ISO 27001:2013

GUÍA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

nqa.

> ISO 27001:2013

GUÍA DE IMPLANTACIÓN

*UK and Ireland only

Contenido

INTRODUCCIÓN A LA NORMA

La mayoría de negocios dispone o tiene acceso a información sensible. El hecho de no proteger adecuadamente dicha información puede tener consecuencias operativas, financieras y legales graves, que pueden incluso llevar a la quiebra del negocio.

El reto que la mayoría de negocios afronta es el de proporcionar una adecuada protección. Particularmente, cómo asegurar que han identificado los riesgos a los que están expuestos y cómo gestionarlos de forma proporcionada, sostenible y efectiva.

La ISO 27001 es la norma internacional para los sistemas de gestión de la seguridad de la información (SGSI). Proporciona un marco robusto para proteger la información que se puede adaptar a organizaciones de todo tipo y tamaño. Las organizaciones más expuestas a los riesgos relacionados con la seguridad de la información eligen cada vez más implementar un SGSI que cumpla con la norma ISO 27001.

La familia 27000

Las normas de la serie 27000 nacen 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.

Revisiones y actualizaciones

Las normas ISO están sujetas a una revisión cada 5 años para evaluar la necesidad de actualizaciones.

La actualización más reciente de la norma ISO 27001 en 2013 produjo un cambio significativo con la adopción de la estructura del "Anexo SL". 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.

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.

BENEFICIOS DE LA IMPLANTACIÓN

La seguridad de la información está ganando notoriedad en las organizaciones y la adopción de la ISO 27001 es cada vez más común. La mayoría de las organizaciones reconoce que las brechas de seguridad ocurren, solo es cuestión de tiempo verse afectado por este hecho.

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. Los clientes que están expuestos a riesgos importantes de seguridad de la información están haciendo cada vez más que la certificación ISO 27001 sea un requisito en la presentación de ofertas. Si su cliente está certificado en ISO 27001, elegirá trabajar solo con proveedores cuyos controles de seguridad de la información sean fiables y tengan la capacidad de cumplir con los requisitos contractuales.

Para las organizaciones que desean trabajar con este tipo de cliente, contar con un SGSI acorde a la ISO 27001 es un requisito clave para mantener y aumentar los ingresos comerciales.

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. Esta coherencia de enfoque conduce a controles que son más robustos en el manejo de amenazas. El costo de implementarlos y mantenerlos también se minimiza, y en caso de que fallen, las consecuencias se minimizarán y se mitigarán de manera más efectiva.

TRANQUILIDAD

Muchas organizaciones tienen información que es crítica para sus operaciones, vital para mantener su ventaja competitiva o que es parte inherente de su valor financiero.

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

La economía se basa en el conocimiento, y casi todas las organizaciones dependen de la seguridad de la información. La implementación de un SGSI proporciona dicha seguridad.

La ISO 27001 es un marco reconocido internacionalmente para una mejor práctica del SGSI y su cumplimiento se puede verificar de forma independiente para mejorar la imagen de una organización y dar confianza a sus clientes.

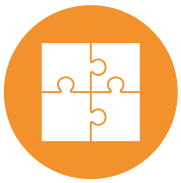
PRINCIPIOS Y TERMINOLOGÍA

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 la información sensible y de valor sufren pueden agruparse 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.

Estos tipos de riesgo de seguridad de la información se conocen comúnmente como "CID".

Los riesgos en la seguridad de la información generalmente surgen debido a la presencia de amenazas para los activos que procesan, almacenan, mantienen, protegen o controlan el acceso a la información, lo que da lugar a incidentes.

Los activos en este contexto suelen ser personas, equipos, sistemas o infraestructura.

La información es el conjunto de datos que una organización desea proteger, como registros de empleados, de clientes, datos financieros, de diseño, de prueba, etc.

Los incidentes son eventos no deseados que resultan en una pérdida de confidencialidad (violación de datos), integridad (corrupción de datos) o disponibilidad (fallo del sistema).

Las amenazas son las que causan ncidentes y pueden ser maliciosas (por ejemplo, un robo), accidentales (por ejemplo, un error tipográfico) o un acto de divino (por ejemplo, una inundación).

Las vulnerabilidades, como las ventanas abiertas de la oficina, los errores del código fuente o la ubicación junto a los ríos, aumentan la probabilidad de que la amenaza provoque un incidente no deseado y costoso.

En seguridad de la información, el riesgo se gestiona mediante el diseño, implementación y mantenimiento de controles como ventanas bloqueadas, pruebas de software o la ubicación de equipos vulnerables por encima de la planta baja.

Un SGSI que cumple con la ISO 27001 tiene un conjunto interrelacionado de procesos de mejores prácticas que facilitan y respaldan el diseño, implementación y mantenimiento de los controles. Los procesos que forman parte del SGSI suelen ser una combinación de procesos comerciales centrales existentes (por ejemplo, reclutamiento, inducción, capacitación, compras, diseño de productos, mantenimiento de equipos, prestación de servicios) y aquellos específicos para mantener y mejorar la seguridad de la información (por ejemplo, gestión de cambios, respaldo de información, control de acceso, gestión de incidentes, clasificación de la información).

CICLO PHVA

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.

Modelo PHVA para ISO 27001

PHVA es un ejemplo de un sistema cerrado en círculo. Esto asegura el aprendizaje de las fases de hacer y verificar y su uso en las fases de planificación y actuación. En teoría hablamos de un proceso cíclico.

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. Las auditorías son un ejemplo brillante de como la mentalidad basada en riesgos se adopta en el sistema de gestión.

Auditorías de 1ª parte: – Auditorías internas

Las auditorías internas son una gran oportunidad para comprender su organización. Proporcionan tiempo para enfocarse en un proceso o departamento en particular para evaluar verdaderamente su desempeño. 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. Cualquier proceso de alto riesgo, ya sea porque tiene un alto potencial de fallo o porque las consecuencias serían graves en caso de fallo, deberá auditarse con mayor frecuencia que un proceso de riesgo bajo.

Cómo evaluar el riesgo depende totalmente de usted. 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.

Es posible que tenga poco control sobre el tiempo y la frecuencia de estas auditorías, sin embargo, el establecimiento de su propio SGSI le asegurará que está preparado.

3ª parte: Auditorías de certificación

Las auditorías de 3ª parte son llevadas a cabo por organismos externos de certificación acreditados como NQA. El organismo de certificación evaluará la conformidad con la norma ISO 27001:2013. Esto implica la visita de un auditor del organismo de certificación a la organización para evaluar el sistema relevante y sus procesos. Mantener la certificación también implica reevaluaciones periódicas.

La certificación demuestra a los clientes que está comprometido con la calidad.

LA CERTIFICACIÓN GARANTIZA:

- Una evaluación regular para controlar y mejorar procesos de forma continua.
- Credibilidad del sistema para conseguir objetivos deseados.
- Reducir riesgos e incertidumbre y aumentar las oportunidades de negocio.
- Consistencia de los resultados diseñados para cumplir con las expectativas de las partes interesadas.

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

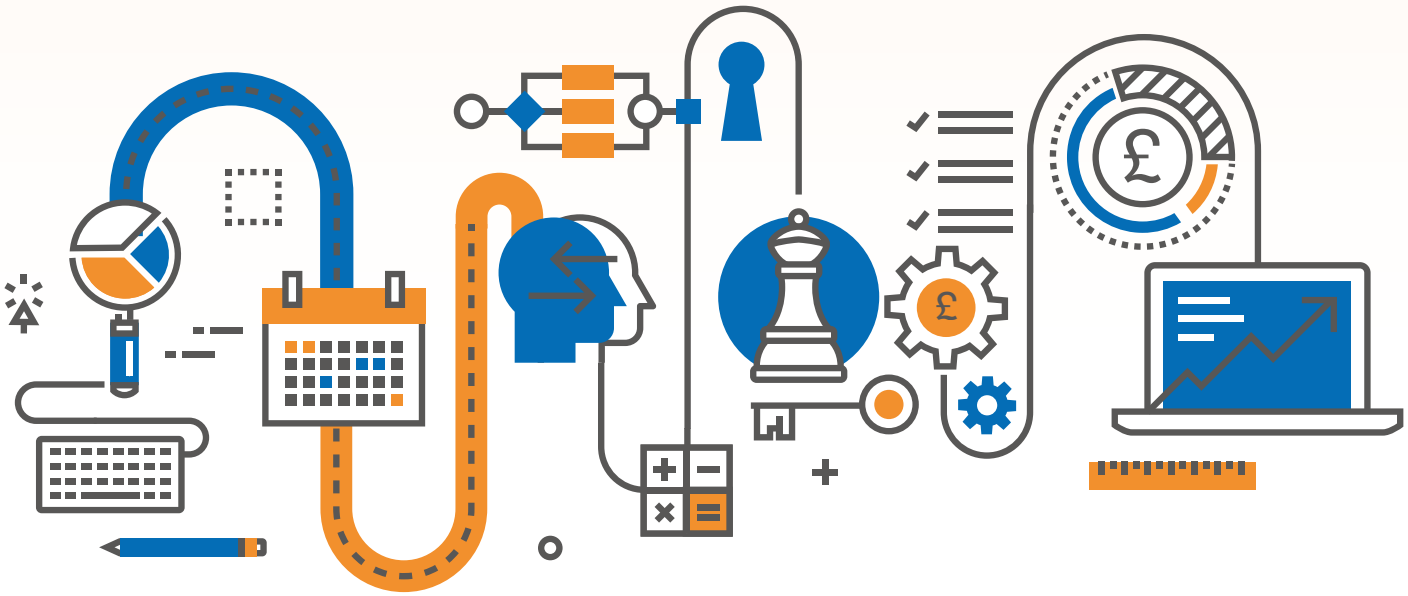
Incluso una auditoría tiene un enfoque de proceso. Comienza con la identificación del alcance y los criterios, establece un curso de acción claro para lograr el resultado y tiene un resultado definido (el informe de auditoría). El uso del enfoque basado en procesos garantiza que se asignen el tiempo y las habilidades necesarias para la auditoría. Esto hace de la auditoría una evaluación efectiva del rendimiento del SGSI.

"Los resultados consistentes y predecibles se logran de manera más efectiva y eficiente cuando las actividades se entienden y gestionan como procesos interrelacionados que funcionan como un sistema coherente".

ISO 27001:2013 Fundamentales y vocabulario.

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. También es aplicable cuando los procesos, o partes de los procesos, se subcontratan. Comprender cómo afecta o podría afectar esto al resultado y comunicarlo claramente al socio comercial (que proporciona el producto o servicio subcontratado) garantiza la claridad y responsabilidad en el proceso.

El paso final del proceso es revisar el resultado de la auditoría y garantizar que la información obtenida se utilice correctamente. La revisión por la dirección supone la oportunidad de reflexionar sobre el desempeño del QMS y de tomar decisiones sobre cómo y dónde mejorar. Dicho proceso se trata con más detalle en la Sección 9: Evaluación del desempeño.

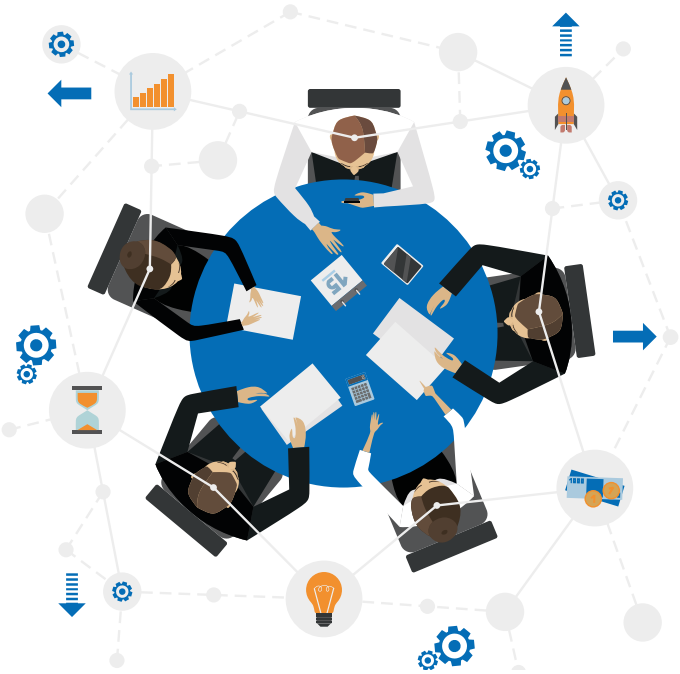


ANEXO SL

Uno de los mayores cambios introducidos en la revisión de la ISO 27001 del 2013 es la adopción de la estructura del Anexo SL. El Anexo SL (antes conocido como Guía 83 ISO) es utilizado por los autores de las normas ISO para proporcionar una estructura común para las normas de sistemas de gestión.

La ISO 27001 (seguridad de la información) adoptó esta estructura durante su revisión de 2013. La ISO 14001(medioambiente) adoptó esta estructura durante su revisión de 2015. La recientemente publicada ISO 45001(seguridad y salud laboral) también sigue esta misma estructura común.

Antes de la adopción del Anexo SL, existían diferencias entre las estructuras de las cláusulas, los requisitos y los términos y definiciones utilizados en las varias normas de sistema de gestión. Esto dificultaba la integración, la implementación y gestión de múltiples normas. Medioambiente, calidad, seguridad y salud laboral y seguridad de la información se encuentran entre las normas más comunes.



Estructura de alto nivel

El Anexo SL consiste en 10 cláusulas:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

Los términos comunes y las definiciones básicas no se pueden cambiar. Los requisitos no pueden eliminarse ni modificarse, sin embargo, se pueden agregar requisitos y recomendaciones específicos de la disciplina.

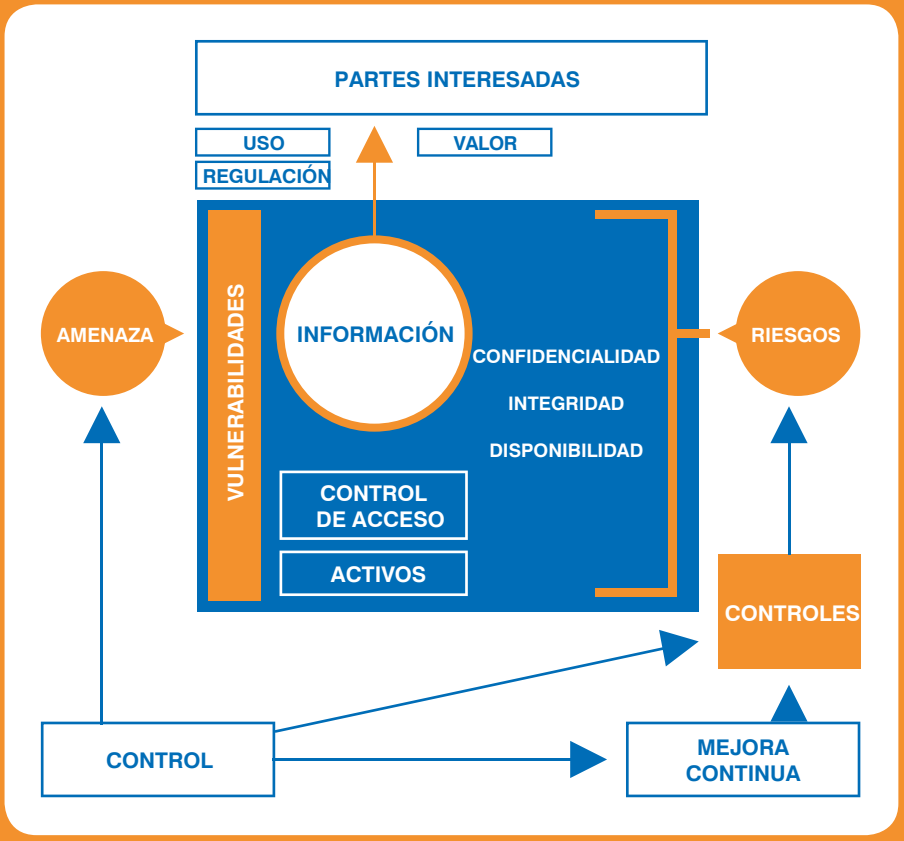
Todos los sistemas de gestión requieren una consideración del contexto de la organización; un conjunto de objetivos relevantes para la disciplina, y alineados con la dirección estratégica de la organización; una política documentada para apoyar el sistema de gestión y sus objetivos; auditorías internas y revisión por la dirección. Cuando existen múltiples sistemas de gestión, muchos de estos elementos se pueden combinar para abordar más de una norma.

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 proporcionan 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 hay 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 ciertosd activos disponen de dicho acceso yla necesidad se determina acorde a los requisitos del negocio y la seguridad.

'Efectividad'

– Medida en que las actividades planeadas (procesos, procedimientos...) se ejecutan de forma planeada o específica y se consiguen los resultados o salidas esperados.

'Riesgo'

– Combinación de probabilidad de ocurrencia de un evento de seguridad de la información y su resultante consecuencia.

'Evaluación de riesgos'

–Proceso de identificación de riesgos, analizando el nivel de riesgo de cada riesgo en particular y evaluando acciones adicionales necesarias para reducir los riesgos a niveles aceptables.

'Tratamiento de riesgos

– Procesos o acciones que reducen los riesgos indetificados 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.

Al redactar la documentación de su SGSI, no tiene que usar estos términos exactos. Sin embargo, definir los términos utilizados puede esclarecer su significado e intención. Puede ser útil proporcionar un glosario junto a la documentación de su sistema.

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.

Contexto interno

A continuación se muestran ejemplos de las áreas que pueden considerarse al evaluar los problemas internos que pueden influir en los riesgos del SGSI:

- **Madurez:** ¿Es usted una nueva empresa con un lienzo en blanco para trabajar, o una institución con procesos y controles de seguridad bien establecidos?
- **Cultura organizativa:** ¿Es su organización flexible o rígida respecto a cómo, cuándo y dónde trabaja la gente? ¿Podría su cultura resistir la implementación de los controles de Seguridad de la Información?
- **Gestión:** ¿Existen canales y procesos de comunicación claros desde los tomadores de decisiones hasta el resto de la organización?
- **Recursos:** ¿Está trabajando con un equipo de seguridad de la información o solo uan persona se encarga de todo?
- **Madurez de los recursos:** ¿Están los recursos disponibles (empleados/contratistas) bien informados, totalmente capacitados, son de confianza y son consistentes, o el personal no tiene experiencia y cambia constantemente?
- **Formato de los activos de información:** ¿Sus activos de información se almacenan principalmente en formato impreso o se almacenan electrónicamente en un servidor en o en sistemas remotos basados en la nube?
- **Sensibilidad/valor de los activos de información:** ¿Su organización tiene que administrar activos de información altamente valiosos o especialmente sensibles?
- **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

Los siguientes son ejemplos de las áreas que se pueden considerar al evaluar los problemas externos que pueden influir en los riesgos del SGSI:

- **Competencia:** ¿opera en un mercado innovador y cambiante, que requiere muchas actualizaciones del sistema para mantenerse competitivo, o en un mercado maduro y estable con poca innovación?
- **Dueño:** ¿Necesita aprobación para actualizar la seguridad física?
- **Organismos reguladores:** ¿Existe un requisito en su sector para realizar cambios estatutarios, o hay poca supervisión en su sector de mercado?
- **Económico/político:** ¿Afectan las fluctuaciones monetarias y políticas a su organización?
- **Consideraciones ambientales:** ¿Está su sede en una lzona inundable con los servidores ubicados en un sótano? ¿Existen factores que hacen que su sede sea objetivo de ataque terrorista o junto a un posible objetivo?
- **Frecuencia de ataques a la información:** ¿Su organización opera en un sector que regularmente atrae el interés de los hackers?
- **Accionistas:** ¿Están preocupados por la vulnerabilidad frente a las violaciones de datos? ¿Cuán preocupados están por el costo de los esfuerzos de la organización para mejorar la seguridad de su información?

Partes interesadas

Una parte interesada es cualquier persona que sea, pueda ser o se considere afectada por una acción u omisión de su organización. Sus partes interesadas serán claras a través del proceso de llevar a cabo un análisis exhaustivo de los problemas internos y externos. Probablemente incluirán accionistas, propietarios, reguladores, clientes, empleados y competidores y pueden extenderse al público en general y al medio ambiente, dependiendo de la naturaleza de su negocio. No tiene que tratar de comprender o satisfacer todos sus caprichos, pero sí tiene que determinar cuáles de sus necesidades y expectativas son relevantes para su SGSI.

Alcance del sistema de gestión

Para cumplir con al ISO 27001, debe documentar el alcance de su SGSI. Los alcances suelen describir:

- Los límites del sitio físico o sitios incluidos (o no incluidos);
- Los límites de las redes físicas y lógicas incluidas (o no incluidas);
- Los grupos de empleados internos y externos incluidos (o no incluidos);
- tLos procesos, actividades o servicios internos y externos incluidos (o no incluidos); y
- Interfaces clave en los límites del alcance.

Si desea priorizar los recursos mediante la creación de un SGSI que no cubra toda su organización, seleccione un alcance que se limite a la gestión de los intereses clave de las partes interesadas. Esto se puede hacer incluyendo solo sitios, activos, procesos y unidades de negocio o departamentos específicos. Algunos ejemplos de alcance son:

- **Todas las operaciones realizadas por el departamento de TI.**
- **Soporte y gestión de correo electrónico.**
- **Todos los equipos, sistemas, datos e infraestructura en el centro de datos de la organización.**

CONSEJO: Documente o mantenga un archivo de toda la información recopilada en su análisis del contexto de su organización y las partes interesadas, tales como:

- Conversaciones con un representante de la gerencia de la empresa.
- Actas de reuniones o planes de negocios.
- Un documento específico que identifica problemas internos/externos y partes interesadas y sus necesidades y expectativas. Por ejemplo, un análisis FODA, estudio PESTLE o evaluación de riesgo empresarial de alto nivel.

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 demostrar que está alineado con el contexto de su organización y los requisitos de las partes interesadas clave, se recomienda que haga referencia o contenga un resumen de los principales problemas y requisitos que debe administrar. También debe incluir un compromiso para:

- Cumplir requisitos aplicables relacionados con la seguridad de la información, tales como requisitos legales, expectativas del cliente y compromisos contractuales; y
- La mejora continua de su SGSI.

La política de seguridad de la información puede referirse o incluir subpolíticas que cubran los controles clave del SGSI de la organización. Los ejemplos incluyen: la selección de proveedores críticos para la seguridad de la información, el reclutamiento y la capacitación de los empleados, el escritorio y monitor limpios, los controles criptográficos, los controles de acceso, etc. Para demostrar la importancia de la Política de Seguridad de la Información, es aconsejable que esté autorizado por la gerencia.

CONSEJO: Para aegurar que la política de la seguridad de la información está bien comunicada y disponible para las partes interesadas, le recomendamos:

- Incluirlo en paquetes de inducción y presentaciones para nuevos empleados y contratistas;
- Publicar la declaración clave en tableros de anuncios internos, intranets y el sitio web de su organización;
- Hacer que su cumplimiento y /o soporte sea un requisito contractual para los empleados, contratistas y proveedores críticos de seguridad de la información.

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 requisito en la norma respecto al nombramiento de un representante de Seguridad de la Información, puede ser útil para algunas organizaciones designar a uno para dirigir un equipo de seguridad de la información que coordine la capacitación, el control de los controles y la presentación de informes sobre el desempeño del SGSI a la gerencia. Este individuo puede ser el responsable de la protección de datos o servicios de TI. Sin embargo, para llevar a cabo su función de manera efectiva, lo ideal sería que fuese miembro de la gerencia y con conocimiento de la gestión de seguridad de la información.

Evidenciar el liderazgo al auditor

La gerencia será el grupo de personas que establezca la dirección estratégica y apruebe la asignación de recursos para la organización dentro del alcance del SGSI. Dependiendo de cómo esté estructurada su organización, estas personas pueden o no ser el equipo de administración. Generalmente, el auditor evaluará el liderazgo entrevistando a uno o más miembros de la gerencia y evaluando su nivel de participación en:

- Evaluación de riesgos y oportunidades;
- Establecimiento y comunicación de políticas;
- Establecimiento y comunicación de objetivos;
- Revisión y comunicación del desempeño del sistema;
- Asignación de recursos y responsabilidades apropiadas.

CONSEJO: antes de su auditoría externa, identifique que individuo de la gerencia se reunirá con el auditor externo y prepárelos para la entrevista con un repaso de las posibles preguntas que se les harán.

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 adaptarse 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.

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 écnicas 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.

La mayoría de los marcos de evaluación de riesgos consisten en una tabla que contiene los resultados de los elementos 1-4 con una tabla complementaria que cubre el punto 5.

El auditor externo esperará ver un registro de su evaluación de riesgos, un responsble asignado para cada riesgo identificado y los criterios que ha utilizado.

CONSEJO: el Anexo A (8.1.1) contiene requisitos sobre listas de activos de información, activos asociados con la información (edificios, archivadores, ordenadores...) e instalaciones de procesamiento de información. Si completa su evaluación de riesgos evaluando sistemáticamente los riesgos planteados para cada elemento de esta lista, entonces habrá cumplido dos requisitos dentro del mismo ejercicio. Además, si asigna un responsable, también habrá cumplido con otro requisito del Anexo A (8.1.2).

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.

Tratamiento de riesgos

Para cada riesgo identificado en su evaluación de riesgos, deberá aplicar criterios para determinar si:

- **Acepta el riesgo.**
- **Trata el riesgo (tratamiento de riesgos).**

Las opciones para el tratamiento de riesgos incluyen una de las siguientes opciones;

- **Evasión**: dejar de realizar la actividad o procesar la información que está expuesta al riesgo.
- **Eliminación**: Eliminar la fuente del riesgo.
- **Cambio de probabilidad**: implementar un control que reduzca los incidentes de seguridad de la información.
- **Cambio en las consecuencias**: Implemente un control que disminuya el impacto si ocurre un incidente.
- **Transferencia del riesgo**: Externalizar la actividad a un tercero que tenga mayor capacidad para gestionar el riesgo.
- **Aceptar el riesgo**: Si no hay un tratamiento de riesgo práctico disponible para la organización, o si se considera que el costo del tratamiento de riesgo es mayor que el costo del impacto, puede tomar la decisión de aceptar el riesgo. Esto debe ser aprobado por la gerencia.

El auditor externo esperará ver un plan de tratamiento de riesgos (por ejemplo, una lista de acciones) que detalle las acciones de tratamiento de riesgos que ha implementado o planea implementar. El plan debe ser lo suficientemente detallado para permitir que se verifique el estado de implementación de cada acción. También será necesario que exista evidencia de que este plan ha sido aprobado por los responsables de los mismos y por la gerencia.

Anexo A y declaración de aplicabilidad

Todas las opciones de tratamiento de riesgos (a excepción de la aceptación) implican la implementación de controles. El anexo A de la ISO 27001 contiene una lista de 114 controles de seguridad de la información de buenas prácticas. Deberá considerar cada uno de estos controles al formular su plan de tratamiento de riesgos. La descripción de la mayoría de los controles es bastante vaga, por lo que se recomienda que revise la ISO 27002, que contiene más información sobre su implementación.

Como evidencia de que usted ha completado esta evaluación, un auditor externo esperará que usted presente un documento llamado declaración de aplicabilidad. Para cada uno de los 114 controles debe registrar:

- Si es aplicable a sus actividades, procesos y riesgos de seguridad de la información.
- Si lo has implementado o no.
- Si lo ha considerado no aplicable, su justificación para hacerlo.

Para la mayoría de las organizaciones, los 114 controles serán aplicables, y es probable que ya hayan implementado algunos de ellos.

Consejo: La declaración de aplicabilidad no necesita un documento demasiado complejo. Basta con una simple tabla con datos sobre el control, aplicabilidad, implementación y justificación. También es aconsejable registrar cierta información sobre cómo se ha aplicado el control (por ejemplo, hacer referencia a un procedimiento o política) para ayudarlo a responder más fácilmente cualquier pregunta del auditor externo.

Objetivos de seguridad de la información y planificación

En los niveles relevantes, necesitará tener objetivos documentados y relacionados con la seguridad de la información. Estos pueden estar en un nivel superior y aplicarse a toda la organización o solo a nivel departamental.

Cada objetivo establecido debe ser:

- Medible.
- Estar alineado con la política del SGSI.
- Considerar los requisitos a nivel de seguridad de la información.
- Considerar los resultados de la evaluación de riesgos y del proceso de tratamiento de riesgos.

Los objetivos relevantes para la seguridad de la información incluyen:

- No exceder la frecuencia definida para ciertos tipos de incidentes de seguridad de la información.
- Conseguir un nivel medible de cumplimiento con los controles de seguridad de la información.
- Proporcionar una disponibilidad definida para los servicios de la información.
- No exceder un número medible de errores de datos.
- Mejoras en los recursos disponibles a través de selección, formación o adquisición.
- Implementación de nuevos controles.
- Conseguir cumplimiento las normas relativas a la seguridad de la información.

Cada objetivo debe comunicarse a las personas relevantes. Los objetivos deben actualizarse cuando sea necesario para estra actualizados y evaluar el desempeño en función de ellos.

Para cada uno de los objetivos, necesita indicar cómo va a lograrlos. Esto incluye determinar:

- Qué necesidades deben conseguirse.
- Qué recursos se asignan.
- Quién tiene la responsabilidad sobre el objetivo.

- Si hay una fecha objetivo para completar el objetivo o es continuo.
- El método para evaluar el desempeño frente al objetivo (es decir, cuál es su medida).

CONSEJO: las formas efectivas de comunicar los objetivos de seguridad de la información incluyen cubrirlos en la formación, establecerlos como objetivos de los empleados o incluirlos en las evaluaciones de los empleados, establecerlos en acuerdos de nivel de servicio con proveedores o evaluar el desempeño con respecto a ellos en las revisiones de desempeño del proveedor.

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

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;
- Establezca cómo evaluar que las personas adecuadas tengan los conocimientos y habilidades adecuados.

Su auditor esperará que tenga documentos que detallen sus requisitos de conocimientos y habilidades. Cuando crea que se cumplen los requisitos, será necesario respaldarlo con registros como certificados de capacitación, registros de asistencia al curso o evaluaciones de competencia interna.

CONSEJO: la mayoría de las organizaciones que ya utilizan herramientas como matrices de capacitación/habilidades, evaluaciones o evaluaciones de proveedores pueden satisfacer el requisito de registros de competencia al expandir las áreas cubiertas para incluir la seguridad de la información.

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.

CONSEJO: la comunicación de esta información normalmente se puede realizar a través de los procesos y documentos existentes, como formación, contratos de trabajo, charlas, acuerdos con proveedores, informes o actualizaciones de los empleados.

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.

CONSEJO: si sus requisitos de comunicación están bien definidos en sus procesos, políticas y procedimientos, entonces no necesita hacer nada más para satisfacer este requisito. Si no lo están, debería considerar documentar sus actividades clave de comunicación en forma de una tabla o procedimiento que incluya los títulos detallados anteriormente. Recuerde que el contenido de estos documentos también debe ser comunicado.

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.

Para que su información documentada siempre satisfaga estos requisitos, necesitará contar con procesos para garantizar que:

- La información documentada se revisa cuando lo requieren las personas apropiadas antes de que se divulgue a la circulación general.
- El acceso a la información documentada se controla para que no pueda ser cambiado, corrompido, eliminado o accedido por individuos sin permiso.
- La información se elimina de forma segura o se devuelve a su propietario cuando existe el requisito de hacerlo.
- Puede realizar un seguimiento de los cambios en la información para garantizar que el proceso esté bajo control.

La fuente de su información documentada puede ser interna o externa, por lo que sus procesos de control deben administrar la información documentada de ambas fuentes.

CONSEJO: las organizaciones que tienen un buen control de documentos se caracterizan por tener:

- Una sola persona o un pequeño equipo responsable de garantizar que los documentos nuevos / modificados se revisen antes de su emisión, se almacenen en la ubicación correcta, se retiren de la circulación cuando se reemplacen y se mantenga un registro de cambios.
- Un sistema de gestión de documentos electrónicos que contiene controles y flujos de trabajo automáticos.
- Robusto respaldo de datos electrónicos y procesos de archivado/almacenamiento de archivos impresos.
- Fuerte conocimiento de los empleados sobre el control de documentos, el mantenimiento de registros y los requisitos de acceso/retención de información.

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.

Gestionar sus riesgos de seguridad de la información y alcanzar sus objetivos requiere la formalización de sus actividades en un conjunto de procesos claros y coherentes.

Es probable que muchos de estos procesos ya existan y simplemente necesiten modificaciones para incluir elementos relevantes para la seguridad de la información. Otros procesos pueden ser ad-hoc (por ejemplo, aprobaciones de proveedores), o no existir aún (por ejemplo, auditoría interna).

Para implementar procesos efectivos, las siguientes prácticas son cruciales:

1. Los procesos se crean adaptando o formalizando las actividades de negocio en costumbres dentro de la organización.
2. Identificación sistemática de los riesgos de seguridad de la información relevantes para cada proceso.
3. Definición clara y comunicación de las actividades requeridas para gestionar los riesgos de seguridad de la información asociados cuando ocurre un evento (por ejemplo, un nuevo empleado que se une a la empresa).
4. Asignación clara de las responsabilidades para llevar a cabo actividades relacionadas.
5. Asignación de recursos para garantizar que las actividades puedan llevarse a cabo cuando sea necesario
6. Evaluación rutinaria de la consistencia con la que se sigue cada proceso y su efectividad en la gestión de riesgos de seguridad de la información.

CONSEJO: designe a un individuo como responsable de garantizar que se realicen los pasos 2 a 6 para cada proceso. A menudo se hace referencia a este individuo como el propietario o responsable del proceso.

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.

Dado que los riesgos no son estáticos, los resultados de estas evaluaciones deben revisarse frecuentemente, al menos una vez al año, o con mayor frecuencia si la evaluación identifica la presencia de uno o más riesgos significativos. Los riesgos también deben revisarse siempre que:

- Se complete un tratamiento de riesgos (ver más abajo);
- Haya cambios en los activos, la información o los procesos de la organización;
- Se identifiquen nuevos riesgos;
- Los datos indiquen que la probabilidad y consecuencia de cualquier riesgo identificado haya cambiado.

CONSEJO: para garantizar que su proceso de evaluación de riesgos cubra los tipos de eventos que requerirían una revisión, también debe tener en cuenta los controles del Anexo A para la gestión de vulnerabilidades técnicas (A.12.6), seguridad en los procesos de desarrollo y soporte (A.14.2) y gestión de entrega de servicios de proveedores (A.15.2).

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 implementarlo. Cuando se necesitan cambios para tener en cuenta la nueva información sobre los riesgos y los cambios en los criterios de evaluación de riesgos, el plan debe actualizarse y volver a autorizarse.

También se debe evaluar el impacto del plan y registrar los resultados de esta evaluación. Esto puede hacerse como parte de su proceso de revisión por la dirección o auditoría interna o mediante el uso de evaluaciones técnicas como pruebas de penetración de red, auditorías de proveedores o auditorías de terceros no anunciadas.

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.

Seguimiento, medición, análisis y evaluación

Su organización necesitará decidir qué debe controlar para asegurar que el proceso del SGSI y los controles de seguridad de la información estén funcionando según lo previsto. No es práctico controlar a cada momento, si intenta hacerlo, es probable que el volumen de datos sea tan grande que sea prácticamente imposible usarlo de manera efectiva. Por lo tanto, en la práctica, deberá tomar una decisión informada sobre qué monitorear. Las siguientes consideraciones serán importantes:

- ¿Qué procesos y actividades están sujetos a las amenazas más frecuentes y significativas?
- ¿Qué procesos y actividades tienen las vulnerabilidades más significativas?
- ¿Qué es práctico para controlar y generar información significativa y oportuna?
- Cada proceso de control que implemente, para que sea efectivo, debe definir claramente:
- Cómo se lleva a cabo el control(por ejemplo, esto se define en un procedimiento);
- Cuándo se lleva a cabo;
- Quién es responsable de llevarlo a cabo;
- Cómo se informan los resultados, cuándo, a quién y qué hacen con ellos;
- Si los resultados del control identifican un desempeño inaceptable, ¿cuál es el proceso o procedimiento para afrontar esta situación?

Para demostrarle a un auditor que tiene implementado el procesamiento de monitoreo adecuado, deberá conservar registros de los resultados de monitoreo, análisis, revisiones de evaluación y cualquier actividad relacionada.

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.

Las auditorías internas deben comprobar:

- La consitencia del seguimiento de los procesos, procedimientos y controles;
- El éxito de los procesos, procedimientos y controles para conseguir los resultados esperados;
- Si su SGSI cumple con la norma ISO 27001 y los requisitos de las partes interesadas.

Para asegurar que las auditorías se llevan a cabo a un alto nivel y de forma que aporten valor a la empresa, deben ser llevadas acabo por personas que:

- Sean respetadas.
- Sean competentes.
- Comprendan los requisitos de la ISO 27001.
- Pueden interpretar rápidamente su documentación y tiene experiencia en técnicas de auditoría.

Se les debe asignar el tiempo suficiente para realizar la auditoría y asegurar la cooperación de los empleados relevantes. Debe mantener un plan de auditorías internas. El auditor externo verificará dicho plan para garantizar que todos los procesos del SGSI se auditen durante un ciclo de tres años y que incluya:

- Evidencias de bajo rendimiento (es decir, a través de auditorías previas, o monitoreando resultados o incidentes de seguridad de la información);
- La gestión de riesgos de seguridad de la información.
- Los procesos que se auditan con mayor frecuencia.

El auditor externo también esperará que cualquier acción identificada en la auditoría sea registrada, revisada por los empleados apropiados y tenga acciones implementadas de manera oportuna para rectificar cualquier problema significativo. Al momento del cierre, denen considerar cualquier oportunidad de mejora identificada que requiera una inversión significativa de recursos.

Revisión por la dirección

La revisión por la dirección es un elemento esencial del SGSI. Es el punto formal en el que la gerencia revisa la efectividad del SGSI y asegura su alineación con la dirección estratégica de la organización. Las revisiones por la dirección deben realizarse a intervalos planificados y el programa de revisión general debe cubrir como mínimo una lista de áreas básicas especificadas en la cláusula 9.3 de la norma.

No es esencial que realice una sola reunión de revisión por la dirección que abarque la agenda completa. Si actualmente dispone de una serie de reuniones que cubren las áreas básicas requeridas, no hay necesidad de duplicarlas.

Deberá conservar información documentada de dichas revisiones por la dirección. Normalmente, actas de reuniones o tal vez grabaciones de llamadas si realiza llamadas teleconferencias. No es necesario extenderse mucho, pero deben contener un registro de las decisiones tomadas y las acciones acordadas, incluyendo responsabilidades y plazos.

CONSEJO: si decide modificar el calendario de las revisiones por la dirección y estas reuniones cubren varias áreas, puede considerar resumir las áreas cubiertas en forma de tablas o procedimientos para esclarecer los aspectos cubiertos en cada reunión.

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

La mejora se consigue aprendiendo de los incidentes de seguridad, los problemas identificados en las auditorías, los problemas de rendimiento, las quejas de las partes interesadas y las ideas generadas durante las revisiones por la dirección.

Para cada oportunidad identificada, deberá mantener registros de:

- Lo que ocurrió.
- Si el evento tuvo consecuencias indeseables, qué acciones se tomaron para controlarlo y mitigarlo.
- La causa raíz del evento (si se determina).
- La acción tomada para eliminar la causa raíz (si es necesario).
- La evaluación de la efectividad de cualquier acción tomada.

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 pregunta es suficiente, pero los problemas complejos pueden requerir más preguntas.

Por ejemplo:

Declaración del problema:
La organización estba 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 enlances en e-mails sospechosos.

¿Por qué?
La esponsable 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.

CONSEJO: es posible que no tenga suficientes recursos para realizar el análisis de causa raíz en cada evento. Para priorizar esfuerzos, primero debe considerar completar una evaluación de riesgo simple y luego realizar un análisis de causa raíz solo para aquellos riesgos de valor medio o alto.

SACAR EL MÁXIMO DE SU SISTEMA DE GESTIÓN

Consejos para la correcta implementación de un SGSI:

1. Pregúntese ¿Por qué?. Asegúrese de que las razones de implantación del SGSI son claras y están alineadas con su dirección estratégica. De lo contrario corre el riesgo de no obtener la aceptación de la gerencia.

2. Considere ¿Para qué?. Implementar y mantener un SGSI requiere un compromiso, así que asegúrese de que su alcance sea lo suficientemente amplio como para cubrir la información crítica que necesita protección, pero no tan amplio como para carecer de recursos para implementarlo y mantenerlo.

3. Involucre a todas las partes interesadas en los momentos apropiados. Alta dirección para el contexto, requisitos, políticas y establecimiento de objetivos; gerentes y empleados con conocimiento para la evaluación de riesgos, diseño de procesos y procedimientos.

4. Comunique durante el proceso a las partes interesadas. Hágales saber lo que está haciendo, por qué lo está haciendo, cómo planea hacerlo y cuál será su participación. Proporcione actualizaciones del progreso.

5. Obtenga ayuda externa. No falle por falta de habilidades o conocimiento. La gestión de los riesgos de seguridad de la información a menudo requiere conocimientos especializados. Asegúrese de verificar las credenciales de un tercero antes de contratarlo.

6. Mantenga procesos y documentación simples. Puede desarrollarlos más adelante si fuese necesario.

7. Diseñe e implemente reglas que pueda seguir en la práctica. No cometa el error de documentar una regla demasiado elaborada que nadie pueda seguir. Es mejor aceptar un riesgo y seguir buscando formas de gestionarlo.

8. Recuerda a los proveedores. Algunos lo ayudarán a mejorar su SGSI, otros aumentarán su riesgo. Debe asegurarse de que los proveedores de alto riesgo tengan controles establecidos tan buenos como los suyos. Si no los tienen, busque alternativas.

9. Forme al personal. Es probable que la seguridad de la información sea un concepto nuevo para sus empleados. Las personas pueden necesitar cambiar sus hábitos y es improbable que una sola sesión informativa de sensibilización sea suficiente.

10. Recuerde asignar recursos suficientes para probar rutinariamente sus controles. Las amenazas a las que se enfrenta su organización cambiarán constantemente y debe probar la respuesta a dichas amenazas.

PASOS TRAS LA IMPLANTACIÓN

1 FORMACIÓN DE CONCIENCIACIÓN

- Su organización debe crear conciencia sobre los diversos estándares cubiertos por el sistema de gestión.
- Debe celebrar reuniones de capacitación separadas para los diferentes niveles de la gerencia, lo que ayudará a crear un ambiente motivador, listo para la implantación.

2 POLÍTICA Y OBJETIVOS

- YSu organización debe desarrollar una política de calidad/integrada y objetivos relevantes para ayudar a cumplir los requisitos.
- Al trabajar con la gerencia, su empresa debe realizar talleres con todos los niveles de personal de gestión para delinear los objetivos integrados.

3 ANÁLISIS DE DEFICIENCIAS INTERNO

- Su organización debe identificar y comparar el nivel de cumplimiento de los sistemas con los requisitos de las normas de su nuevo sistema.
- Todo el personal relevante debe comprender las operaciones de la organización y desarrollar un mapa de procesos para las actividades del negocio.

4 DOCUMENTACIÓN/PROCESO DE DISEÑO

- La organización debe crear documentación de los procesos según los requisitos de las normas relevantes.
- Debe redactar e implantar un manual, procedimientos funcionales, instrucciones de trabajo, procedimientos del sistema y proporcionar los términos asociados.

5 DOCUMENTACIÓN/PROCESO DE IMPLANTACIÓN

- Los procesos/documentos desarrollados en el paso 4 deben implementarse en toda la organización y abarcar todos los departamentos y actividades.
- La organización debe realizar un taller sobre la implementación según corresponda para los requisitos de la norma ISO.

6 AUDITORÍA INTERNA

- Un sistema de auditoría interna robusto es esencial. Recomendamos la formación de auditor interno y NQA puede proporcionar dicha formación para las normas que esté implantando.
- IEs importante implementar acciones correctivas para las mejoras, en cada uno de los documentos auditados, a fin de cerrar las deficiencias y garantizar la eficacia del sistema de gestión.

7 ORGANIZAR LA REVISIÓN POR LA DIRECCIÓN DEL SISTEMA

- La gerencia de debe revisar varios aspectos comerciales de la organización, que son relevantes para las normas a implantar.
- Revise la política, los objetivos, los resultados de la auditoría interna y del desempeño del proceso, los resultados de las quejas, el cumplimiento legal, la evaluación de riesgos y desarrolle un plan de acción y un acta de revisión.

8 ANÁLISIS DE DEFICIENCIAS DE SISTEMAS IMPLANTADOS

- Debe realizar un análisis de deficiencias para evaluar la efectividad y el cumplimiento de la implantación del sistema en la organización.
- Este análisis de deficiencias preparará a su organización para la auditoría de certificación final.

9 ACCIONES CORRECTIVAS

- La organización estará lista para la auditoría de certificación final, siempre que el análisis de deficiencias y todas las no conformidades (NC) hayan recibido acciones correctivas.
- Verifique que todas las NC significativas estén cerradas y que la organización esté lista para la auditoría de certificación final.

10 AUDITORÍA DE CERTIFICACIÓN FINAL

- Una vez completada la auditoría de forma satisfactoria, su organización recibirá el certificado.
- ¡Enhorabuena!

USEFUL LINKS

Information Security Management Training
https://www.nqa.com/training/information-security

Information Commissioners Office
https://ico.org.uk/

ISO - International Organization for Standardization
https://www.iso.org/home.html

Authored on behalf of NQA by: Julian Russell