ManageEngine
Log360

Cómo cumplir con los

CONTROLES DE SEGURIDAD

de la ISO 27001:2022

USANDO SIEM

Anupama. A

Tabla de contenidos

Capítulos

La ISO 27001 es una certificación y marco en seguridad informática que ayuda a las compañías a implementar un sistema de gestión para la seguridad de la información (ISMS) personalizada para satisfacer sus requisitos de seguridad y corporativos.

Un ISMS ayuda a las organizaciones a determinar los controles que necesita para la seguridad de sus datos, por lo que ayuda a estructurar el método de una organización para la seguridad de la información.

La última actualización de este marco se publicó el 25 de octubre de 2022, y resulta evidente que hay algunos cambios importantes. Los auditores y las organizaciones por igual estuvieron esperando con ansias esta versión actualizada y consolidada de la norma, luego de varias correcciones que se añadieron en 2014, 2015 y 2017. Distintas organizaciones adoptaron diferentes versiones de esta norma, lo que causó problemas tanto para ellas como para los auditores.

En este e-book obtendrá un resumen general detallado de la ISO 27001 y su proceso de certificación. Asimismo, aprenderá sobre las tecnologías de seguridad que puede implementar para adherirse a los controles mencionados en la norma.

Capítulo 1

Presentamos la ISO 27001

La familia de normas ISO 27000 consta de las mejores prácticas y controles que las organizaciones pueden usar para implementar un sistema de gestión de la seguridad de la información (ISMS) y la triada CID (confidencialidad, integridad y disponibilidad) para proteger sus datos. El objetivo principal de la norma de seguridad ISO 27001 es ayudar a que las organizaciones establezcan un ISMS que se ajuste mejor a su perfil de riesgos y requisitos.[1]

¿Por qué escoger la ISO 27001?

La ISO 27001 es una norma regulatoria ampliamente reconocida. Aparte de la sobresaliente reputación de tener la certificación ISO 27001, cumplir con la norma ayuda a las organizaciones a:

1. Mantener una mejor postura de seguridad informática.
2. Cumplir con otras normas regulatorias.
3. Mitigar los riesgos de las amenazas cibernéticas.
4. Sobresalir entre los competidores.

¿Qué es la ISO 27001?

La ISO 27001 es una norma y marco de seguridad informática que ayuda a las organizaciones a implementar un ISMS. Ya que se trata de un método basado en riesgos, ayuda a las organizaciones a estimar su postura de seguridad. Lo primero es que se requiere de las organizaciones que realicen una evaluación de riesgos de seguridad informática e identificar sus áreas de riesgo. Luego, necesitan implementar controles y medidas de seguridad para implementar un ISMS que las ayude a satisfacer sus requisitos de riesgos.

¿Cómo llegó a existir la ISO 27001?

La versión original de la ISO 27001 era conocida como BS 7799, redactada por el Departamento de Comercio e Industria del Reino Unido. La British Standards Institution la publicó en dos partes, la primera en 1995 y la segunda en 1999. La primera parte se volvió la ISO/CE 17799 y se le llamó Tecnología de la información: Código de Práctica para la Gestión de la Seguridad de la Información. La segunda parte, denominada Sistema de Gestión para la Seguridad de la Información, se adoptó como parte de la gestión y evaluación de riesgos en la serie de ISO 27000. Ahora se lo conoce como ISO 27001.

La última versión de la ISO 27001 se publicó en 2013 con algunas actualizaciones menores implementadas en 2014, 2015 y 2017.

¿Cómo está estructurada la ISO 27001?

La ISO 27001 se divide en dos partes:

Parte uno:

Consta de 12 secciones. Estas secciones incluyen la introducción, el alcance y 10 cláusulas:

a. Introducción
b. Alcance
c. Detalles normativos
d. Términos y definiciones
e. Contexto de la organización
f. Liderazgo
g. Planeación
h. Soporte
i. Operación
j. Evaluación del rendimiento
k. Mejora
l. Objetivos y controles del control de referencias

Parte dos:

Anexo A: la segunda parte de la ISO 27001 es el Anexo A, que consta de 93 controles, repartidos en cinco secciones. Es una continuación de la parte uno y llega hasta la cláusula 10.

¿Es una norma de cumplimiento obligatoria?

La ISO 27001 no es una obligación de cumplimiento. Ayuda a las organizaciones a enfocarse en su requisitos de seguridad únicos e implementar un ISMS. Sin embargo, las organizaciones que buscan obtener una certificación ISO 27001, deben con cumplir la norma.

¿Cuál es la diferencia entre la ISO 27001 y 27002?

Mientras que la ISO 27001 es un marco por el que las organizaciones pueden obtener una certificación, la ISO 27002 es una guía de mejores prácticas que suministra recomendaciones para implementar los controles de la ISO 27001 en el Anexo A. Las organizaciones pueden escoger qué mejores implementar a partir de la ISO 27002, ya que no se da certificación alguna.

En el siguiente capítulo miraremos en qué es un ISMS, cómo las organizaciones se benefician al implementarlo y cómo pueden hacerlo.

Capítulo 2

Implementación de un sistemas de gestión de la seguridad de la información (ISMS)

Un ISMS ayuda a las organizacionesa determinar los controles que necesita para la seguridad de sus datos, por lo que ayuda a definir el mátodo de una organizaciên para la seguridad de la informaciên.[2]

¿Por qué las compañías necesitan un ISMS?

Un ISMS permite a las organizaciones implementar la triada DIC para la protecciên de datos. La triada CID consta de:

A

Confidencialidad

Las organizaciones deben tomar medidas para proteger la privacidad de sus datos, como garantizar el acceso autorizado y restringido.

B

Integridad

Las organizaciones deben sostener la autenticidad y fiabilidad de los datos, y garantizar que estÄn libres de errores para facilitar la integridad de los datos.

C

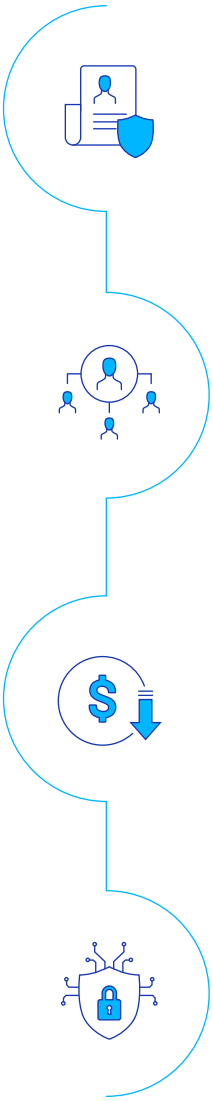
Disponibilidad

Las organizaciones deben garantizar la disponibilidad de los datos en cualquier momento. Esto significa garantizar que todos los sistemas y operaciones que tienen contacto con los datos funcionan sin problemas, ademÄs de que se deben tomar medidas para eliminar servidores redundantes y mejorar la velocidad de las actualizaciones.

Implementar todas las tres partes de la triada CID aumenta significativamente la resiliencia informÄtica y mejora la capacidad de las organizaciones para manejar amenazas.

Ventajas de un ISMS

Aparte de cumplir con la ISO 27001, tener un ISMS implementado da varias ventajas a la organizaciên:



Salvaguarda la información privilegiada

Con el objetivo principal de proteger la confidencialidad, integridad y disponibilidad de la informaciên, un ISMS funciona para salvaguardar los distintos activos de informaciên en una organizaciên.

Sistema de gestión centralizado

Un ISMS garantiza que todos los datos de almacenan, protegen y gestionan de forma centralizada. Este mátodo holãstico conlleva un aumento en la seguridad y contribuye al crecimiento general de la organizaciên.

Reducción de los costos en seguridad

Ya que un ISMS se implementa con base en la evaluaciên de riesgos de cada organizaciên, puede ayudar a evitar que se incurra en costos debido a la experimentaciên con varias soluciones de seguridad. Asumir un mátodo centralizado conlleva tambián la reducciên en los costos generales.

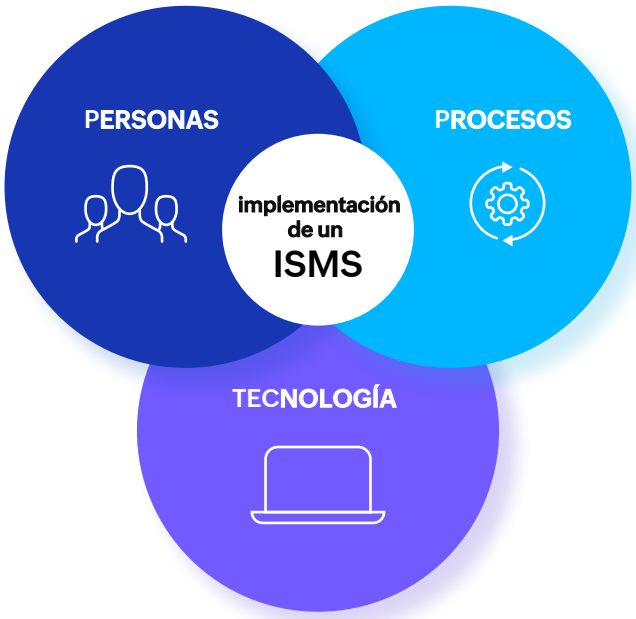
Aumento de la resiliencia informática

Un ISMS que cumpla con la ISO 27001 requiere que la organizaciên cambie sus medidas de seguridad constantemente y evolucione con su panorama de amenazas. Esto conlleva un aumento general en la resiliencia informÄtica.

Implemente un ISMS

La ISO 27001 recomienda el mátodo planear-hacer-verificar-actuar,o PHVA, para implementar un ISMS. El mátodo PHVA se sigue activamente en todas las normas ISO y aparece en la parte uno de la norma ISO 27001. El PHVA es un mátodo cãclico en el que las compaèãas deben verificar su progreso continuamente. Se alinea con la fêrmula de mejora continua de la ISO 27001 y ayuda a las compaèãasa evaluarse congruentemente, en lugar de solo depender de auditorãas.

Esta fêrmula hace que la implementaciên de un ISMS sea segïn la compaèãa, lo que incluye la interseccièn con personas, procesos y tecnologãaimportantes, como se ilustra en la siguiente imagen. Demos un vistazo breve a lo que implica.



Personas

Hay varios interesados involucradosen la implementaciên de un ISMS. La clÄusula4.2 en la norma habla de las necesidades y expectativas de las "partes interesadas" que la organizaciên debe determinar mientras implementa un ISMS.

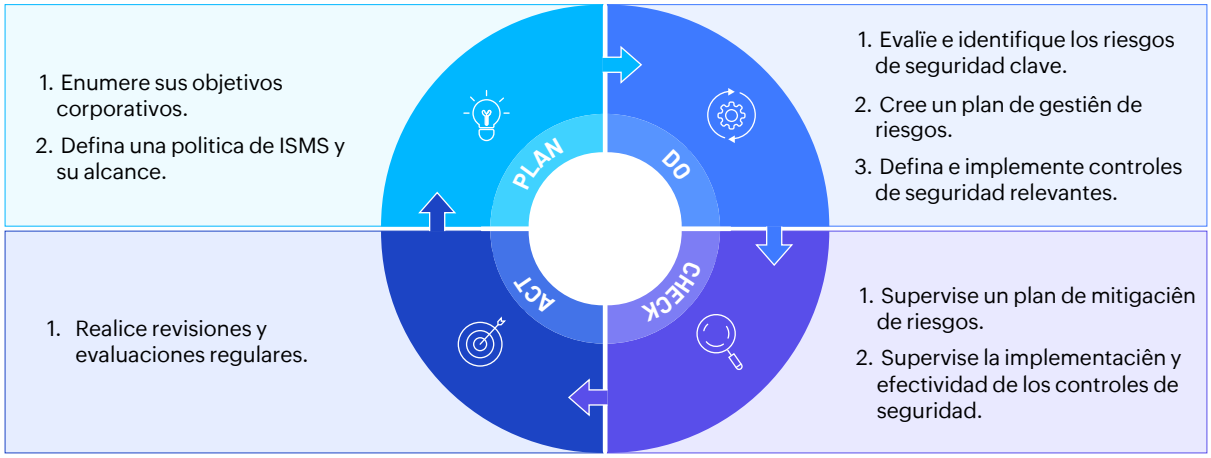
Cláusula 4.2: [3]
La organizaciên determinarÄ:
a) las partes interesadas pertinentes al sistema de gestiên para la seguridad de la informaciên
b) los requisitos de estas partes interesadas
c) cuÄles de estos requisitos se abordarÄn mediante el sistema de gestiên para la seguridad de la informaciên

Las partes interesadas significarÄ cualquier interesado o entidad que podrãa verse afectada por la continuidad corporativa o los controles de seguridad de la informaciên en una organizaciên. Esto podrãa incluir:

- Empleados
- Gobierno o agencias de acreditaciên
- Clientes
- Gestiên principal
- Lãderes de departamentos

Procesos

Aquã es donde el PHVA encaja. Implementar un ISMS se puede definir mediante los siguientes pasos, como se ilustra en la siguiente imagen:



Se implementan los cambios necesarios con base en la evaluaciên. Esto se sigue de forma cãclica para garantizar la mejora continua y una postura de riesgo actualizada para la organizaciên.

Tecnología

Implementar un ISMS puede ser una tarea tediosa para las organizaciones.Ya que la nueva actualizaciên introduce cambios notables, las organizaciones deben invertir en tecnologãas automatizadas que puedan ayudarlas a cumplir fÄcilmente con los controles de seguridad enumerados en la norma.

Algunas de estas tecnologãas incluyen:

- Plataformas de seguridad de datos.
- Soluciones para la gestiên del cumplimiento.
- Soluciones para la gestiên de eventos e informaciên de seguridad (SIEM).

En este capãtulohemos explorado cêmo implementar un ISMS y las distintas personas, procesos y tecnologãasinvolucrados en dicha implementaciên. La ïltima norma, publicada en 2022, tiene cambios importantes que afectan estos factores. En el siguiente capãtulose exploran estos cambios en detalle y se da a las organizaciones la esencia de todo lo que necesitan saber sobre la obtenciên del certificado de ISO 27001:2022.

Capítulo 3

Entienda los principales cambios en la ISO 27001:2022

Luego de la ïltima correcciên en 2017, se esperaba mucho la ïltima versiên de la ISO 27001, publicada en octubre de 2022; no fue una decepciên.

Aunque hay varias actualizaciones estructurales, la versiên de 2022 se enfocê notablemente en las consecuencias prÄcticasy basadas en resultados para las organizaciones.Al desviarse del mátodo usual de lista de control de cumplimiento para la implementaciên de un ISMS, esta nueva versiên enfatiza un mátodo mÄs basado en la evidencia para los controles de seguridad.[4]

Resumen general de los principales cambios

Algunos de los principales cambios en la ISO 27001 son cambios estructurales hechos a los controles de seguridad enumerados en la parte dos y algunas ediciones menores hechas a las clÄusulas en la parte uno.

Mientras que las ediciones hechas a la parte dos significan un cambio en la disposiciên hacia la implementaciên de un ISMS, los cambios hechos a la parte uno indican un cambio de perspectiva cuando se trata de la seguridad informÄtica.

Cambios por cláusulas hechos en la parte uno

Cláusula/ subcláusula	Título	Subcláusula en la ISO 27001:2013	Cambio en la ISO 27001:2022
Cláusula 4	**Contexto de la organización**		
4.2	**Entender las necesidades y expectativas de las partes interesadas**	La organizaciên determinarÄ: a. las partes interesadas pertinentes al sistema de gestiên para la seguridad de la informaciên; y b. los requisitos de estas partes interesadas relevantes para la seguridad de la informaciên.	Se aèadiê un nuevo subelemento: c. cuÄles de estos requisitos se abordarÄn mediante el sistema de gestiên para la seguridad de la informaciên.
4.4	**Sistema de gestión para la seguridad de la información**	La organizaciên establecerÄ, implementarÄ, mantendrÄ y mejorarÄ continuamente un sistema de gestiên para la seguridad de la informaciên, de conformidad con los requisitos de la norma internacional.	La organizaciên establecerÄ, implementarÄ, mantendrÄ y mejorarÄ continuamente un sistema de gestiên para la seguridad de la informaciên,

			incluyendo los procesos necesarios y sus interacciones, de conformidad con los requisitos de esta norma internacional.
Cláusula 6	**Planeación**		
6.2	**Information security objectives and planning to achieve them**	La organizaciên establecerÄ objetivos de seguridad de la informaciên en las funciones y niveles relevantes. Los objetivos de seguridad de la informaciên: a. serÄn congruentes con la polãtica de seguridad de la informaciên b. serÄn medibles (si corresponde) c. ttendrÄn en cuenta la informaciên, requisitos de seguridad y resultados pertinentes a partir de la evaluaciên y tratamiento de riesgos d. se comunicarÄn; y e. se actualizarÄn segïn corresponda. La organizaciên retendrÄ informaciên documentada sobre los objetivos de seguridad de la informaciên. Cundo se planee cêmo alcanzar los objetivos de seguridad de la informaciên, la organizaciên determinarÄ: f. quá se va a hacer g. quá recursos se requerirÄn h. quián serÄ el responsable i. cuando se completarÄn j. cêmo se evaluarÄn los resultados.	Se aèadieron nuevos subelementos: (Los objetivos de seguridad de la informaciên:) d.se monitorearÄn g. estarÄn disponibles en la informaciên documentada
6.3	**Planeación de cambios**	Esta subclÄusula se aèadiê recientemente y no estÄ presente en la versiên de 2013.	Cualquier cambio hecho al ISMS debe realizarse de manera planificada.

Cláusula 7	Soporte		
7.4	**Comunicaciones**	La organizaciên determinarÄ la necesidad de comunicaciones internas y externas relevantes para el sistema de gestiên para la seguridad de la informaciên, incluyendo: a. sobre quá comunicarse b. cuÄndo comunicarse c. con quián comunicarse d. quián se comunicarÄ y e. el proceso por el cual se efectuarÄ la comunicaciên.	Se aèadiê un nuevo subelemento: d. cêmo comunicarse
Cláusula 8	**Operación**		
8.1	**Planeación y control operativos**	La organizaciên planearÄ, implementarÄ y controlarÄ los procesos necesarios para cumplir los requisitos de seguridad de la informaciên y para implementar las medidas determinadas en 6.1. La organizaciên tambián	La organizaciên garantizarÄ que se controlan procesos, productos o servicios provistos externamente que son relevantes para el ISMS.
Cláusula 9	**Evaluación del rendimiento**		
9.1	**Monitoreo, medición, análisis y evaluación**	La organizaciên evaluarÄ el rendimiento de la seguridad de la informaciên y la efectividad del ISMS. La organizaciên determinarÄ: a. quá necesidades se monitorearÄn y medirÄn, incluyendo procesos y controles de seguridad de la informaciên b. los mátodos de monitoreo, mediciên, anÄlisis y evaluaciên, segïn corresponda para garantizar resultados vÄlidos. c. cuÄndo se realizarÄ el monitoreo y la mediciên d. quien monitorearÄ y medirÄ	• La informaciên documentada estarÄ disponible como evidencia de los resultados. • Las organizaciones evaluarÄn el rendimiento de la seguridad de la informaciên y la efectividad del ISMS.

		e. cuÄndo los resultados del monitoreo y mediciên se analizarÄn y evaluarÄn, y f. quián analizarÄ estos resultados. La organizaciên retendrÄ informaciên documentada apropiada como evidencia de los resultados de monitoreo y mediciên.	

Cambios estructurales hechos en la parte dos (controles de seguridad) [5]

Consolidación y adición de controles

An ISO-27001-compliant ISMS requires organizations to change their security measures constantly and evolve with the threat landscape. This leads to an overall increase in cyber resilience.

- Inteligencia de amenazas
- Seguridad de la informaciên para el uso de servicios en la nube
- Disposiciên de la TIC para la continuidad corporativa
- Monitoreo de seguridad fãsica
- Actividades de monitoreo
- Filtrado de contenido web
- Codificaciên segura
- Gestiên de la configuraciên
- Eliminaciên de informaciên
- Enmascaramiento de datos
- Prevenciên de la pérdida de datos

Disminución en el número de secciones

Antes, todos los 114 elementos de control se dividãan en 14 dominios. Cada uno de los 14 dominios abordaba una funciên distinta en una organizaciên. Ahora, los 93 controles actuales se han dividido en cuatro grupos o temas; se eliminê la divisiên basada en funciones. Estos cuatro temas incluyen:

- Controles organizacionales
- Controles de personas
- Controles fãsicos
- Controles tecnolêgicos

Adición de una nueva subclase

La ClÄusula 6.3—Planeaciên de cambios—se introdujo en la ïltima versiên. Exploraremos esto en detalle en la secciên titulada Cambios por clÄusulas hechos en la parte uno.

Atributos

Cada control en la nueva versiên tiene atributos. Estos atributos ayudarÄn a la organizaciên a personalizar y seleccionar controles que mejor se ajusten a sus necesidades de seguridad informÄtica. Hay cinco de estos atributos usados para categorizar lo s93 controles:

- Tipos de control
- Propiedades de seguridad de la informaciên
- Conceptos de seguridad informÄtica
- Funciones operativas
- Dominio de seguridad

Algunos de los atributos se tomaron prestados de otros marcos. Por ejemplo, bajo conceptos de seguridad informÄtica, el marco enumera el ciclo Identificar-Detectar-Proteger-Recuperar-Responder encontrado en el marco NIST. Los atributos también permiten a las organizaciones entender claramente quá procesos, personas y tecnologãasson esenciales y estÄn involucrados en la implementaciên y mantenimiento de un ISMS.

Cambios de lenguaje y contenido

Hay un cambio notable en el lenguaje utilizado en la ISO 27001:2022, empezando con el tãtulo de la norma ISO 27001. Antes conocidos como los Requisitos de tecnologãa de la informaciên —Tácnicas de seguridad— los sistemas de gestiên para la seguridad de la informaciên—, la ïltima versiên de 2022 contiene Requisitos de seguridad de la informaciên, seguridad informÄtica y protecciên de la privacidad —Sistemas de gestiên para la seguridad de la informaciên.

La adiciên del tármino seguridad informÄtica es un indicador de la urgente necesidad de que las organizaciones protejan sus sistemas en el actual panorama de amenazas. La ISO 27001 busca abordar esto mediante la implementaciên de los distintos controles de seguridad enumerados en el documento para crear un ISMS.

En varios lugares, el lenguaje es todavãamÄs activo en comparaciên con la versiên de 2013. El mátodo general detallado en la norma es prÄcticoy basado en resultados o evidencias, en oposiciên al mátodo de lista de control seguido antes.

Énfasis en la seguridad en la nube

La adopciên emergente de las tecnologãas de la nube ha llevado a las organizaciones a aumentar sus medidas de seguridad con respecto a la nube, lo cual también se refleja en la ISO 27001:2022. Uno de los nuevos 11 controles aèadidos a la lista es la seguridad de la informaciên para el uso de servicios en la nube, y explora extensivamente cêmo las organizaciones deben usar dichos servicios. Implementar este control ayudarÄ a fortalecer las medidas de seguridad en la nube en una organizaciên.

Todos los cambios apuntan colectivamente a un nuevo mátodo basado en procesos adoptado por la norma, similar a la ISO 9000.

Lo que significan los nuevos cambios

El marco ISO 27001 ha recibido constantes crãticaspor ser una norma de gestiên, en oposiciên a una norma de seguridad informÄtica. Su mátodo de gestiên basado en riesgos depende del mátodo definido por cada organizaciên para identificar riesgos y abordarlos usando los controles de seguridad enumerados en la norma.[6] La versiên anterior se enfoca en la capacidad de la organizaciên de identificar correctamente riesgos sin profundizar en las personas o procesos involucrados en hacer que eso suceda. La versiên ISO 27001:2022 es mÄs orientada a los procesos, en consonancia con el mátodo de la ISO 9000, y se enfoca en hacer que las organizaciones reconozcan y mejoren continuamente los procesos implementados.

Lo que toda organización certificada debe saber

Las organizaciones con certificaciên ISO 27001 tienen un tiempo de transiciên de tres aèos desde la fecha de publicaciên de la nueva versiên de la norma para empezar a hacer los cambios arriba mencionados. La versiên de 2022 de la norma se publicê el 25 de octubre de 2022.

Lo que toda organización que desea el certificado de la ISO 27001 debe saber

No ha habido cambio alguno en el proceso de certificaciên de la ISO 27001, lo que se detalla y explica con detalle en el siguiente capãtulo.

Capítulo 4

Cumplimiento de los controles de seguridad de la ISO 27001 usando SIEM

Para obtener la ansiada certificaciên ISO 27001 una organizaciên tendrÄ que mostrar que ha implementado correctamente un ISMS y que ha tomado las medidas necesarias para abordar los riesgos.

Diferentes etapas en un proceso de certificación ISO

La auditorãa ara una **certificación ISO 27001** tiene lugar en dos etapas:

Etapa 1

Esta se da cuando un auditor hace una revisiên del ISMS documentado y evalïa si cumple los requisitos de la norma. Las organizaciones necesitan producir una Declaraciên de Aplicabilidad, que es un requisito fundamental para la certificaciên. Consta de controles escogidos de la lista de 93 controles en el Anexo A, el procedimiento de implementaciên de cada uno y la lista de controles omitidos y por quá se omitieron. Este es sobre todo un ejercicio de desktop; hay una interacciên mãnima con las personas cuya tarea es supervisar la implementaciên del ISMS.

Etapa 2

Se audita a la organizaciên para ver si los procesos que ha implementado son como se documentan en el ISMS. Los auditores también entrevistan a los responsables de las operaciones, miran la evidencia de toda la documentaciên y revisan los controles implementados para abordar los riesgos. Por lo general se requiere una prueba de tres meses.

Una vez adquirida, la certificaciên ISO 27001 es vÄlida por tres aèos, después de los cuales se realiza una evaluaciên de recertificaciên. Luego de la certificaciên, las organizaciones pueden esperar visitas de vigilancia al menos una vez al aèo para garantizar que estÄn evolucionando y aèadiendo las ïltimas medidas de seguridad para permanecer vigilantes y actualizados.

Cumplimiento de los nuevos controles de seguridad de la ISO 27001 usando SIEM

Implementar un ISMS que cumpla con la ISO 27001 significa implementar medidas estrictas de control de acceso para mantener la confidencialidad, integridad y disponibilidad de los datos sensibles. Las organizaciones necesitan registrar y revisar regularmente los logs de eventos, protegerse ante accesos no autorizados y garantizar que se usan procedimientos de inicio de sesiên seguros![7]

He aquã cêmo una soluciên de SIEM puede ayudar con los 11 nuevos controles que se aèadieron recientemente a la ISO 27001. Los nïmeros y tãtulos mencionados a continuaciên son similares al formato seguido en el documento de la ISO 27001:2022.

5.7 Inteligencia de amenazas

De qué trata el control: Se requiere que las organizaciones recopilen inteligencia de amenazas de varias fuentes y usen esta informaciên para implementar controles preventivos en sus sistemas para la gestiên de incidentes, operaciones de seguridad y fines de seguridad en las relaciones con proveedores o socios.

Cómo una solución de SIEM puede ayudarlo con esto: Las soluciones de SIEM estÄn equipadas con una funciên de inteligencia de amenazas que puede ayudar a las organizaciones a estar al tanto de las ïltimas amenazas. Las herramientas de SIEM como ManageEngine Log360 recopilan inteligencia de fuentes STIX y TAXII y la integra con servicios de inteligencia de amenazas Webroot y BrightCloud. Esto ayuda a que la soluciên proporcione alertas en tiempo real cuando se detectan actividades en la red que involucran IP y URL en listas negras.

5.23 Seguridad de la información para el uso de servicios en la nube[8]

De qué trata el control: Las organizaciones necesitan definir un proceso para monitorear el uso de la nube, incluyendo la adquisiciên, uso y gestiên de servicios en la nube.

Cómo una solución de SIEM puede ayudarlo con esto: Las organizaciones deben tener la capacidad de monitorear la nube y detectar ataques basados en ella. Ya que las organizaciones se estÄn pasando a infraestructuras multi nube, es vital monitorear las actividades en varios proveedores de nube. Log360 estÄ equipado con un componente de monitoreo de la seguridad en la nube, que permite a las compaèãas monitorear Amazon Web Services, Google Cloud Platform y Microsoft Azure, ademÄs de generar informes para sobre la actividad de la red.

5.30 Disposición de la TIC para la continuidad corporativa

De qué trata el control: Este control aborda la planeaciên de la disposiciên de la tecnologãade la informaciên y comunicaciên (TIC) para garantizar que la organizaciên está preparada con respaldos y un plan de recuperaciên de datos en caso de cualquier alteraciên de los sistemas.

Un administrador de recuperaciên de datos como ManageEngine Recovery Manager Plus puede ayudar a las organizaciones a respaldar sus buzones de Exchange online, on-premises y Google Workspace al analizar instantÄneas de datos y almacenarlas en un espacio de aire.

7.4 Monitoreo de seguridad física

De qué trata el control: Las organizaciones deben establecer medidas de seguridad fãsicas adecuadas para garantizar que las Äreas sensibles estÄn debidamente protegidas mediante cÄmaras o guardias de seguridad, y tener un plan de gestiên de incidentes para incidente de seguridad fãsicos.

Cómo una solución de SIEM puede ayudarlo con esto: La IoT ha allanado el camino para nuevas dimensiones en la seguridad informÄtica. Las cÄmaras de seguridad establecidas para el monitoreo de la seguridad fãsicaproducen log s de sistema de grabadora de video de red y de video digital. Constan de logs de encendido y apagado, ademÄs de logs de reinicio, acceso a cuentas o errores en el disco duro. Asimismo, se pueden analizar y monitorear para detectar actividades sospechosas.

8.9 Gestión de la configuración

De qué trata el control: Este control requiere que las organizaciones tengan configuraciones o parÄmetros implementados para gestionar y monitorear todos los componentes de hardware y software que son parte de una red. Esto es parte de la gestiên de activos y se debe documentar y presentar durante una auditorãa.

Cómo una solución de SIEM puede ayudarlo con esto: Una herramienta de SIEM puede ayudar a las organizaciones a monitorear continuamente sus redes y controlar los dispositivos y endpoints de la red. Recopila y analiza logs generados a partir de estos dispositivos y los presenta como informes. Esto facilita a los analistas de seguridad monitorear estos dispositivos y detectar cualquier cambio no deseado en la red.

8.10 Eliminación de información

De qué trata el control: Las organizaciones generan muchos datos y necesitan establecer un proceso protegido para eliminar datos de manera segura periêdicamente.

Cómo una solución de SIEM puede ayudarlo con esto: Una soluciên de SIEM como Log360 tiene un mêdulo para el anÄlisis de almacenamiento de archivos y visibilidad de datos que ayuda a las organizaciones a identificar y eliminar datos redundantes de manera segura y rentable.

8.11 Enmascaramiento de datos

De qué trata el control: Como su nombre lo indica, el enmascaramiento de datos se refiere al proceso de restringir el acceso a datos sensibles y garantizar la disponibilidad al personal autorizado. Esto es especialmente pertinente para datos personales, debido a las distintas regulaciones sobre privacidad implementadas sobre ellos.

Cómo una solución de SIEM puede ayudarlo con esto: Un administrador de TI o analista de seguridad puede usar una soluciên de SIEM para supervisar quián accede a los datos que necesitan enmascararse o protegerse, y recibir alertas cuando esto suceda.

8.12 Prevención de la pérdida de datos

De qué trata el control: Junto con establecer procesos que determinen cuÄn sensible es un archivo o la cantidad de riesgo que supone, las organizaciones deben también establecer sistemas para monitorear vãaspor las cuales haya un mayor riesgo de pérdidas de datos. En el caso de que suceda una pérdida de datos o un incidente de seguridad similar, se debe resolver de manera oportuna.

Cómo una solución de SIEM puede ayudarlo con esto: En este mundo postpandemia, que estÄ ocupado en la transiciên de un entorno completamente remoto a uno de trabajo hãbrido,los sistemas remotos son altamente vulnerables. Una soluciên de SIEM puede ayudar a monitorear sistemas remotos al controlar los ataques basados en VPN o nube. Los analistas pueden generar informes sobre actividades de archivos y monitoreo de la integridad de los archivos para buscar y analizar regularmente anomalãasen la red. Un agente de seguridad de acceso a la nube o soluciên de SIEM habilitada para CASB puede ayudar a controlar el uso sospechoso de aplicaciones en la nube y detectar actividades como descargas de archivos maliciosos.

8.16 Actividades de monitoreo

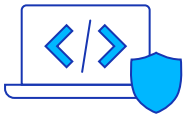
De qué trata el control: Este requisito establece que todas las organizaciones deben monitorear y actualizar todos los logs de eventos, incluyendo aquellos de las aplicaciones de seguridad, para controlar todo el trÄfico de la red y monitorear el acceso a informaciên confidencial. Las organizaciones deben también tener implementado un plan de respuesta ante incidentes en caso de que se presente un incidente de seguridad asã.

Cómo una solución de SIEM puede ayudarlo con esto: Una herramienta de SIEM con funciones de SOAR y de gestiên de incidentes es la soluciên perfecta para todas las organizaciones. La soluciên de SIEM de ManageEngine, Log360, puede ayudar a las organizaciones a controlar la actividad de la red con mÄs de 1000 informes predefinidos que ayudan a los analistas de seguridad a detectar incidentes de seguridad sospechosos. Tiene informes basados en MITRE-ATT&CK®-, que les ayudan a crear perfiles de alertas para los ïltimos ataques cibernáticos.

8.23 Filtrado web

De qué trata el control: Las organizaciones deben garantizar que implementan medidas para evitar que los usuarios visiten sitios web maliciosos y para detectar la ejecuciên de cêdigos maliciosos.

Cómo una solución SIEM puede ayudarlo con esto: las soluciones SIEM vienen equipadas con fuentes de inteligencia de amenazas que tienen una lista de IP en la lista negra de todo el mundo e informes preconstruidos que ayudan a detectar ejecuciones de cêdigos maliciosos. Los equipos de seguridad también pueden crear informes personalizados y perfiles de alerta para actividades sospechosas en la nube y configurar polãticas de acceso a la nube para evitar la manipulaciên de archivos y proteger los datos. Una soluciên SIEM se integra con firewalls, que las organizaciones pueden usar para configurar polãticas que pueden bloquear solicitudes de conexiên de direcciones IP maliciosas, que se pueden obtener de la integraciên con fuentes de inteligencia de amenazas como STIX y TAXII.



8.28 Codificación segura

De qué se trata el control: las organizaciones deben establecer las mejores prÄcticas de codificaciên segura aplicables durante y después de la codificaciên. También deben asegurarse de que todos los codificadores los sigan regularmente. Los cêdigos fuente deben estar protegidos con acceso limitado y protocolos de autorizaciên adecuados. Cualquier violaciên o intento no autorizado de acceder a este debe ser detectado y frenado.

Cómo una solución de SIEM puede ayudarlo con esto: Las soluciones de SIEM pueden ayudar a las organizacionesa detectar accesos no autorizados y ejecutar un conjunto de protocolos para congelarlosapenas aparezcan usando flujos de trabajo automatizados.

Para obtener mÄs informaciên sobre cêmo una soluciên de SIEM como ManageEngine Log360 puede ayudarlo a cumplir estos nuevos 11 controles en la 27001:2022, puede registrarse aquã para una demostraciên personalizada gratuita con nuestros expertos en productos.

Sobre ManageEngine Log360

ManageEngine Log360, una soluciên de SIEM con extensivas funciones de gestiên de logs, automatiza la recopilaciên de logs en terabytes. Garantiza que los logs recopilados se almacenan de manera segura para su anÄlisis mediante monitoreo de la integridad de los archivos y ayuda a las organizaciones a mantener medidas de control de acceso mediante sus informes de seguridad out-of-the-box. Estos ayudan a controlar intentos correctos y fallidos de inicio de sesiên, la actividad de los usuarios y el acceso de autorizaciên a dispositivos y aplicaciones crãticos. Log360 también ayuda a controlar los cambios hechos a las polãticas de usuarios, dominios y auditorãas que las organizaciones pueden usar para garantizar que se implementan procedimientos de inicio de sesiên fiables. Estos cambios pueden monitorearse, analizarse y generarse como informes en tiempo real listos para auditorãas que pueden contribuir significativamente a los procedimientos de cumplimiento.

Para obtener mÄs informaciên sobre cêmo Log360 puede ayudarlo a cumplir con la ISO 27001, regãstrese para una prueba gratuita de 45 dãas y evalïelo por sãmismo, o solicite una demostraciên personalizada con nuestros expertos en productos.

Sobre la autora

Anupama es una asociada de mercadeo de productos en ManageEngine, la divisiên de gestiên de TI empresarial de Zoho Corporation. En su cargo actual estÄ al tanto de las ïltimas tendencias en el espacio de la seguridad informÄtica, especialmente las relacionadas con SIEM. Como una escritora entusiasta, contribuye a la conciencia de la seguridad informÄtica en las organizaciones a travás de su informaciên obtenida a travás de investigaciones.

Referencias

1. A, Anupama. “Getting Started with ISO 27001? Here's What You Need to Know.” ManageEngine Log360 Expert Talks . ManageEngine, May 26, 2022. https://www.manageengine.com/log-management/cyber-security/iso-27001-certification-what-you-need-to-get-started.html.

2. “ISO/IEC 27001:2013 Information Technology-Security Techniques-Information Security Management Systems-Requirements.” BSI . Accessed January 23, 2023.

3. Clark, Quentin. “ISO 27001 - Understanding & Communicating with Stakeholders.” StandardFusion, November 8, 2022. https://www.standardfusion.com/blog/iso-27001-understanding-communicating-with-stakeholders/.

4. Sepulveda, Sebastian. “ISO 27001:2022 Everything You Need to Know about the Main Changes.” StandardFusion, December 20, 2022. https://www.standardfusion.com/blog/iso-27001-changes-2022/.

5. “2022 Update ISO 27001 Information Security Management.” 2022 update ISO 27001 Information Security Management | India. Accessed January 23, 2023. https://www.bsigroup.com/en-IN/ISOIEC-27001-Information-Security/ISOIEC-27001-revision/.

6.Jansen, Dr. Henk Jan. “Why ISO 27001 Is Not Enough.” LinkedIn. Accessed January 23, 2023. https://www.linkedin.com/pulse/why-iso-27001-enough-prof-dr-ir-henk-jan-jansen.

7. Kosutic, Dejan. “What Are the 11 New Security Controls in ISO 27001:2022?” 27001Academy, January 20, 2023. https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/.

8.“ISO 27002:2022 – Control 5.23 – Information Security for Use of Cloud Services.” ISMS.online. Accessed January 23, 2023. https://www.isms.online/iso-27002/control-5-23-information-security-for-use-of-cloud-services/.