



**UNIVERSIDAD
MAYOR DE SAN SIMÓN**
Ciencia y Conocimiento desde 1832

Seguridad de Sistemas

Unidad 2: SGSI - ISO/IEC 27001:2013

Msc. Ing. Marcelo Antezana C.



2.1 SGSI

Sistemas de Gestión de Seguridad de Información, tienen un enfoque sistémico sobre la seguridad de una organización.

Centra su atención en la gestión de riesgo que puede afectar a un activo de información.

2.1. Composición de un SGSI



» Un sistema de Gestión para la Seguridad de la Información consta de una serie de políticas, procedimientos e instrucciones o directrices específicas para cada actividad o sistema de información, los cuales tienen como objetivo la protección de los activos de información de la organización.



2.2 ISO/IEC 27001:2013

Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013 segunda edición). Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

Para acceder a un documento oficial puede consultar el siguiente enlace del gobierno de España el cual cuenta con la ISO/IEC 27001:2013 muy similar a la original:
<https://www.industriaconectada40.gob.es/difusion/Paginas/enlaces-interes.aspx>

2.2.1 Introducción a la Norma

La ISO 27001 es la norma internacional para SGSI. Proporciona un marco robusto para proteger la información que se puede adaptar a organizaciones de todo tipo y tamaño. La actualización más reciente de la ISO 27001 fue el 2013, si bien se realizaron algunos cambios menores en la redacción en 2017 para aclarar el requisito de mantener un inventario de activos de información, la ISO 27001: 2013 sigue siendo la norma actual para que las organizaciones puedan obtener la certificación.

La familia 27000

Las normas de la serie 27000 nacieron en 1995 con la BS 7799, redactada por el Departamento de Comercio e Industria (DTI) del Reino Unido. Las normas se denominan correctamente "ISO / IEC" porque son desarrolladas y mantenidas conjuntamente por dos organismos internacionales de normas: ISO (la Organización Internacional de Normalización) y la IEC (la Comisión Electrotécnica Internacional). Sin embargo, en el uso diario, la parte "IEC" a menudo se descarta.

Actualmente hay 45 normas publicados en la serie ISO 27000. La ISO 27001 es la única norma destinada a la certificación. Los otros estándares brindan orientación sobre la implementación de mejores prácticas. Algunos brindan orientación sobre cómo desarrollar el SGSI para industrias particulares; otros brindan orientación sobre cómo implementar procesos y controles clave de gestión de riesgos de seguridad de la información.

Si está interesado en implantar un SGSI, estas 3 normas le resultarán de ayuda. Son las siguientes:

- **ISO 27000 Tecnologías de la información – Resumen y vocabulario.**
- **ISO 27002 Tecnologías de la información– Técnicas de seguridad** – Código para prácticas en materia de controles de seguridad de la información. Es la norma más referenciada y está ligada al diseño e implantación de los 114 controles especificados en el Anexo A de la ISO 27001.
- **ISO 27005 Tecnologías de la información– Técnicas de seguridad** – Gestión de la seguridad de la información.

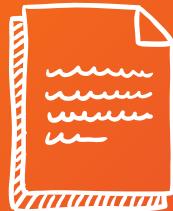
2.2.2 Beneficios de la implementación

Implementar un SGSI y lograr la certificación ISO 27001 es una tarea importante para la mayoría de las organizaciones. Sin embargo, si se hace de manera efectiva, existen beneficios significativos para aquellas organizaciones que dependen de la protección de información valiosa o sensible. Estos beneficios generalmente se dividen en tres áreas:



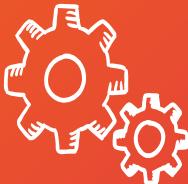
Comercial.

Tener el respaldo independiente de un SGSI por parte de un tercero puede proporcionar a la organización una ventaja competitiva y permitirle "ponerse al día" con sus competidores.



Legal. (Compliance)

Contar con un SGSI sólido y efectivo permite a la gerencia administrar los riesgos y dormir tranquilamente, sabiendo que no están expuestos a un riesgo de multa, interrupción del negocio o un impacto significativo en su reputación.



Operacional

El enfoque de la ISO 27001 fomenta el desarrollo de una cultura interna que esté alerta a los riesgos de seguridad de la información y tenga un enfoque coherente para enfrentarlos.



2.2.3 Principios y Terminología

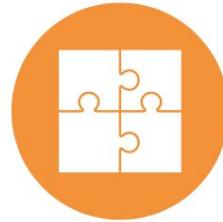
El propósito central de un SGSI es proporcionar protección a la información sensible o de valor. La información sensible incluye información sobre los empleados, clientes y proveedores. La información de valor incluye propiedad intelectual, datos financieros, registros legales datos comerciales y datos operativos.

Los tipos de riesgos que los activos de información están expuestos se agrupan en 3 categorías.



Confidencialidad

Cuando una o más personas ganan acceso no autorizado a la información.



Integridad

Cuando el contenido de la información se cambia de manera que ya no es precisa o completa.



Disponibilidad

Cuando se pierde o daña el acceso a la información.

2.2.4 Ciclo PHVA - PDCA

La ISO 27001 se basa en el ciclo PHVA, también conocido como ciclo de Deming. El ciclo PHVA puede aplicarse no solo al sistema de gestión, sino también a cada elemento individual para proporcionar un enfoque en la mejora continua.

A modo de resumen:

Planificar:

Establecer objetivos, recursos, requisitos del cliente y accionistas, política organizativa e identificar riesgos y oportunidades.

Hacer:

Implantar lo planificado.

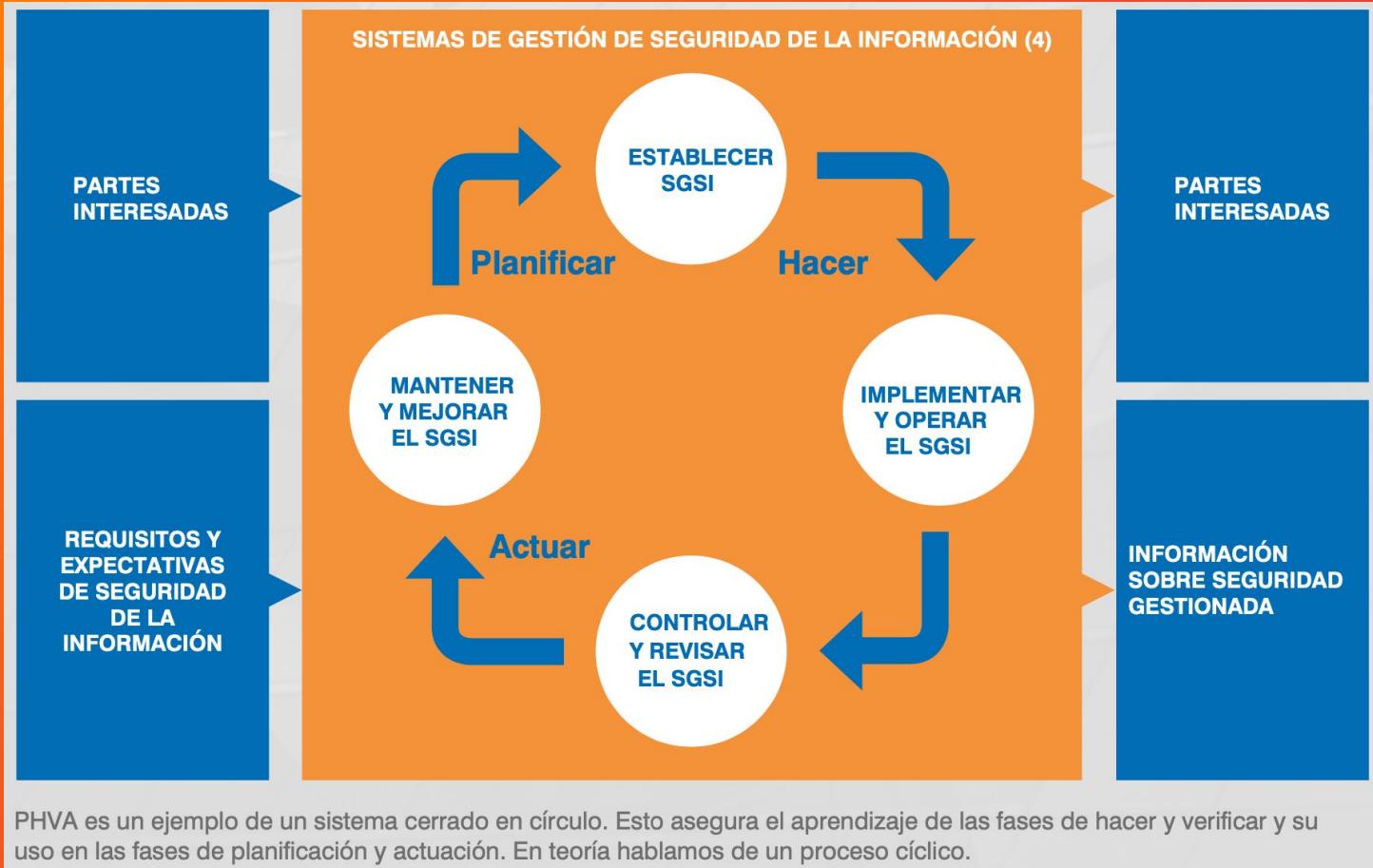
Verificar:

Controlar y medir los procesos para establecer el rendimiento de la política, objetivos, requisitos y actividades planificadas e informar de los resultados.

Actuar:

Tomar acciones para mejorar el rendimiento, en la medida de lo necesario.

2.2.4 Modelo PHVA - PDCA para la ISO 27001



2.2.5 MENTALIDAD/AUDITORÍA BASADA EN RIESGOS

Las auditorías son un proceso de acercamiento sistemático y basado en evidencias para evaluar su SGSI. Se llevan a cabo de forma interna y externa para verificar la efectividad de un SGSI.

Auditorías de 1a parte:

– Auditorías internas

Su propósito es garantizar el cumplimiento de las políticas, procedimientos y procesos según su organización, y confirmar el cumplimiento de los requisitos de la norma ISO 27001.

– Planificación de la auditoría

Diseñar un calendario de auditoría puede parecer complicado. Dependiendo de la escala y complejidad de sus operaciones, puede programar auditorías internas mensuales o anuales. Hay más detalles sobre esto en la sección 9: evaluación del desempeño.

– Mentalidad basada en riesgos

La mejor manera de considerar la frecuencia de las auditorías es observar el riesgo del proceso o área a auditar. La ISO 27001 no dicta ningún método particular de evaluación de riesgos o gestión de riesgos.

2a parte: Auditorías externas

Las auditorías de 2a parte suelen ser realizadas por clientes o proveedores externos. También pueden ser realizadas por reguladores o cualquier otra parte externa que tenga un interés formal en la organización.

3a parte: Auditorías de certificación

Las auditorías de 3a parte son llevadas a cabo por organismos externos de certificación acreditados. El organismo de certificación evaluará la conformidad con la norma ISO 27001:2013. La certificación demuestra a los clientes que está comprometido con la calidad.

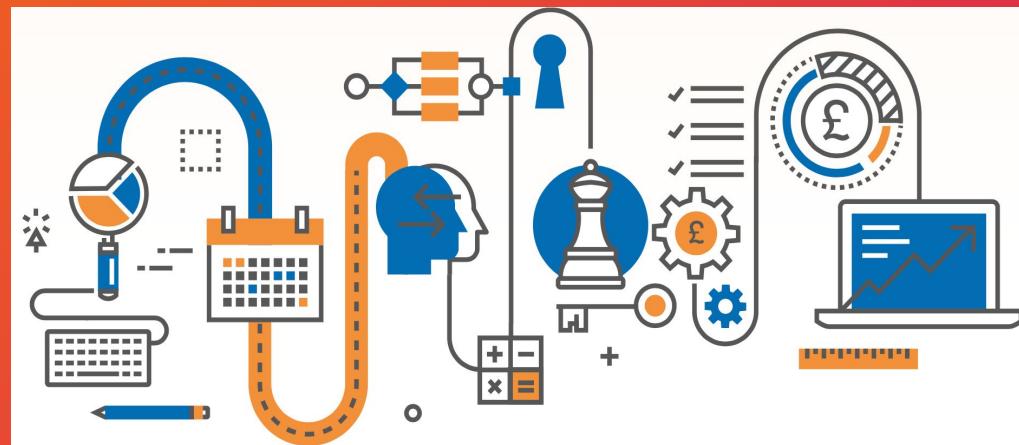
2.2.6 MENTALIDAD/AUDITORÍA BASADA EN PROCESOS

Un proceso es la transformación de una entrada en una salida, que tienen lugar como consecuencia una serie de pasos o actividades que tienen unos objetivos planificados. Frecuentemente, la salida de un proceso se convierte en la entrada de otro proceso posterior. Muy pocos procesos actúan de forma aislada.

Proceso: conjunto de actividades relacionadas o que interactúan que utilizan entradas para proporcionar resultados esperados.

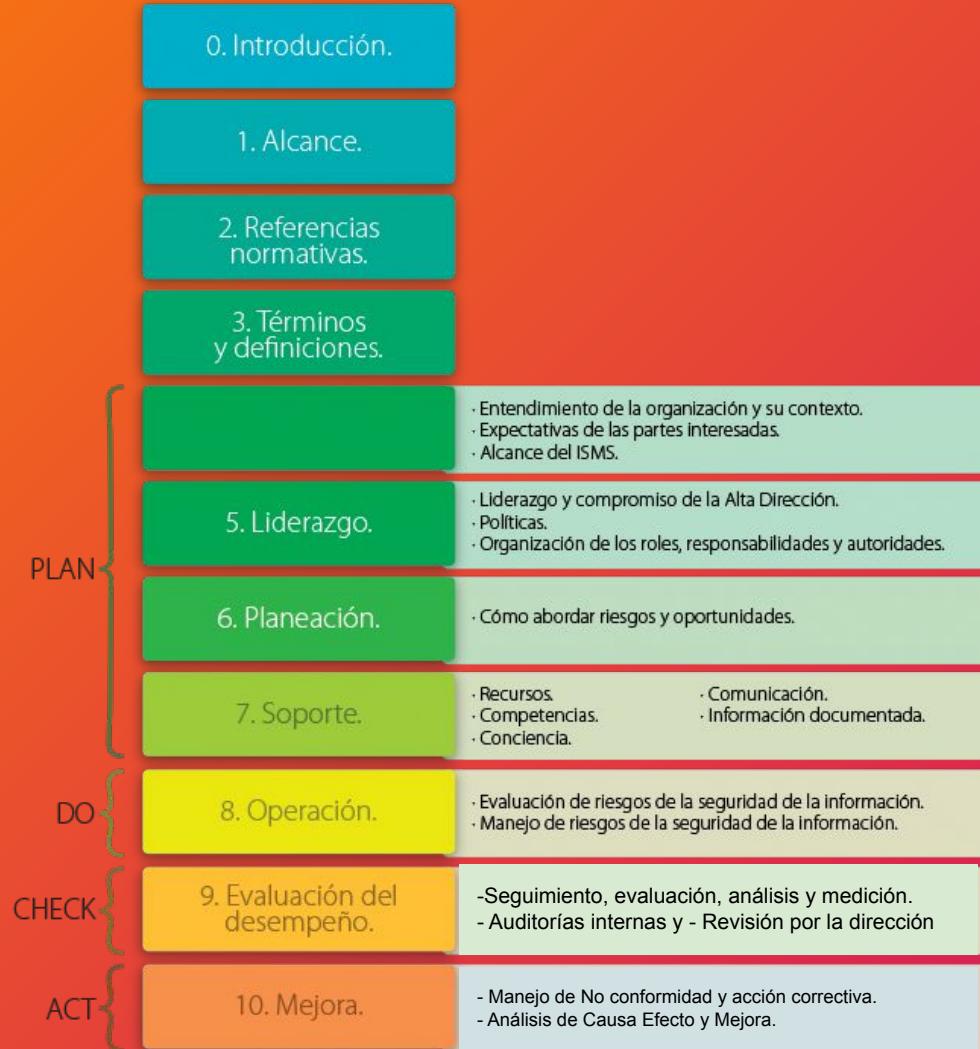
ISO 27001:2013 Fundamentales y vocabulario

Incluso una auditoría tiene un enfoque de proceso. Comienza con la identificación del alcance y los criterios, establece un curso de acción claro para lograr el resultado y tiene un resultado definido (el informe de auditoría).



Comprender cómo los se interrelacionan los procesos y cómo producen resultados puede ayudarlo a identificar oportunidades de mejora y, por lo tanto, a optimizar el rendimiento general.

2.2.7 Estructura de la ISO 27001

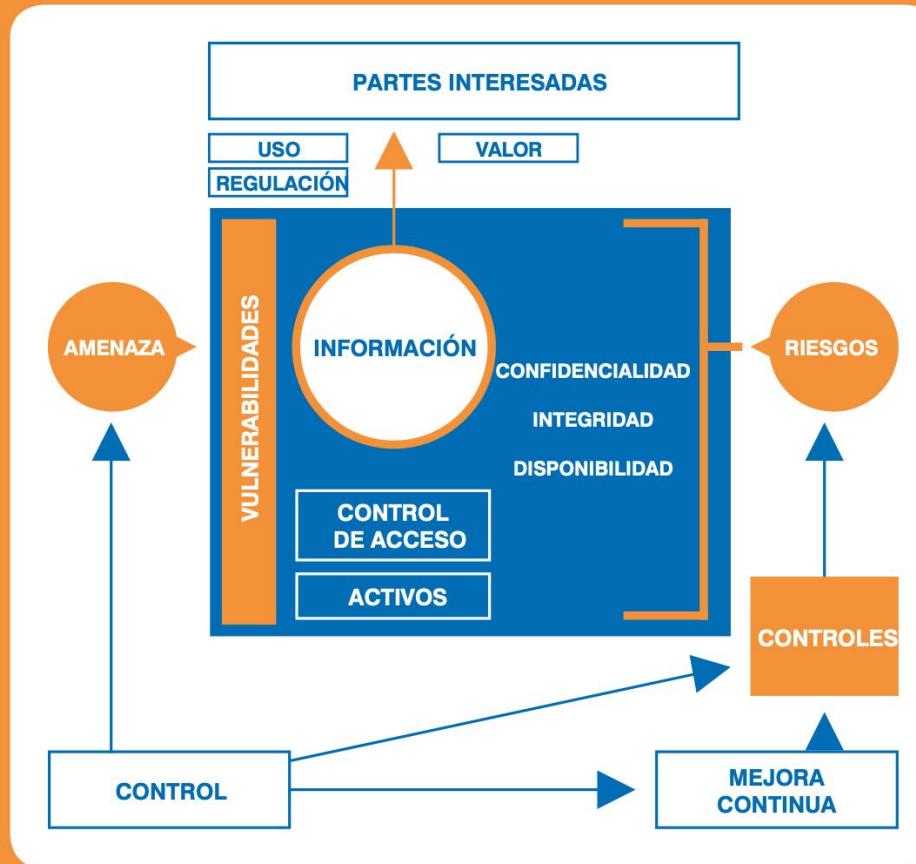


LAS 10 CLÁUSULAS DE LA ISO 27001:2013

La ISO 27001:2013 se compone de 10 secciones conocidas como cláusulas.

Al igual que con la mayoría de normas de sistemas de gestión ISO, los requisitos de la ISO 27001 que deben cumplirse se especifican en las cláusulas 4.0 - 10.0. A diferencia de la mayoría de las demás normas ISO, una organización debe cumplir con todos los requisitos de las cláusulas 4.0-10.0 no se pueden declarar una o más cláusulas como no aplicables.

La ISO 27001, además de las cláusulas 4.0-10.0, tiene un conjunto adicional de requisitos detallados en una sección llamada Anexo A, a la que se hace referencia en la Cláusula 6.0. El Anexo A contiene 114 controles de seguridad de la información a modo de buenas prácticas. Cada uno de estos 114 controles debe ser considerado. Para cumplir con la ISO 27001, la organización debe implementar estos controles, o se debe dar una justificación aceptable para no implementar un control en particular. Esta guía proporciona una explicación del propósito de cada cláusula, resaltando el tipo de evidencia que un auditor esperaría ver para confirmar el cumplimiento.



CLÁUSULA 1: ALCANCE

La sección de alcance de la ISO 27001 establece:

- El propósito de la norma.
- Los tipos de organizaciones para las que se ha diseñado.
- Las cláusulas y los requisitos que una organización debe cumplir para que la organización sea considerada como conforme con la norma.

La ISO 27001 está diseñada para ser aplicable a cualquier tipo de organización. Independientemente del tamaño, la complejidad, el sector industrial, el propósito o la madurez, su organización puede implementar y mantener un SGSI que cumpla con la ISO 27001.



CLÁUSULA 2: REFERENCIAS NORMATIVAS

En las normas ISO, la sección de referencias normativas enumeran otras normas que contengan información relevante para determinar el cumplimiento de una organización con la norma. En la ISO 27001 solo nos encontramos con un documento en cuestión, la ISO 27000 Tecnologías de la información - Resumen y vocabulario.

Algunos de los términos utilizados o requisitos detallados en la ISO 27001 se explican en la ISO 27000. La ISO 27000 es muy útil para la comprensión de los requisitos y su cumplimiento.

CONSEJO: Los auditores externos esperarán que hayan considerado la información de la ISO 27000 en el desarrollo e implantación de su SGSI.

CLÁUSULA 3: TÉRMINOS Y DEFINICIONES

No hay términos y definiciones en la ISO 27001. Sin embargo, se hacen referencias a la versión más reciente de la ISO 27000 Sistemas de gestión de seguridad de la información - Resumen y vocabulario. La versión más reciente de dicho documento contiene 81 términos y definiciones utilizados en la ISO 27001.

Además de los términos anteriormente explicados en los "principios y terminología", otros términos muy utilizados son:

'Control de accesos'

– Procesos que garantizan que solo las personas que necesitan acceso a ciertos activos disponen de dicho acceso y la necesidad se determina acorde a los requisitos del negocio y la seguridad.

'Tratamiento de riesgos'

– Procesos o acciones que reducen los riesgos indetectados a un nivel tolerable o aceptable.

'Gerencia'

– Grupo de individuos que toman las decisiones dentro de una empresa. Pueden ser responsables de establecer la dirección estratégica y determinar y conseguir los objetivos de los accionistas.

Revisar
esta
cláusula en
bibliografía
del
Classroom

CLÁUSULA 4: CONTEXTO DE LA ORGANIZACIÓN

El objetivo de su SGSI es proteger los activos de información de su empresa, de manera que la empresa pueda alcanzar sus objetivos.

La forma y las áreas específicas de prioridad dependerán del contexto en el que opere su organización. Se incluyen dos niveles:

- **Interno:** Aspectos sobre los que la organización tiene control.
- **Externo:** Aspectos sobre los que la organización no tiene control directo.

Un análisis cuidadoso del entorno en el que opera su organización es fundamental para identificar los riesgos inherentes a la seguridad de sus activos de información. El análisis es la base que le permitirá evaluar qué procesos necesita considerar agregar o fortalecer para construir un SGSI efectivo.

- **Consistencia:** ¿Cuenta con procesos uniformes en toda la organización o una multitud de prácticas operativas diferentes con poca coherencia?
- **Sistemas:** ¿Su organización tiene muchos sistemas heredados que se ejecutan en versiones de software que ya no son compatibles con el fabricante, o mantiene la tecnología más actualizada?
- **Complejidad del sistema:** ¿opera un sistema principal que hace todo el trabajo o múltiples sistemas departamentales con transferencia de información?
- **Espacio físico:** ¿Tiene una oficina segura y exclusiva o opera en un espacio compartido con otras organizaciones?

Contexto externo

CLÁUSULA 5: LIDERAZGO

La importancia del liderazgo

El liderazgo significa una participación activa en la dirección del SGSI, promover su implementación y garantizar la disponibilidad de recursos apropiados. Esto incluye:

- Asegurar que los objetivos del SGSI sean claros y estén alineados con la estrategia general.

- Claridad sobre las responsabilidades.
- Que el pensamiento basado en el riesgo está en el corazón de toda toma de decisiones; y
- Hay una comunicación clara de esta información a todas las personas dentro del alcance del SGSI.

La ISO 27001 otorga gran importancia a la participación activa de la gerencia en el SGSI, basándose en el supuesto de que es crucial para garantizar la implementación y el mantenimiento efectivo de un SGSI efectivo.

Política de seguridad

Una responsabilidad vital del liderazgo es establecer y documentar una Política de Seguridad de la Información que esté alineada con los objetivos clave de la organización. Debe incluir objetivos o un marco para establecerlos. Para

Roles y responsabilidades

Para que las actividades de seguridad de la información formen parte de las actividades cotidianas para el personal de la organización, las responsabilidades que tienen deben definirse y comunicarse claramente. Aunque no hay ningún

CLÁUSULA 6: PLANIFICACIÓN

La ISO 27001 es una herramienta de gestión de riesgos que guía a una organización en la identificación de riesgos de seguridad de la información. Como tal, el propósito subyacente de un SGSI es:

- Identificar los riesgos estratégicamente importantes, obvios y ocultos pero peligrosos;
- Asegurarse de que las actividades y los procesos operativos diarios de una organización estén diseñados, dirigidos y tengan recursos para gestionar inherentemente esos riesgos; y
- Responder y se adapte automáticamente a los cambios para hacer frente a los nuevos riesgos y reducir continuamente la exposición a los mismos.

Tener un plan de acción detallado que esté alineado, actualizado y respaldado por revisiones y controles regulares es crucial y proporciona evidencia para el auditor de una planificación del sistema claramente definida.

2.2.7 Cláusula 6 Planificación

Evaluación de riesgos

La evaluación de riesgos es el núcleo de cualquier SGSI eficaz. Incluso la organización con más recursos no puede descartar la posibilidad de sufrir un incidente de seguridad de la información. La evaluación de riesgos es esencial para:

- Aumentar la probabilidad de identificar riesgos potenciales mediante la participación de personal que utiliza técnicas de evaluación sistemática;
- Asignar recursos para abordar las áreas de mayor prioridad;
- Tomar decisiones estratégicas sobre cómo gestionar los riesgos de seguridad de la información significativos y lograr así sus objetivos.

ISO 27005: la gestión de riesgos de seguridad de la información ofrece orientación en el desarrollo de una técnica de evaluación de riesgos. Cualquiera que sea la técnica que desarrolle, debe incluir los siguientes elementos clave:

- 1 Proporcionar aviso para la identificación sistemática de riesgos (revisión de activos, grupos de activos, procesos, tipos de información), verificando la presencia de amenazas y vulnerabilidades comunes y registrando los controles que actualmente tiene implementados para administrarlos.
- 2 Proporcionar un marco para evaluar la probabilidad de que el riesgo ocurra de manera persistente (una vez al mes, una vez al año).
- 3 Proporcione un marco para evaluar las consecuencias de cada riesgo que ocurra de manera consistente (por ejemplo, pérdidas de capital monetario).
- 4 Proporcione un marco para calificar o categorizar cada riesgo identificado (por ejemplo, alto/medio/bajo), teniendo en cuenta su evaluación de probabilidad y las consecuencias.
- 5 Establezca criterios documentados que especifiquen, para cada categoría de riesgo, qué tipo de acción debe tomarse y el nivel o prioridad que se le asigna.

CLÁUSULA 7: SOPORTE

La cláusula 7 se refiere a los recursos. Esto se aplica a las personas, infraestructura, medioambiente, recursos físicos, materiales, herramientas, etc. También existe un enfoque renovado en el conocimiento como un recurso importante dentro de su organización. Cuando planifique sus objetivos de calidad, una consideración importante será la capacidad actual y la capacidad de sus recursos, así como aquellos recursos de proveedores/socios externos.

Para implementar y mantener un SGSI efectivo, necesita contar con recursos de apoyo. Estos recursos deberán ser:

- **Capaces:** Si son equipos o infraestructura.
- **Competentes:** Si se trata de personal.
- Disponibles en la revisión por la dirección.

- **Competencia.**
- **Concienciación.**
- **Comunicación.**
- **Información documentada.**

2.2.7 Clausula 7 Soporte

Competencia

La implementación de controles efectivos de seguridad de la información depende del conocimiento y las habilidades de sus empleados, proveedores y contratistas. Para asegurar una base adecuada de conocimientos y habilidades, debe:

- Definir qué conocimientos y habilidades se requieren;
- Determinar quién necesita del conocimiento y habilidades;
- Establecer cómo evaluar que las personas adecuadas tengan los conocimientos y habilidades adecuados.

Concienciación

Además de garantizar la competencia del personal clave en relación con la seguridad de la información, los empleados, proveedores y contratistas deberán conocer los elementos del SGSI. Esto es fundamental para establecer una cultura de soporte dentro de la organización.

Todos los empleados, proveedores y contratistas deben tener en cuenta lo siguiente:

La existencia de un SGSI y su razón de ser.

- Que tiene una política de seguridad de la información y cuáles son sus elementos relevantes.
- Cómo pueden contribuir a que su organización proteja la información y lo que deben hacer para ayudar a la organización a lograr sus objetivos de seguridad de la información.
- Qué políticas, procedimientos y controles son relevantes para ellos y cuáles son las consecuencias de no cumplirlos.

2.2.7 Clausula 7 Soporte

Comunicación

Para permitir que los procesos en su SGSI funcionen de manera efectiva, deberá asegurarse de tener actividades de comunicación bien planificadas y gestionadas. La ISO 27001 los detalla de manera concisa al exigirle que determine:

- Lo que necesita ser comunicado;
- Cuándo necesita ser comunicado;
- A quién necesita ser comunicado;
- Quién es responsable de la comunicación;
- Cuáles son los procesos de comunicación.

Información documentada

Para ser de utilidad, la información documentada para implementar y mantener su SGSI debe:

- Ser precisa.
- Ser comprensible para las personas que lo usan regularmente u ocasionalmente.
- Apoyarlo para cumplir los requisitos legales, administrar los riesgos y alcanzar sus objetivos.

CLÁUSULA 8: OPERACIÓN

Tras la planificación y evaluación de riesgos, estamos listos para pasar a la etapa de "hacer". La cláusula 8 trata de tener un control adecuado sobre la creación y entrega del producto o servicio.

Evaluación de riesgos de la seguridad de la información

Los métodos de evaluación de riesgos descritos en la cláusula 6 deben aplicarse a todos los procesos, activos, información y actividades dentro del alcance del SGSI.

Tratamiento de riesgos de seguridad de la información

El plan de tratamiento de riesgos que desarrolle no puede permanecer simplemente como una declaración de intenciones, debe implementar.

CLÁUSULA 9: EVALUACIÓN DEL DESEMPEÑO

Existen 3 formas para evaluar el rendimiento del SGSI:

- Seguimiento de la efectividad de los controles de SGSI.
- Auditorías internas.
- Durante la revisión por la dirección.

Auditorías internas

El propósito de las auditorías internas es evaluar sus deficiencias en los procesos del SGSI e identificar oportunidades de mejora. También proporcionan una verificación de la realidad para la gerencia sobre el desempeño del SGSI. Las auditorías internas pueden ayudar a evitar sorpresas en sus auditorías externas.

CLÁUSULA 10: MEJORA

El objetivo de la implementación del SGSI debe ser reducir la probabilidad de que ocurran eventos de seguridad de la información, así como su impacto. Ningún SGSI es perfecto, sin embargo, dichos sistemas de gestión mejoran con el tiempo y aumentarán la resistencia frente a los ataques de seguridad de la información.

**No conformidad y
acción correctiva**

Análisis de causa-raíz

2.2.7 Cláusula 10 Mejora: Causa - Raiz



Análisis de causa-raíz

Para identificar acciones correctivas efectivas, es recomendable completar un análisis de causa raíz del problema. Si no llega al fondo de por qué o cómo sucedió, es probable que cualquier solución que implemente no sea completamente efectiva. El enfoque de los "5 por qué" es una buena herramienta de análisis de causa raíz: comience con el problema y luego pregunte "por qué" hasta llegar a la causa raíz. Por lo general, con 5 preguntas es suficiente, pero los problemas complejos pueden requerir más preguntas.

Por ejemplo:

Declaración del problema:

La organización estuvo infectada por el virus Wannacry.

¿Por qué?

Alguien hizo click en un enlace de un e-mail y descargó el virus que infectó su PC.

¿Por qué?

No recibieron ninguna formación sobre enlaces en e-mails sospechosos.

¿Por qué?

La responsable de formación está de baja por maternidad y la organización no ha cubierto su baja.

¿Por qué?

El proceso de baja por maternidad no está cubierto en el procedimiento de gestión de cambios, por ello no se realizó una evaluación para identificar riesgos de seguridad de la información.

Gracias!

Preguntas?

@mantezanac

marcelo.a@umss.edu