Esta política será revisada al menos una vez al año y actualizada en caso de ser necesario, a fin de asegurar su eficiencia y efectividad.