ISO 27001:2013

Sistema de Gestión de la Seguridad de la Información

ISO 27001:2013 Sistema de Gestión d
la Seguridad de la Información

La Norma ISO 27001:2022, también conocida como Seguridad de la Información, Ciberseguridad y Protección de la Privacidad, es un estándar reconocido mundialmente para gestionar la seguridad de la información. Esta norma establece los requisitos que debe cumplir un Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando directrices claras para establecer, implementar, mantener y mejorar continuamente dicho sistema. En un entorno donde la protección de la información es crucial, ISO 27001 se establece como un referente fundamental para garantizar la seguridad y confidencialidad de los datos en las organizaciones.

El establecimiento de un sistema de gestión de seguridad de la información en una organización se construye por una serie de factores clave, que incluyen las necesidades y metas específicas de la organización, los requisitos de seguridad aplicables, los procesos organizativos, así como su tamaño y la estructura interna. Estos elementos influyen de manera significativa en el diseño y la adaptación del sistema de gestión, asegurando que esté alineado de manera óptima con las características y particularidades de la organización.

El sistema de gestión de seguridad de la información se encarga de salvaguardar la confidencialidad, integridad y disponibilidad de la información mediante la adopción de un proceso de gestión de riesgos. Su función es asegurar que los riesgos asociados con la información se aborden de manera efectiva, brindando así confianza a todas las partes interesadas de que estos riesgos están siendo gestionados de manera adecuada y proactiva.

Un SGSI se enfoca diferentes aspectos clave:

¿Qué es un Sistema de Gestión de seguridad de la Información?

Un SGSI ayuda a una organización a identificar, evaluar y gestionar los riesgos de seguridad de la información de manera efectiva. Esto incluye la adopción de medidas de seguridad para prevenir, mitigar y responder a amenazas potenciales que podrían afectar la información valiosa de la organización. El objetivo es garantizar que la información esté protegida contra accesos no autorizados, pérdidas, fugas o cualquier otro tipo de daño, tanto interno como externo

1. Enfoque al cliente

Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz.

2. Liderazgo

La alta dirección deberá demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información mediante:
a) Garantizar que se establezcan la política de seguridad de la información y los objetivos de seguridad de la información y son compatibles con la dirección estratégica de la organización.
b) Garantizar la integración de los requisitos del sistema de gestión de seguridad de la información en el los procesos de la organización los procesos de la organización.
c) Asegurar que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.
d) Comunicar la importancia de una gestión eficaz de la seguridad de la información y de cumplir con los requisitos del sistema de gestión de la seguridad de la información.
f) Dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información.
g) Promover la mejora continua.

3. Compromiso con las personas

La alta dirección puede asignar responsabilidades y autoridades para informar sobre el rendimiento del sistema de gestión de la seguridad de la información dentro de la organización.

- La alta dirección debe asegurarse de que las responsabilidades y autoridades de los roles relevantes para la seguridad de la información se asignen y comuniquen dentro de la organización.
- La asignación de roles y responsabilidades de seguridad de la información debe realizarse de acuerdo con la política de seguridad de la información y las políticas específicas del tema (ver 5.1).
- La gerencia debe exigir que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos de cada tema de la organización.
- Todos los usuarios deben conocer los requisitos y procedimientos de seguridad para proteger los dispositivos terminales de los usuarios.

4. Enfoque a procesos

ISO/IEC 27001 promueve un enfoque holístico de la seguridad de la información: investigación de personas, políticas y tecnología. Un sistema de gestión de la seguridad de la información implementado de acuerdo con esta norma es una herramienta para la gestión de riesgos, la ciber resiliencia y la excelencia operativa.

5. Mejora continua

El objetivo de la mejora continua de un SGSI es aumentar la probabilidad de alcanzar objetivos relacionados con la preservación de la confidencialidad, disponibilidad e integridad de la información. El enfoque de la mejora continua es buscar oportunidades de mejora y no asumir que las actividades de gestión existentes son lo suficientemente buenas o tan buenas como pueden.

6. Toma de decisión basada en evidencia

La toma de decisiones basada en evidencia en ISO 27001 es uno de los ejes en los que se basa la gestión de la seguridad de la información. La idea es que, para alcanzar la excelencia, se deben tomar decisiones basadas en información confiable, y no en elucubraciones, presentimientos o vaticinios. Consiste en basarse en los datos y superar las intuiciones.

- Confidencialidad: Garantizar que la información sensible esté protegida contra accesos no autorizados. Integridad: Asegurar que la información sea precisa, completa y no se haya alterado de manera no autorizada.
- Disponibilidad: Asegurar que la información esté disponible y accesible cuando sea necesario para los usuarios autorizados.
- Gestión de riesgos: Identificar, evaluar y gestionar los riesgos de seguridad de la información que podrían afectar a la organización.
- Cumplimiento normativo: Asegurar que la organización cumpla con las leyes, regulaciones y estándares relevantes relacionados con la seguridad de la información.
- Mejora continua: Buscar constantemente maneras de mejorar el SGSI.

¿Beneficios de la certificación ISO 27001?

Permite demostrar altos estándares de seguridad de la información. La certificación se obtiene tras una auditoría satisfactoria conforme a los requisitos de la ISO 27001, y brinda a las organizaciones las siguientes ventajas:

La certificación ISO 27001 ofrece una serie de beneficios que pueden contribuir significativamente a la protección de la información, la mejora de la eficiencia operativa y la construcción de la confianza con los clientes y socios comerciales.

- Mejora de la seguridad de la información.
- Gestión de riesgos más efectiva.
- Cumplimiento normativo.
- Fortalecimiento de la confianza de los clientes y socios.
- Mejora de la competitividad.
- Reducción de costos y eficiencia operativa.
- Resiliencia a los ciberataques.
- Preparación para nuevas amenazas.
- Integridad, confidencialidad y disponibilidad de los datos.
- Seguridad en todos los soportes.
- Protección en toda la organización.
- Ahorro de costos.
- Implementación del marco de seguridad de la información específico.
- Reducción de vulnerabilidad ante la creciente amenaza de los ciberataques.
- Responda a la evolución de los riesgos de seguridad.
- Asegúrese de que los activos, como los estados financieros, la propiedad ntelectual, los datos de los empleados y la información confiada por terceros, permanezcan intactos, confidenciales y disponibles según sea necesario.
- Proporcione un marco de gestión centralizada que proteja toda la información en un solo lugar.

- Preparar a las personas, los procesos y la tecnología disponible para hacer frente a los riesgos basados en la tecnología y otras amenazas.
- Protección de la información (papel, digital o nube) de sus operaciones, procesos y servicios.
- Ahorro de recursos, incrementando la eficiencia.
- Reducción de los gastos en tecnología de defensa ineficaz.
- Establecimiento de reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
- Se establecerán e implementarán reglas para controlar el acceso físico y lógico a la información y otros activos asociados en función de los requisitos de seguridad empresarial y de la información.
- Prevención de la pérdida, robo o extravío de información importante.
- Confianza en las partes interesadas de que su información estará cuidada.

¿Por qué elegir Intercet para realizar una auditoría de certificación de la norma ISO 27001?

Hemos perfeccionado nuestro enfoque para adaptarnos a las exigencias del mercado, por ello somos líderes en el servicio de certificación de sistemas de gestión, con el compromiso de asegurar la satisfacción de nuestros clientes.

Entendemos que la industria tiene sus propias particularidades y desafíos. Por lo tanto, nuestro servicio de certificación se adapta específicamente a las necesidades de su sector, asegurando una evaluación efectiva del estándar.

Acreditaciones

SCC
Consejo de normas de Canadá

UAF
Fundación de Acreditación USA

KAB
Junta de Acreditación de Corea

EXEMPLAR GLOBAL

Reconocimientos

IAF
Foro Internacional de Acreditación

APAC
Cooperación de Acreditación Asia-Pacífico

Proceso de Certificación