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 organizaciones a 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 información.[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 están 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 informática 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 organización:

Salvaguarda la información privilegiada

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

Sistema de gestión centralizado

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

Reducción de los costos en seguridad

Ya que un ISMS se implementa con base en la evaluación de riesgos de cada organización, puede ayudar a evitar que se incurra en costos debido a la experimentación con varias soluciones de seguridad. Asumir un método centralizado conlleva también la reducción en los costos generales.

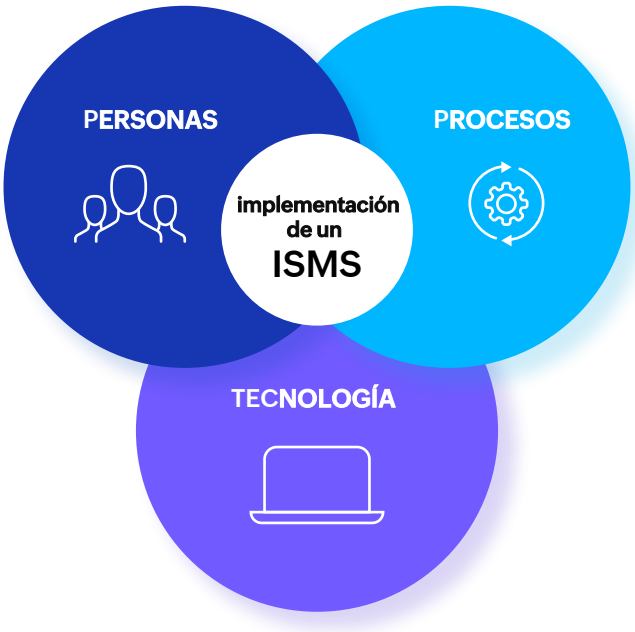
Aumento de la resiliencia informática

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

Implemente un ISMS

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

Esta fórmula hace que la implementación de un ISMS sea según la compañía, lo que incluye la intersección con personas, procesos y tecnología importantes, como se ilustra en la siguiente imagen. Demos un vistazo breve a lo que implica.



Personas

Hay varios interesados involucrados en la implementación de un ISMS. La cláusula 4.2 en la norma habla de las necesidades y expectativas de las "partes interesadas" que la organización debe determinar mientras implementa un ISMS.

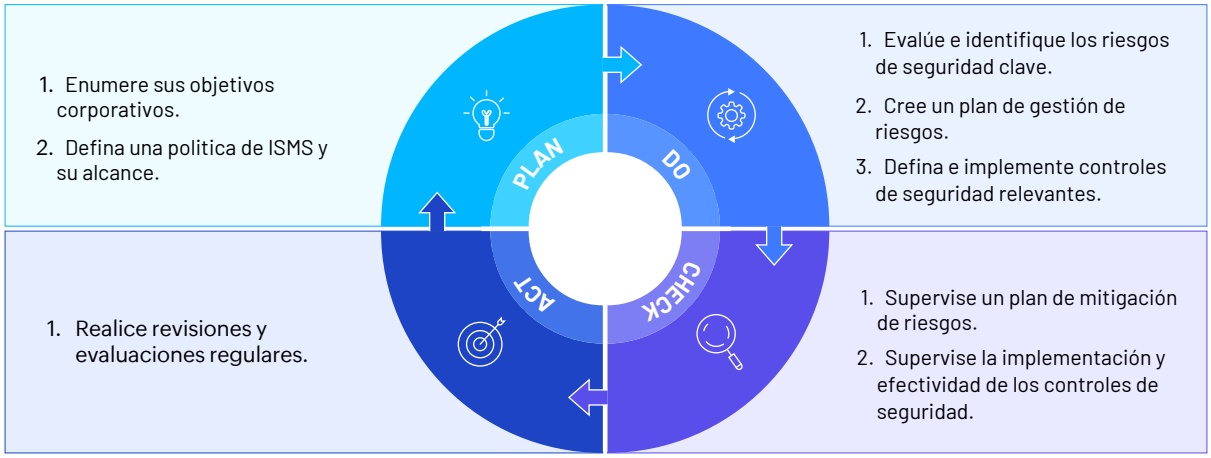
> **Cláusula 4.2:** [3]
> La organización determinará:
>
> a) las partes interesadas pertinentes al sistema de gestión para la seguridad de la información
> b) los requisitos de estas partes interesadas
> c) cuáles de estos requisitos se abordarán mediante el sistema de gestión para la seguridad de la información

Las partes interesadas significará cualquier interesado o entidad que podría verse afectada por la continuidad corporativa o los controles de seguridad de la información en una organización. Esto podría incluir:

- Empleados
- Gobierno o agencias de acreditación
- Clientes
- Gestión principal
- Líderes del departamentos

Procesos

Aquí 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 evaluación. Esto se sigue de forma cíclica para garantizar la mejora continua y una postura de riesgo actualizada para la organización.

Tecnología

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

Algunas de estas tecnologías incluyen:

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

En este capítulo hemos explorado cómo implementar un ISMS y las distintas personas, procesos y tecnologías involucrados en dicha implementación. La última norma, publicada en 2022, tiene cambios importantes que afectan estos factores. En el siguiente capítulo se exploran estos cambios en detalle y se da a las organizaciones la esencia de todo lo que necesitan saber sobre la obtención del certificado de ISO 27001:2022.

Capítulo 3

Entienda los principales cambios en la ISO 27001:2022

Luego de la última corrección en 2017, se esperaba mucho la última versión de la ISO 27001, publicada en octubre de 2022; no fue una decepción.

Aunque hay varias actualizaciones estructurales, la versión de 2022 se enfocó notablemente en las consecuencias prácticas y basadas en resultados para las organizaciones. Al desviarse del método usual de lista de control de cumplimiento para la implementación de un ISMS, esta nueva versión enfatiza un método más 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 cláusulas en la parte uno.

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

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 organización determinará: a. las partes interesadas pertinentes al sistema de gestión para la seguridad de la información; y b. los requisitos de estas partes interesadas relevantes para la seguridad de la información.	Se añadió un nuevo subelemento: c. cuáles de estos requisitos se abordarán mediante el sistema de gestión para la seguridad de la información.
4.4	**Sistema de gestión para la seguridad de la información**	La organización establecerá, implementará, mantendrá y mejorará continuamente un sistema de gestión para la seguridad de la información, de conformidad con los requisitos de la norma internacional.	La organización establecerá, implementará, mantendrá y mejorará continuamente un sistema de gestión para la seguridad de la información,

			incluyendo los procesos necesarios y sus interacciones, de conformidad con los requisitos de esta norma internacional.
Cláusula 6	**Planeación**		
6.2	**Objetivos de seguridad de la información y planificación para lograrlos**	La organización establecerá objetivos de seguridad de la información en las funciones y niveles relevantes. Los objetivos de seguridad de la información: a. serán congruentes con la política de seguridad de la información b. serán medibles (si corresponde) c. tendrán en cuenta la información, requisitos de seguridad y resultados pertinentes a partir de la evaluación y tratamiento de riesgos d. se comunicarán; y e. se actualizarán según corresponda. La organización retendrá información documentada sobre los objetivos de seguridad de la información. Cundo se planee cómo alcanzar los objetivos de seguridad de la información, la organización determinará: f. qué se va a hacer g. qué recursos se requerirán h. quién será el responsable i. cuando se completarán j. cómo se evaluarán los resultados.	Se añadieron nuevos subelementos: (Los objetivos de seguridad de la información:) a. se monitorearán b. estarán disponibles en la información documentada
6.3	**Planeación de cambios**	Esta subcláusula se añadió recientemente y no está presente en la versión de 2013.	Cualquier cambio hecho al ISMS debe realizarse de manera planificada.

Cláusula 7	Soporte		
7.4	**Comunicaciones**	La organización determinará la necesidad de comunicaciones internas y externas relevantes para el sistema de gestión para la seguridad de la información, incluyendo: a. sobre qué comunicarse b. cuándo comunicarse c. con quién comunicarse d. quién se comunicará y e. el proceso por el cual se efectuará la comunicación.	Se añadió un nuevo subelemento: a. cómo comunicarse
Cláusula 8	**Operación**		
8.1	**Planeación y control operativos**	La organización planeará, implementará y controlará los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las medidas determinadas en 6.1. La organización también	La organización garantizará 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 organización evaluará el rendimiento de la seguridad de la información y la efectividad del ISMS. La organización determinará: a. qué necesidades se monitorearán y medirán, incluyendo procesos y controles de seguridad de la información b. los métodos de monitoreo, medición, análisis y evaluación, según corresponda para garantizar resultados válidos. c. cuándo se realizará el monitoreo y la medición d. quien monitoreará y medirá	• La información documentada estará disponible como evidencia de los resultados. • Las organizaciones evaluarán el rendimiento de la seguridad de la información y la efectividad del ISMS.

		e. cuándo los resultados del monitoreo y medición se analizarán y evaluarán, y f. quién analizará estos resultados. La organización retendrá información documentada apropiada como evidencia de los resultados de monitoreo y medición.	

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

Consolidación y adición de controles

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

- Inteligencia de amenazas
- Seguridad de la información para el uso de servicios en la nube
- Disposición de la TIC para la continuidad corporativa
- Monitoreo de seguridad física
- Actividades de monitoreo
- Filtrado de contenido web
- Codificación segura
- Gestión de la configuración
- Eliminación de información
- Enmascaramiento de datos
- Prevención de la pérdida de datos

Disminución en el número de secciones

Antes, todos los 114 elementos de control se dividían en 14 dominios. Cada uno de los 14 dominios abordaba una función distinta en una organización. Ahora, los 93 controles actuales se han dividido en cuatro grupos o temas; se eliminó la división basada en funciones. Estos cuatro temas incluyen:

- Controles organizacionales
- Controles de personas
- Controles físicos
- Controles tecnológicos

Adición de una nueva subclase

La Cláusula 6.3—Planeación de cambios—se introdujo en la última versión. Exploraremos esto en detalle en la sección titulada Cambios por cláusulas hechos en la parte uno.

Atributos

Cada control en la nueva versión tiene atributos. Estos atributos ayudarán a la organización a personalizar y seleccionar controles que mejor se ajusten a sus necesidades de seguridad informática. Hay cinco de estos atributos usados para categorizar lo s93 controles.

- Tipos de control
- Propiedades de seguridad de la información
- Conceptos de seguridad informática
- Funciones operativas
- Dominio de seguridad

Algunos de los atributos se tomaron prestados de otros marcos. Por ejemplo, bajo conceptos de seguridad informática, el marco enumera el ciclo Identificar-Detectar-Proteger-Recuperar-Responder encontrado en el marco NIST. Los atributos también permiten a las organizaciones entender claramente qué procesos, personas y tecnologías son esenciales y están involucrados en la implementación 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 título de la norma ISO 27001. Antes conocidos como los Requisitos de tecnología de la información —Técnicas de seguridad— los sistemas de gestión para la seguridad de la información—, la última versión de 2022 contiene Requisitos de seguridad de la información, seguridad informática y protección de la privacidad —Sistemas de gestión para la seguridad de la información.

La adición del término seguridad informática 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 implementación de los distintos controles de seguridad enumerados en el documento para crear un ISMS.

En varios lugares, el lenguaje es todavía más activo en comparación con la versión de 2013. El método general detallado en la norma es práctico y basado en resultados o evidencias, en oposición al método de lista de control seguido antes.

Énfasis en la seguridad en la nube

La adopción emergente de las tecnologías 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 añadidos a la lista es la seguridad de la información para el uso de servicios en la nube, y explora extensivamente cómo las organizaciones deben usar dichos servicios. Implementar este control ayudará a fortalecer las medidas de seguridad en la nube en una organización.

Todos los cambios apuntan colectivamente a un nuevo método 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 críticas por ser una norma de gestión, en oposición a una norma de seguridad informática. Su método de gestión basado en riesgos depende del método definido por cada organización para identificar riesgos y abordarlos usando los controles de seguridad enumerados en la norma. [6] La versión anterior se enfoca en la capacidad de la organización de identificar correctamente riesgos sin profundizar en las personas o procesos involucrados en hacer que eso suceda. La versión ISO 27001:2022 es más orientada a los procesos, en consonancia con el método 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 certificación ISO 27001 tienen un tiempo de transición de tres años desde la fecha de publicación de la nueva versión de la norma para empezar a hacer los cambios arriba mencionados. La versión de 2022 de la norma se publicó 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 certificación de la ISO 27001, lo que se detalla y explica con detalle en el siguiente capítulo.

Capítulo 4

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

Para obtener la ansiada certificación ISO 27001 una organización tendrá 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 auditoría para una **certificación ISO 27001** tiene lugar en dos etapas:

Etapa 1

Esta se da cuando un auditor hace una revisión del ISMS documentado y evalúa si cumple los requisitos de la norma. Las organizaciones necesitan producir una Declaración de Aplicabilidad, que es un requisito fundamental para la certificación. Consta de controles escogidos de la lista de 93 controles en el Anexo A, el procedimiento de implementación de cada uno y la lista de controles omitidos y por qué se omitieron. Este es sobre todo un ejercicio de desktop; hay una interacción mínima con las personas cuya tarea es supervisar la implementación del ISMS.

Etapa 2

Se audita a la organización 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 documentación y revisan los controles implementados para abordar los riesgos. Por lo general se requiere una prueba de tres meses.

Una vez adquirida, la certificación ISO 27001 es válida por tres años, después de los cuales se realiza una evaluación de recertificación. Luego de la certificación, las organizaciones pueden esperar visitas de vigilancia al menos una vez al año para garantizar que están evolucionando y añadiendo las últimas 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 sesión seguros.[7]

He aquí cómo una solución de SIEM puede ayudar con los 11 nuevos controles que se añadieron recientemente a la ISO 27001. Los números y títulos mencionados a continuación 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 estÃn 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 gestión 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 están pasando a infraestructuras multi nube, es vital monitorear las actividades en varios proveedores de nube. Log360 está 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, además 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 planeación de la disposición de la tecnología de la información y comunicación (TIC) para garantizar que la organización esté preparada con respaldos y un plan de recuperación de datos en caso de cualquier alteración 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 instantáneas 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 físicas adecuadas para garantizar que las áreas sensibles están debidamente protegidas mediante cámaras o guardias de seguridad, y tener un plan de gestión de incidentes para incidente de seguridad físicos.

Cómo una solución de SIEM puede ayudarlo con esto: La IoT ha allanado el camino para nuevas dimensiones en la seguridad informática. Las cámaras de seguridad establecidas para el monitoreo de la seguridad física producen log s de sistema de grabadora de video de red y de video digital. Constan de logs de encendido y apagado, además 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 parámetros implementados para gestionar y monitorear todos los componentes de hardware y software que son parte de una red. Esto es parte de la gestión de activos y se debe documentar y presentar durante una auditoría.

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 periódicamente.

Cómo una solución de SIEM puede ayudarlo con esto: Una solución de SIEM como Log360 tiene un módulo para el análisis 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 solución de SIEM para supervisar quién 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 cuán sensible es un archivo o la cantidad de riesgo que supone, las organizaciones deben también establecer sistemas para monitorear vías por 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 está ocupado en la transición de un entorno completamente remoto a uno de trabajo híbrido, los sistemas remotos son altamente vulnerables. Una solución 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 anomalías en la red. Un agente de seguridad de acceso a la nube o solución 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 tráfico de la red y monitorear el acceso a información confidencial. Las organizaciones deben también tener implementado un plan de respuesta ante incidentes en caso de que se presente un incidente de seguridad así.

Cómo una solución de SIEM puede ayudarlo con esto: Una herramienta de SIEM con funciones de SOAR y de gestión de incidentes es la solución perfecta para todas las organizaciones. La solución de SIEM de ManageEngine, Log360, puede ayudar a las organizaciones a controlar la actividad de la red con más 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 últimos ataques cibernéticos.

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 ejecución de códigos 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 códigos 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 solución SIEM se integra con firewalls, que las organizaciones pueden usar para configurar polãticas que pueden bloquear solicitudes de conexión de direcciones IP maliciosas, que se pueden obtener de la integración 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 prácticas de codificaciên segura aplicables durante y después de la codificación. También deben asegurarse de que todos los codificadores los sigan regularmente. Los códigos fuente deben estar protegidos con acceso limitado y protocolos de autorización adecuados. Cualquier violación 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 organizaciones a detectar accesos no autorizados y ejecutar un conjunto de protocolos para congelarlos apenas aparezcan usando flujos de trabajo automatizados.

Para obtener más información sobre cómo una solución de SIEM como ManageEngine Log360 puede ayudarlo a cumplir estos nuevos 11 controles en la 27001:2022, puede registrarse aquí para una demostraciên personalizada gratuita con nuestros expertos en productos.

ManageEngine
Log360

ManageEngine Log360, una solución unificada de SIEM con funciones de DLP y CASB integradas, ayuda a las empresas a impedir ataques, monitorear acontecimientos de seguridad y cumplir con obligaciones regulatorias. La solución tiene incorporado un componente de gestión de logs que da una mejor visibilidad de la actividad de la red, un módulo de gestión de incidentes que ayuda a detectar, analizar, priorizar y resolver rápidamente incidentes de seguridad, un add-on de análisis de comportamiento de usuarios y entidades basado en ML que establece referencias para comportamientos normales de los usuarios y señala actividades anómalas de estos, una plataforma de inteligencia de amenazas que aprovecha fuentes dinámicas de amenazas para monitorear la seguridad y ayudar a las empresas a estar al tanto de los ataques.

Para más información sobre Log360, visite www.manageengine.com/latam/log-management/

$ Cotización Descargar

Sobre ManageEngine Log360

ManageEngine Log360, una solución de SIEM con extensivas funciones de gestión de logs, automatiza la recopilación de logs en terabytes. Garantiza que los logs recopilados se almacenan de manera segura para su análisis 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 sesión, la actividad de los usuarios y el acceso de autorización a dispositivos y aplicaciones críticos. Log360 también ayuda a controlar los cambios hechos a las políticas de usuarios, dominios y auditorías que las organizaciones pueden usar para garantizar que se implementan procedimientos de inicio de sesión fiables. Estos cambios pueden monitorearse, analizarse y generarse como informes en tiempo real listos para auditorías que pueden contribuir significativamente a los procedimientos de cumplimiento.

Para obtener más información sobre cómo Log360 puede ayudarlo a cumplir con la ISO 27001, regístrese para una prueba gratuita de 45 días y evalúelo por ustedmismo, o solicite una demostración personalizada con nuestros expertos en productos.

Sobre la autora

Anupama es una asociada de mercadeo de productos en ManageEngine, la división de gestión de TI empresarial de Zoho Corporation. En su cargo actual está al tanto de las últimas tendencias en el espacio de la seguridad informática, especialmente las relacionadas con SIEM. Como una escritora entusiasta, contribuye a la conciencia de la seguridad informática en las organizaciones a través de su información obtenida a través 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/.