Unidad 2
Implementación de una ISO 27001

Normas de seguridad

UNIVERSIDAD MAYOR
para espíritus emprendedores

Introducción

La implementación de la **norma ISO 27001** es un paso decisivo para cualquier organización que busque asegurar la confidencialidad, integridad y disponibilidad de su información. Este estándar internacional proporciona un marco robusto para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).

En esta unidad, aprenderás que antes de iniciar un proyecto de implementación, es comprender la estructura y los requisitos que exige este estándar en particular. Este conocimiento te permitiría una planificación adecuada para garantizaría que todos los aspectos de la norma se aborden de manera efectiva.

Además, aprenderás los pasos clave para comenzar con la implementación de la ISO 27001, entendiendo la importancia de un enfoque sistemático y metódico para alcanzar el éxito. Revisarás desde la evaluación inicial de riesgos hasta la definición de políticas de seguridad, puesto que cada etapa del proceso es vital para crear un entorno seguro y resiliente para la información de tu organización.

1. Comenzar proyecto ISO 27001

Para comenzar un proyecto bajo la norma ISO 27001, es fundamental entender la estructura y los elementos clave de este estándar.

Para contextualizar, la norma ISO 27001 es un marco internacionalmente reconocido para la gestión de la seguridad de la información en las organizaciones. Por lo tanto, antes de sumergirnos en la planificación de un proyecto, en los apartados siguientes se aclaran los requisitos y beneficios que ofrece este estándar.

1.1 Estructura de la ISO 27001

A continuación, haremos una revisión general del propósito de la norma y su relación con otros estándares de gestión, para ello es importante destacar que la ISO 27001 se organiza a través de las cláusulas que revisaremos a continuación.

1.1.1 Cláusula 1: Alcance

Esta cláusula establece los límites y la aplicación de la norma, definiendo el alcance del Sistema de Gestión de la Seguridad de la Información (SGSI). Ella es fundamental para asegurar que el SGSI se aplique de manera efectiva y coherente en toda la organización.

Pasos para cumplir con esta cláusula:

1.Definir los límites del SGSI:

Identificar los activos, procesos, áreas y ubicaciones que se incluirán en el alcance del sistema. Esto abarca todas las áreas de la organización que manejan o procesan información.

2. Evaluar los riesgos:

Identificar y evaluar todos los riesgos que puedan afectar la seguridad de la información. Esto incluye amenazas a la confidencialidad, integridad y disponibilidad de la información.

3. Establecer controles adecuados:

Implementar controles para mitigar los riesgos identificados. Estos controles deben ser proporcionales a la magnitud de los riesgos y adaptarse a las necesidades específicas de la organización.

Fuente: Elaboración propia

La aplicación de la norma ISO 27001 no se limita a la seguridad de la información en sí misma, sino que abarca toda la organización y sus actividades. Esto incluye a las partes interesadas y terceros relacionados. Por lo tanto, la norma se aplica a todas las áreas de la organización, incluyendo la gestión de recursos humanos, finanzas, tecnología de la información y procesos de negocio.

Aunque la norma ISO 27001 no es obligatoria para todas las organizaciones, aquellas que buscan mejorar su seguridad de la información y mantener la confianza de sus clientes, proveedores y otras partes interesadas pueden optar por certificarse. La certificación ISO 27001 es un reconocimiento formal de que la organización ha implementado un SGSI efectivo y cumple con los requisitos de la norma.

1.1.2 Cláusula 2: Referencias normativas

La ciberseguridad es un campo en constante evolución, en el que mantenerse actualizado sobre las últimas normas y estándares es crucial para asegurar la protección efectiva de la información sensible de una organización. Esta cláusula de la norma ISO 27001 desempeña un papel fundamental al establecer las referencias normativas que deben seguirse para garantizar la conformidad y efectividad del Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO 27001 se apoya en normas y estándares reconocidos internacionalmente, como ISO/IEC 27002 e ISO/IEC 27000. Estas normas ofrecen una orientación detallada sobre los requisitos técnicos y de gestión necesarios para implementar y mantener un SGSI robusto. ISO/IEC 27002, por ejemplo, proporciona directrices específicas sobre controles de seguridad que pueden ser implementados para abordar diversos riesgos de seguridad de la información.

Además de estas normas, la cláusula 2 de ISO 27001 también hace referencia a otros marcos y estándares relevantes. Por ejemplo, la norma ISO 22301 sobre continuidad del

negocio e ISO/IEC 15408 para la evaluación de la seguridad de la información, complementan el enfoque de seguridad integral de ISO 27001. Estas referencias aseguran que el SGSI no solo proteja los datos críticos de la organización, sino que también mantenga la continuidad operativa y la capacidad de respuesta frente a incidentes de seguridad.

Es importante destacar que ISO 27001 se integra perfectamente con otros marcos de referencia ampliamente utilizados en la industria, como COBIT, ITIL y NIST. Esta integración permite a las organizaciones adoptar un enfoque coherente y holístico hacia la gestión de la seguridad de la información, alineando los objetivos de seguridad con los objetivos estratégicos y operativos del negocio.

Adherirse a las referencias normativas establecidas en la cláusula 2 de ISO 27001 asegura que el SGSI de una organización sea efectivo y cumpla con los estándares internacionales. Mantenerse al día con las últimas normas y estándares en ciberseguridad no solo fortalece la defensa contra amenazas emergentes, sino que también garantiza que se implementen las mejores prácticas para proteger la información crítica de la organización de manera efectiva.

1.1.3 Cláusula 3: Términos y definiciones

En el contexto de la seguridad de la información, es esencial tener una comprensión clara y precisa de los términos y definiciones clave utilizados en la norma ISO 27001. Aquí se presentan algunos términos fundamentales que debemos identificar:

DEFINICIÓN

Activo: cualquier elemento que posea valor para la organización, como datos, sistemas informáticos, instalaciones físicas y equipos.

Amenaza: evento potencial que podría comprometer la seguridad de los activos de la organización, como ataques de hackers, desastres naturales, errores humanos, entre otros.

Análisis de riesgos: proceso sistemático para identificar, evaluar y gestionar los riesgos que podrían afectar a los activos de la organización.

DEFINICIÓN

Control: medida implementada para mitigar o eliminar un riesgo, como firewalls, políticas de seguridad, controles de acceso, etc.

Gestión de la seguridad de la información: proceso para gestionar los riesgos de seguridad con el objetivo de proteger los activos de la organización.

Incidente de seguridad: evento que indica una posible violación de la seguridad de la información o una falla en los controles de seguridad.

Política de seguridad: declaración de principios que define los objetivos y la dirección de la seguridad de la información en la organización.

Riesgo: probabilidad de que una amenaza explote la vulnerabilidad de un activo y cause un impacto negativo.

Es importante tener en cuenta que estos términos y definiciones son el punto de partida para implementar y mantener un sistema de gestión de la seguridad de la información eficaz según los requisitos de ISO 27001. Al comprender estos conceptos, los profesionales de la ciberseguridad pueden trabajar de manera efectiva para proteger los activos de la organización y prevenir incidentes de seguridad.

1.1.4 Cláusula 4: Contexto de la organización

La implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), según la norma ISO 27001, comienza con el análisis del contexto de la organización por varias razones. Este proceso no solo permite a la organización comprender su entorno interno y externo, sino que también sienta las bases para determinar el alcance del SGSI de manera efectiva.

El **contexto interno** abarca todos los elementos dentro de la organización que influyen en la seguridad de la información, como sus procesos operativos, estructura organizativa, recursos humanos, activos y cultura empresarial. Por otro lado, el **contexto externo** incluye factores políticos, económicos, sociales, tecnológicos, legales y ambientales que pueden impactar la seguridad de la información.

Identificar estos contextos ayuda a la organización a definir claramente qué áreas, procesos, activos y servicios deben incluirse dentro del alcance del SGSI. Esta delimitación asegura que los objetivos y metas del sistema estén alineados con los objetivos estratégicos generales de la organización, proporcionando así una dirección clara y coherente.

La evaluación de riesgos de seguridad de la información permite identificar y categorizar los riesgos, amenazas y vulnerabilidades que podrían afectar los activos de información de la organización. A partir de esta evaluación, se pueden implementar medidas de control y mitigación adecuadas para reducir estos riesgos a un nivel aceptable.

Es importante destacar que el contexto de la organización no es estático; puede evolucionar con el tiempo, debido a cambios en el entorno interno y externo. Por lo tanto, la norma ISO 27001 exige que las organizaciones revisen regularmente su contexto y el alcance del SGSI para asegurar su relevancia y efectividad continua.

La cláusula 4 de la norma ISO 27001 proporciona el marco esencial para establecer un SGSI robusto y efectivo. Comprender y gestionar adecuadamente el contexto de la organización, junto con una evaluación rigurosa de riesgos, son pasos críticos para proteger los activos de información y garantizar la continuidad y reputación de la organización frente a las amenazas de seguridad.

1.1.5 Cláusula 5: Liderazgo

En esta cláusula se enfatiza el papel crucial de la alta dirección al liderar y comprometerse con el sistema de Sistema de Gestión de la Seguridad de la Información (SGSI) dentro de una organización. Este compromiso establece una dirección estratégica y proporciona los recursos necesarios para asegurar que la seguridad de la información se gestione de manera efectiva y consistente en todos los niveles.

Para garantizar un SGSI efectivo, la alta dirección debe adoptar las siguientes prácticas:

1. **Liderazgo y ejemplo**: la alta dirección (dependiendo de la organización pueden ser Directivos, CEOS, Gerentes) debe liderar con el ejemplo demostrando un compromiso activo con la seguridad de la información. Esto implica respaldar las iniciativas de seguridad, participar en actividades de sensibilización y promover una cultura organizacional centrada en la seguridad.

2. **Asignación de recursos**: es responsabilidad de la alta dirección asignar los recursos adecuados, tanto financieros como humanos, para la implementación y mantenimiento del SGSI. Esto incluye la designación de personal capacitado, la inversión en tecnología y la financiación de programas de formación en seguridad.
3. **Establecimiento de políticas y objetivos**: la alta dirección debe desarrollar y comunicar políticas claras de seguridad de la información que establezcan los principios y directrices para proteger los activos críticos. Además, deben establecer objetivos medibles y alcanzables que guíen la implementación del SGSI y permitan la mejora continua.
4. **Cultura de seguridad**: promover una cultura de seguridad en toda la organización significa generar conciencia sobre la seguridad entre todos los empleados, desde la alta dirección hasta el personal operativo. La cultura de seguridad fortalece el compromiso organizacional con la protección de la información y ayuda a mitigar los riesgos de manera proactiva.
5. **Compromiso a largo plazo**: el compromiso de la alta dirección no debe ser temporal, sino que debe mantenerse a largo plazo. Esto asegura la sostenibilidad del SGSI a medida que la organización enfrenta nuevos desafíos y cambios en su entorno operativo y tecnológico.

La Cláusula 5 de la norma ISO 27001 subraya que la seguridad de la información es responsabilidad de toda la organización, pero que requiere un liderazgo efectivo y un compromiso visible por parte de la alta dirección para ser exitosa. Este compromiso garantiza la implementación adecuada del SGSI y también fortalece la resiliencia organizacional frente a las amenazas cibernéticas. Además, contribuye a mantener la confianza de las partes interesadas en la seguridad de la información.

1.1.6 Cláusula 6: Planificación

La planificación es una de las cláusulas fundamentales de la norma ISO 27001, ya que establece las bases para la implementación efectiva del Sistema de Gestión de la Seguridad de la Información (SGSI). Este proceso garantiza que la organización aborde de manera adecuada los riesgos de seguridad y proteja sus activos de información. Sus pasos son:

Paso 1: Identificación de activos críticos y riesgos asociados

El primer paso en la planificación es identificar los activos de información críticos de la organización. Estos pueden incluir datos sensibles, sistemas de TI, infraestructuras, y otros recursos vitales. Junto con esta identificación, se deben evaluar los riesgos asociados a cada activo. Este análisis de riesgos permitirá a la organización entender qué amenazas y vulnerabilidades existen, y qué impacto podrían tener en caso de materializarse.

Paso 2: Desarrollo de un plan de acción

Una vez que se han identificado los activos críticos y los riesgos, la organización debe desarrollar un plan de acción para implementar las medidas de seguridad necesarias. Este plan debe ser detallado, especificando las tareas a realizar, los plazos para cada tarea y las personas responsables de su ejecución. El plan debe ser realista y alinearse con los recursos disponibles, tanto en términos de personal como de presupuesto.

Paso 3: Integración con los procesos de negocio

Es esencial que el SGSI se integre con los procesos de negocio de la organización. La planificación efectiva debe considerar cómo las medidas de seguridad pueden incorporarse sin interrumpir las operaciones diarias. Esto asegura que la seguridad de la información se convierta en una parte integral de la cultura organizacional y no en una carga adicional.

Paso 4: Revisión y mejora continua

La planificación también debe incluir un proceso para la revisión y mejora continua del SGSI. Esto implica monitorear el desempeño del sistema, realizar auditorías regulares, y actualizar las medidas de seguridad conforme evolucionan las amenazas y cambian las circunstancias de la organización. La mejora continua es fundamental para asegurar que el SGSI permanezca relevante y efectivo a lo largo del tiempo.

La planificación es una parte crítica del proceso de implementación de un SGSI efectivo según la norma ISO 27001. Los pasos incluyen la identificación de activos críticos y riesgos, el desarrollo de un plan de acción detallado, la integración con los procesos de negocio, y la revisión y mejora continua. Al considerar todos estos elementos, la organización asegura que su SGSI proteja los activos de información y que mitigue los riesgos asociados de manera eficiente y adaptativa. Este enfoque integral no solo fortalece la seguridad de la información, sino que también contribuye a la resiliencia y la sostenibilidad a largo plazo de la organización.

1.1.7 Cláusula 7: Soporte

Esta cláusula se centra en el soporte esencial para implementar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) efectivo. Abarca aspectos como la asignación de recursos, la competencia del personal, la comunicación, la documentación y el control de los registros. Es fundamental que quien implemente el SGSI deba asegurarse de que la organización disponga de todos los elementos necesarios para mantener un alto nivel de seguridad de la información. Revisemos a continuación estos elementos.

Recursos

La primera parte de la cláusula 7 enfatiza la importancia de disponer de los recursos adecuados. Esto incluye recursos humanos, financieros, técnicos y materiales necesarios para implementar, operar y mejorar continuamente el SGSI. La alta dirección debe asegurarse de que se asignen suficientes recursos para cumplir con los objetivos de seguridad de la información de la organización.

Competencia

La competencia del personal es otro aspecto relevante. La organización debe cautelar que todos los empleados involucrados en la gestión de la seguridad de la información tengan las habilidades y conocimientos necesarios. Esto puede implicar capacitación regular, certificaciones relevantes y programas de concienciación sobre seguridad de la información. El personal debe entender los riesgos asociados y las medidas de control necesarias para proteger los activos de información.

Comunicación

La comunicación efectiva es crucial para el soporte del SGSI. La organización establece canales de comunicación claros para difundir las políticas, procedimientos y responsabilidades relacionadas con la seguridad de la información. Además, fomenta una cultura de seguridad en la que todos los empleados comprendan la importancia de su papel en la protección de la información. La comunicación debe ser continua y adaptarse a las necesidades cambiantes de la organización y sus empleados.

Documentación

La organización debe identificar y mantener la documentación necesaria para la gestión de la seguridad de la información. Esto incluye políticas, procedimientos, planes y otros documentos relevantes. La documentación tiene que ser accesible, actualizada y controlada adecuadamente para asegurar su integridad y disponibilidad. Una gestión documental efectiva facilita la implementación, la operación y la mejora continua del SGSI.

Control de registros

El control de los registros es el último aspecto crítico de la Cláusula 7. La organización establece y mantiene registros precisos y detallados relacionados con la seguridad de la información. Esto incluye registros de incidentes de seguridad, auditorías, revisiones y cumplimiento de políticas y procedimientos. Los registros deben ser gestionados de manera que aseguren su confidencialidad, integridad y disponibilidad.

1.1.8 Cláusula 8: Operación

En esta cláusula se aborda la operación del Sistema de Gestión de Seguridad de la Información (SGSI), estableciendo las medidas y los controles necesarios para garantizar la

confidencialidad, integridad y disponibilidad de la información. En esta fase la implementación del SGSI se convierte en una realidad palpable y operativa.

a. Definición, implementación y mantenimiento de políticas y procedimientos:

La primera etapa en la operación del SGSI implica definir, implementar y mantener políticas y procedimientos de seguridad. Estos documentos establecen las directrices y prácticas que aseguran la protección de la información de la organización. Por ser la tecnología de la información un proceso mediante el cual se crea y almacena información sobre softwares que evoluciona día a día, un SGSI debe estar sujeto a una mejora continua. Las políticas y procedimientos deben revisarse y actualizarse periódicamente para responder a nuevas amenazas y cambios en el entorno empresarial.

b. Funcionamiento de procesos y cumplimiento:

La operación del SGSI implica asegurar que los procesos definidos estén en funcionamiento efectivo. La organización debe cumplir con las políticas y procedimientos establecidos, garantizando que todos los empleados y partes interesadas comprendan y sigan las prácticas de seguridad. La capacitación y concienciación continua sirven para mantener el cumplimiento y la efectividad del SGSI.

c. Monitoreo y reporte del desempeño del SGSI:

Una parte crítica de la operación del SGSI es el monitoreo y reporte del desempeño del sistema. La organización debe establecer mecanismos de seguimiento para evaluar la efectividad de los controles implementados y detectar cualquier desviación o problema. El monitoreo puede incluir auditorías internas, revisiones regulares de los registros de seguridad y el uso de herramientas de monitoreo automatizado. Los resultados del monitoreo tienen que ser reportados a la alta dirección para garantizar que se tomen las acciones correctivas necesarias.

d. Respuesta a incidentes de seguridad:

La organización establece un proceso de gestión de incidentes que incluya la detección, análisis, respuesta y recuperación de incidentes de seguridad de manera oportuna. Esto implica tener equipos de respuesta a incidentes bien entrenados, procedimientos claros para manejar incidentes y planes de recuperación para minimizar el impacto en la organización.

e. Implementación de controles específicos:

La cláusula 8 requiere la implementación de controles específicos para proteger la información de la organización. Estos controles pueden incluir:

- **Gestión de contraseñas**: políticas para la creación, uso y protección de contraseñas seguras.
- **Protección de recursos de información**: medidas para asegurar la infraestructura y los datos críticos.
- **Gestión de la seguridad de los sistemas**: prácticas para asegurar el software y hardware utilizado por la organización.
- **Gestión de copias de seguridad y recuperación de datos**: procedimientos para realizar copias de seguridad regulares y asegurar la recuperación rápida de datos en caso de pérdida o corrupción.

f. Personalización de controles y medidas:

Cada organización debe personalizar sus controles y medidas de seguridad para adaptarse a sus necesidades y riesgos específicos. Esto requiere una evaluación continua de los riesgos y la efectividad de los controles implementados, asegurando que se ajusten a las amenazas y vulnerabilidades actuales.

IDEA

¡A considerar!
Esta cláusula es el núcleo del SGSI, en la que se lleva a cabo la operación del sistema y se implementan los controles necesarios para proteger la información de la organización. Para los profesionales de ciberseguridad, es vital tener un conocimiento profundo de ella y estar actualizados con las mejores prácticas en la materia. Solo así se puede garantizar la seguridad y protección de la información en todo momento y lugar, asegurando la continuidad y resiliencia de la organización frente a posibles amenazas y riesgos.

1.1.9 Cláusula 9: Evaluación del desempeño

Esta cláusula monitorea, mide, analiza y evalúa el desempeño del Sistema de Gestión de la Seguridad de la Información (SGSI) de una organización. Proporciona directrices sobre cómo una organización debe evaluar su SGSI y utilizar los resultados de dicha evaluación para mejorar continuamente el sistema.

a. Importancia de la evaluación del desempeño:

La evaluación del desempeño permite a una organización determinar si su SGSI está funcionando eficazmente y cumpliendo con los objetivos de seguridad de la información establecidos. Este proceso identifica áreas de mejora y asegura que la organización pueda adaptarse a las amenazas y cambios en el entorno de seguridad de la información.

b. Indicadores de desempeño clave (KPIs):

Para evaluar el desempeño del SGSI, la norma ISO 27001 establece la necesidad de definir Indicadores de Desempeño Clave (KPIs) y objetivos de seguridad de la información. Los KPIs son métricas que ayudan a medir el desempeño del sistema y deben estar alineados con los objetivos de seguridad de la información de la organización. Algunos ejemplos comunes de KPIs incluyen:

- **Tasa de incidentes de seguridad de la información**: número de incidentes de seguridad que ocurren en un período específico.
- **Cantidad de vulnerabilidades identificadas y corregidas**: cantidad de vulnerabilidades detectadas y solucionadas en un período determinado.
- **Tiempo promedio de respuesta a incidentes**: tiempo que tarda la organización en responder a un incidente de seguridad desde su detección hasta su resolución.

c. Monitoreo y medición:

El monitoreo y la medición constantes son esenciales para la evaluación del desempeño del SGSI. La organización debe establecer procesos para recopilar y analizar datos relevantes sobre el desempeño del sistema. Esto incluye la implementación de herramientas y técnicas de monitoreo que permitan una evaluación precisa y continua del SGSI.

d. Auditorías internas y externas:

La realización de auditorías internas y externas es un componente clave de la evaluación del desempeño. Las auditorías internas permiten a la organización verificar si el SGSI cumple con los requisitos de la norma ISO 27001 y con las políticas y procedimientos establecidos. Las auditorías externas, llevadas a cabo por organismos de certificación, aseguran el cumplimiento de la norma y brindan una evaluación objetiva del sistema.

e. Revisión por la dirección:

La alta dirección de la organización debe revisar regularmente el desempeño del SGSI. Esta revisión debe incluir la evaluación de los resultados de las auditorías, el análisis de los KPIs y la identificación de áreas de mejora. La alta dirección debe tomar decisiones informadas sobre las acciones necesarias para mejorar el SGSI y asegurar su alineación con los objetivos estratégicos de la organización.

f. Mejora continua:

La evaluación del desempeño debe conducir a la mejora continua del SGSI. Basándose en los resultados de las evaluaciones y auditorías, la organización debe implementar acciones correctivas y preventivas para abordar cualquier deficiencia y fortalecer la seguridad de la información. De esta manera mantiene la efectividad del SGSI y asegura que la organización esté preparada para enfrentar nuevas amenazas y desafíos.

1.1.10 Cláusula 10: Mejora

La norma ISO 27001 proporciona un marco sólido para la implementación y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). La cláusula 10 de esta norma se centra en la mejora continua del SGSI, lo que significa que la organización debe trabajar para mejorar constantemente la efectividad y eficiencia del sistema.

a. Importancia de la mejora continua:

La mejora continua es un proceso cíclico que involucra la identificación de áreas para mejorar la implementación de cambios y la evaluación de su efectividad. En el contexto de la norma ISO 27001, la mejora continua del SGSI puede ayudar a una organización a:

- **Identificar y abordar vulnerabilidades de seguridad de la información**: detectar y corregir debilidades antes de que puedan ser explotadas.
- **Reducir el riesgo de incidentes de seguridad de la información**: minimizar la probabilidad y el impacto de los incidentes de seguridad.

- **Mejorar la eficiencia y eficacia del SGSI**: optimizar los procesos y recursos para una gestión más efectiva de la seguridad de la información.
- **Demostrar el compromiso de la organización con la seguridad de la información a los stakeholders**: aumentar la confianza de clientes, socios y reguladores en la capacidad de la organización para proteger la información.

b. Ciclo PDCA (Planificar, Hacer, Verificar, Actuar):

La norma ISO 27001 establece que la organización debe implementar, mantener y mejorar continuamente el SGSI, utilizando el ciclo PDCA. Este ciclo es un enfoque sistemático que implica:

c. Gestión del riesgo de seguridad de la información:

La mejora continua del SGSI también gestiona el riesgo de seguridad de la información. La norma ISO 27001 establece que la organización debe evaluar y tratar sistemáticamente los riesgos de seguridad de la información. Esto puede involucrar:

- **Implementación de controles de seguridad adicionales**: añadir nuevas medidas de seguridad para mitigar los riesgos identificados.
- **Revisión y actualización de los controles existentes**: evaluar la efectividad de los controles actuales y ajustarlos según sea necesario para mejorar la protección de la información.

d. Beneficios de la mejora continua:

Implementar la mejora continua en el SGSI ofrece varios beneficios:

- **Adaptabilidad a nuevas amenazas y vulnerabilidades**: mantenerse al día con la evolución de las amenazas de seguridad cibernética.
- **Cumplimiento con regulaciones y estándares**: garantizar que la organización cumple con las normativas y estándares internacionales.
- **Mejora de la resiliencia organizacional**: fortalecer la capacidad de la organización para resistir y recuperarse de incidentes de seguridad.
- **Optimización de recursos**: utilizar los recursos de manera más eficiente y efectiva.

Además de estas secciones principales, ISO/IEC 27001 también incluye el Anexo A, que contiene una lista de controles y sus objetivos de control. Estos controles se seleccionan y aplican según la declaración de aplicabilidad (SOA) de cada organización.

Esta estructura proporciona un marco completo y sistemático para establecer, implementar, mantener y mejorar continuamente un SGSI efectivo, adaptado a las necesidades y riesgos específicos de cada organización.

1.2 Convencer a la alta dirección

Lo primero que debemos realizar para la implementación de la norma ISO 27001 en una empresa se centra en la importancia de convencer a la alta dirección para obtener su apoyo. Aquí se detallan los pasos y estrategias para lograrlo.

Para comenzar, se debe entender que el principal desafío al implementar cualquier sistema de gestión radica en persuadir a la alta dirección de los beneficios tangibles que aportará a la organización. Más allá de discutir sobre una tecnología específica o detalles técnicos, lo que realmente captará su atención son los beneficios concretos y estratégicos que se derivan de adoptar un Sistema de Gestión de Seguridad de la Información (SGSI).

Uno de los beneficios principales es el **cumplimiento normativo**. En un entorno global, en el que las leyes y regulaciones sobre seguridad de la información son cada vez más estrictas, implementar ISO 27001 asegura que la empresa esté alineada con los estándares internacionales, evitando posibles sanciones y mejorando su reputación.

Además, ISO 27001 proporciona una ventaja competitiva significativa. Obtener la certificación **demuestra el compromiso de la empresa con la seguridad de la información**, lo que puede diferenciarla de los competidores que no cuentan con esta acreditación. Sin embargo, es decisivo no exagerar esta ventaja en términos de marketing, ya que el objetivo principal es fortalecer la seguridad interna y no solo promover la imagen externa.

Otro punto es la **reducción de costos**. Aunque inicialmente la inversión en seguridad de la información puede parecer un gasto, en realidad, ayuda a prevenir incidentes costosos como interrupciones en el servicio, pérdida de datos o tiempo de inactividad del sistema. Esto se traduce directamente en ahorros financieros a largo plazo y una operación más eficiente.

Para convencer a la alta dirección de estos beneficios, es esencial adoptar un enfoque estratégico y efectivo:

1. **Discurso motivador y enfocado en beneficios**: utilizar un lenguaje claro y directo centrado en cómo la implementación de ISO 27001 contribuirá a los objetivos estratégicos de la empresa, como la reducción de riesgos, la mejora del cumplimiento y la optimización de costos operativos.
2. **Identificación de aliados y stakeholders**: identificar a aquellos dentro de la organización que tienen influencia sobre la alta dirección y que pueden respaldar el proyecto. Estos aliados pueden ser fundamentales para proporcionar apoyo adicional y legitimar la necesidad del SGSI.
3. **Presentación efectiva de argumentos**: aplicar principios de presentación efectiva, como la regla de 30-20-10, donde se destacan solo los puntos clave en una presentación concisa y enfocada en los beneficios empresariales.
4. **Enfoque en la reducción de riesgos y probabilidades**: hablar menos sobre los riesgos técnicos y más sobre la probabilidad de reducirlos. Mostrar cómo la implementación de medidas de seguridad puede mitigar posibles pérdidas y daños a la empresa.

IMPORTANTE

¡La paciencia y la persistencia son clave!

Convencer a la alta dirección puede llevar tiempo y requerir una comunicación continua y efectiva. Al destacar los beneficios estratégicos, financieros y competitivos de ISO 27001, se puede ganar el apoyo necesario para asegurar una implementación exitosa y sostenible del SGSI en la organización.

1.3 Brechas entre TI y el negocio

A continuación, nos referiremos a las brechas que existen entre el Departamento de Tecnología de la Información (TI) y las áreas del negocio (rama operativa de la empresa, dirigida a un mercado concreto) en relación con la implementación de la norma ISO 27001, así como de estrategias para superar estos desafíos y aprovechar las oportunidades.

En primer lugar, hay que desmitificar el concepto de que la seguridad de la información es responsabilidad exclusiva del departamento de TI. Se enfatiza que, si bien TI desempeña su papel como soporte tecnológico, la implementación de la ISO 27001 debe ser liderada

por alguien que comprenda tanto la tecnología como los procesos de negocio. Esto sirve para integrar eficazmente la seguridad de la información en la gestión de riesgos generales de la empresa.

El personal de TI puede enfrentar resistencia inicial debido a la percepción de que la implementación de normas de seguridad como ISO 27001 generará más trabajo y documentación adicional. Para contrarrestar esta actitud negativa, es fundamental destacar los beneficios que la norma puede ofrecer a la empresa, como la reducción de riesgos, la eficiencia operativa mejorada y la protección contra posibles incidentes.

Una estrategia efectiva para captar la atención de la alta dirección y obtener su apoyo es **presentar propuestas bajo un enfoque de gestión de riesgos**. Esto implica realizar análisis de riesgos detallados y proponer controles específicos que mitiguen dichos riesgos. En lugar de simplemente solicitar nuevas tecnologías o recursos, se debería demostrar cómo estas inversiones pueden proteger activos críticos de la empresa y evitar posibles pérdidas financieras o de reputación.

Además, se debe destacar que la implementación de la ISO 27001 puede ayudar al departamento de TI a clarificar roles y responsabilidades. Definir claramente quién es responsable de qué y cómo se deben manejar los incidentes contribuye a una operación más eficiente y menos propensa a errores humanos.

Debemos mencionar, además, que el enfoque en la seguridad de la información no solo protege los activos de la empresa, sino que también puede mejorar las perspectivas profesionales del personal de TI. Con el crecimiento acelerado de la industria de la seguridad de la información, los empleados que adquieran experiencia en este campo pueden avanzar rápidamente en sus carreras.

Por último, se debe destacar la importancia de superar las percepciones erróneas y las brechas entre TI y el negocio al implementar la ISO 27001. Al centrarse en los beneficios estratégicos, la gestión de riesgos y la mejora de la eficiencia operativa, el departamento de TI puede jugar un papel decisivo en fortalecer la seguridad de la información en toda la organización.

1.4 Factores de éxito para justificar la implementación de una ISO 27001.

Para lograr incentivar una implementación de la norma ISO 27001 y superar las brechas entre el Departamento de Tecnología de la Información (TI) y el negocio, el proyecto se debe enfocar en varios factores clave:

1. **Perspectiva de beneficios**: el proyecto se debe presentar desde la perspectiva de los beneficios para la empresa en lugar de centrarse únicamente en aspectos técnicos. La alta dirección está más interesada en cómo la implementación de la ISO 27001 puede mejorar la eficiencia operativa, reducir riesgos y proteger los activos críticos de la organización. Evitar el lenguaje técnico complejo y enfocarse en los impactos positivos para el negocio es fundamental para captar su atención y apoyo.
2. **Identificación de beneficios relevantes**: encontrar dos o tres beneficios específicos y relevantes para el negocio actual es crucial. Estos beneficios deben ser tangibles y directamente relacionados con los desafíos o necesidades actuales de la empresa. Por ejemplo, hay que destacar cómo la norma puede ayudar a cumplir con requisitos regulatorios, mejorar la seguridad de los datos de clientes o reducir costos operativos debido a incidentes de seguridad.
3. **Enfoque integral**: hay que eliminar la percepción de que la seguridad de la información es solo responsabilidad del departamento de TI. La implementación de la ISO 27001 debe ser vista como un proyecto integral que involucra a todos los departamentos y niveles de la organización. Esto implica comunicar claramente que el éxito del proyecto depende del compromiso y la colaboración de todos los empleados, no solo de TI.
4. **Presentación y comunicación efectiva**: utilizar técnicas efectivas de presentación, como la regla del 30-20-10 mencionada anteriormente, para comunicar los beneficios de manera clara y concisa a la alta dirección. Evitar el uso de jerga técnica innecesaria y enfocarse en cómo la implementación mejorará directamente los resultados comerciales y operativos de la empresa.
5. **Compromiso y participación de la alta dirección**: asegurarse de que los líderes clave de la organización estén plenamente comprometidos con el proyecto desde el inicio. Esto no solo implica su aprobación inicial, sino también su participación en la definición de objetivos, asignación de recursos y seguimiento del progreso del proyecto.

Al seguir estos factores de éxito, el equipo de implementación puede mejorar significativamente las posibilidades de éxito al implementar la ISO 27001 y cerrar las brechas entre TI y el negocio dentro de la organización. Esto fortalecerá la seguridad de la información y contribuirá a una mayor integración y alineación de los objetivos empresariales y tecnológicos.

2. Preparando la implementación (plan)

A continuación, abordaremos cómo iniciar la implementación de un proyecto de seguridad de la información en una empresa. Exploraremos las diferentes opciones de implementación y las brechas que debemos evaluar antes de empezar un proyecto de este tipo. **Lo primero es saber dónde estamos y hacia dónde queremos llegar.**

Analizaremos el modelo o la secuencia para iniciar el ciclo de Deming de mejora continua en cualquier sistema de gestión de seguridad de la información, lo cual nos permitirá llevar a cabo la implementación de manera adecuada. La norma ISO 27001 se adecúa muy bien a este modelo.

Discutiremos cómo establecer la duración y el tiempo de un proyecto de seguridad de la información, así como los documentos obligatorios que nos pide la ISO y aquellos documentos no obligatorios, pero que, por buenas prácticas, conviene tener a mano. Estos documentos son frecuentemente solicitados en auditorías y contribuyen a una mejor gestión de la seguridad de la información.

2.1 Opciones para la implementación

En esta sección empezamos a interpretar qué es lo que nos pide el estándar. Se debe implementar bajo un enfoque de proyecto. Esto significa que debemos tener una persona encargada al 100% del desarrollo o implementación del SGC en la empresa. No podemos considerar un proyecto como una tarea adicional o una función más de un rol existente en la empresa, ya que este es un error común.

Por ejemplo, a menudo se asigna un proyecto a un jefe del Departamento de Tecnología de Información, Sistemas o el departamento informático, dependiendo del tipo de empresa. Sin embargo, estas personas ya tienen sus propias responsabilidades, por lo que

agregar esta carga adicional podría resultar en una implementación incompleta o ineficiente.

Debemos considerar que una planificación exitosa no garantiza una ejecución exitosa del proyecto. A continuación, hablaremos de las opciones recomendadas para la implementación del SGC:

1. **Implementar el estándar con personal propio de la empresa:** aquí se decide implementar el estándar sin ayuda externa, utilizando el conocimiento y la capacidad de los propios empleados.

   Pro: Es probablemente la opción más barata, ya que no se paga por un servicio externo. Además, se controla de mejor manera el acceso a los procesos internos.

   Contra: Puede ser la opción más lenta, ya que tomará tiempo para que el personal se adapte y aprenda. Si el personal ya tiene conocimiento en ISO 27001, esto podría ser más **fácil.**

2. **Contratar un consultor o una empresa consultora**: en esta opción, se contrata una empresa con experiencia en este tipo de proyectos.

   Pro: La implementación será más rápida debido a la experiencia de la empresa consultora.

   Contra: Los consultores cuestan dinero, lo que puede ser caro para empresas pequeñas. Además, se deberá dar acceso a los procesos internos, lo cual puede gestionarse con acuerdos de confidencialidad.

3. **Enfoque mixto**: Se implementa por cuenta propia **y se cuenta** con una empresa consultora para consultas específicas. Este enfoque es cada vez más popular y combina lo mejor de ambas opciones anteriores.

Pro: No es tan caro y se obtiene apoyo especializado. El personal aprende en el proceso, lo cual es útil para el mantenimiento continuo del SGC.

Contra: Aunque puede haber una curva de aprendizaje, los empleados adquirirán conocimiento para mantener el sistema a largo plazo.

La elección de la opción dependerá de la realidad de cada empresa. Se **recomienda un enfoque mixto, donde consultes** con un experto y se capacite al personal para trabajar en el proyecto.

2.2 Análisis de brechas

Antes de comenzar el proyecto de implementación del ISO 27001 o del Sistema de Gestión de Seguridad de la Información (SGSI) en una empresa, se debería realizar un análisis de brecha. Este análisis consiste en revisar cada cláusula del estándar ISO 27001 y evaluar si realmente cada requisito está implementado en la empresa.

A modo de sugerencia, es útil considerar una escala de evaluación para este proceso. Es importante confirmar que este tipo de escalas se pueden ajustar de acuerdo con la realidad de una determinada empresa. En este sentido, la elección del tipo de escala dependerá de cada empresa. A continuación, se presenta un ejemplo de escala de evaluación.

Ejemplo escala de evaluación

Nivel 0: El requisito no está implementado y opcionalmente, ni siquiera planificado.
Nivel 1: El requisito está planificado, pero aún no implementado.
Nivel 2: El requisito está parcialmente implementado.
Nivel 3: El requisito está implementado, pero no medido ni revisado.
Nivel 4: El requisito está implementado, medido y revisado.

Fuente: Elaboración propia

IDEA

Considera esta idea

Es recomendable usar un archivo Excel para enumerar cada cláusula del estándar y revisar si se están cumpliendo o no, evaluando con la escala mencionada.

El ISO 27001 no obliga a hacer un análisis de brecha de los requisitos. Sin embargo, es una buena práctica realizarlo porque proporciona un enfoque claro para la planificación del proyecto, indicando qué falta, en qué nivel estamos y qué porcentaje de los requisitos ya se han cubierto. Este análisis nos ayuda a entender mejor nuestra situación actual y a planificar adecuadamente.

La cláusula 6.1.3 del ISO 27001 dice que es necesario determinar si los controles que se encuentran en el anexo “A” de esta norma, están implementados. Por lo tanto, es obligatorio hacer un análisis de brecha de los controles para ver si están implementados, no implementados o parcialmente implementados en la organización.

ENLACE WEB

Visita este enlace

Te invitamos a revisar la siguiente página web, en ella encontrarás todas las cláusulas y sus respectivos requisitos. Esto les puede ayudar a armar su Excel. Para acceder haz clic **ACÁ.**

En la página web revisada anteriormente, podremos encontrar la estructura de la ISO 27001:2013 con las cláusulas desde la 4 hasta la 10, que son obligatorias. Por ejemplo, en la cláusula 5.2 sobre la Política de Seguridad de la Información, se especifican los requisitos que debe cumplir esta política, cómo ser adecuada al propósito de la organización, incluir los objetivos de seguridad y el compromiso de mejora continua del SGSI.

PREGUNTA

¿Ayuda a la implementación de la ISO 27001 realizar un análisis de brecha?

Aunque la norma no lo exige, realizar un análisis de brechas es una buena práctica que proporciona claridad y dirección para el proyecto de implementación del SGSI.

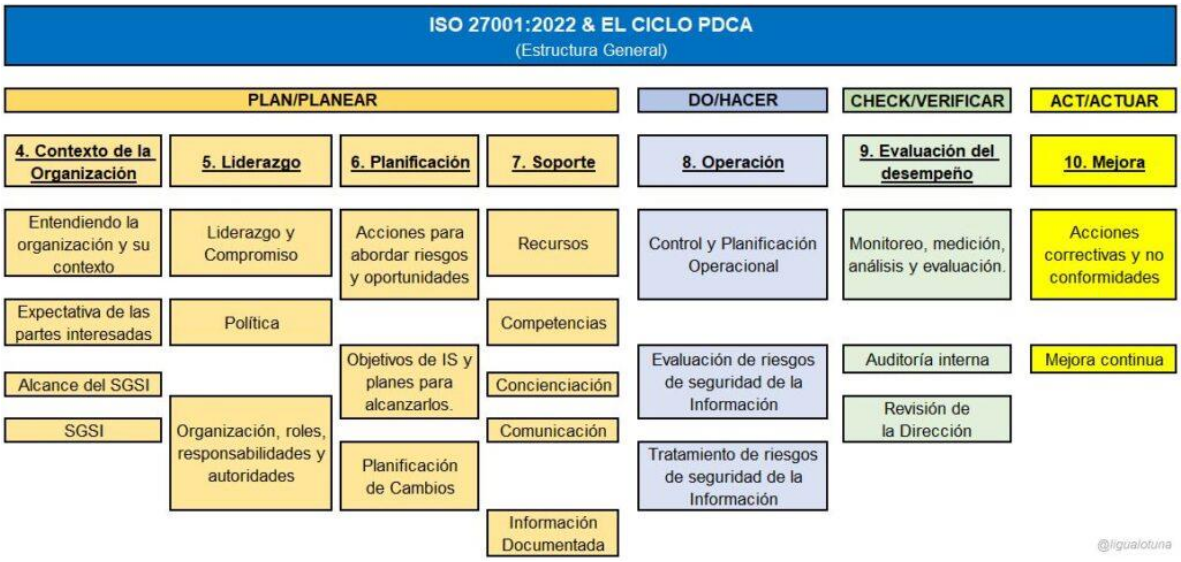
2.3 Secuencia para la implementación (PDCA)

El ciclo PDCA (Plan-Do-Check-Act), también conocido como el ciclo de Deming, es una metodología ampliamente utilizada para la gestión y mejora continua de procesos en diversas organizaciones.

En lo que respecta a la norma ISO 27001, el «enfoque por proceso», que incluye el modelo PDCA se ha eliminado, sin embargo, menciona que se requiere una gestión de mejora

continua, dando la apertura y flexibilidad para que se use cualquier otro modelo. A pesar de lo anterior, en este curso se utilizará por ser uno de los modelos más conocidos en la industria informática.

PDCA asociado a la estructura general de la ISO 27001



Fuente: Gobierno electrónico de ecuador - https://www.gobiernoelectronico.gob.ec/ciclo-de-deming-pdca/

En el contexto de la seguridad de la información, la norma ISO 27001 se adapta perfectamente a este ciclo, proporcionando un marco estructurado para la implementación, operación, monitoreo y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI).

2.3.1 El Ciclo PDCA y la ISO 27001

El ciclo PDCA se compone de cuatro fases principales: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act). La norma ISO 27001 sigue esta estructura de manera clara y secuencial a través de sus cláusulas, desde la cláusula 4 hasta la cláusula 10.

Planificar (Plan):

- **Cláusula 4: Contexto de la organización**: esta cláusula requiere que la organización entienda su contexto interno y externo, identifique las partes interesadas y determine el alcance del SGSI.
- **Cláusula 5: Liderazgo**: aquí se establece la importancia del liderazgo y el compromiso de la alta dirección en el SGSI, definiendo roles y responsabilidades.
- **Cláusula 6: Planificación**: implica la identificación de riesgos y oportunidades, y la planificación de cómo abordar estos elementos. Se establecen los objetivos de seguridad de la información y se planifican las acciones para lograrlos.
- **Cláusula 7: Soporte**: esta cláusula se centra en la provisión de recursos necesarios, competencia, concienciación y comunicación para apoyar el SGSI.

Estas cuatro cláusulas forman parte de la fase de planificación, estableciendo las bases para la implementación efectiva del SGSI.

Hacer (Do):

- **Cláusula 8: Operación**: en esta fase, se implementan y operan los procesos planificados. Se trata de llevar a cabo las acciones necesarias para gestionar los riesgos y alcanzar los objetivos de seguridad de la información.

Verificar (Check):

- **Cláusula 9: Evaluación del desempeño**: esta cláusula establece los requisitos para monitorear, medir, analizar y evaluar el desempeño del SGSI. Incluye la realización de auditorías internas y la revisión de la dirección para asegurar que el SGSI está funcionando eficazmente.

Actuar (Act):

- **Cláusula 10: Mejora**: aquí se enfoca en la mejora continua del SGSI. La organización debe tomar acciones para corregir no conformidades y mejorar continuamente la idoneidad, adecuación y eficacia del SGSI.

2.3.2 La Secuencialidad y la importancia de cada fase

La secuencialidad de estas cláusulas es crucial para garantizar un SGSI eficaz. Cada fase del ciclo PDCA debe seguir un orden lógico:

1. **Planificación**: Se comienza con la comprensión del contexto de la organización y la planificación de acciones necesarias para abordar riesgos y oportunidades.
2. **Implementación (Operación)**: Una vez planificadas, las acciones deben ser implementadas y los procesos deben ser operados de acuerdo con los planes.
3. **Evaluación**: Después de la implementación, se debe verificar si los procesos están funcionando como se esperaba mediante monitoreo y medición.
4. **Mejora Continua**: Basado en los resultados de la evaluación, se deben tomar acciones para mejorar continuamente el SGSI.

Este enfoque secuencial asegura que el SGSI esté alineado con los objetivos estratégicos de la organización, sea efectivo en la gestión de riesgos y esté en constante mejora para adaptarse a nuevos desafíos y amenazas.

2.4 Duración y costo de la implementación

Uno de los aspectos clave al planificar un proyecto de implementación de la norma ISO 27001 es tener expectativas realistas sobre la duración del proyecto. A menudo, se escucha que este tipo de proyectos puede completarse en un par de meses o, a lo sumo, en seis meses. Sin embargo, estas expectativas pueden ser poco realistas y conducir a decepciones.

Un proyecto de implementación de ISO 27001, en la mayoría de los casos, requiere al menos **de un año** para completarse. Esto se debe a que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) implica mucho más que la simple elaboración de documentos como políticas, manuales y procedimientos. También es necesario monitorear incidentes, evaluar la efectividad de los controles y realizar ajustes continuos.

- **Empresas pequeñas (hasta 50 empleados)**: un tiempo razonable para la implementación de ISO 27001 en una empresa pequeña es de aproximadamente ocho meses. Sin embargo, es prudente considerar una holgura de 1-2 meses adicionales para imprevistos.

- **Empresas medianas (hasta 500 empleados)**: para empresas medianas, la duración del proyecto puede variar entre doce y quince meses. Esto incluye tiempo adicional para abordar las complejidades organizativas y asegurar la efectividad de los controles.
- **Empresas grandes (más de 500 empleados)**: en el caso de empresas grandes, el proyecto puede durar entre dieciocho y veinte meses. La mayor cantidad de procesos y la necesidad de coordinar múltiples departamentos hacen que el tiempo de implementación sea más extenso.

La implementación de un SGSI no solo se trata de planificar (Planificar y Hacer) sino también de verificar (Check) y actuar (Actuar), siguiendo el ciclo PDCA (Plan-Do-Check-Act). Las fases de **planificación e implementación** son generalmente las más largas, ya que requieren una comprensión profunda de la organización y la implementación efectiva de los controles.

2.4.1 Costo del proyecto

El costo de un proyecto de implementación de ISO 27001 varía significativamente según el tamaño y las necesidades específicas de la organización. Aunque no se puede proporcionar un número exacto sin un análisis detallado, se pueden considerar los siguientes componentes de costos:

Recursos Humanos:

- **Responsable de Seguridad de la Información (CISO)**: esta persona será la encargada de liderar el proyecto y su salario debe ser considerado.
- **Equipo de Proyecto**: incluir a los empleados que participarán directamente en la implementación, su tiempo y salarios deben ser calculados.
- **Consultoría**: en muchos casos, es beneficioso contratar una consultoría externa para guiar el proceso. Los costos de consultoría pueden variar, pero es una inversión clave para asegurar el éxito del proyecto.

Tecnología:

- **Software**: puede ser necesario adquirir software específico para la gestión de riesgos, inventario de activos, y gestión de documentos. Esto incluye licencias y suscripciones.

- **Infraestructura**: cualquier actualización o adición a la infraestructura tecnológica existente para soportar los nuevos controles de seguridad.

Formación y concienciación:

- **Capacitación**: capacitar al personal en la implementación y gestión de ISO 27001 es esencial. Esto incluye formación específica para el equipo del proyecto y programas de concienciación para todo el personal.
- **Materiales de formación**: costos asociados a la creación y distribución de materiales de formación y concienciación.

Auditorías y certificación:

- **Auditorías internas**: realizar auditorías internas para asegurar que el SGSI está en conformidad con los requisitos de la norma.
- **Auditoría externa y certificación**: costos asociados a la auditoría de certificación por una entidad externa y el mantenimiento de la certificación.

Gastos generales:

- **Oficinas y equipos**: costos relacionados con el espacio de oficina y equipos necesarios para el equipo del proyecto.
- **Comunicación**: gastos en herramientas de comunicación y colaboración, especialmente si parte del trabajo se realiza de forma remota.

Implementar un SGSI basado en la norma ISO 27001 es una inversión significativa en tiempo y recursos, pero sirve para proteger la información y mitigar los riesgos. Las empresas deben planificar cuidadosamente la duración y el costo del proyecto, asegurando que se asignen los recursos adecuados y que se mantenga el compromiso de la alta dirección.

2.5 Documentación

La implementación de la norma ISO 27001 requiere una serie de documentos y registros obligatorios que deben ser mantenidos y actualizados. A continuación, revisaremos una lista de los documentos obligatorios y no obligatorios.

a. Documentos obligatorios:

1. Alcance del SGSI (Cláusula 4.3)
2. Política de Seguridad de la Información (Cláusula 5.2)
3. Objetivos de Seguridad de la Información (Cláusula 6.2)
4. Metodología y el Informe del Análisis de Riesgos (Cláusula 6.1.2)
5. Declaración de Aplicabilidad (Cláusula 6.1.3)
6. Plan de Tratamiento del Riesgo (Cláusula 6.1.3)
7. Roles y Responsabilidades de la Seguridad (Cláusula 5.3)
8. Inventario de Activos (Cláusula 8.1)
9. Uso Aceptable de los Activos de Información (Control A.8.1.3)
10. Política de Control de Acceso (Control A.9.1.1)
11. Procedimientos Operacionales de TI (Control A.12.1)
12. Principios de Ingeniería de Sistemas Seguros (Control A.14.2.5)
13. Política de Seguridad para Proveedores (Control A.15.1.1)
14. Procedimiento de Gestión de Incidentes (Control A.16.1.5)
15. Requerimientos Contractuales, Regulatorios y Legales (Cláusula 18.1)

b. Registros obligatorios:

16. Formación, Habilidades, Experiencia y Calificaciones del Personal (Cláusula 7.2)
17. Concienciación sobre Seguridad de la Información (Cláusula 7.3)
18. Resultados del Seguimiento y Medición de los Controles (Cláusula 9.1)
19. Programa de Auditoría Interna (Cláusula 9.2)
20. Resultados de las Auditorías Internas (Cláusula 9.2)
21. Revisión de la Dirección (Cláusula 9.3)
22. Acciones Correctivas (Cláusula 10.1)
23. Actividad de los Usuarios y Eventos de Seguridad (Control A.12.4.1)

c. Documentos no obligatorios:

24. Procedimiento de control de documentos (Clausula 7.5)
25. Controles para la gestión de registros (Clausula 7.5)
26. Procedimiento para auditoría interna (Clausula 9.2)
27. Procedimiento para acciones correctivas (Clausula 10.1)
28. Política de dispositivos móviles o teletrabajo (Control A.6.2.1)
29. Política de clasificación de información (Control A.8.2.1, A.8.2.2, A.8.2.3)
30. Política de contraseñas (Control A.9.2.1, A.9.2.2, A9.2.4, A.9.3.1, A.9.4.3)
31. Política de eliminación y destrucción (Control A.8.3.2, A.11.2.7)
32. Política e pantalla y escritorios limpios (Control A.11.2.9)
33. Política de gestión de cambios (Control A.12.1.2, A.14.2.4)
34. Política de copias de seguridad (Control A.12.3.1)
35. Política de transferencia de información (Control A.13.2.1, A.13.2.2, A13.2.3)
36. Análisis de impacto al negocio (BIA) (Control A.17.1.1)
37. Plan de pruebas y verificación (Control A.17.1.3)
38. Plan de mantenimiento y revisión (Control A.17.1.3)
39. Estrategia de continuidad del negocio (Control A.17.2.1)

d. Documentos No Obligatorios pero Recomendados:

- Política de Pantallas y Escritorios Limpios**.**
- Política de Contraseñas**.**
- Política de Copias de Seguridad**.**

La implementación de ISO 27001 no solo se centra en la creación de documentos, sino también en el mantenimiento de registros que demuestren la efectividad del SGSI. Estos documentos y registros forman la base de un sistema de gestión robusto y aseguran el cumplimiento de los requisitos de la norma.

2.6 Comenzando la implementación

Vamos a ver cómo definir nuestro alcance para este sistema de gestión, para lo cual se debe entender y conocer a la organización.

a. Contexto de la organización (Clausula 4.1):

Para empezar con la implementación de la ISO 27001, debemos abordar la cláusula 4.1, que nos pide comprender la organización y su contexto. Esto implica conocer a fondo la empresa, sus procedimientos, estrategias y objetivos de negocio. Este conocimiento es crucial para definir los objetivos de seguridad de la información que estarán alineados con los objetivos de negocio.

Propósito: Lograr una integración sólida entre el negocio y la seguridad de la información. El sistema de gestión de seguridad de la información debe estar alineado con las circunstancias específicas de la empresa, no solo con las percepciones del profesional de seguridad.

b. Partes interesadas y requerimientos (Cláusula 4.2):

Ya sabemos lo que hace la empresa, porque hemos revisamos toda la documentación, todos sus procesos, ya se conoce qué es lo que hace la empresa.

Propósito: Saber qué es lo que la empresa espera. Eso quiere decir que nuestro sistema de gestión de seguridad de información debe satisfacer a todas las partes interesadas. Por lo tanto, debemos conocer las partes interesadas y conocer cuáles son sus necesidades o requerimientos en relación con la seguridad de la información.

Entradas: Habiendo conocido la documentación de la empresa (cláusula 4.1), tenemos que hacer entrevistas precisamente a estas partes interesadas. Por ejemplo, a los directores de la empresa, a los gerentes, a los jefes de cada uno de los diferentes departamentos que hay en la empresa. También tenemos que comunicarnos con clientes para conocer un poco cuál es su expectativa en relación con la seguridad y qué es lo que ellos esperan. Estas serían las entradas para luego tomar decisiones.

c. Alcance del SGSI (Clausula 4.3)

Propósito: El propósito de esta cláusula es definir qué información vamos a proteger, sin importar dónde, cómo y quiénes tendrán acceso a esta información. No importa si esta información está dentro de las oficinas. Lo importante es que seamos responsables sobre qué información vamos a proteger, la cual tiene que estar enmarcada en el alcance del sistema de gestión de seguridad de la información.

IMPORTANTE

¡Recuerda!
Es importante definir el alcance ya hoy en día existe mucho desarrollo desde dispositivos móviles, por ejemplo, y este debe estar dentro del alcance del SGSI.

Los productos asociados al negocio también son parte del alcance, como las tarjetas débito o tarjetas de crédito de un banco enfocado a la seguridad de la información. La información que se puede obtener de una tarjeta de débito o crédito es información que se debe proteger porque está dentro de unos de los procesos principales del banco.

Se debe involucrar para la definición del alcance a todas las personas que forman parte del proyecto, el sistema de gestión, involucrar si es que existe un comité de riesgo en la empresa, a la alta dirección o directores que también participan en la gestión de riesgo y sobre todo con personas que tienen decisión estratégica dentro de la empresa.

d.Liderazgo y compromiso de la alta dirección (Clausula 5.1)

La cláusula de liderazgo y compromiso de la alta dirección es parte obligatoria de cumplimiento del ISO 27001.

Propósito: El liderazgo y el compromiso de la alta dirección es muy importante, si no contamos con este liderazgo y con este compromiso, el proyecto de implementación del SGSI va a fallar.

Entradas: Tenemos que indicar a la alta dirección cuáles son los beneficios de implementar un SGSI en la empresa. Estos beneficios van a ayudar a definir los objetivos claros de la seguridad de la información y esto es lo que se busca en la cláusula 5.6, que también es una cláusula obligatoria del estándar. Con esto queda en claro de que los beneficios vienen a ser las entradas para esta cláusula, siempre y cuando hayamos logrado convencer a la alta dirección y que ellos ya tengan claro cuáles serían los beneficios y los objetivos.

e. Política de seguridad de la información (Clausula 5.2)

Esta cláusula nos pide uno de los documentos más importantes que tiene un SGSI y nos referimos en tener una política de seguridad de la información. Una política de seguridad

de la información es una política que abarca, abarca todos los procesos involucrados en el alcance del sistema gestión. Tiene que ser una política entendible por toda la organización y no sólo por las personas que están participando en el proyecto.

Propósito: El principal propósito es lo que la empresa quiere lograr con la seguridad de la información. Se tiene que enmarcar el propósito general que necesita la organización para cumplir con proteger la información de la empresa. Debe ser un documento fácil de entender que permita controlar todo lo que se gestiona en el SGSI.
Básicamente, una política de seguridad de la información debe servir como vínculo principal entre la alta dirección y las actividades de seguridad de información.
Los objetivos de seguridad de la información se relacionan con los objetivos del negocio.

f. Objetivos de la seguridad de la informaciónión (Clausula 5.2b y 6.2)

En la cláusula 5.2, opción B, se indica incluir en la política, la información que proporcione el marco de referencia para el establecimiento de objetivos de la seguridad para el SGSI. Aquí se ve que objetivos se está cumpliendo con este requisito.

En la cláusula 6.2, hay que ser coherentes con la política de seguridad de la información. Además, tienen que ser medibles. Y para saber si son alcanzables o no, los tengo que medir.

Tener en cuenta los requisitos de la seguridad, los resultados de la valoración y el tratamiento de los riesgos. La comunicación de lo anterior debe ser parte de la política.

Propósito: Medir el trabajo que se viene realizando con el SGSI, con el fin de que se evidencie que los objetivos tienen que ser medibles. De lo contrario, no sabemos si realmente estamos cumpliendo esos objetivos.

3. Gestión de riesgo (plan - do)

A continuación, revisaremos cuatro pasos para gestionar el riesgo:

1- Definir la metodología de evaluación de riesgos.
2- Hacer el análisis de riesgos.
3- Hacer el tratamiento de estos riesgos.
4- Hacer el acuerdo o documento de aplicabilidad.

Al finalizar esta gestión de riesgos, se aplica la etapa de hacer (do). Definiendo los controles del anexo A de la ISO 27001 que se utilizarán y cómo hacer el plan de tratamiento al riesgo.

3.1 Continuando la implementación

En base al levantamiento de los activos de información, se deberá realizar sobre ellos un análisis de riesgos.

Riesgos y oportunidades (Clausula 6.1)

Cuando hablamos de riesgos nos estamos refiriendo a eventos no deseados que pueden causar un impacto y ese impacto puede perjudicar alguno de los procesos de la empresa. Por eso siempre hay que identificarlos.

Cuando hablamos de oportunidades, nos estamos refiriendo a acciones. Estas acciones nos van a ayudar a mejorar la seguridad de la información, pero para poder identificarlas debemos tener claros nuestros riesgos, porque si no los conocemos, no vamos a poder implementar estas acciones que van a ser oportunidades que de alguna forma van a ayudar con la seguridad de la información.

Revisemos a continuación los pasos para la gestión de riesgos.

a. El primer paso sería definir una metodología:

Es necesario definir las reglas sobre cómo vamos a realizar la gestión de riesgos, realizándola del mismo modo, estableciendo metodología, definiendo escalas para hacer una evaluación ya sea cualitativa o cuantitativa, para establecer el nivel aceptable del riesgo.

b. El segundo paso es implementar un análisis de riesgos:

Una vez que ya sabemos nuestra metodología y cuáles son las reglas que debemos seguir, hay que empezar a averiguar qué problemas podrían aparecer en los activos de información de la organización, además de las amenazas y vulnerabilidades que se relacionan con estos activos. Con este análisis identificamos cuáles son las amenazas que

puede afectar a un activo, siempre y cuando tenga una vulnerabilidad presente. Si tenemos esa vulnerabilidad, se va a materializar el riesgo.

c. **El tercer paso es implementar un tratamiento de los riesgos que identificamos:**

Hay que centrarnos en los riesgos más importantes llamados riesgos inaceptables como aquellos catalogados como críticos o altos. Los cuales debemos mitigar a toda costa. Pero posiblemente identificamos además otros riesgos de menor impacto como los de criticidad media o baja, que dependiendo del impacto que cause si se materialice la vulnerabilidad, no se piense en gestionar o mitigar.

La primera opción es aplicar un control de seguridad y tratar de disminuir el riesgo; la segunda, sería transferir el riesgo a un tercero, si es que nosotros no lo podemos tratar, la tercera opción, es evitar el riesgo y finalmente aceptarlo, en el caso de que la empresa no cuente con recursos necesarios para enfrentarlo. A lo mejor es un riesgo que no se presenta con frecuencia o la empresa podría evaluar si lo acepta; Por último, la cuarta opción, es definir nuestra declaración de aplicabilidad. La declaración de aplicabilidad es un requisito de ISO 27001.

d. **Como cuarto paso se encuentra la declaración de aplicabilidad:**

Se trata de realizar un análisis de brecha de los controles que se está implementando, para qué riesgos y cómo está haciendo su tratamiento.

4. Implementar controles de seguridad (do)

Estos controles son muy importantes y la ISO 27001 trae un anexo que se conoce como el **anexo A. En** este documento están cada uno de los controles que se deben implementar en las empresas con relación a la seguridad de la información.

ENLACE WEB

Recurso complementario

Para conocer la estructura de este anexo A, conformado por 14 secciones, te invitamos a revisar el documento **"ANEXO A"** que se encuentra en el material de estudio obligatorio de la unidad.

5. Asegurar funcionamiento (check-act)

Esta sección se centrará en cómo medir y mejorar un sistema de gestión, especialmente en el contexto de la seguridad de la información. Es crucial asegurarse de que los objetivos y controles sean medibles para evaluar adecuadamente el funcionamiento del sistema. Además, abordará la importancia de las auditorías internas y externas para verificar la efectividad del sistema de gestión de la seguridad de la información.

5.1 Medir, analizar y evaluar el SGSI (Cláusula 9.1)

En esta sección del curso se aborda la importancia de las fases CHECK y del ciclo PDCA para monitorear y evaluar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

1. **Fases CHECK y PDCA**: estas fases son cruciales para evaluar cómo está funcionando el SGSI y determinar dónde se necesitan correcciones. Se centran en la cláusula 9.1 de la ISO 27001, que trata sobre el monitoreo, medición, análisis y evaluación del desempeño del sistema.
2. **Monitoreo vs. Medición**: el monitoreo implica observar y examinar el funcionamiento del sistema, mientras que la medición consiste en determinar el tamaño o la cantidad de algo específico, como incidentes de seguridad.
3. **Objetivos medibles**: los objetivos del SGSI deben ser medibles para poder evaluar si se están cumpliendo. Esto incluye objetivos estratégicos y tácticos, que deben estar alineados con la política de seguridad de la información.
4. **Métodos de medición**: el método de medición varía según el objetivo establecido. Puede implicar cumplir con regulaciones dentro de un plazo específico o reducir la cantidad de incidentes de seguridad en un período determinado.

5. **Comunicación y evaluación**: los resultados de las mediciones tácticas se comunican al CISO u oficial de seguridad de la información, mientras que los resultados estratégicos se reportan a la alta dirección. La evaluación de resultados puede ser realizada por analistas internos o externos según la complejidad de la organización.
6. **Documentación**: la ISO 27001 no especifica una documentación exhaustiva para esta cláusula, pero se recomienda documentar informes de medición o monitorización con cierta periodicidad (por ejemplo, semestral o anual) y establecer metodologías y responsables de las mediciones como buenas prácticas.

Este enfoque sistemático permite asegurar que el SGSI cumpla con sus objetivos y que las medidas de seguridad se ajusten continuamente a las necesidades y riesgos de la organización.

5.2 Auditorías internas (Cláusula 9.2)

Las auditorías internas tienen como objetivo principal descubrir problemas o no conformidades dentro del SGSI. Esto permite identificar áreas de mejora continua y asegurar que el sistema esté cumpliendo con los estándares y regulaciones pertinentes.

1. Opciones para realizar auditorías internas:
   - **Auditor interno a tiempo completo**: es apropiado para grandes empresas que pueden sostener un auditor dedicado exclusivamente a la seguridad de la información.
   - **Auditor interno a tiempo parcial**: auditores que trabajan dentro del departamento de auditoría de la empresa y pueden tener especialización en seguridad de la información, además de otras competencias.
   - **Auditor interno independiente**: contratación externa de un auditor especializado en seguridad de la información cuando no se puede cubrir internamente esta necesidad.

2. Entradas para las auditorías internas:
   - Conocimiento y aplicación de la ISO 27001 y otras regulaciones relevantes.
   - Documentos del SGSI: políticas, procedimientos, manuales, controles, etc.
   - Programa de auditoría interna: planificación anual de las auditorías que debe ser aprobado por la alta dirección.

3. Nivel jerárquico del auditor:
   Se recomienda que el auditor tenga un nivel jerárquico similar o superior al CISO para asegurar una evaluación imparcial y objetiva del SGSI.

4. Documentación requerida:
   - **Informe de auditoría interna**: documento obligatorio que detalla los hallazgos y recomendaciones.
   - **Programa de auditoría interna**: documento que establece la planificación anual de las auditorías.
   - **Procedimiento de auditoría interna**: aunque no es obligatorio según la ISO 27001, se considera una buena práctica para definir cómo se realizarán las auditorías, seleccionar auditores, planificar las actividades de auditoría, etc.

5. Apoyo de la alta dirección:
   Es crucial que la alta dirección apoye las auditorías internas viéndolas como una herramienta para mejorar el SGSI, no solo como un gasto. Esto es fundamental para la efectividad del proceso de auditoría y la implementación de recomendaciones.

Este enfoque sistemático y documentado asegura que las auditorías internas sean efectivas en identificar áreas de mejora y en mantener la conformidad con los estándares de seguridad de la información.

5.3 Revisión de la dirección (Cláusula 9.3)

La ISO 27001 requiere que la alta dirección participe activamente en el SGSI, tomando decisiones que impacten positivamente en la seguridad de la información y en el sistema de gestión en general. Esto se logra a través de revisiones regulares y efectivas.

1. **Formas de participación**: es recomendable establecer un comité de seguridad de la información donde participen miembros de la alta dirección. Esto asegura que las decisiones estratégicas, como asignación de recursos y aprobación de presupuestos para implementar la ISO 27001, sean tomadas por quienes tienen el poder de decisión.
2. **Entradas para la revisión por la alta dirección**:

- Estado de acciones de revisiones anteriores: revisión de acuerdos y avances previos.
- Análisis y estado de acciones correctivas: resultados de auditorías internas y acciones tomadas para corregir no conformidades.
- Monitorización y resultados de objetivos del SGSI: evaluación del progreso hacia los objetivos establecidos.
- Comentarios de partes interesadas: retroalimentación de directores, empleados, clientes, etc., sobre el SGSI.
- Resultados de análisis de riesgos: exposición de riesgos identificados y controles implementados.
- Oportunidades de mejora del SGSI: propuestas para mejorar el sistema.

3. **Decisiones resultantes**:
   - Cumplimiento de objetivos del SGSI.
   - Mejoras necesarias: aprobación de recursos y ajustes estratégicos.
4. **Documentación requerida**:
   - Minuta de reuniones o acuerdos de revisiones: documento obligatorio que detalla los resultados de las revisiones por la alta dirección y las decisiones tomadas.
5. **Importancia de la participación**: involucrar a la alta dirección desde el inicio del proceso asegura el éxito en la implementación de la ISO 27001. Esto garantiza que las decisiones estratégicas sean informadas y apoyadas, lo que contribuye a la efectividad del SGSI en la organización.

Esta cláusula no solo cumple con los requisitos de la ISO 27001, sino que también promueve una cultura organizacional donde la seguridad de la información es una prioridad estratégica y continua.

5.4 No conformidades y acciones correctivas (Cláusula 10.1)

El propósito principal de esta cláusula es implementar acciones correctivas de manera sistemática para abordar no conformidades identificadas y mejorar continuamente los procesos de seguridad de la información.

1. **Entradas**: las entradas incluyen la identificación de no conformidades o áreas de mejora a través de auditorías internas, sugerencias de empleados u otras partes

interesadas, y la necesidad de cambios estructurales o revisiones estratégicas del SGSI por parte de la alta dirección.

2. **Decisiones**: durante este proceso, las decisiones clave incluyen cómo controlar y corregir las no conformidades, eliminar las causas subyacentes para prevenir su recurrencia, asignar responsabilidades claras para implementar acciones correctivas, y evaluar la eficacia de estas acciones para asegurar que realmente resuelvan los problemas identificados.
3. **Documentación**: es obligatorio mantener un registro de todas las acciones correctivas tomadas, asegurando que se documenten adecuadamente para futuras referencias y auditorías. Aunque no es obligatorio tener un procedimiento formal para las acciones correctivas, es recomendable para guiar a los empleados en el proceso de implementación.

La Cláusula 10.1 se centra en corregir los problemas identificados, además de garantizar que la organización aprenda de ellos y mejore continuamente su enfoque de seguridad de la información.

5.5 Mejora del SGSI (Cláusula 10.2)

Esta Cláusula se centra en la mejora continua del sistema de gestión de seguridad de la información (SGSI). Aquí están los puntos clave:

Cambio y adaptación: el entorno empresarial y los estándares cambian constantemente, afectando los riesgos y la efectividad de los controles de seguridad de la información.

Herramientas y automatización: se recomienda utilizar herramientas adecuadas para la gestión del SGSI, desde simples como Excel hasta soluciones más avanzadas, considerando tanto soluciones gratuitas como de pago.

Política de mejora continua: aunque la ISO 27001 no requiere un documento específico, es una buena práctica establecer un procedimiento de mejora continua. Esto debe definir responsabilidades claras y fomentar la participación de todos los empleados.

Documentación y registro: todas las mejoras realizadas en el SGSI deben ser documentadas y registradas para mantener un historial de los cambios implementados y sus resultados esperados.

Proceso continuo: la mejora continua es un proceso dinámico que requiere revisión y ajuste constante. Es fundamental aprender de los errores y corregirlos rápidamente para mantener la eficacia del SGSI a lo largo del tiempo.

Este enfoque garantiza que el SGSI evolucione con las necesidades y los riesgos cambiantes de la organización, promoviendo así la seguridad de la información de manera efectiva y sostenida.

Conclusión

Las cláusulas de la ISO 27001 enfatizan en la importancia de establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de una organización, estableciendo un marco sólido y sistemático para su cumplimiento exitoso. Desde la definición del alcance del sistema hasta la mejora continua, cada fase del ciclo de vida del SGSI se enfoca en asegurar la confidencialidad, integridad y disponibilidad de la información.

La norma promueve la evaluación rigurosa de riesgos, la implementación de controles adecuados y la adaptación constante a los cambios tecnológicos y organizacionales. Al seguir estas cláusulas, las empresas protegen sus activos críticos y también fortalecen su resiliencia frente a amenazas; además, demuestran su compromiso con la seguridad de la información ante clientes, socios y reguladores.

En resumen, la ISO 27001 proporciona un marco detallado para que las organizaciones implementen un SGSI robusto y efectivo que proteja la información crítica y mejore continuamente su capacidad para hacer frente a los riesgos de seguridad de la información. La adherencia a estos principios no solo fortalece la seguridad de la organización, sino que también refuerza la confianza de las partes interesadas y clientes en la gestión de la información sensible.

Referencias bibliográficas

NCh-ISO27031:2015, ISO (2015), Tecnologías de la información - Técnicas de seguridad - Directrices para la preparación de las tecnologías de la informática y comunicaciones para la continuidad del negocio. Recuperado de https://ecommerce.inn.cl/nch-iso27031201552291.

International Estándar, ISO (2022), Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Recuperado de https://ecommerce.inn.cl/isoiec-27001202283707

ISACA. (2019). *COBIT*. Recuperado el 31.07.2024 de https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCDEA0

OGC. (2019). *ITIL*. Recuperado el 31.07.2024 de http://www.ogc.gov.uk/index.asp?ID=2261

National Institute of Standars and Technology. (2024). *NIST*. Recuperado el 31.07.2024 de https://www.nist.gov/

Este material fue desarrollado por el docente Joaquín Morales para la Universidad Mayor y ha sido diseñado para su lectura en formato digital.

Última actualización agosto, 2024.