safetica

SEGURIDAD AMÉRICA.COM
Fortaleciendo Internet

Versión: 2023-10-18

Cómo Safetica le ayuda a cumplir con los requisitos de la norma ISO 27001

Introducción a la norma ISO 27001

ISO/IEC 27001 es una norma de gestión de la seguridad de la información (SGSI) publicada conjuntamente por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La norma ISO 27001 establece cómo las empresas deben gestionar los riesgos asociados a las amenazas a la seguridad de la información, incluidas las políticas, los procedimientos, las medidas técnicas y la formación de los empleados.

La norma ISO 27001 define las directrices de seguridad de la información, los requisitos para la protección de datos contra la pérdida o el acceso no autorizado, y las certificaciones que demuestran un compromiso con ellos.

La norma ISO 27001 incluye un proceso de evaluación de riesgos, estructura organizativa, clasificación de la información, control de acceso, salvaguardas físicas y técnicas, principios de seguridad de la información y directrices de auditoría y presentación de informes.

¿Qué es un SGSI?

Un SGSI es un enfoque holístico para garantizar la confidencialidad, integridad y disponibilidad (CIA) de los activos de información corporativa.

Intimidad

Las medidas de confidencialidad protegen la información del acceso no autorizado y el uso indebido.

Integridad

Las medidas de integridad protegen la información de modificaciones no autorizadas.

Disponibilidad

Las medidas de disponibilidad protegen el acceso oportuno y continuo al sistema.

Desafíos y cómo Safetica ayuda a resolverlos

1. Política de Seguridad de la Información

La norma ISO 27001 requiere que desarrolle e implemente políticas de seguridad de la información y supervise su cumplimiento de esas políticas de forma continua. Pero, ¿cómo se puede supervisar cómo los empleados trabajan con la información a nivel de TI?

Safetica le permite auditar las operaciones de los usuarios en toda su organización. Puede reconocer información sensible o confidencial y proporcionar informes sobre cómo se procesan los datos.

Con base en la clasificación de datos en Safetica, se pueden aplicar políticas DLP y así lograr el comportamiento de usuario deseado al trabajar con información sensible o confidencial. Esto permite a los empleados y contratistas seguir las mejores prácticas o bloquear métodos inseguros o prohibidos de trabajar con datos confidenciales.

2. Clasificación de datos

Un SGSI requiere que se asegure de que la información reciba un nivel adecuado de protección de acuerdo con su relevancia para la organización. Esto significa que la información se procesa en función de la importancia y la sensibilidad.

Safetica ofrece clasificación de datos configurable y personalizable. Los datos sensibles o confidenciales se pueden clasificar mediante el análisis de OCR de contenido basado en el contexto, incluida la clasificación de usuarios.

Esto puede ir seguido de la configuración de políticas de seguridad (DLP) para garantizar que los niveles de clasificación de datos adecuados se administran correctamente.

Los niveles posteriores de protección de clasificación de datos también son configurables, lo que permite el registro silencioso, las notificaciones de usuario o la detención forzada de operaciones de usuario seleccionadas.

3. Notificación de una (potencial) violación de datos

Si hay un incidente de seguridad asociado con una fuga de datos, debe ser notificado del incidente de inmediato para que pueda reaccionar y minimizar cualquier impacto, o mejor aún, para evitar la fuga de información.

En el caso de un incidente de seguridad real o un intento de incidente de seguridad, Safetica informa a los empleados pertinentes en tiempo real a través de notificaciones por correo electrónico. La solución informará inmediatamente del incidente y proporcionará suficientes detalles para que pueda evaluar el impacto de la situación y tomar medidas de seguimiento.

Safetica también proporciona extensos registros de auditoría de las operaciones realizadas con datos confidenciales. Esto ayuda a identificar la profundidad de la infracción, los documentos confidenciales involucrados y las personas afectadas.

Con la integración de API, todos los registros también se pueden enviar a SIEM o herramientas de análisis de datos, como Power BI o Tableau.

4. Encriptación

La norma ISO 27001 exige el uso de claves criptográficas y cifrado cuando corresponda.

Safetica ayuda a las organizaciones a administrar el cifrado de almacenamiento (Microsoft BitLocker) para proteger los datos en reposo. El cifrado se gestiona de forma centralizada en la consola de mantenimiento de Safetica, y las claves de cifrado se distribuyen de forma segura en los endpoints seguros, lo que elimina la necesidad de compartirlas entre los usuarios.

5. Cumplimiento de normas y leyes

Una parte importante de la norma ISO 27001 es el cumplimiento de todas las obligaciones contractuales y legales que afectan a su negocio, lo que puede ser una tarea desalentadora para cualquier persona que no tenga las herramientas adecuadas a su disposición.

Con Safetica, puede implementar políticas de DLP que le permitan manejar sus datos de la manera que desee, asegurando el cumplimiento de requisitos legislativos, reglamentarios o contractuales específicos. La solución DLP de Safetica también ayuda a proteger los datos contra pérdidas, falsificaciones, accesos no autorizados y divulgaciones no autorizadas. Esto también se aplica a la protección de la privacidad y los datos personales. Gracias a las características anteriores, Safetica le ayuda a cumplir con GDPR, TISAX, NIS2 y cumplir con los requisitos contractuales utilizando sus propias políticas de seguridad.

ISO 27001 Anexo A

Al implementar Safetica, dará un paso significativo hacia el cumplimiento de los objetivos de los siguientes capítulos del anexo A de la norma ISO 27001:

5 Política de Seguridad de la Información

6 Organización de Seguridad de la Información

7 Seguridad de los recursos humanos

8 Gestión de activos

9 Control de acceso

10 Encriptación

12 Seguridad operacional

13 Seguridad de las comunicaciones

14 Adquisición, desarrollo y mantenimiento del sistema

16 Gestión de incidentes de seguridad de la información

18 Cumplimiento normativo

Casos de uso clave

Caso de uso 1: Banca y finanzas

Los servicios de contabilidad y la gestión de las instalaciones de la empresa bancaria matriz necesitaban ayuda con la implementación de los requisitos de seguridad establecidos por la norma ISO/IEC 27001.

Problema: La empresa maneja información bancaria confidencial de los clientes y documentación de proyectos y necesitaba fortalecer su sistema de seguridad de gestión de la información, así como su sistema de gestión de riesgos.

Solución: Para abordar sus necesidades de cumplimiento, el departamento de TI eligió Safetica, que proporciona una gama de herramientas para ayudar a las empresas a cumplir con los requisitos de la norma ISO/IEC 27001:

- Analizar la forma de trabajar de los usuarios finales, con especial énfasis en los procesos de tratamiento de datos.
- Directivas establecidas para administrar dispositivos externos: permiten solo unidades USB cifradas.
- Se han establecido y ajustado políticas de protección de datos (no se imprimen archivos confidenciales, se copian archivos confidenciales a dispositivos externos no autorizados, se envían a cuentas de correo electrónico externas, se realiza capturas de pantalla o se cargan en la web).

El resultado: los archivos solo se pueden transferir de formas predefinidas y las grabaciones están disponibles para todas las acciones. La administración recibe informes

resumidos semanales sobre la actividad de los usuarios en Internet, el uso de aplicaciones, la impresión de documentos y los ciclos de vida de los archivos. En caso de un incidente de seguridad, se informa inmediatamente a la dirección.

Caso de uso 2: Transporte

Franco Compañía Naviera, una empresa de gestión de envíos, debe cumplir con los requisitos de la norma ISO 27001.

Problema: La empresa crea y administra información confidencial que debe ser manejada y protegida de acuerdo con los estándares de seguridad y brindar el mejor servicio posible a sus clientes.

Solución: Safetica proporciona las funciones DLP necesarias para hacer cumplir las políticas de seguridad. Todos los datos creados o movidos dentro de una organización se pueden clasificar para protegerlos contra fugas. En caso de que se produzca un incidente de seguridad de los datos, se notifica inmediatamente a los responsables de TI/seguridad para que puedan investigar y responder a la situación.

Resultado: La empresa implementó la solución en 2 meses sin la ayuda de una organización externa. Ahora puede supervisar mejor el cumplimiento de las políticas de la empresa por parte de los empleados, cumplir con los requisitos de la norma ISO 27001 y supervisar el flujo de información confidencial dentro de la empresa.