SGSI10

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Elaborado: 11/06/2018

Revisado y aprobado: 25/09/2024

izertis

Índice

1. CAPÍTULO I. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE IZERTIS

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de IZERTIS publicándose esta en nuestra página web bajo el apartado **Catálogo de Políticas** de la página web de IZERTIS.

IZERTIS ha seleccionado el estándar internacional UNE-ISO/IEC 27001 considerando su Anexo A (ISO /IEC 27002) así como el Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, como el marco general para la definición de un Sistema de Gestión de Seguridad de la Información, y aquellas medidas y controles aplicables. En base a estas normas y legislación se han determinado los principios generales para la seguridad de la información en el conjunto de documentos (procedimientos, planes y formatos) del Sistema de Gestión de Seguridad de la Información.

El presente documento constituye la Política de la Seguridad de la Información y tendrá vigencia una vez aprobada por la Dirección, poniéndose en conocimiento de todo el personal de la organización, incluidos aquellos externos a los que sea de aplicación. La presente política está alineada con las directrices de las leyes y regulaciones existentes y proporciona un marco de referencia para el establecimiento de los objetivos de seguridad de la información. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente a la organización.

Toda violación de la presente política o de las normas y procedimientos que las desarrollan, será considerado por el procedimiento disciplinario, incluyéndose proveedores y colaboradores externos.

En virtud de lo expuesto, la Política de Seguridad de la Información de IZERTIS se regirá por el siguiente articulado:

Artículo 1. Objeto y ámbito de aplicación

Constituye el objeto de la presente resolución la aprobación de la Política de Seguridad de la Información, en adelante Política de Seguridad, de IZERTIS y el establecimiento de un marco organizativo y tecnológico de la misma.

Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuación puntual o de tratamiento coyuntural.

Debe ser conocida y cumplida por todo el personal de IZERTIS, independientemente del puesto, cargo y responsabilidad dentro del mismo.

Artículo 2. Misión

La información y los procesos que la apoyan, sistemas y redes son importantes activos de IZERTIS. La confidencialidad, integridad, disponibilidad, trazabilidad, y autenticidad de la información son esenciales para mantener la calidad de los servicios y la reputación e imagen de la entidad.

Este documento tiene como objetivo establecer las directrices que garanticen la seguridad de la información en IZERTIS a un nivel adecuado según el nivel de riesgo de los activos, necesidades y recursos.

Asimismo, corresponden a IZERTIS las competencias y funciones establecidas por los estatutos de la propia organización, así como aquellas que deriven de su relación con el resto de las empresas, entidades jurídicas, Administraciones Públicas del Estado o personas físicas.

Artículo 3. Legislación y normativa de referencia

Serán base del cumplimiento normativo para la generación de la presente política de seguridad, la legislación y normativa aplicable relacionada en el documento **PO.SEG.13_Procedimiento de Cumplimiento Legal.**

Igualmente serán de aplicación otras normativas internas.

Artículo 4. Principios de la Seguridad de la Información

Los principios que conforman la Política de Seguridad de la Información son los siguientes:

a) La información que posee y trata IZERTIS tiene un valor muy importante para la propia compañía, así como para todas las partes interesadas.
b) La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola adecuada a los niveles de confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad debida.
c) La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
d) Los servicios prestados deberán proteger la información proporcionada y a sí mismos, en observación de las dimensiones de seguridad de integridad y disponibilidad.
e) La Seguridad de la Información es responsabilidad de todos. Todas las personas que tengan acceso a la información de IZERTIS deben atender a la necesidad de protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
f) La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
g) La información relativa a las personas y ciudadanos que trate IZERTIS pertenece a ellos y no a la entidad, conforme a la normativa de protección de datos de carácter personal del que se da debido cumplimiento.

h) Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos, según los preceptos marcados por la normativa interna.

i) Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad reguladas a través de los estándares internacionales y normativas en vigor.

j) El sistema de información de Izertis está configurado otorgando los mínimos privilegios necesarios para su correcto desempeño.

- Toda información generada por IZERTIS deberá ser calificada según los criterios establecidos en la normativa interna, **SGSI08 Clasificación de la información**, por la persona responsable de la misma; la persona que ha generado el documento o su responsable dentro de la estructura organizativa.

k) La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

Artículo 5. Alcance

El alcance es esta política son los sistemas de información que dan soporte a los servicios gestionados:

A. Instalación y configuración de infraestructuras, sistemas operativos y ofimática

B. Mantenimiento correctivo/evolutivo de aplicaciones de cliente (instalación de soluciones publicadas por el fabricante)

C. Mantenimiento de hardware

D. Desarrollo de aplicaciones software.

E. Consultoría de seguridad y tecnológica

Artículo 6. Compromiso de la dirección

La presente Política de Seguridad es una línea de actuación clara, manifiesta y pública de IZERTIS, por lo que la Dirección expresa su apoyo total a la misma y se compromete a mantener las directrices fijadas en el presente Documento. Asimismo, publicará y entregará a todos sus empleados y de la forma más apropiada el presente Documento, para que todos conozcan el objetivo establecido por la Dirección, las políticas, principios y normas adoptadas y su importancia para la seguridad de la Organización, las responsabilidades generales y específicas en materia de seguridad de cada miembro de la empresa y otras referencias a documentación que puedan ser útiles.

2. CAPÍTULO II. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Artículo 7. Comité de Seguridad

La Seguridad de la Información será regida por un Comité de Seguridad. Dicho comité estará formado por los siguientes perfiles:

- Dirección de operaciones como Responsable del Sistema.
- Security & Compliance Manager como Responsable de Seguridad.
- Otros miembros representantes con responsabilidades en las principales áreas de negocio de IZERTIS.

Las funciones del responsable del servicio y responsable de la Información recaen en el propio Comité de Seguridad, dado que está constituido por este conjunto de representantes con responsabilidades en los distintos departamentos de la compañía, que son los principales conocedores de la información y servicios de IZERTIS.

Además de los miembros permanentes, podrán ser requeridos a participar en el Comité de Seguridad otros responsables o personal de la organización cuando los asuntos tratados así lo requieran previa convocatoria de los mismos.

Las funciones del Comité de seguridad se detallan en el **PO.SEG.03 Procedimiento de Comité, Roles y Responsabilidades, apdo. 3.1 Roles y Responsabilidades**.

Artículo 8. Roles

Adicionalmente de las funciones comunes definidas para el Comité de Seguridad, han sido definidos una serie de roles y sus responsabilidades en el **PO.SEG.03 Procedimiento de Comité, Roles y Responsabilidades, apdo. 3.1 Roles y Responsabilidades**.

La designación y nombramiento de roles será llevaba a cabo por la dirección general de IZERTIS, quien podrá recabar asesoría del Comité de Seguridad o cualquier personal de la organización.

Se renovarán de forma automática con carácter anual salvo que desde dirección se estime oportuno un cambio en estas designaciones

Artículo 9. Persona de contacto (POC)

El Responsable de Seguridad actuará como PoC (Persona de Contacto) inicial para la seguridad de la información tratada y el servicio prestado a los clientes, de conformidad con lo descrito en el PO.SEG.03 Procedimiento de Comité, Roles y Responsabilidades.

Artículo 10. Resolución de conflictos

En caso de conflicto entre los diferentes responsables de seguridad y del sistema, éste será resuelto por el comité de seguridad de la información como parte de sus roles y responsabilidades

Artículo 11. Obligaciones del Personal

Todo el personal de IZERTIS, así como el que preste servicios relacionados con los Sistemas de información, tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y lo procedimientos derivados de la misma. Se encontrarán entre ellas las relativas a la protección de datos de carácter personal, debiendo el Responsable de Seguridad disponer de los mecanismos necesarios para que la información llegue a todos.

El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

3. CAPÍTULO III. PROTECCIÓN DE DATOS, FORMACIÓN Y GESTIÓN

Artículo 12. Tratamiento de los datos de carácter personal y riesgos derivados

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en la documentación asociada conforme a lo exigido para el tratamiento de datos de carácter personal según legislación aplicable (ver artículo 3 de esta política).

Se han realizado las correspondientes evaluaciones de impacto (EIPD), conforme al artículo 35 del RGPD, para los tratamientos de datos realizados en la organización, resultando en la no necesidad de realizar análisis de riesgos para dichos tratamientos.

Se realizará una revisión periódica de dichas EIPD evaluando posibles modificaciones en los tratamientos que puedan requerir la realización de un análisis de riesgos.

Artículo 13. Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal de IZERTIS y a todas las actividades de acuerdo con los principios de seguridad integral recogidos en los estándares internacionales. A estos efectos, IZERTIS, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Anualmente se diseña un plan de formación para completar y actualizar las competencias del personal, evaluando la eficacia de la formación recibida.

En el caso poco probable de que se precisaran servicios de proveedores externos para prestar servicios de seguridad, Izertis exigiría, de manera objetiva y no discriminatoria, que cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Artículo 14. Análisis y gestión de riesgos de los sistemas de información

IZERTIS asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad en análisis y gestión de riesgos.

Con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en seguridad, el responsable de seguridad acordará la realización de un análisis de riesgos con carácter anual, cuyas conclusiones se plasmarán en actuaciones para tratar y mitigar el riesgo, e incluso replantear la seguridad de los sistemas en caso necesario.

Se contemplará la realización adicional de un análisis de riesgos de los sistemas de información cuando:

a) Se modifiquen los servicios prestados, así como aquellos que almacenan o tratan la información

b) Ocurran incidentes graves de seguridad

c) Se reporten vulnerabilidades graves que afecten a los sistemas de la información de la Organización

Las conclusiones de los análisis de riesgos serán revisadas por el Responsable de Seguridad y éste las comunicará al Comité de Seguridad.

4.CAPÍTULO IV. PROTECCIÓN Y GESTIÓN DE LOS SISTEMAS

Artículo 15. Protección de los sistemas

Los sistemas de la información de IZERTIS estarán protegidos físicamente mediante la separación de las áreas donde están ubicados, incluyendo en su protección sistemas de control de acceso y el cierre físico del acceso mediante llaves u otros mecanismos que IZERTIS considere adecuados.

Todo acceso a los sistemas de IZERTIS deberá ser autorizado debidamente. Se aplicarán las restricciones definidas según las funciones a desempeñar en el caso de procesos o el perfil definido en el caso de acceso de usuario

Artículo 16. Seguridad en el ciclo de vida de los sistemas y servicios contratados

En la adquisición de productos de seguridad se valorarán de manera prioritaria productos con funcionalidad certificada de acuerdo con normas y estándares de reconocimiento internacional, prevaleciendo en caso de equivalencia funcional aquellos recogidos dentro de la Guía del CCN 105: Catálogo de Productos y Servicios STIC. Se valorará la proporcionalidad respecto a los riesgos asumidos, analizándose la taxonomía de seguridad del componente siempre que resulte necesario. En el caso de proveedores críticos o con acceso a los sistemas de información, estos con evidencias de cumplimiento de esquema nacional de Seguridad en categoría alta en cuyo alcance debe encontrarse recogido el objeto de la prestación del servicio contratado.

Los sistemas de IZERTIS se diseñarán y configurarán garantizando el mínimo privilegio que permita alcanzar los objetivos de la organización:

a) Mínima funcionalidad

b) Restricciones de acceso a funciones de mantenimiento, operación, y administración tanto a usuarios, como desde localizaciones específicas

- Eliminación de las funciones innecesarias para el fin perseguido, mediante el control de la configuración

- Se requerirá una acción consciente del usuario para que se genere un uso inseguro del sistema

Todo elemento físico deberá ser autorizado previa instalación en el sistema. Se mantendrá una constante vigilancia sobre los dispositivos aplicando las especificaciones de los fabricantes en cuanto a actualizaciones y

vulnerabilidades, así como reaccionando a cualquier riesgo que afecte al elemento como consecuencia su estado de seguridad.

La información en tránsito deberá ser protegida con las mismas medidas de seguridad que la información almacenada, disponiendo de normas y procedimientos que regulen la seguridad de la información almacenada en entornos inseguros (portátiles, smartphones, dispositivos USB, y redes abiertas o de cifrado débil) así como la recuperación de esta.

Se protegerá el perímetro del sistema ante cualquier conexión realizada desde el exterior, controlando el punto de acceso y analizando los riesgos derivados de la interconexión previamente a su autorización. Todas las interconexiones entre sistemas se llevarán a cabo según las directrices establecidas en la Guía del CCN 811: Interconexión en el ENS.

En la contratación de servicios de seguridad se aplicará lo dispuesto en este artículo, así como lo relacionado en el artículo 12 de esta política sobre formación, concienciación y profesionalidad del personal.

Artículo 17. Registros de actividad y detección de código dañino

La vigilancia continua exige la monitorización de los registros de actividad. Se registrará la información estrictamente necesaria para la investigación de actividades indebidas o no autorizadas que permitan identificar a la persona responsable de la actividad.

Se analizarán las comunicaciones en la medida estrictamente necesaria y proporcionada con el objetivo de detectar cualquier intento de acceso no autorizado, ataques de denegación de servicio, distribución malintencionada de código dañino, o cualquier otro comportamiento que pueda resultar en daños a las redes y sistemas de la información de IZERTIS.

Como consecuencia de dichas actuaciones, todo usuario del sistema deberá estar inequívocamente identificado, del tal modo que se pueda conocer en todo momento sus derechos de acceso y quién ha realizado determinada actividad.

Artículo 18. Incidentes de seguridad

Se dispondrá de sistemas de detección y reacción frente a código dañino.

Se dispondrá de procedimientos de gestión de incidentes que cubrirán: detección, clasificación, análisis, comunicación, resolución, aprendizaje, y registro de estos.

Artículo 19. Continuidad de la actividad

Se dispondrá de un sistema de replicación de servicios y copias de seguridad, así como de los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de indisponibilidad de los medios habituales de trabajo.

Artículo 20. Mejora continua

El proceso de seguridad deberá ser monitorizado de forma continua, tanto en cuanto a medidas técnicas como normativas y procedimentales. Para ello los datos y la información recogida cualitativa y cuantitativamente a través de la gestión de nuestro Sistema y de nuestras actividades (los objetivos, los resultados de las auditorías internas y externas, el análisis de datos, las actividades de monitorización, la información de los paneles de control de las aplicaciones de seguridad, las inspecciones de permisos por muestreo, los resultados de las auditorías técnicas de seguridad, las acciones correctivas, el informe de revisión por la Dirección, etc.), se ponen en conocimiento del Comité de Seguridad en las reuniones que este mantiene y se utilizan para determinar las necesidades relacionadas con el Sistema de Gestión y decidir qué acciones se llevarán a cabo para mejorarlo.

La Dirección será quien lidere la organización y promueva una cultura de seguridad, asignando los roles requeridos y potenciando la transversalidad de la seguridad a cada proceso desarrollado o servicio a terceros.

5. CAPÍTULO V. ESTRUCTURA NORMATIVA

Artículo 21. Estructura de la documentación de seguridad

La documentación relativa a la Seguridad de la Información estará clasificada en cinco niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

a) Primer nivel: Política de Seguridad de la Información

b) Segundo nivel: Políticas de seguridad

c) Tercer nivel: Procedimientos y documentos del SGSI.

d) Cuarto nivel: Instrucciones técnicas

e) Quinto nivel: Informes, registros y evidencias electrónicas

Artículo 22. Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, recogido en el presente documento y aprobada por la alta Dirección de IZERTIS.

Artículo 23. Segundo Nivel: Políticas de Seguridad

De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad en delegación del Comité de Seguridad.

Artículo 24. Tercer Nivel: Procedimientos y Documentos del SGSI

Documentos de gestión que especifican las tareas que, a posteriori, se desarrollan en las instrucciones técnicas correspondientes.

La responsabilidad de aprobación de estos procedimientos es del Responsable de Seguridad.

Artículo 25. Cuarto Nivel: Instrucciones técnicas

Documentos técnicos orientados a resolver las tareas de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos técnicos es de cada uno de los Responsables de los Sistemas de Información en su ámbito de actuación.

Artículo 26. Quinto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida de los sistemas de la información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito de actuación.

Artículo 27. Otra documentación

Se podrá adaptar la presente política en todo momento a los procedimientos descritos en otras normativas, así como en las futuras legislaciones que pueda entrar en vigor.

Disposición final primera. Publicidad de la Política de Seguridad

La presente Resolución se publicará en la página web y en la intranet de IZERTIS.

Disposición final segunda. Entrada en vigor

La Política de Seguridad será de aplicación a partir del día siguiente al de su aprobación por la Dirección de IZERTIS.

Disposición final tercera. Derogación

La presente Política de Seguridad que se aprueba deroga las anteriores Políticas de Seguridad que existieran en IZERTIS.

Esta política ha sido aprobada por la dirección de IZERTIS y será revisada anualmente.

25 de Septiembre de 2024

Firma: Pablo Martín,

Presidente

6. CONTROL DE VERSIONES

Todo usuario de este fichero que encuentre un error u oportunidad de mejora deberá comunicarlo al responsable de este para su evaluación y, en su caso, modificación.

La versión en vigor del fichero es la que se encuentra en el repositorio documental de la empresa.

VERSIÓN	FECHA	MODIFICACIONES
1	11/06/2018	Primera versión. Se incorpora como documento independiente del Manual de Seguridad, incluyendo los requisitos del Esquema Nacional de Seguridad.
2	23/08/2019	Cambio en el formato a nueva plantilla corporativa
3	11/09/2019	Cambio en el formato
4	4/10/2019	Cambios derivados de la auditoría externa del ENS, se añade referencia al manual de seguridad SGSI/01.
5	15/01/2020	Cambio de repositorio a Alfresco. Cambio de ITSM (iTOP – Remedy).
6	17/09/2020	Se incorpora reseña a los objetivos
7	24/06/2022	Se incorporan las dimensiones de autenticidad y trazabilidad
8	04/08/2023	Cambios de adecuación a Real Decreto 311/2022 y su estructura
9	04/12/2023	Cambios derivados de la auditoría externa del ENS
10	17/06/2024	Actualización menor roles y requisitos mínimos de seguridad

11	25/09/2024	Cambio formato. Reorganización y actualización del documento.

izertis

Passion for Technology