Ibermática

Política General de Seguridad de la Información

SGQ-SGSI-POLSEG (02)

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 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) Ana Corrales / Consultor QMSi
Aprobado por:	Juan Carlos Chamizo Aragon / Chief Information Security Officer (CISO)

Memoria

Versión	Fecha aprobación	Cambio producido
01	31/12/2019	Primera versión.
02	24/01/2022	• Revisión erratas y actualización de contenidos. • Actualización organización 2022.

Contenidos

1. Introducción

La Política de Seguridad de la Información proporciona el marco para que Ibermática cumpla sus objetivos de protección de la información y de los activos tecnológicos que posee.

Esta política se basa en la norma de la Organización Internacional de Normalización (ISO) 27002:2017 para la gestión de la seguridad de la información (Tecnología de la información-Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información). Esta norma proporciona un enfoque estructurado para identificar el amplio espectro de actividades de seguridad de la información en el ciclo de vida de los sistemas de información.

La política de seguridad de la información incorpora un enfoque de la seguridad basado en los riesgos, utilizando las evaluaciones de amenazas y riesgos para determinar sus implicaciones en los procesos empresariales y la prestación de servicios, así como las implicaciones tecnológicas y las estrategias de comunicación, incluidos los programas de concienciación sobre la seguridad de la información.

1.1. Objeto

El objeto de la Política de Seguridad de la Información es asegurar la continuidad del negocio de Ibermática y minimizar el riesgo de daños monitorizando, previniendo o mitigando incidentes de seguridad y reduciendo su potencial impacto. También establece la estructura formal de la organización de la seguridad con funciones, responsabilidades y rendición de cuentas claramente definidas.

1.2. Alcance

El alcance de esta política se extiende a:

- Ibermática S.A. y a todas las sociedades del Grupo Ibermática, así como al personal interno, externo y empleados de terceros bajo contrato, que tienen acceso o participación en los procesos comerciales, los activos de información y los activos y procesos de TI de apoyo cubiertos por el alcance del SGSI.
- Procesos de Ibermatica: todos los procesos basados en las tecnologías de la información (adquisición, almacenamiento, transporte y distribución), así como los activos de información críticos y sensibles, incluyendo los documentos en papel.
- Activos de Ibermática: todos los activos de hardware, de software, de red, servicios de telecomunicaciones y de mantenimiento, así como la Intranet de la organización.

1.3. Contenido

Además de este capítulo introductorio, el presente documento incluye:

- Política General de la Seguridad de la Información
- Cumplimiento y revisión

1.4. Documentos relacionados

- Listado de Requisitos legales y reglamentarios
- Convenio colectivo de Ibermática, vigente.
- UNE-EN ISO/IEC 27000:2021. Documento de AENOR: Sistemas de Gestión de Seguridad de la Información - Visión de conjunto y vocabulario
- UNE-EN ISO/IEC 27001:2017. Documento de AENOR: Sistemas de Gestión de Seguridad de la Información - Requisitos.
- UNE-EN ISO/IEC 27002:2017. Documento de AENOR: Código de prácticas para 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
- UNE-EN ISO/IEC 27018:2020 Documento de AENOR: Código de práctica para la protección de indentificación personal (PII) en nubes públicas que actúan como procesadores PII
- UNE-EN ISO/IEC 27701:2021 Documento de AENOR: Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestion de privacidad de la Información. Requisitos y directrices
- Manual del Sistema de Gestión de Seguridad de la Información
- Manual de Análisis de Riesgos
- Manual del Sistema de Gestión de Continuidad del Negocio

2. Política General de Seguridad de la Información

2.1. Principios de la Seguridad de la Información en Ibermatica

En Ibermática, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

La gestión de la seguridad de la información en Ibermatica se fundamenta en los siguientes pilares:

- Asegurar la **integridad** de todos los procesos comerciales, los activos de información y los activos y procesos de TI de apoyo, a través de la protección contra modificaciones no autorizadas, o contra la modificación o destrucción indebida de la información. También incluye garantizar el no repudio y el rechazo de la información. La modificación o destrucción no autorizada de información podría tener un efecto adverso grave o catastrófico en las operaciones de la organización, los activos de la organización o las personas.
- Asegurar la **disponibilidad** de todos los procesos de negocio, activos de información y activos y procesos de TI de apoyo para los usuarios autorizados cuando sea necesario, lo que garantiza el acceso y el uso oportunos y confiables de la información. La interrupción del acceso o uso de la información o un sistema de información podría tener un efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.
- Asegurar la **confidencialidad** de todos los activos de información (la información no se divulga a personas no autorizadas mediante una acción deliberada o descuidada). Preservar las restricciones autorizadas sobre el acceso y la divulgación de información, incluidos los medios para proteger la privacidad personal y la información de propiedad. La divulgación no autorizada de información podría tener un efecto adverso limitado en las operaciones de la organización, los activos de la organización o las personas.

Consciente de las necesidades actuales, Ibermática implementa un Sistema de Gestión de Seguridad de la Información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

La Política General de Seguridad de la Información de Ibermática se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información. Se establecen políticas de seguridad de la información, las cuales se fundamentan en los dominios y objetivos de control de la norma internacional ISO/IEC 27001:2017. También se concreta y desarrolla en normativas y procedimientos del SGSI, las cuales se integran, en la medida de lo posible, con los demás sistemas de gestión de la organización compartiendo aquellos recursos en pro de la optimización y buscando la mejora continua de la eficiencia y eficacia de la gestión de los procesos: Sistema de Gestión de Calidad, Sistema de Gestión de Servicios de TI, Sistema de Gestión de Continuidad del Negocio, Sistema de Gestión de Privacidad de la Información, Sistema de Gestión de Medioambiente.

Ibermática establece, define y revisa unos objetivos dentro de su Sistema de Gestión de Seguridad de la Información (SGSI) encaminados a mejorar su seguridad, entendiéndola como la conservación de la confidencialidad, disponibilidad e integridad de su información, así como de los sistemas que la soportan, aumentando la confianza de nuestros clientes y otras partes interesadas; junto con el cumplimiento de todos los requisitos legales, reglamentarios y contractuales que le sean de aplicación.

El diseño, implantación y mantenimiento del SGSI se apoya en los resultados de un proceso continuo de análisis y gestión de riesgos del que se derivan las actuaciones a desarrollar en materia de seguridad dentro del alcance de su sistema que es “Sistema de Gestión de la Seguridad de la Información (SGSI) asociado a los servicios de atención a usuarios, comunicaciones, desarrollo y mantenimiento de software, data center y sistemas distribuidos, desplegados en el Centro de Servicios Madrid (CSM), el Servicio CDATEX (Centro Distribuido de Atención Técnica de Extremadura) del Servicio Extremeño de Salud (SES), el Servicio de Mantenimiento de aplicaciones de Ibermática para Kutxabank (SIK), y los Servicios de Soporte Técnico Plataformas para Batera, Osakidetza y EJIE, de acuerdo a la Declaración de Aplicabilidad IB_SOA-V09 de fecha 10/01/2022".

2.2. Objetivos

La implantación de este sistema de gestión (SGSI) en Ibermática se encuentra encaminada al cumplimiento de los siguientes objetivos:

- Cumplimiento de las leyes, regulaciones y obligaciones contractuales que son aplicables a la organización en general y en particular a su SGSI.
- Cumplimiento de todos los requisitos de seguridad de la información aplicables.
- Realizar mantenimiento y supervisión de todos los registros de auditoría.
- Implantación de un proceso de mejora continua del sistema de gestión de seguridad de la información (PDCA).
- Seguimiento de los cambios operativos y de sistemas, a través de una herramienta de monitorización que asegure el cumplimiento del proceso de gestión de cambios.
- Implantación de un proceso de gestión de incidentes de seguridad en todas las etapas de su ciclo de vida: preparación, identificación, contención, mitigación, recuperación, post-incidente. Este proceso debe explicar manera clara y sin ambigüedades los mecanismos y métodos para realizar los reportes de incidentes de seguridad, así como también la información mínima a proporcionar.
- Realización de un inventario de los activos de información, infraestructuras y dependencias externas que representan algún valor para la compañía, que se encuentre debidamente actualizado, estando cada uno de los activos perfectamente identificado con un propietario y un responsable asignado.
- Todos los procesos de gestión de la seguridad deben tener asignados un responsable.

2.3. Responsabilidades

La Dirección de Ibermática establece los criterios de evaluación del riesgo de manera que todos aquellos escenarios que impliquen un nivel de riesgo inaceptable sean tratados adecuadamente. Como parte del SGSI, la Dirección desarrolla, implanta y mantiene actualizado un Plan de Continuidad de Negocio acorde a las necesidades de Ibermática y dimensionado a los riesgos que le afectan.

La Dirección de Ibermática se compromete a la implantación, mantenimiento y mejora del SGSI dotándolo de aquellos medios y recursos que sean necesarios e instando a todo el personal para que asuma este compromiso. Para ello Ibermática implanta las medidas requeridas para la formación y concienciación del personal con la seguridad de la información. A su vez, cuando los empleados incumplan las políticas de seguridad, la Dirección se reserva el derecho de aplicar las medidas disciplinarias acordes al convenio de Ibermática vigente y dentro del marco legal aplicable, y dimensionadas al impacto que tengan sobre la organización.

La responsabilidad general de la seguridad de la información recae sobre el CISO, siendo la responsabilidad última de la Dirección como máximo responsable del SGSI implantado.

Todo el personal interno, proveedores, y en general todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de Ibermática, deben adoptar los lineamientos contenidos en el presente

documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

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

La Dirección de Ibermática tiene potestad de modificar la Política General o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de estas.

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

3. Cumplimiento y revisión

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

A fin de asegurar la eficiencia y efectividad, 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.