INTRODUCCION

ISO 27001

Implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI).

JUAN LOAYZA MARQUEZ
PE: DESARROLLO DE SISTEMAS DE INFORMACIÓN

1

1.1 Introducción a la ISO 27001

Esta sección le dará una visión general de ISO 27001, el estándar internacional líder en seguridad de la información, y le ayudará a comprender el lenguaje y la terminología de la norma, así como la lógica y los beneficios de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001.
Aquí hay algunos materiales que lo ayudarán a prepararse mejor para esta sección:

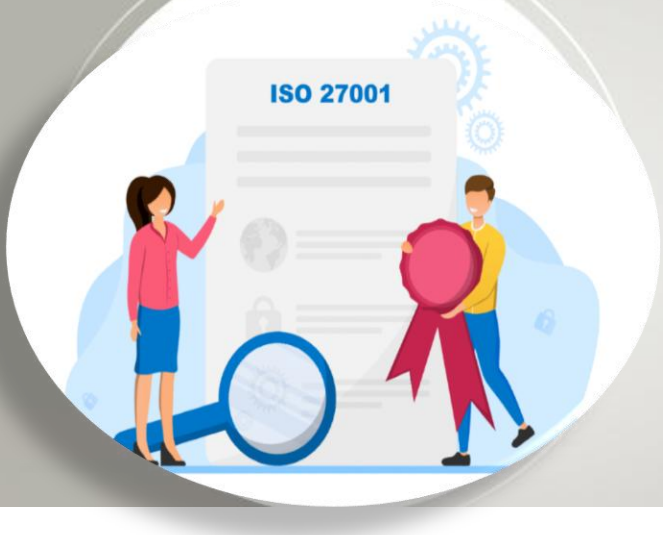
Lectura obligatoria:

- artículo: ¿La lógica básica de ISO 27001: Cómo funciona la seguridad de la información?
- artículo: Entender el lenguaje de la ISO 27001
- artículo: Cuatro beneficios clave de la implementación de ISO 27001

Lectura adicional:

- libro: Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own
- libro: Preparations for the ISO Implementation Project: A Plain English Guide

¿La lógica básica de ISO 27001: Cómo funciona la seguridad de la información?



Cuando se habla con alguien nuevo para ISO 27001, muy a menudo me encuentro con el mismo problema: esta persona piensa que el estándar describirá en detalle todo lo que necesita hacer – por ejemplo, con qué frecuencia necesitará realizar una copia de seguridad, qué tan distante debería estar su sitio de recuperación ante desastres, o peor aún, qué tipo de tecnología debe usar para la protección de la red o cómo debe configurar el enrutador.

Aquí está la mala noticia: ISO 27001 no prescribe estas cosas; funciona de una manera completamente diferente. Aquí hay por qué...

ISO 27001 le brinda un marco para una visión general sistemática de las cosas malas que pueden sucederle (evaluar los riesgos) y luego decidir qué salvaguardas implementar para evitar que sucedan esas cosas malas (tratar los riesgos).

¿Por qué la ISO 27001 no es prescriptiva?

¿Imaginemos que el estándar prescribe que necesita realizar una copia de seguridad cada 24 horas – es esta la medida correcta para usted? Puede ser, pero créanme, muchas empresas hoy en día encontrarán esto insuficiente – la tasa de cambio de sus datos es tan rápida que necesitan hacer copias de seguridad si no en tiempo real, al menos cada hora. Por otro lado, todavía hay algunas compañías que encontrarían la copia de seguridad una vez al día con demasiada frecuencia – su tasa de cambio sigue siendo muy lenta, por lo que realizar la copia de seguridad con tanta frecuencia sería excesivo.

El punto es – si este estándar es para adaptarse a cualquier tipo de empresa, entonces este enfoque prescriptivo no es posible. Por lo tanto, es simplemente imposible no solo definir la frecuencia de copia de seguridad, sino también qué tecnología usar, cómo configurar cada dispositivo, etc.

La gestión de riesgos es la idea central de ISO 27001

Entonces, podrías preguntarte, "¿Por qué necesitaría un estándar que no me diga nada concretamente?"

Porque ISO 27001 le brinda un marco para que decida sobre la protección adecuada. De la misma manera, por ejemplo, no puede copiar una campaña de marketing de otra empresa a la suya, este mismo principio es válido para la seguridad de la información – necesita adaptarlo a sus necesidades específicas.

Y la forma en que ISO 27001 le dice que logre este traje a medida es realizar una evaluación de riesgos y un tratamiento de riesgos. Esto no es más que una visión general sistemática de las cosas malas que pueden sucederle (evaluar los riesgos), y luego decidir qué salvaguardas implementar para evitar que sucedan esas cosas malas (tratar los riesgos).

La idea aquí es que debes implementar solo aquellas salvaguardas (controles) que se requieren debido a los riesgos, no aquellas que alguien piensa que son elegantes; pero, esta lógica también significa que debes implementar todos los controles que se requieren debido a los riesgos, y que no puedes excluir algunos simplemente porque no te gustan.

TI por sí sola no es suficiente

Si trabaja en el departamento de TI, probablemente sepa que la mayoría de los incidentes ocurren no porque las computadoras se hayan averiado, sino porque los usuarios del lado comercial de la organización están utilizando los sistemas de información de manera incorrecta.
Y tales irregularidades no se pueden prevenir con salvaguardas técnicas solo – lo que también se necesita son políticas y procedimientos claros, capacitación y conciencia, protección legal, medidas disciplinarias, etc. La experiencia de la vida real ha demostrado que cuanto más diversas salvaguardas se aplican, se logra un mayor nivel de seguridad.
Y cuando se tiene en cuenta que no toda la información sensible está en forma digital (probablemente todavía tiene documentos con información confidencial sobre ellos), la conclusión es que las salvaguardas de TI no son suficientes, y que el departamento de TI, aunque es muy importante en un proyecto de seguridad de la información, no puede ejecutar este tipo de proyecto solo.

De nuevo, este hecho que La seguridad de TI es solo el 50% de la seguridad de la información es reconocido en ISO 27001 – esta norma le dice cómo ejecutar la implementación de seguridad de la información como un proyecto de toda la empresa donde no solo TI, sino también el lado comercial de la organización, debe participar.

Conseguir la alta dirección a bordo

Pero, ISO 27001 no se detiene con la implementación de varias salvaguardas – sus autores entendieron perfectamente que las personas del departamento de TI, o de otros puestos de nivel inferior o medio en la organización, no pueden lograr mucho si los ejecutivos de la parte superior no hacen algo al respecto.

Por ejemplo, puede proponer una nueva política para la protección de documentos confidenciales, pero si su alta gerencia no hace cumplir dicha política con todos los empleados (y si ellos mismos no la cumplen), dicha política nunca ganará un punto de apoyo en su empresa.

Por lo tanto, ISO 27001 le ofrece una lista de verificación sistemática de lo que debe hacer la alta dirección:

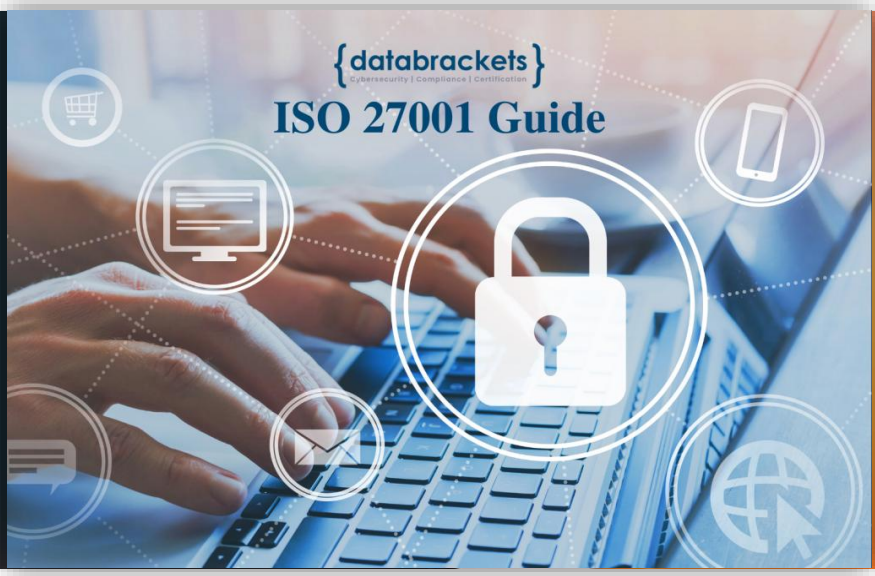
- Establecer sus expectativas de negocio (objetivos) para la seguridad de la información
- Publicar una política sobre cómo controlar si se cumplen esas expectativas
- Designar las principales responsabilidades en materia de seguridad de la información
- Proporcionar suficiente dinero y recursos humanos.
- revise regularmente si todas las expectativas se cumplieron realmente.

No permitir que su sistema se deteriore

Si trabajas en una empresa durante un par de años o más, entonces probablemente sepas cómo funcionan las nuevas iniciativas/proyectos – al principio se ven agradables y brillantes y todos (o al menos la mayoría de las personas) están tratando de hacer todo lo posible para que todo funcione. Sin embargo, con el tiempo, el interés y el celo se deterioran, y con ellos, todo lo relacionado con tal proyecto también se deteriora.

Por ejemplo, es posible que haya tenido una política de clasificación que funcionó bien inicialmente, pero con el tiempo la tecnología cambió, la organización cambió y la gente cambió, y si a nadie le ha importado actualizar la política, se volverá obsoleta. Y, como bien sabe, nadie querrá cumplir con un documento obsoleto, lo que significa que su seguridad empeorará.
Para evitar esto, ISO 27001 ha descrito un par de métodos que evitan que se produzca tal deterioro; aún más, esos métodos se utilizan para mejorar la seguridad a lo largo del tiempo, haciéndola aún mejor de lo que era en el momento en que el proyecto estaba en su punto más alto. Estos métodos incluyen monitoreo y medición, auditorías internas, acciones correctivas, etc.
Por lo tanto, no debería ser negativo sobre ISO 27001 – puede parecer vago en primera lectura, pero puede llegar a ser un marco extremadamente útil para resolver muchos problemas de seguridad en su empresa.

Entender el lenguaje de la ISO 27001



Una de las principales reglas de una buena comunicación es ajustar su discurso al público objetivo. ISO 27001 tiene su propio conjunto de términos, útil para aprovechar la comprensión entre los profesionales de la seguridad. Sin embargo, una organización es más que su personal de seguridad. La alta gerencia, la gerencia media, los trabajadores de línea, los clientes y muchas otras personas interactúan con el negocio, y también deben comprender la seguridad de la información.

El problema es que, si usa solo los términos ISO 27001, es probable que confunda a las personas y las personas confundidas son de poca ayuda para proteger la información comercial. Por lo tanto, debe hacer que la información de seguridad sea fácil de entender en su punto de vista. Esto nos lleva a esta sección, para mostrar algunos términos ISO 27001 traducidos en palabras comerciales más comunes que te ayudarán en el proceso de explicación de ISO 27001 y el proceso de certificación.

Algunos de los términos principales de ISO 27001:

- *Lista de verificación de auditoría*
- *Certificación*
- *Proceso de certificación*
- *Empresa certificada*
- *Controles*

ISO 27001 términos principales a través de nuevas palabras
Los siguientes son algunos de los términos más importantes y comúnmente buscados en relación con ISO 27001, y cómo puede presentarlos de una manera que consideramos fácil de explicar:

Lista de verificación de auditoría: Un conjunto de información utilizada para ayudar a garantizar que algo se haya hecho o hecho como se esperaba. Una lista de deseos es un buen ejemplo de una lista de verificación. Un vuelo previo lista de verificación es otro. Una lista con elementos obligatorios estándar (de ISO o definidos por su propia organización) es otro ejemplo.

Certificación: Confirmación de que una persona, proceso, sistema o producto ha demostrado que ha alcanzado criterios predefinidos. Una certificación de beca confirma que una persona ha asistido a los cursos necesarios y ha demostrado el conocimiento para obtener una designación o se le permite ejercer una profesión. Una certificación de seguridad confirma que una persona/proceso/sistema ha alcanzado criterios de seguridad predefinidos (por ejemplo, ISO 27001, PCI, etc.).

Proceso de certificación: Un proceso a través del cual una persona/proceso/sistema/producto va a demostrar que ha logrado criterios predefinidos. Probar zapatos para encontrar el ajuste más cómodo es un ejemplo de la realización de un proceso de certificación. Si su organización verifica sistemáticamente los resultados/productos con criterios predefinidos, tiene un proceso de certificación. Si los criterios están relacionados con la seguridad, entonces usted tiene un proceso de certificación de seguridad.

Empresa certificada: Cualquier organización que haya demostrado que ha logrado criterios predeterminados. Una empresa certificada ISO 27001 ha alcanzado los requisitos obligatorios definidos por la norma ISO 27001.

Controles: Métodos utilizados para evitar/minimizar resultados no deseados. Miras a ambos lados antes de cruzar una calle para evitar ser atropellado por un automóvil. La bolsa de aire puede minimizar el daño en un accidente automovilístico. Cualquier práctica que utilice en su organización para evitar problemas o minimizar sus consecuencias son controles.

Análisis de brechas: Cualquier práctica utilizada para comparar el rendimiento real y esperado/potencial, para identificar en qué elementos está bien y en cuáles tiene que mejorar/cumplir, ayudándole a determinar qué debe hacer para cumplir con los resultados propuestos.

ISMS (Sistema de Gestión de Seguridad de la Información): Parte del sistema general de gestión con el objetivo de proteger la seguridad de la información. Un sistema de gestión de Recursos Humanos se encarga de los recursos humanos. Un sistema de gestión financiera se encarga de los ingresos, gastos, activos, etc.

Política ISMS: La gestión declaración sobre lo que espera de quienes interactúan con las organizaciones' información, respecto a su uso y protección.

Auditor principal: Una persona que es capaz de planificar y ejecutar los pasos necesarios para verificar si una persona/proceso/sistema/producto logra criterios predefinidos. Cualquier persona de su organización que, utilizando criterios predefinidos, pueda planificar y ejecutar la verificación de procesos/productos puede considerarse un auditor principal.

Implementador principal: Una persona que es capaz de planificar y ejecutar los pasos necesarios para implementar un proceso de acuerdo con criterios predefinidos. Cualquier persona de su organización que, utilizando criterios predefinidos, pueda planificar y ejecutar la implementación de un proceso puede considerarse un implementador principal.

Evaluación de riesgos: Cualquier proceso sistemático para identificar y tratar el riesgo de acuerdo con lo predefinidos **criterios**. La película de Clint Eastwood "Dirty Harry" es uno de los mejores ejemplos de evaluación de riesgos. (El malo tiene que decidir si agarrar el arma. A Harry Callaghan le queda una bala en su .44 Magnum? – "¿Te sientes afortunado? Bueno, sí, punk?"). Otro ejemplo es The Matrix (la píldora roja y la azul, ¿te acuerdas?).

Estándar: Cualquier conjunto de reglas acordadas sobre cómo lograr algo. El patrón de color de un semáforo es un ejemplo de un estándar. Si su organización siempre utiliza las mismas prácticas para proteger la comunicación de la información, tiene un estándar de seguridad de comunicación.

Declaración de aplicabilidad: Documento en el que declara qué controles considera relevantes y sus objetivos, en función de los requisitos de su negocio. Si realiza un chequeo médico anualmente para asegurarse de que está sano y para mejorar sus posibilidades de vivir más tiempo, y poner esa práctica (control) en un documento, esto podría considerarse una declaración de salud de aplicabilidad.

Por supuesto, estos son algunos ejemplos. Puede ajustarlos a su industria comercial. Lo importante es que sus términos deben mantener el mismo significado de los términos ISO 27001.

Recuerde: la comunicación no se trata de lo que dice, sino de lo que su audiencia entiende. Asegúrese de elegir las palabras con las que se sienten más cómodos y de que la seguridad de la información sea más fácil de ser parte de sus vidas y actividades.

Cuatro beneficios clave de la implementación de ISO

¿Alguna vez ha tratado de convencer a su administración para financiar la implementación de la seguridad de la información? Si lo has hecho, probablemente sepas cómo se siente – te preguntarán cuánto cuesta, y si suena demasiado caro, dirán que no.

En realidad, no deberías culparlos – después de todo, su responsabilidad final es la rentabilidad de la empresa. Eso significa que cada una de sus decisiones se basa en el equilibrio entre la inversión y el beneficio, o en ponerlo en el lenguaje "management" – ROI (retorno de la inversión).
Esto significa que primero debe hacer su tarea antes de tratar de proponer tal inversión – piense cuidadosamente cómo presentar los beneficios, utilizando un lenguaje que la administración comprenderá y respaldará.
En mi experiencia, los siguientes cuatro son los más importantes:

°También es importante saber que ISO 27001 por sí sola no incluye todos los requisitos de seguridad de la información de las leyes y regulaciones locales en países específicos. Por lo tanto, para cumplir con todas ellas, una empresa necesitará implementar algunas salvaguardas adicionales que son requeridas por estas leyes y regulaciones.

**Para ser honesto, todavía no existe una metodología y/o tecnología para calcular cuánto dinero podría ahorrar si evitara tales incidentes. Pero siempre suena bien si traes tales casos a la atención de los directivos.*

1) Cumplimiento: A menudo esto representa el más rápido "retorno de la inversión" – si una empresa debe cumplir con varias regulaciones con respecto a la protección de datos, la privacidad y la gobernanza de TI (especialmente si es una organización financiera, de salud o gubernamental), entonces ISO 27001 puede incorporar la metodología que le permite hacerlo de la manera más eficiente.
Aún más importante, si un cliente existente le pide que cumpla con ISO 27001, entonces debe cumplir con el estándar para mantener al cliente.

2) Ventaja de marketing: A veces es muy difícil encontrar algo que lo diferencie a los ojos de los clientes potenciales.
ISO 27001 podría ser un punto de venta único que puede diferenciarlo de sus competidores, especialmente si los nuevos clientes desean que sus datos sean tratados con gran cuidado.

3) Bajar los gastos: La seguridad de la información generalmente se considera como un costo sin una ganancia financiera obvia. Sin embargo, hay una ganancia financiera si reduce sus gastos causados por incidentes. Probablemente tenga interrupciones en el servicio, fugas de datos ocasionales o empleados descontentos. O ex empleados descontentos.

4) Poner orden a su negocio: Este es probablemente el más subestimado – si eres una empresa que ha estado creciendo rápidamente durante los últimos años, puede experimentar problemas como – que tiene que decidir qué, quién es responsable de ciertos activos de información, quién tiene que autorizar el acceso a los sistemas de información, etc.*****
ISO 27001 es particularmente bueno para clasificar estas cosas – lo obligará a definir roles y responsabilidades con mucha precisión y, por lo tanto, fortalecerá su organización interna.
Para concluir, en la mayoría de los casos, si presenta esos beneficios de manera clara, la gerencia comenzará a escucharlo.°

1.2 Que es ISO 27001

Antes de entrar en detalles sobre la estructura y los requisitos de la ISO 27001, veamos qué es exactamente este estándar. Lo primero que se debe mencionar es que ISO 27001 es un estándar reconocido internacionalmente que especifica los requisitos para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) en una empresa.

ISO 27001 consta de dos partes, la parte principal del estándar y el Anexo A. La parte principal del estándar comprende 11 cláusulas. Sin embargo, las cláusulas de cero a tres describen el estándar en sí, por lo que no son importantes para la implementación. Mientras que las cláusulas de 4 a 10 establecen los requisitos para la seguridad de la información, los requisitos que tu empresa debe cumplir si deseas ser conforme al estándar. El Anexo A contiene 93 salvaguardas o controles que deben considerarse al diseñar el SGSI (Sistema de Gestión de Seguridad de la Información).

Prueba:

¿Es ISO 27001 un estándar que define los detalles técnicos para la seguridad de la información, por ejemplo, cómo configurar un firewall?

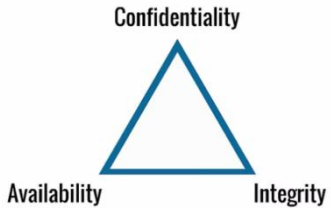
1.3 Estructura de la ISO 27001

Ahora veamos la estructura de la norma ISO 27001 traducida al español:

***0. Introducción*:** La cláusula introductoria ofrece una visión general de la norma y su propósito, y explica su compatibilidad con otras normas ISO.
1. Alcance: Define el alcance de la norma, señalando que es aplicable a todo tipo de organizaciones.
2. Referencias normativas: La segunda cláusula menciona las referencias normativas, y la tercera cláusula, términos y definiciones, ambas refieren a la norma ISO 27000 para la seguridad de la información y los términos y definiciones proporcionados.
3. Términos y definiciones: Define los términos y conceptos clave relacionados con la seguridad de la información.
4. Contexto de la organización: Requiere comprender los problemas externos e internos, las partes interesadas, los requisitos y también definir el alcance del SGSI (Sistema de Gestión de Seguridad de la Información).
5. Liderazgo: Esta sección define las responsabilidades de la alta dirección, estableciendo las leyes generales, roles y responsabilidades para el SGSI y define el contenido de la política de seguridad de la información de alto nivel.
6. Planificación: Define los requisitos para la evaluación de riesgos, el tratamiento de riesgos, la declaración de aplicabilidad, el plan de tratamiento de riesgos y el establecimiento de los objetivos de seguridad de la información.
7. Apoyo: Esta cláusula define los requisitos para la disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
8. Operación: Establece los requisitos para la reevaluación y tratamiento regular de riesgos, así como la implementación de controles y otros procesos necesarios para proteger la información.
9. Evaluación del desempeño: Define los requisitos para el monitoreo, medición, análisis, evaluación, auditoría interna y revisión por la dirección.
10. Mejora: Esta cláusula define los requisitos para la mejora continua, acciones correctivas y corrección.
Anexo A: Objetivos de control y controles de referencia. Este anexo proporciona un catálogo de 93 controles agrupados en 4 secciones.
Todas estas cláusulas de la norma ISO 27001, comenzando desde la cuarta cláusula sobre el contexto de la organización hasta el Anexo A, serán discutidas en las siguientes secciones de este módulo.

PRUEBA

¿Por qué se describe la sección de Planificación antes de la sección de Operación en el estándar?



1.4 Principios de seguridad de la información

Antes de continuar, permíteme explicar algunos conceptos básicos importantes para la seguridad de la información. Primero, definamos qué es la ***información***. La información es un activo* que tiene valor para la organización y necesita ser protegida. La información puede presentarse en diversas formas y puede almacenarse en diferentes medios, como digital o en papel, pero también puede ser en forma hablada, por ejemplo. Por otro lado, la seguridad de la información se define como garantizar la confidencialidad, integridad y disponibilidad de la información. Permíteme explicar lo que realmente significa. La confidencialidad es la garantía de que solo las personas autorizadas pueden acceder a la información. La integridad es la garantía de que solo las personas autorizadas pueden modificar los datos, lo que significa la protección de la exactitud y la integridad de la información. La disponibilidad es la garantía de acceso oportuno y confiable a los datos y servicios para los usuarios autorizados.

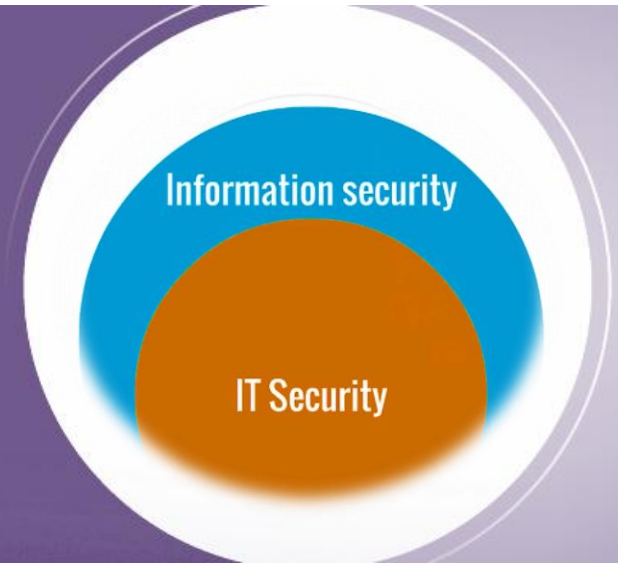
**Un activo es algo que tiene valor monetario y que la persona posee, obtiene un beneficio o usa.*

Un ejemplo simple para explicar estos elementos sería abrir una cuenta de ahorros en un banco con, digamos, $10,000. Primero, no me gustaría que todos supieran cuánto dinero tengo en esta cuenta. Esperaría que el banco protegiera la confidencialidad de esta información y que solo el banco y las autoridades financieras pudieran conocer mi cuenta. Luego, no quiero ir al banco después de un tiempo y que me informen que de repente solo tengo $1,000 en mi cuenta porque alguien ha hackeado su sistema. Me gustaría que mis ahorros se mantuvieran igual, $10,000 más los intereses, por lo que el banco también debería proteger la integridad de esta información. Y finalmente, cuando vaya a retirar mi dinero, no quiero que me digan que el sistema está caído y que no puedo obtener mi dinero. Quiero que esta información esté disponible. Estos tres principios o estos tres elementos son los principios básicos de la seguridad de la información. Por lo general, cuando se habla de seguridad de la información, la gente piensa instantáneamente en proteger. Sin embargo, es importante saber que para proteger la información, la confidencialidad no es suficiente. También se deben lograr la integridad y la disponibilidad. Así que necesitas tener en cuenta estos tres principios en todo momento.

PRUEBA

Para los siguientes controles de seguridad, elija cuál de los tres principios de seguridad de la información (confidencialidad, integridad y disponibilidad) más impactan:

1.5 Introducción al Sistema de Gestión de Seguridad de la Información



Un sistema de gestión de la seguridad de la información (SGSI) es un enfoque sistemático para gestionar y proteger la información de las empresas. El SGSI consiste en controles organizacionales como políticas y procedimientos que establecen las reglas de seguridad de la información en una organización, así como controles técnicos y de otro tipo. Los tipos de seguridad que se implementarán en una empresa se decidirán en función de los requisitos de las partes interesadas y los resultados de la evaluación de riesgos, pero también, por supuesto, en función de la decisión de la dirección sobre cómo tratar cada riesgo. Se necesitará una combinación de diferentes tipos de controles.

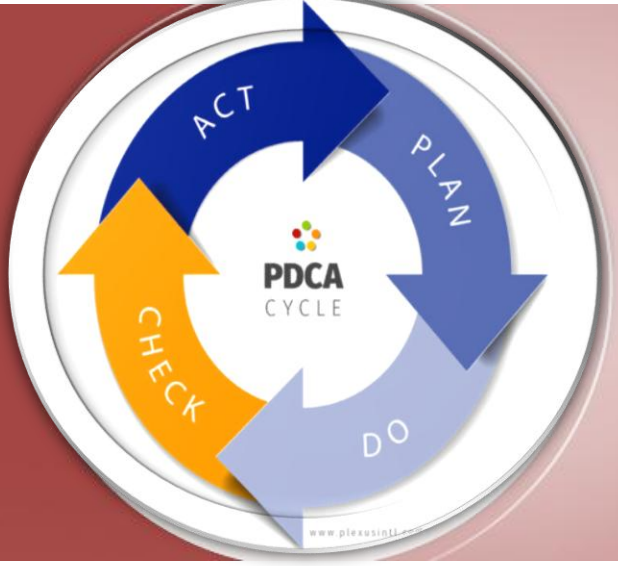
Supongamos que tienes un empleado que frecuentemente deja su laptop en el coche. Las probabilidades son que tarde o temprano esta laptop será robada. Entonces, ¿qué puedes hacer para disminuir este riesgo para la información que está en esta laptop? Necesitarás aplicar algunos controles. En primer lugar, puedes redactar un procedimiento que indique que los empleados no pueden dejar las laptops en el coche. También puedes proteger todas las laptops con una contraseña, de modo que, si se roban, será más difícil para alguien acceder a tu información. Además, puedes cifrar el disco en las laptops, lo que hace que tus datos estén aún más protegidos. Y puedes pedir a tus empleados que firmen una declaración en la que se comprometan a pagar por los daños que ocurran si tal incidente sucede. Finalmente, debes capacitar a tus empleados para usar este procedimiento de la manera correcta y también hacerles conscientes de los riesgos de usar las laptops de esta manera.

¿Qué se puede concluir de este ejemplo? Los controles de seguridad de la información nunca son solo técnicos o, al menos, no solo relacionados con TI. Deben ser una combinación de diferentes tipos de controles. Documentar un procedimiento es un control organizacional, implementar el cifrado es, por supuesto, un control de TI, y la capacitación y la concienciación son controles relacionados con las personas. Otra percepción general, que también es incorrecta, es que la seguridad de la información y la seguridad de TI son una y la misma cosa. Como expliqué anteriormente, la seguridad de la información es un concepto más amplio que la seguridad de TI porque incluye la protección de diferentes tipos de información, no solo la información almacenada y transmitida a través de TI. Por ejemplo, la seguridad de la información se encargará de que las notas hechas en papel o en el cuaderno de papel por nuestro CEO también estén protegidas.

PRUEBA

Identifique cuáles de los siguientes controles de seguridad de la información son controles organizacionales:

1.6 Implementación de los requisitos ISO 27001:2022



Explicado anteriormente, ISO 27001 es un estándar que especifica los requisitos para establecer, implementar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI) en tu empresa. Para cumplir con ISO 27001, tu organización debe implementar todos los requisitos especificados en las cláusulas 4 a 10. ISO 27001 se implementa y mantiene mejor a través de un método llamado Ciclo PDCA, que es el acrónimo de Planificar, Hacer, Verificar y Actuar. Este ciclo PDCA es un método de cuatro fases utilizado en todos los estándares de gestión ISO para el control y la mejora continua de procesos y sistemas.

La fase de Planificar trata sobre qué lograr y cómo hacerlo. La fase de Hacer trata sobre implementar lo que has planificado en la fase anterior. La fase de Verificar trata sobre confirmar si las cosas salieron como se planificaron y si se lograron los objetivos deseados. Y la fase de Actuar trata sobre cerrar la brecha entre la fase de Planificar (esto es lo que has planificado) y la fase de Verificar (esto es lo que realmente has logrado). Y más importante aún, esta última fase trata sobre mejorar la forma en que haces las cosas.

Ahora pasaré brevemente por las cuatro fases del ciclo PDCA y explicaré lo que esto significa para tu SGSI. La fase de Planificar incluye las siguientes actividades: entender el contexto de la organización, definir el alcance del SGSI, planificar la política de seguridad de la información, realizar la evaluación de riesgos, documentar la declaración de aplicabilidad y el tratamiento de riesgos.

La fase de Hacer incluye la implementación del plan de tratamiento de riesgos y varios controles y procesos para lograr los objetivos de seguridad de la información, así como la evaluación de riesgos de manera regular.

La fase de Verificar incluye la realización de monitoreos y mediciones regulares, auditorías internas y revisiones por la dirección. Finalmente, la fase de Actuar incluye la implementación de acciones correctivas e iniciativas de mejora.

En las siguientes secciones, explicaré todos estos requisitos con más detalle, pero lo que es importante recordar ahora es que la fase de Planificar está cubierta en las cláusulas 4 a 7, la fase de Hacer en la cláusula 8, la fase de Verificar en la cláusula 9 y la fase de Actuar en la cláusula 10 de la ISO 27001.

PRUEBA

Elija cuáles de las siguientes actividades son parte de la fase del Plan:

1.7 Implementación de ISO 27001 como proyecto

Implementar ISO 27001 en su empresa es un proyecto en sí mismo y debe tratarse como tal. Una buena práctica para la implementación efectiva de ISO 27001 es formar un equipo de proyecto y asignar roles concretos a los miembros del equipo. Los roles básicos en el proceso de implementación del SGSI suelen ser los siguientes:

Gerente de proyecto: Esta es la persona que coordinará el proyecto de implementación de ISO 27001 en su empresa.

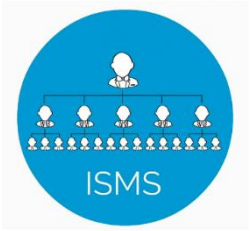
Equipo de proyecto: Estas son las personas que, bajo la coordinación del gerente de proyecto, estarán involucradas en la documentación e implementación de los controles de seguridad de la información, y que organizarán a otras personas, darán consejos, liderarán el cambio, etc.

Oficial de seguridad de la información: Esta es la persona responsable del mantenimiento del SGSI y su mejora continua. A menudo, esta persona también es el gerente de proyecto al mismo tiempo.

Alta dirección: Deben apoyar el proyecto mostrando compromiso, estableciendo los objetivos, tomando decisiones cruciales y, lo más importante, proporcionando los recursos relevantes, como asignar a las personas adecuadas con suficiente tiempo y proporcionando suficiente dinero para el proyecto.

PRUEBA

El gerente del proyecto, como uno de los roles básicos en el proceso de implementación de ISMS, tiene las siguientes características:



1.8 Documentación de los requisitos ISO 27001

Mencionado anteriormente, la documentación del Sistema de Gestión de Seguridad de la Información (SGSI) consiste en un conjunto de políticas, procedimientos y varios otros documentos que describen las reglas de seguridad de la información en una empresa. Pero, ¿cómo decides qué políticas y procedimientos documentar y con qué nivel de detalle? Cada cláusula del estándar especifica si los requisitos de esa cláusula necesitan ser documentados o no. Así que esto es lo primero que debes verificar. Si el documento es obligatorio, no tienes nada que pensar. Debes escribirlo si quieres cumplir con el estándar. Sabrás si el documento es obligatorio leyendo el propio estándar. Este establece con bastante claridad lo que necesita ser documentado usando una frase como: "La organización deberá conservar información documentada". De algo, por ejemplo, los resultados de la evaluación de riesgos. Aquí está la lista de documentos y registros obligatorios que prescribe la ISO 27001:

- *El alcance del ISMS*
- *Política y objetivos de seguridad de la información*
- *Metodología de evaluación y tratamiento de riesgos*
- *Declaración de aplicabilidad*
- *Plan de tratamiento de riesgos*
- *Informe de evaluación de riesgos*
- *Registros de formación, habilidades, experiencia y cualificaciones*
- *Resultados de monitoreo y medición*
- *Programa de auditoría interna*
- *Resultados de auditorías internas*
- *Resultados de la revisión por la dirección*
- *Resultados de acciones correctivas*

Ten en cuenta que incluso cuando el estándar no requiere explícitamente que algo se escriba, podría ser útil para tu empresa tener algún tipo de documento adicional de políticas y procedimientos. Así que, si el documento no es obligatorio, podrías encontrarte dudando sobre si necesitas escribirlo o no. Ahora, aquí hay algunos criterios que pueden ayudarte a tomar esta decisión:

Riesgos y requisitos de las partes interesadas: Revisa los resultados de la evaluación de riesgos y la lista de requisitos de las partes interesadas para ver si hay necesidad de un control y de documentar dicho control. Si no hay riesgo o requisito, entonces ciertamente no necesitarás documentar un control en particular.
Tamaño de la empresa: Las empresas más pequeñas tenderán a tener menos documentos, por lo que en tal caso deberías tratar de evitar escribir procedimientos para cada pequeño proceso. Por ejemplo, si tienes una empresa pequeña, no necesitas 50 documentos para tu SGSI. Por supuesto, si eres una organización multinacional con, digamos, 10,000 empleados, escribir varias políticas, donde cada política tendría un par de procedimientos relacionados y luego para cada procedimiento un par de instrucciones de trabajo, este enfoque tendría sentido para una empresa tan grande.
Importancia y complejidad: Cuanto más importante y complejo sea un proceso o actividad, más probable es que desees escribir una política o procedimiento para describirlo. Esto se debe a que querrás asegurarte de que todos entiendan cómo realizar el proceso o actividad para evitar cualquier tipo de interrupción en tus actividades.

PRUEBA

¿Cómo decide qué políticas y procedimientos documentar?

Beneficios de ISO 27001

Además de mejorar la seguridad de la información en tu empresa, implementar la norma te ayuda a lograr los siguientes beneficios comerciales de cumplimiento. ISO 27001 te proporciona el marco que te ayuda a cumplir con las regulaciones pertinentes. En cuanto a la protección de datos, la privacidad, la gobernanza de TI, así como tus obligaciones contractuales, como diversas cláusulas de seguridad o acuerdos de nivel de servicio. Además, ISO 27001 te proporciona una ventaja de marketing al ayudarte a diferenciarte de tus competidores. La norma podría ser un punto de venta único, especialmente si manejas información sensible de clientes y si tienes un certificado que tus competidores no tienen.

El siguiente beneficio es la reducción de los gastos que pueden ser causados por incidentes. La seguridad de la información suele considerarse un costo sin un beneficio financiero obvio. Sin embargo, cada incidente te cuesta dinero. Si tus operaciones se ven interrumpidas o si tienes una fuga de datos sensibles, tendrás que pagar bastante dinero para resolver estos incidentes. Sin embargo, prevenir tales incidentes mediante la implementación de un SGSI es mucho más barato y puedes usar este argumento para presentar el retorno de la inversión a tus ejecutivos.
Finalmente, ISO 27001 te ayuda a organizar mejor tu negocio al definir responsabilidades y procedimientos.

Si eres una empresa que ha estado creciendo rápidamente en los últimos años, podrías experimentar problemas como quién tiene que hacer qué, quién es responsable de qué, quién tiene que autorizar procesos o acceso a sistemas de información, y así sucesivamente. ISO 27001 es particularmente bueno para aclarar estas cosas. Te obligará a definir muy precisamente tanto las responsabilidades como los procesos y, por lo tanto, fortalecerá tu organización interna.

También es importante saber que ISO 27001 por sí sola no incluye todos los requisitos de seguridad de la información de las leyes y regulaciones locales en países específicos. Por lo tanto, para cumplir con todas ellas, una empresa necesitará implementar algunas salvaguardas adicionales que son requeridas por estas leyes y regulaciones.

PRUEBA

¿Cuál de los siguientes es un beneficio de implementar un Sistema de Gestión de Seguridad de la Información basado en ISO 27001 en una organización?

Documentación relacionada

Para aprender a estructurar los documentos mencionados en este módulo, consulte las vistas previas gratuitas de estas plantillas:

Política de Seguridad de la Información el objetivo de esta política de alto nivel es definir el propósito, la dirección, los principios y las reglas básicas para la gestión de la seguridad de la información. Tenga en cuenta: esta política de alto nivel está escrita de acuerdo con los requisitos de ISO 27001 en la cláusula 5.2, y no describe reglas de seguridad detalladas – para documentos con reglas detalladas, consulte *Política de Uso Aceptable.*

Declaración de Aplicabilidad- El propósito de este documento es definir qué controles son apropiados para ser implementados en la organización, los objetivos de estos controles y cómo se implementan, así como aprobar los riesgos residuales y aprobar formalmente la implementación de dichos controles.

Documento de alcance SGSI- El propósito de este documento es definir claramente los límites del Sistema de Gestión de Seguridad de la Información (SGSI).

Metodología de Evaluación de Riesgos y Tratamiento de Riesgos
- El propósito de este documento es definir la metodología para la evaluación y tratamiento de los riesgos de información, y definir el nivel aceptable de riesgo.

Plan de Tratamiento de Riesgos
- El propósito de este documento es determinar con precisión quién es responsable de la implementación de los controles, en qué plazo, con qué presupuesto, etc.

Informe de Evaluación y Tratamiento de Riesgos
- El propósito de este documento es dar una visión detallada del proceso y los documentos utilizados durante la evaluación de riesgos y el tratamiento.

Programa Anual de Auditoría Interna
El propósito de este documento es definir con qué frecuencia se llevarán a cabo las auditorías internas y según qué reglas.

https://github.com/afalconr/ISO27001-plantillasES

https://advisera.com/27001academy/blog/2014/10/06/how-personal-certificates-can-help-companys-isms/

Preguntas de Recapitulación

Seguridad de la información y seguridad de TI se refieren a lo mismo:

Un Sistema de Gestión de Seguridad de la Información es un enfoque sistemático para administrar y proteger la información de una empresa.

El ciclo PDCA es:

Cuál de los siguientes roles es común en el proceso de implementación de ISMS:

Lograr el cumplimiento es uno de los principales beneficios de implementar ISO 27001: