Una publicación del Capítulo eV de ISACA Alemania
Grupo de especialistas en seguridad de la información

Guía de implementación
ISO/CEI 27001:2022

Guía práctica para la implementación de un sistema de gestión de seguridad de la información (SGSI) según ISO/IEC 27001:2022

ISACA Germany Chapter

dpunkt.verlag

Editor
Capítulo de ISACA Alemania e. v.
Storkower Str. 158
10407 Berlín

www.isaca.de
info@isaca.de

Equipo de autores 2022

- Erik Gremeyer (CISA, CISM), Consultoría ATM
- Andreas Kirchner (CISM, CISSP), abat AG
- Ralf Knecht (CISM)
- Ying-Yeung John Man (CISA, CISM)
- Dirk Meissner (CISA, CDPSE), Allevio AG
- Nico Müller (CISA, CISM, ITGM)
- Jan Rózek
- Dr. Markus Ruppel, RIMOC GmbH
- Andrea Rupprich (CISA, CISM), usd AG
- Dr. Tim Sattler (CISA, CISM, CGEIT, CRISC, CDPSE, CISSP, CCSP), Jungheinrich AG
- Michael Schmid (CISM), Hubert Burda Media

Equipo de autores 2016

- Gerhard Funk (CISA, CISM), consultor independiente
- Julia Hermann (CISSP, CISM), Giesecke y Devrient GmbH
- Angelika Holl (CISA, CISM), Unicredit Bank AG
- Nikolay Jeliazkov (CISA, CISM), Unión de Inversiones
- Oliver Knörle (CISA, CISM)
- Boban Krsic (CISA, CISM, CISSP, CRISC), DENIC eG
- Nico Müller, BridgingIT GmbH
- Jan Oetting (CISA, CISSP), Consileon Business Consultancy GmbH
- Jan Rózek
- Andrea Rupprich (CISA, CISM), usd AG
- Dr. Tim Sattler (CISA, CISM, CGEIT, CRISC, CISSP), Jungheinrich AG
- Michael Schmid (CISM), Hubert Burda Media
- Holger Schrader (CISM, CRISC)

Estado: noviembre de 2022 (Final luego de revisión y revisión por parte del Grupo de Especialistas en Seguridad de la Información de ISACA).

Guía de Implementación ISO/IEC 27001:2022

Guía práctica para la implementación de un sistema de gestión de seguridad de la información (SGSI) según ISO/IEC 27001:2022

ISACA
Germany Chapter

¿Por qué esta guía?

La seguridad de la información es indispensable. Como componente de la gestión corporativa, debe estar orientado a brindar un soporte óptimo a los objetivos comerciales. Incluso o especialmente en tiempos de las llamadas "amenazas cibernéticas" y los desafíos emergentes de la "seguridad cibernética" en muchos lugares, un sistema de gestión de seguridad de la información (SGSI) bien estructurado de acuerdo con estándares internacionalmente reconocidos proporciona la base óptima para la eficiencia y la implementación efectiva de una estrategia holística de seguridad de la información.

Que el enfoque elegido sea las amenazas que se originan en Internet, la protección de la propiedad intelectual, el cumplimiento de regulaciones y obligaciones contractuales o la salvaguardia de los sistemas de producción depende de las condiciones marco (por ejemplo, industria, modelo de negocio o apetito de riesgo) y los objetivos de seguridad específicos de la organización respectiva. En todos los casos, es fundamental ser consciente de los riesgos de seguridad de la información existentes en el contexto respectivo o descubrirlos y seleccionar, implementar y, en última instancia, también realizar un seguimiento coherente de las estrategias, procesos y medidas de seguridad necesarios.

La implementación concreta de un SGSI requiere experiencia, pero se basa ante todo en la decisión y el compromiso de la alta dirección con el tema. Un mandato de gestión claro y una estrategia de seguridad adaptada a la estrategia empresarial, junto con personal competente y los recursos que, en última instancia, siempre se necesitan, son los requisitos básicos para apoyar de forma óptima la consecución de los objetivos empresariales con un SGSI.

La Guía de implementación actualizada ISO/IEC 27001: 2022 (en resumen: Guía de implementación) contiene recomendaciones prácticas y consejos para organizaciones que ya operan un SGSI de acuerdo con el estándar internacional ISO/IEC 27001, "Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de seguridad de la información - Requisitos", o desean establecer uno, independientemente de la certificación existente o posible. La guía ofrece asistencia y enfoques pragmáticos a todos aquellos a quienes se les ha confiado el establecimiento y/o la operación de un SGSI.

Las ventajas de un SGSI adaptado individualmente y, si es necesario, al mismo tiempo conforme a las normas, se destacan claramente. En particular, se presentan recomendaciones prácticas para establecer o aumentar el nivel de madurez de los procesos SGSI existentes y ejemplos típicos de implementación de varios requisitos.

Reconocimiento

El Capítulo eV de ISACA Alemania desea agradecer al Grupo de Seguridad de la Información de ISACA y a los autores por preparar la guía: Erik Gremeyer, Andreas Kirchner, Ralf Knecht, Ying-Yeung John Man, Dirk Meissner, Nico Müller, Jan Rozek, Dr. Markus Ruppel, Andrea Rupprich, Dr. Tim Sattler, Michael Schmid.

Gestión y edición del proyecto: Andrea Rupprich

Tabla de contenido

1. Introducción

La gestión sistemática de la seguridad de la información de acuerdo con la norma ISO/IEC 27001:2022 tiene como objetivo garantizar la protección efectiva de la información y los sistemas de TI con respecto a los objetivos esenciales de protección de la seguridad de la información (confidencialidad, integridad y disponibilidad).

Esta protección no es un fin en sí misma, sino que sirve para respaldar los procesos comerciales, lograr objetivos corporativos y preservar los valores corporativos mediante el suministro y el procesamiento de información sin problemas. En la práctica, un SGSI utiliza las siguientes tres perspectivas para este propósito:

G - Vista de gobernanza
- Metas de TI y objetivos de seguridad de la información derivados de se
  derivan de objetivos corporativos de nivel superior (por ejemplo, respaldados o derivados de COSO o COBIT)

R - Vista de riesgo
- Necesidades de protección y exposición al riesgo de los valores corporativos y los sistemas informáticos.
- Apetito de riesgo de la empresa.
- Oportunidades y riesgos

C - Vista de cumplimiento
- Requisitos externos debidos a leyes, reglamentos y Estándares
- Especificaciones y directrices internas
- Obligaciones contractuales

Estas opiniones determinan qué medidas de protección son apropiadas y efectivas para

las capacidades y los procesos de negocio de la organización,

la necesidad de protección dependiendo de la criticidad de los respectivos activos de la empresa, así como

cumplimiento de las leyes y regulaciones aplicables.

Medidas

Por un lado, las medidas para lograr y mantener un procesamiento de información libre de errores deben ser efectivas para alcanzar el nivel de protección requerido. Por otro lado, también deben ser económicamente apropiados (eficientes).

ISO/IEC 27001:2022 y los requisitos y medidas establecidos de manera sistemática y exhaustiva en ella, que - en diversos grados y calidad - son parte del funcionamiento de cada SGSI, apoyan el logro de los objetivos enumerados al principio desde las tres perspectivas (ver figura 1):

La visión de gobernanza se refiere a los aspectos de control del SGSI, como la estrecha participación de la dirección.
Se deben tener en cuenta los siguientes aspectos: el compromiso de la alta dirección (ver sección 3.2 Liderazgo y Compromiso), la coherencia entre los objetivos de negocio y de seguridad de la información (ver sección 3.3 Objetivos de SI), la definición de estrategias y directrices (ver sección 3.4 Política de SI), una estrategia de comunicación eficaz adaptada al grupo objetivo (ver sección 3.9 Comunicación), responsabilidades y estructuras organizativas apropiadas (ver sección 3.5 Roles, responsabilidades y competencias) y un seguimiento específico del desempeño (ver sección 3.7 Objetivos de SI) .

Capítulo 3.9 Comunicación), responsabilidades y estructuras organizativas apropiadas (consulte el Capítulo 3.5 Roles, responsabilidades y competencias) y monitoreo de desempeño específico, Capítulo 3.7 Monitoreo de desempeño/riesgo/ (ver cumplimiento). ISO/IEC 27014:2020 proporciona más información sobre la gobernanza de la seguridad de la información.

La visión de riesgos, que sirve, entre otras cosas, como base para una toma de decisiones comprensible y una priorización de riesgos, es un elemento clave del proceso de gestión de riesgos.
Está representado por la gestión de riesgos de SI (cf. Sección 3.6 Gestión de riesgos) e incluye especificaciones y métodos para identificar, analizar y evaluar riesgos en el contexto de la seguridad de la información, es decir, riesgos que representan una amenaza potencial a la confidencialidad, integridad y/o disponibilidad. de los sistemas de TI y la información y, en última instancia, los procesos de negocio que dependen de ellos.

La visión del cumplimiento está firmemente anclada en todo el estándar. Por un lado, incluye la definición de requerido
requisitos (de seguridad), que está respaldado por la medidas del Anexo A. Por otro lado, se refiere a el cumplimiento concreto de precisamente estos requisitos, que se apoya en un seguimiento periódico por parte de la dirección y los responsables de la información seguridad (consulte la Sección 3.7 Desempeño/Riesgo/Cumplimiento seguimiento) y por auditorías internas (ver capítulo 3.12 Auditoría Interna y 3.14 Mejora Continua). Documentación adecuada (ver capítulo 3.8 Documentación) y la conciencia de seguridad exist empleados y directivos (ver capítulo 3.10 Concienc) También son esenciales para la visión del cumplimiento.

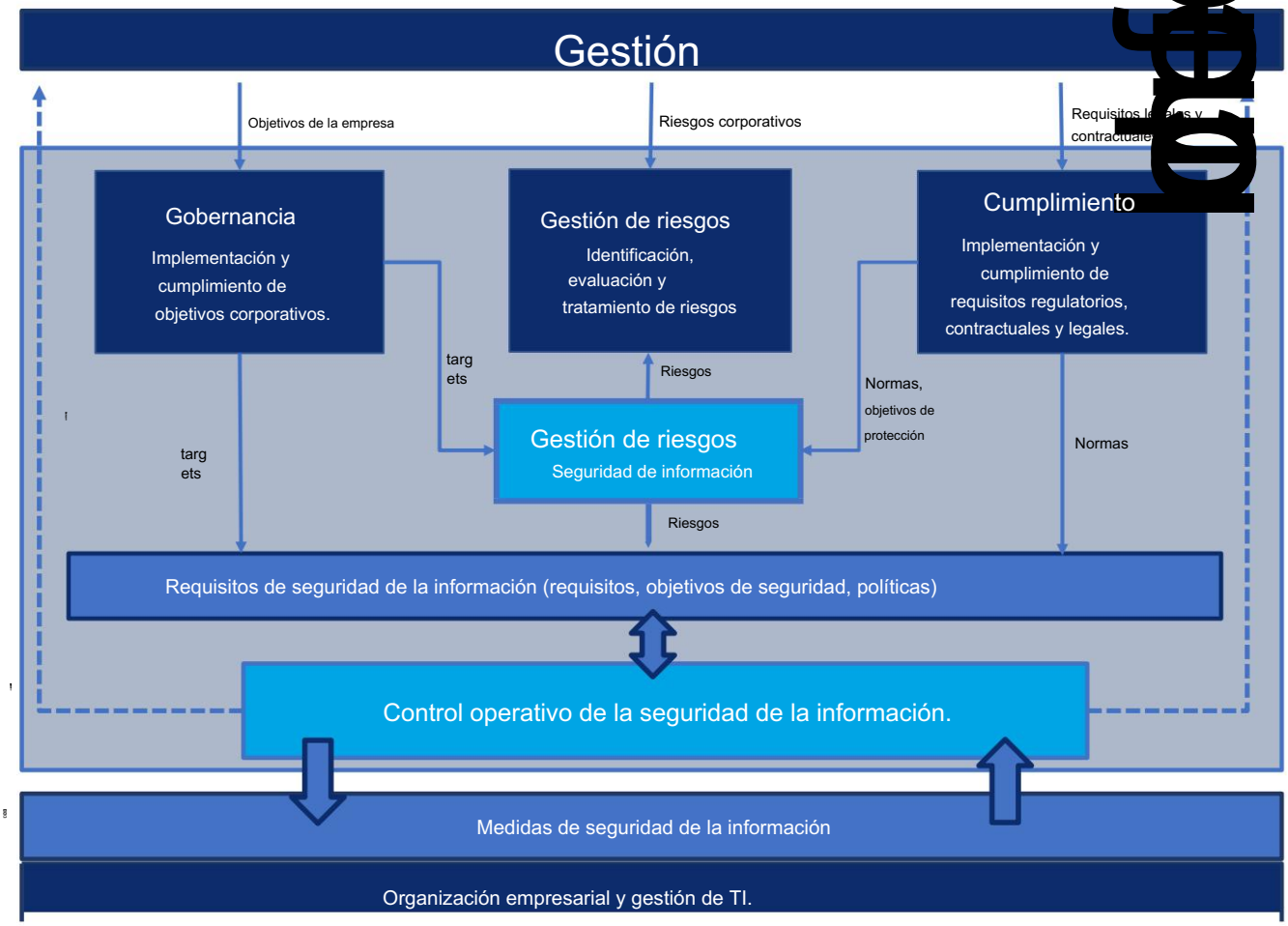


Figura 1: Integración del SGSI en las empresas gestión1

1Fuente : Carmao GmbH.

2 Estructura de la guía

2.1 Temas

Esta guía de implementación se basa en los principales temas de la norma ISO/IEC 27001:2022, pero sin reproducir la estructura de secciones de la norma de forma idéntica. En cambio, el áreas temáticas relevantes de un SGSI según ISO/IEC 27001:2022 se describen como "bloques de construcción" que tienen demostrado ser relevante y necesario en la práctica. Contra esto antecedentes, el contenido de las secciones pertinentes del estándar se reestructuran y combinan en focales individuales temas. Desde el punto de vista de los autores, el edificio de 14 " bloques" que se enumeran a continuación se pueden resaltar en función de la estándar, que en conjunto representan el SGSI de un organización (ver Figura 2):

1. Contexto de la Organización (Contexto de la Organización)
2. Liderazgo y Compromiso (Liderazgo y Compromiso)
3. Objetivos de SI
4. Política de SI (Política de SI)
5. Roles, Responsabilidades y Competencias
6. Gestión de riesgos
7. Evaluación del desempeño y KPI (monitoreo de desempeño/riesgo/cumplimiento)
8. Documentación (Documentación)
9. Comunicación
10. Conciencia (Conciencia)
11. Relaciones con proveedores
12. Auditoría Interna (Auditoría Interna)
13. Gestión de incidentes
14. Mejora continua

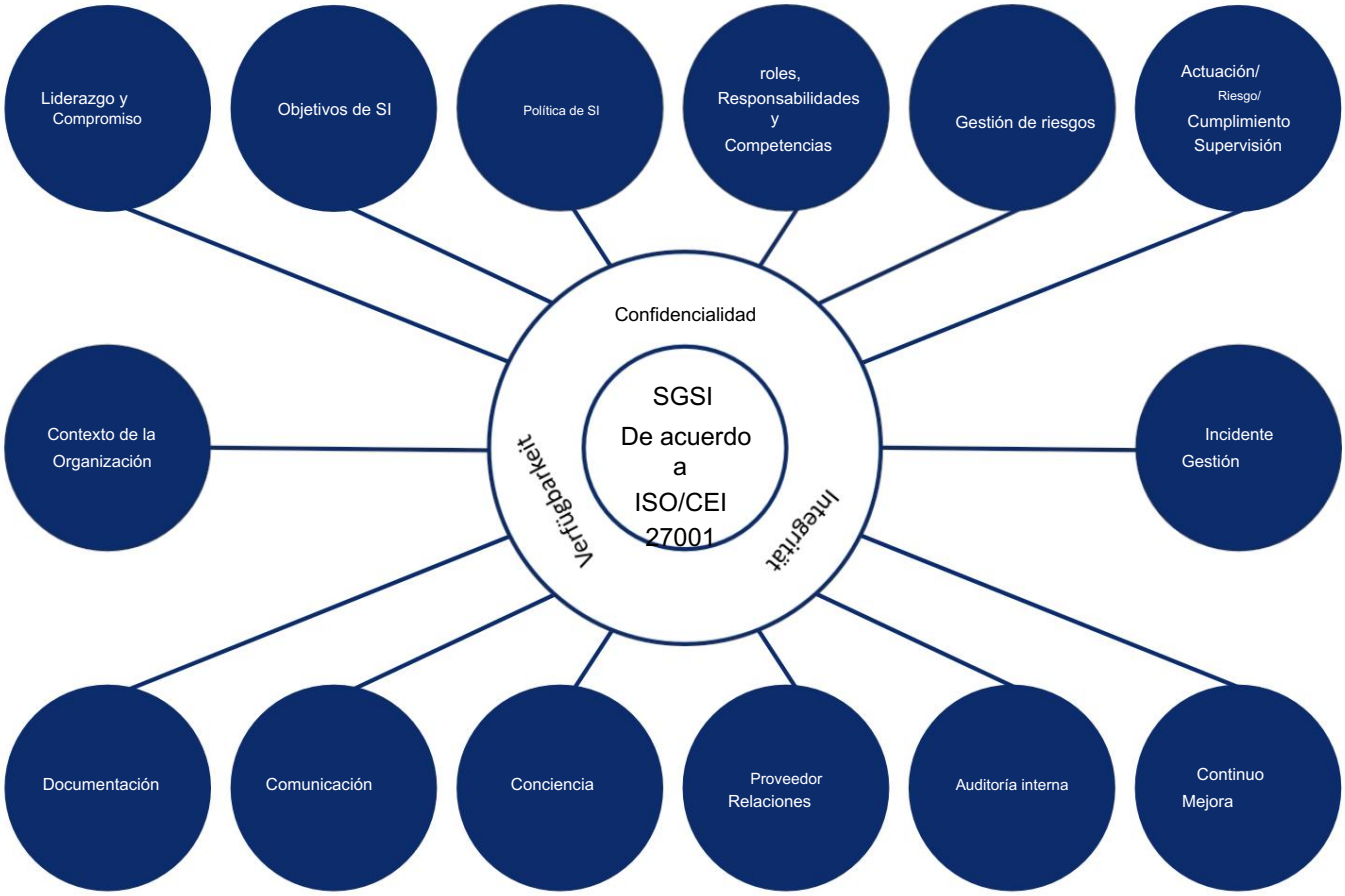


Figura 2: Componentes básicos de un SGSI según ISO/IEC 27001:2022

En los siguientes capítulos, se describen para todos los componentes los factores clave de éxito para una implementación probada y compatible con los estándares.

Dado que esta guía también pretende proporcionar asistencia práctica, las explicaciones de los componentes básicos van más allá del contenido puramente normativo de ISO/IEC 27001:2022 (o ISO/IEC 27002:2022). Por el contrario, esto también significa que no todas las referencias de este documento son igualmente "adecuadas" para todos los SGSI o para todas las organizaciones.

El establecimiento de un SGSI, ya sea por compromiso propio o con intención de certificación, es un proyecto ambicioso que, como cualquier otro proyecto, requiere objetivos "inteligentes " [1] , recursos suficientes y expertos, un director de proyecto adecuado y una persona motivada y equipo calificado. Además, el apoyo constante y visible de la alta dirección es crucial para la finalización exitosa del proyecto y la posterior transición a la operación SGSI.

Además de la asistencia, la guía de implementación también incluye referencias a otras normas, estándares u otras fuentes útiles, que luego se identifican como tales.

2.2 Estructura del capítulo

Cada uno de los capítulos tiene la misma estructura y se divide en las tres secciones siguientes:

Factores de éxito de la práctica
Presentación de, desde el punto de vista de los autores, elementos esenciales. Factores de éxito para el establecimiento y operación de una SGSI según ISO/IEC 27001:2022

Requisitos de documentación
Presentación de los requisitos de documentación, tanto desde el punto de vista normativo como desde el punto de vista práctico.

Referencias
Indicación del apartado relevante al área temática. números de ISO/IEC 27001:2022, así como información fuente adicional, si es necesaria y significativa

2.3 Convenciones

Para una mejor legibilidad, en estas directrices se utiliza el masculino genérico. A menos que se indique lo contrario, los términos personales utilizados se refieren a todos los géneros.

Cuando los términos "estándar" o "norma" se utilizan sin más especificaciones, siempre se refieren a la norma ISO/IEC 27001:2022.

El término "capítulo" se utiliza cuando se hace referencia dentro de esta guía, el término "sección" se utiliza cuando se hace referencia a la norma.

El término "Anexo" se utiliza cuando se hace referencia a los Anexos de esta Guía, y los términos "Anexo" o "Anexo A" se utilizan cuando se hace referencia al Anexo A de la norma.

Los términos "organización" y "compañía" se refieren cada uno a la institución o área dentro de la cual se implementa el SGSI.
Los términos se utilizan como sinónimos en la guía.

Las abreviaturas utilizadas en el documento y otras definiciones de términos se pueden encontrar en el glosario del Capítulo 5.

[1] INTELIGENTE : específico, mensurable, aceptado, realista, programado.

3 componentes básicos de un SGSI según ISO/CEI 27001:2022

3.1 Contexto de la Organización

Una de las primeras tareas en la implementación de un SGSI es definir el alcance específico del sistema de gestión y realizar un análisis de requisitos y entorno con respecto a la organización y sus partes interesadas. Al considerar el contexto de la organización, una organización puede garantizar que sus medidas de seguridad de la información se adapten a sus necesidades y circunstancias específicas y, por lo tanto, sean efectivas. Por lo tanto, ISO/IEC 27001 requiere que las organizaciones analicen e incorporen cuidadosamente el contexto de la organización en su planificación e implementación de seguridad de la información.

Determinación del alcance

Según la norma, el alcance debe estar documentado y describe el alcance del SGSI dentro de una empresa, es decir, define los límites y define qué activos (procesos, unidades de negocio, ubicaciones, aplicaciones, etc.) están dentro y cuáles fuera. el alcance.

La identificación del alcance generalmente se realiza con la ayuda de un análisis del entorno y de los requisitos.

El documento de alcance es esencialmente un documento para las partes interesadas del sistema de gestión y debe estar disponible para ellas cuando lo soliciten, ya que esta es la única manera para que las partes interesadas, por ejemplo los clientes, verifiquen si los procesos, infraestructuras, temas o requisitos relevantes. para ellos están cubiertos por el SGSI.

En la práctica, las organizaciones suelen hacer referencia a cualquier Certificados ISO/IEC 27001 al realizar consultas, que son luego, tras una inspección más cercana, a menudo no son relevantes o suficientes para la solicitud, ya que el proceso solicitado no está cubierto por el SGSI o solo está cubierto parcialmente. Por lo tanto, para evitar sorpresas desagradables, además de un certificado, siempre se debe solicitar el documento de alcance o una descripción precisa del alcance.

Otro documento relevante para ilustrar el alcance y El alcance de un SGSI es la normatividad Declaración sobre la aplicabilidad de la norma (Declaración de Aplicabilidad, SoA). El SoA documenta las decisiones justificadas sobre la implementación de las medidas (controles) del Anexo A, es decir, si la medida respectiva se aplica dentro del SGSI o no, incluida la respectiva justificación para la aplicación o no aplicación.

Es habitual que la política de seguridad de la información defina el alcance, al menos de forma aproximada, de la información. está delineado. A diferencia del documento de alcance, la política de seguridad y el SoA son generalmente documentos internos y no están destinados a transmitirse a partes externas.
Sin embargo, se debe prestar atención a la definición exacta del alcance y al contenido del SoA en el contexto de las relaciones con los proveedores de servicios y, si es necesario, de las auditorías de los proveedores de servicios.

Análisis del entorno

El análisis del entorno sirve para integrar el SGSI en el entorno general para el ámbito en cuestión. Además de las interfaces organizativas y técnicas relevantes para el SGSI, también debe describir las condiciones típicas de la industria o ubicación. El entorno interno, por ejemplo, otros sistemas de gestión (ISO 9001:2015, ISO 22301:2019, etc.), interactúa con otros departamentos importantes como gestión de riesgos, recursos humanos, protección de datos, gestión de instalaciones, auditoría y departamento legal, si no forma parte de Se debe considerar el alcance actual, así como el entorno externo, por ejemplo, proveedores importantes y proveedores de servicios, socios estratégicos y, si corresponde, otras organizaciones.

Análisis de requerimientos

Las personas responsables del sistema de gestión necesitan una visión clara de qué partes interesadas existen y qué requisitos tienen para la organización y el sistema de gestión.

Los requisitos de las partes interesadas pueden incluir requisitos legales y oficiales (por ejemplo, RGPD de la UE, UWG, TMG, autoridades reguladoras), pero también obligaciones contractuales, por ejemplo. La propia organización (o posiblemente una organización de mayor rango en la jerarquía) también puede tener poderes de toma de decisiones y/o de dirección, que deben tenerse en cuenta en consecuencia.

Factores de éxito de la práctica.

Dado que definir el alcance es el primer y decisivo paso en el establecimiento y funcionamiento de un SGSI, esta fase debe llevarse a cabo con especial cuidado. Comprender el contexto es la base para todas las acciones posteriores (por ejemplo, estructura y proceso del análisis de riesgos, estructura organizacional, definición de paquetes de trabajo y su priorización, planificación de proyectos) y también es un requisito previo esencial para estimar la viabilidad y el esfuerzo (recursos). , presupuesto, tiempo) para el desarrollo y posterior funcionamiento del SGSI.

En ISO 31000:2018, en el apartado 5.4.1 "Comprensión de la organización y su contexto" se ofrecen listas con las que se puede lograr la integridad de la representación.

El nivel de detalle requerido para definir el alcance generalmente se deriva de los requisitos internos y externos para la seguridad de la información de la organización.

En la práctica, ha resultado útil describir con suficiente detalle en el alcance las áreas significativamente afectadas por el SGSI, ya que esta descripción es una herramienta de control importante y será relevante para las decisiones estratégicas y las votaciones (posteriores).

La identificación de los stakeholders (y sus requisitos) requerida por el apartado 4.2 de la norma. En cualquier caso, debe llevarse a cabo de forma cuidadosa y exhaustiva, porque sólo así se pueden definir objetivos y contenidos claros del SGSI y lograr los mejores beneficios posibles. Ejemplos de partes interesadas son: propietarios, accionistas, consejo de supervisión, comité de empresa, autoridades reguladoras o legisladores, clientes, proveedores o subcontratistas, proveedores de servicios, empleados, etc.

Los planes de negocios, contratos, etc. se pueden utilizar como base para determinar los requisitos internos y externos relevantes. tales como los requisitos de las autoridades supervisoras y los legisladores para los procesos comerciales en cuestión. En la práctica, esto lo suele hacer una función de cumplimiento o de cumplimiento de TI, que puede respaldar la recopilación de requisitos.

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

Alcance del SGSI (Sección 4.3)

Declaración de Aplicabilidad (Sección 6.1.3 d)

Descripción general de todos los requisitos legales, regulatorios y contractuales relevantes, que influyen en la estrategia de seguridad de la información y el SGSI (Sección 18.1)

Descripción general de todas las partes interesadas relevantes para el alcance específico del SGSI.

Además, el siguiente documento se ha consolidado en la práctica como orientado a objetivos:

Acuerdos de interfaz entre el área de SGSI y los departamentos internos que dan soporte al SGSI. áreas (para asegurar que la cooperación con el área interna esté de acuerdo con ISO/IEC 27001:2022 y los requisitos de SI relevantes de la organización). Ejemplo: Convenios de interfaz con el área de RRHH.

Referencias

ISO/IEC 27001:2022 - Secciones 4.3 y 6.1.3

ISO/IEC TR 27023:2015

ISO 22301:2019

ISO 31000:2018

Norma ISO 9001:2015

3.2 Liderazgo y Compromiso

Un SGSI exitoso se implementa utilizando un enfoque de arriba hacia abajo y establece un vínculo entre los objetivos comerciales y la seguridad de la información al tener en cuenta los requisitos de las partes interesadas, por un lado, y reducir los riesgos que afectan los procesos operativos del negocio a un nivel apropiado utilizando medidas efectivas. en el otro.

Para cumplir esta tarea es necesario conocer los objetivos y requisitos del negocio y crear las condiciones organizativas adecuadas, como la introducción o adaptación de procesos de gestión de riesgos en la organización.

A más tardar, cuando se trata de la necesaria adaptación de los procesos de toda la organización, el liderazgo (en el sentido de fijar una dirección y una visión), la aprobación y el apoyo (liderazgo y compromiso) por parte de la dirección son inevitables, ya que los procesos introducidos por la De lo contrario, el sistema de gestión no tendrá carácter vinculante y, por tanto, no tendrá valor.

Ud. puede no ser aceptado. Por lo tanto, los directivos son responsables de esto, lo que también se denomina "tono desde arriba" en vista de su función de modelo a seguir.

La norma requiere correctamente y explícitamente que la alta dirección debe asumir de manera demostrable la responsabilidad general de la seguridad de la información dentro de la organización. También debe comunicar la importancia de un SGSI eficaz y el cumplimiento de los requisitos del SGSI a los empleados interesados. Esto normalmente se hace a través del llamado Infor-

Directriz de seguridad de la información (cf. Política de seguridad de la información en el capítulo 3.4 Política de SI) , así como a través de una política de usuario.

Bajo el título de gobernanza (TI) y en relación con la responsabilidad de la junta ejecutiva
En el caso de las estrategias, los órganos de supervisión pertinentes también exigen cada vez más la asunción demostrable de una responsabilidad general, especialmente en los ámbitos regulados. autoridades1.

Factores de éxito de la práctica.

Definición "Alta Dirección La alta dirección" se refiere al nivel directivo que es responsable de controlar la organización a proteger por el SGSI y decide sobre el despliegue de los recursos.

En el caso de grandes empresas, el estándar no es el más alto
Definir necesariamente "el nivel de alta dirección de la dirección de todo el grupo empresarial (por ejemplo, el consejo de administración del grupo). También puede ser una dirección local o una dirección de división que sea responsable del SGSI.
El alcance concreto del SGSI respectivo es siempre decisivo.[2]

En el caso de auditorías de certificación externas, es posible que, no obstante, el organismo de certificación requiera la inclusión de la

Por lo tanto, el organismo de certificación debe aclarar este punto de antemano con el organismo de certificación cuando busque la certificación. Por este motivo, tiene sentido aclarar este punto con antelación con el organismo de certificación si se pretende obtener la certificación.

Tareas/responsabilidades "Alta dirección

ISO/IEC 27001:2022 exige que la alta dirección dé un ejemplo claro con respecto a la seguridad de la información. En la práctica, esto incluye no sólo un compromiso visible con la seguridad de la información, sino también la

cumplimiento ejemplar de los requisitos de seguridad de la información,

provisión de recursos suficiente y rastreable,

Exigir al otro una función de modelo a seguir niveles de gestión,

Abordar y responder consistentemente a las no conformidades,

Compromiso propio con la mejora continua.

Las tareas centrales de la alta dirección en el contexto del SGSI son:

Asunción de la responsabilidad global de la información seguridad

Definición de la estrategia de seguridad de la información y los objetivos concretos de SI (ver capítulo 3.3 Objetivos de SI)

Definición de criterios y principios de decisión para la evaluación y tratamiento de riesgos e introducción de procesos de entrada (ver capítulo 3.6 Gestión de riesgos).

Integración de los requisitos de seguridad de la información en procesos de negocio y modelos de gestión de proyectos (ver Capítulo 3.6 Gestión de riesgos)

Realizar revisiones periódicas de la dirección (superior) del SGSI (consulte el capítulo 3.14 Mejora continua)

Provisión de los recursos humanos y financieros necesarios para establecer el SGSI y para implementar la estrategia de seguridad de la información.

Ser visible en eventos o medidas de concientización (p. ej., videos principales mensaje).

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

La Sección 9.3 "Revisión por la dirección" requiere documentación de la revisión del SGSI por parte de la alta dirección. gestión, incluyendo decisiones relativas a cambios y mejoras al SGSI. Estas pueden registrarse como medidas en el plan de tratamiento de riesgos.

En la revisión de la gestión, los resultados, como las decisiones sobre oportunidades de mejora continua, deben ser Los datos se almacenan como información documentada.

Además, los siguientes documentos han demostrado ser útiles en la práctica:

Derivación y evaluación de los riesgos actuales a partir de desviaciones identificadas entre los objetivos estratégicos de SI y el grado de consecución de los objetivos, idealmente como un plan de gestión de riesgos.

Evidencias para informar a la alta dirección, por ejemplo en forma de presentaciones, protocolos o re puertos

1 Circular 10/2021 (BA) - Requisitos Mínimos para la Gestión de Riesgos - MaRisk (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/ Rundschreiben/2021/rs_1021_MaRisk_BA.html).

2 Ver capítulo 3.1 Contexto de la Organización e ISO/IEC 27000:2018, Cláusula 3.75.

Informar sobre el estado de implementación, incluido su control de efectividad para las medidas definidas (especialmente cuando están vencidas) de auditorías, tratamiento de riesgos, incidentes o mejora continua.

Nota: En el contexto de la responsabilidad de gestión, existen varias posibilidades de documentación. Los ejemplos enumerados anteriormente son sugerencias de posibles registros que ayudan a garantizar la trazabilidad de los informes y la toma de decisiones. Cada organización debe encontrar la forma y frecuencia de documentación adecuada para ella.

Referencias

ISO/IEC 27001:2022 - Secciones 5.1, 9.1 y 9.3, 5.36

3.3 Objetivos del SI

El SGSI en su conjunto contribuye a proteger y mantener la confidencialidad, integridad y disponibilidad requeridas de los procesos de negocio y de la información procesada en los mismos. Los objetivos de negocio definidos por la dirección de la empresa sirven como base para el diseño o definición de los objetivos de TI y objetivos específicos de seguridad de la información (objetivos SI) y las medidas resultantes.

Factores de éxito de la práctica.

Dado que los objetivos y principios del SGSI deben derivarse de los objetivos comerciales generales de la organización, el incumplimiento de los objetivos de SI puede tener un impacto directo en el logro de los objetivos comerciales. Por lo tanto, es esencial definir objetivos de SI apropiados y mensurables y su implementación.

Los objetivos de SI deben ser coherentes con el contenido de los objetivos esenciales de protección (confidencialidad, integridad, ver-La política de SI se basa en la política de SI (ver también el capítulo 3.4 Política de SI).

Los objetivos de SI siempre deben estar alineados con los objetivos corporativos generales y deben revisarse periódicamente con respecto a su logro. ser revisados para asegurar que estén actualizados y sean apropiados. Esto hace posible integrar los requisitos de seguridad de la información en las actividades operativas del negocio de tal manera que no necesariamente se perciban como un gasto adicional (o posiblemente incluso disruptivo) y el tema de la seguridad de la información se convierta en una parte integral de los procesos de trabajo.

Los requisitos de seguridad de la empresa y los resultados de riesgo. Las evaluaciones (ver Capítulo 3.6 Gestión de Riesgos) proporcionan una base adicional para la selección y definición de los objetivos de SI.

Al planificar los objetivos de SI, se debe determinar cómo se van a lograr estos objetivos. Esto también incluye la definición de los requisitos previos para la realización. Además de las actividades esenciales para alcanzar los objetivos, se deben definir los recursos y responsabilidades necesarios, así como un calendario y un procedimiento para evaluar la realización. En la práctica, esto suele hacerse mediante referencia directa a proyectos planificados y en curso. Es fundamental que los requisitos no funcionales (y en la mayoría de los casos los requisitos de seguridad no son funcionales) se tengan en cuenta desde el principio y se integren tanto en la planificación de proyectos, productos y sistemas como en la formación posterior de los empleados (" entrenamiento de conciencia").

Al formular objetivos de SI, se debe tener cuidado para garantizar que solo se describan objetivos/metas genuinos y de largo plazo y que no se describan medidas técnicas/ organizativas operativas necesarias para el logro de los objetivos.

Como ocurre con cualquier formulación de objetivos, es aconsejable formular 3 objetivos "inteligentes" al establecer objetivos de SI. y coordinarlos con los niveles pertinentes de responsabilidad.

El grado de consecución de los objetivos de seguridad de la información debe ser mensurable. Lo ideal es que la medición se pueda realizar mediante KPI definidos de antemano. El apoyo práctico para esta tarea lo proporciona, por ejemplo, la guía práctica de ISACA "Evaluación del desempeño de un SGSI utilizando indicadores clave" o COBIT 2019 Focus Area: Information Seguridad.

La formulación de objetivos significativamente mensurables y la implementación de las medidas necesarias para alcanzarlos son, en la práctica, una tarea bastante desafiante. Por lo tanto, es aconsejable, especialmente al comienzo de la implementación de un SGSI, definir inicialmente un pequeño número de objetivos de SGSI que sean significativos para la organización respectiva y equilibrados en términos de esfuerzo y beneficios de implementación.

La mensurabilidad de los objetivos de SI "sólo" está respaldada por el estándar si existe una implementación práctica correspondiente. se requiere viabilidad. En la práctica, se entiende generalmente que "si es posible" es "más suave" que "si es posible". Esto no significa que las mediciones no sean un requisito normativo, sino que la viabilidad de realizar mediciones siempre debe incluirse en el diseño (ver Sección 6.2 b).

3 SMART: específico, mensurable, aceptado, realista, programado.

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

- Se debe mantener la documentación de los objetivos de SI.

Además, en la práctica se han demostrado que los siguientes puntos están orientados a objetivos:

- Los objetivos de SI suelen ser parte de las directrices de SI y también pueden formularse como parte de la estrategia de SI.
- Un plan de implementación que describa cómo se lograrán los objetivos de SI a través de proyectos específicos.
- El grado de implementación de los objetivos de SI se muestra mediante cifras clave (consulte el capítulo 3.7 Monitoreo de desempeño/ riesgo/cumplimiento).

Referencias

ISO/IEC 27001:2022 - Sección 6.2 Área de enfoque de COBIT 2019: Seguridad de la información

ISACA Capítulo Alemania eV, Guía práctica "Evaluación del desempeño de un SGSI a través de indicadores clave".

3.4 Política de SI

La (alta) dirección responsable de la organización debe definir una política de seguridad de la información que documente la decisión estratégica de la organización de implementar un SGSI y, en particular, incluya un compromiso de cumplir con los requisitos de seguridad de la información y un compromiso de mejorar continuamente el SGSI.

La directriz debe ser adecuada para el propósito de la organización y debe abarcar los principios y objetivos previstos del SGSI, así como las metas de seguridad de la información de la organización en general.

Factores de éxito de la práctica.

La directriz representa una herramienta importante para la organización, a través de la cual la dirección responsable puede comunicar la importancia tanto de un SGSI eficaz como del cumplimiento de los requisitos del SGSI. Además, la directriz establece los objetivos estratégicos y tácticos clave que se deben alcanzar con la ayuda del SGSI. Idealmente, también se describen las implicaciones y requisitos para el personal y las unidades de negocio respectivas dentro del alcance.

Además, la dirección responsable debe describir el SGSI establecido, incluidas sus funciones y responsabilidades, con suficiente brevedad en la directriz. Se deben tener en cuenta los siguientes aspectos:

- La directriz IS debe ser aprobada por el nivel más alto de gestión (alta dirección) y presentada al responsable. El Consejo de Supervisión es responsable de la preparación de los estados financieros consolidados.
- La directriz SI debe estar disponible como información documentada y debe estar sujeta a una gestión documental comprensible. sujeto al riesgo de cambios en el mercado.
- La directriz de SI puede incluir una referencia a los objetivos de la empresa y otros objetivos específicos de un tema relevante, como por ejemplo los objetivos de TI.
- El lenguaje de la directriz de SI debe ser coherente con las prácticas de la empresa y reflejar la importancia de los documentos de la mejor manera posible.
- En el marco de la sensibilización de los empleados, se debe garantizar que todos los empleados interesados en el ámbito conozcan las directrices de SI. Debe comunicarse a los empleados afectados y, si es necesario, también ponerse a disposición de las partes interesadas (ver capítulo 3.10 Competencia).
- Para lograr los objetivos en la práctica, es importante que cada empleado sea consciente de sus necesidades individuales. ver-
  Los empleados son conscientes de su responsabilidad e implicación personal en los procesos en el contexto de la seguridad de la información y están familiarizados con los requisitos concretos asociados (que se derivan de la Directriz IS y se reflejan, por ejemplo, en directrices e instrucciones de trabajo específicas de cada tema). .
- La directriz de SI no debe mezclarse con documentación y requisitos de implementación más extensos. como por ejemplo el contenido de conceptos o manuales de seguridad.
  Sin embargo, es muy posible que se haga referencia a las directrices (u otros documentos pertinentes de alto nivel del SGSI) en dichos documentos "descendentes" para lograr coherencia en la "cadena de requisitos".
- Dependiendo del enfoque elegido para el SGSI y de la estructura existente y la organización del trabajo dentro de una organización, el SGSI puede ser una organización,
  puede ser útil utilizar la directriz de SI como La estrategia de SI debe diseñarse como una "poderosa", es decir documento completo y global sobre el tema de la seguridad de la información o, si es necesario, como un "ancla" o "punto de partida" específico para el tema, que a su vez se completa con documentos más detallados. En ambos casos, es importante utilizar una redacción y un alcance apropiados para los objetivos de la estrategia de SI.
- Si la documentación del SGSI se divide en un documento principal y documentos más detallados, un desglose de

También puede resultar útil dividir la responsabilidad en favor de una gestión flexible del cambio. Por ejemplo, la directriz de SI es responsabilidad de la alta dirección, mientras que los documentos detallados pueden ser respondidos por el responsable de seguridad de la información o los departamentos responsables.

Aunque una gran cantidad de plantillas y módulos de texto se puede acceder en la búsqueda adecuada, se recomienda crear la guía de SI como un documento nuevo/propio que cubra los requisitos individuales de la organización de la mejor manera posible. Las plantillas pueden proporcionar ideas y sugerencias para estructurar y posible contenido. Sin embargo, para el éxito de la implementación y la identificación de los empleados con el tema de la seguridad de la información es crucial que la directriz esté visiblemente orientada a los objetivos de la empresa y de los especialistas subordinados y que las declaraciones centrales permitan al lector reconocer una referencia a los organización en cuestión.

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

Directriz de seguridad de la información (ver sección 5.2 e)

Además, los siguientes documentos han demostrado ser útiles en la práctica:

Directrices de seguridad de la información por temas específicos (ver Anexo 5.1)

Documentos y organigramas adjuntos, por ejemplo para aclarar la estructura organizativa en el Contexto Seguridad de la información (si no está incluida en la directriz)

Referencias

ISO/IEC 27001:2022 - Sección 5.2

3.5 Roles, Responsabilidades y Competencias

Según la sección 5.3 de ISO/IEC 27001:2022, la organización debe definir los roles necesarios para un SGSI eficaz y sus responsabilidades para establecer, mantener y mejorar continuamente el SGSI. En particular, se deben identificar y poner a disposición los recursos necesarios (ver ISO/IEC 27001:2022, sección 7.1).

En este contexto, la dirección también debe asignar y comunicar las responsabilidades y autoridades para las tareas relevantes para la seguridad de la información. Se debe tener cuidado para garantizar que las responsabilidades de los roles estén claramente reguladas y definidas. y se evita cualquier conflicto de intereses (por ejemplo, sin la ayuda de un RACI[4] SoD[5] o matriz).

Factores de éxito de la práctica.

Concretización de los roles dentro de la organización SGSI Como mínimo, se debe establecer el rol de un oficial de seguridad de la información (ISO) o director de seguridad de la información (CISO), aunque el requisito descrito en el estándar se refiere a todas las responsabilidades y autoridades relevantes en materia de información. seguridad (ver Sección 7.2 a). Además, las funciones del propietario del riesgo y del propietario de los activos deben definirse y establecerse dentro del SGSI.[6]

En el contexto de la seguridad de la información, por supuesto, se deben definir y describir otras funciones, como administradores de seguridad, auditores internos, etc.

La descripción del rol del CISO/ISB también debe incluir las competencias necesarias (experiencia, formación, escolarización, etc.).

Para este fin se debe utilizar la descripción del puesto o una carta de nombramiento en la que se detallen las tareas asignadas. Para ello, es aconsejable consultar una descripción del puesto o una carta de nombramiento en la que se detallen las tareas asignadas.

Conflictos de intereses que deben evitarse en la práctica a nivel todos los costos:

- Oficial de Seguridad de la Información (ISB o CISO[7]) y TI Gerente/CIO[8]
- Delegado de Protección de Datos (DPO) y Responsable de TI/CIO
- Auditor interno de SGSI y administrador de TI

Los dos roles de ISB/CISO y DPO pueden, bajo ciertas condiciones, también usarse en la práctica en unión personal y son ejercidos por un solo empleado. Sin embargo, esta combinación también está asociada con ciertos conflictos potenciales (inevitables). Por ejemplo, el DPD está protegido por la ley con respecto a sus acciones y está sujeto a un deber de confidencialidad. Sin embargo, no puede transferir automáticamente esta protección o este deber al papel del CISO. También existe una discusión legal sobre la obligación de garante del CISO o del responsable de cumplimiento, etc. Esto no se aplica al DPO. Esto no se aplica al DPO. Por tanto, una unión personal de estas tareas puede, en el peor de los casos, dar lugar a un importante conflicto de intereses.

4 RACI: Responsable (responsabilidad de implementación), Responsable (responsabilidad general), Consultado (experiencia profesional), Ser informado (derecho a la información), ver también glosario.

5 SoD: Segregación de funciones, ver también glosario.

6 Ver apartado 6.1.2 c y Control A.5.9 “Propiedad de activos”.

7 CISO: Director de Seguridad de la Información.

8 CIO: Director de Información.

conflicto y, por lo tanto, deben analizarse y sopesarse en detalle.

Dependiendo del tamaño y las actividades comerciales de la organización, así como del alcance concreto del SGSI elegido. La combinación de las funciones de DPO y CISO también puede dar lugar a sinergias que no existirían si las funciones estuvieran separadas (por ejemplo, con respecto a flujo de información, visión general y diseño de medidas). Pero, por un lado, siempre hay que comprobar atentamente si el candidato en cuestión tiene las competencias profesionales y personales necesarias y si realmente puede afrontar la carga de trabajo en ambos ámbitos. Por otra parte, como ya se ha explicado, hay que comprobar detalladamente si los conflictos de intereses que puedan surgir son "manejables" y no conducirían a desventajas graves en el desempeño de (una de) las dos funciones.

Otro ejemplo de posibles conflictos de intereses entre el DPO y el CISO se relaciona con la recopilación y capacitación de los DPO. Evaluación de tráfico y datos de registro. Si bien el DPO normalmente solo permitirá la recopilación y el análisis de datos personales o relacionados bajo condiciones muy específicas y para un propósito específico, al CISO le gustaría hacer el mejor uso posible de las medidas técnicas para aumentar el nivel de seguridad (protección preventiva) y para detectar y evaluar posibles daños (protección de detectives).

La organización debe garantizar que todas las personas tengan las competencias requeridas a través de la educación, formación o experiencia adecuadas. La organización debe poder acreditar el logro de las competencias, p. ej. mediante los correspondientes certificados de formación complementaria en el expediente personal (historial de formación) del respectivo empleado (ver apartado 7.2 d).

ISO/IEC 27001:2022 proporciona un marco aproximado para la organización de la seguridad de las empresas (por ejemplo, alta dirección, propietario del riesgo, auditor), pero no describe en detalle cómo se deben distribuir las funciones y responsabilidades en la práctica.

Ha resultado ventajoso seleccionar exactamente a los empleados adecuados para desempeñar las funciones requeridas dentro del SGSI. El CISO/ISB debe seleccionar empleados que ya tengan una afinidad "innata" por el tema de la seguridad de la información o que tengan suficiente motivación intrínseca. Además de Conocimientos especializados, el CISO/ISB en particular requiere habilidades sociales, comunicación orientada a objetivos, integridad, capacidad de convencer a los demás y una gestión exitosa de conflictos. Muchas de las tareas que surgen en relación con la implementación de la estrategia de seguridad de la información y (a veces Las consecuencias de las medidas, incluidas las desagradables o impopulares, no pueden resolverse satisfactoriamente de otro modo.

Además, una de las características más importantes de un CISO/ISB es la capacidad de distinguir entre objetivos comerciales y procesos comerciales. y los requisitos de cumplimiento, por un lado, y los riesgos y medidas de seguridad de la información, por el otro. para poder "traducir".

El rol del CISO/ISB requiere competencias de liderazgo y debe ser equivalente en la empresa al estatus de gerencia. estar en pie de igualdad con los demás empleados.

Se pueden encontrar ejemplos de estructuras organizativas en materia de seguridad de la información, entre otros, en " COBIT 2019 Área de enfoque: Seguridad de la información" y el estándar BSI 200-2 - IT-Grundschutz-Methodik. Aquí se describen, entre otras cosas, las funciones y responsabilidades del CISO, el comité de control, el director de seguridad de la información, las funciones en la gestión de riesgos proceso y los propietarios de los datos funcionales.

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

- Prueba de competencia (apartado 7.2 d)

Además, los siguientes documentos se han consolidado en la práctica como orientados a objetivos:

- Descripciones de funciones, incluidos los informes necesarios a la alta dirección (ver sección 5.3 b)
- Perfiles de puesto/cartas de nombramiento
- Diseño de la cooperación estratégica y operativa entre el DPO, QMB y CISO.

Referencias

ISO/IEC 27001:2022 - Secciones 5.3, 7.1 y 7.2 COBIT

Área de enfoque de 2019: Seguridad de la información

Estándar BSI 200-2 - Metodología IT-Grundschutz

3.6 Gestión de riesgos9

Un riesgo de SI describe la posibilidad de que una amenaza específica aproveche las vulnerabilidades de un sistema de información, un sistema de aplicación o (partes de) la infraestructura de TI, lo que constituye una violación de la seguridad de la información (confidencialidad, integridad o disponibilidad) y, por lo tanto, conduce a una impacto negativo en, entre otras cosas, las operaciones comerciales.

9 Este capítulo se refiere exclusivamente a la gestión de riesgos en el contexto de seguridad de información.

Esto afecta el desempeño financiero, los objetivos financieros, la reputación o el fondo de comercio del Grupo.

El riesgo de SI generalmente puede surgir de diversas fuentes, como errores en la configuración o mantenimiento de los sistemas, errores humanos, ataques cibernéticos, desastres naturales u otros eventos imprevisibles.

La gestión de riesgos de SI es un aspecto importante del gobierno corporativo en general y de la gestión de SI en particular. La gestión de riesgos de SI es un proceso global dentro de un sistema de gestión que, en el caso de un SGSI, contribuye al registro sistemático, la evaluación y la presentación transparente de los riesgos en el contexto de la seguridad de la información y tiene como objetivo garantizar un nivel aceptable de seguridad o una mejora sostenible del nivel de seguridad existente dentro del alcance del SGSI.

El objetivo es reducir los riesgos identificados y evitar daños intolerables a la organización considerada o reducirlos hasta tal punto que se alcance un nivel aceptable para la empresa. Lo que se considera aceptable debe ser decidido por los respectivos responsables en el contexto respectivo, a veces también en la situación respectiva. Además, está la decisión sobre cómo abordar los riesgos identificados y evaluados.

En resumen: los daños intolerables a la organización en cuestión deben evitarse o reducirse a un nivel aceptable para la empresa.

Los objetivos específicos de la gestión de riesgos en el contexto de la seguridad de la información son:

- Identificación temprana y remediación de riesgos de seguridad de la información.
- Establecimiento de métodos uniformes de evaluación de los riesgos identificados.
- Asignación clara de responsabilidades al tratar con riesgos
- Documentación estandarizada y clara de los riesgos, incluidas sus evaluaciones.
- Manejo eficiente de riesgos10

10 Por ejemplo, adaptando la estrategia de seguridad o implementando medidas medidas de seguridad.

Conceptos básicos de la gestión y el procedimiento de riesgos de TI.

¿Cómo surgen los riesgos?

Los riesgos en el contexto de la seguridad de la información surgen inherentes al uso de sistemas de TI y tecnologías (emergentes), entre otras cosas. Dado que la seguridad de la información siempre debe verse de manera integral según ISO/IEC 27001, existen otras fuentes de riesgo que (pueden) afectar la información/datos de una organización y surgen, por ejemplo, de los siguientes factores que influyen:

- Intercambio de datos dentro y fuera de la organización
- Adaptación de la organización interna y la cooperación (especialmente en empresas más grandes)
- Sistemas y aplicaciones (existentes) que no se pueden actualizar ni reemplazar
- Cooperación con socios externos/proveedores de servicios
- Acceso remoto a la red corporativa (por ejemplo, desde el socio empresas y fabricantes)
- Fenómenos naturales/desastres naturales
- Sabotaje y delitos de cuello blanco
- "Factor de riesgo humano" (p. ej., ingeniería social)
- Uso de nuevos tipos de sistemas y tecnologías (p. ej., nube y dispositivos móviles)
- Entrar en nuevos mercados (geográficamente y por producto)

Aunque se deben considerar todas las fuentes y factores que influyen, cada organización debe definir sus propias prioridades de gestión de riesgos en función de sus actividades comerciales y los requisitos internos y externos resultantes.

Una gestión de riesgos eficiente sólo puede tener lugar si primero se Se debe analizar la exposición al riesgo y el entorno de la respectiva actividad empresarial. Para saber dónde "buscar" los riesgos, es necesario saber qué áreas de riesgo están presentes en general y evaluarlas. Un buen punto de partida para esto es, por ejemplo, un mapa de procesos o un análisis del entorno (ver capítulo 3.1 Contexto de la organización).

Para apoyar la formulación y diseño del proceso de evaluación de riesgos, por ejemplo, se puede consultar la norma ISO/IEC 27005. Además de la sección principal bien desarrollada, los apéndices en particular también contienen información valiosa sobre la implementación.

Detección y evaluación de riesgos

Antes de que pueda comenzar la identificación y el tratamiento concretos de los riesgos, tanto el proceso de evaluación de riesgos formulado generalmente como los criterios de aceptación de riesgos para toda la empresa o para todo el SGSI deben definirse en coordinación con el nivel más alto de gestión (alta dirección) (en la medida en que estos no puede o no debe adoptarse desde un sistema de gestión de riesgos de nivel superior).11

El proceso de evaluación de riesgos incluye lo siguiente:

- Métodos de identificación de riesgos
- Criterios para la evaluación de riesgos
- Criterios de aceptación de riesgos

Aplicar métodos para la identificación de riesgos.

La identificación de riesgos relevantes generalmente requiere que se consideren y reúnan las opiniones de múltiples partes interesadas o departamentos. Se pueden utilizar varias técnicas y métodos como herramientas, tales como:12

- Entrevistas
- Análisis de escenarios/análisis de hipótesis
- Lluvia de ideas
- Análisis de impacto empresarial (BIA)
- Listas de verificación
- Método Delphi
- Modelo de amenazas STRIDE (Microsoft)

Ejemplo

Durante el análisis de riesgos de una nueva aplicación web de comercio electrónico, las personas involucradas plantean diferentes aspectos de riesgo para debatir. El desarrollador de software ve algunas debilidades en el lenguaje de programación seleccionado que, por ejemplo, pueden contrarrestarse mediante revisiones (automáticas) del código.
El administrador de TI expresa su preocupación por el mantenimiento planificado de la aplicación por parte de proveedores de servicios externos y los derechos de acceso necesarios para ello a la red empresarial. El delegado de protección de datos plantea la cuestión de la protección adecuada de los datos personales y solicita una lista de las medidas técnicas y organizativas para cumplir con los requisitos del artículo 32 (1) del RGPD UE. El oficial de seguridad de la información a su vez reconoce el alcance del proyecto (impacto en caso de restricciones de disponibilidad o fuga de datos) y, por lo tanto, requiere una prueba de penetración antes de entrar en funcionamiento.

Este ejemplo no está tomado de un libro de texto. Sin embargo, esto demuestra que también se puede realizar un análisis de riesgos con la formulación directa de (contra)medidas que vayan de la mano.

Si el proceso de gestión de riesgos es muy dinámico, la formulación directa de (contra)medidas puede ser un El proceso de gestión de riesgos también se puede utilizar para iniciar actividades de gestión de riesgos de manera oportuna. Si, por el contrario, el proceso de gestión de riesgos se lleva a cabo con una dinámica baja, esto también se puede evitar deliberadamente, para poder completar primero el análisis de forma completa y luego definir otras actividades "en el tiempo libre".

Con un proceso de gestión de riesgos "compacto" o "dinámico", que pueda llevarse rápidamente a la discusión y Si no se seleccionan las opciones de tratamiento, existe el riesgo de que el proceso en su conjunto tienda a ser reactivo y centrado en medidas. , y que, como resultado, el análisis de riesgos puede descuidarse.

Por lo tanto, dependiendo del tamaño y alcance de una organización o de un proyecto específico, ¡el enfoque nete más adecuado para elegir!

Definir criterios para evaluar los riesgos.

Los criterios para evaluar los riesgos deben formularse de tal manera que puedan utilizarse para la mayor variación posible de tipos o categorías de riesgo. El uso de un modelo puntual o de un catálogo de parámetros cualitativos queda en manos del diseño específico del proceso de gestión de riesgos.

Desde un punto de vista práctico, es aconsejable, además de los criterios clásicos (como requisitos de protección de confidencialidad/integridad/disponibilidad, procesos de negocio soportados, número de usuarios) proporcionar un conjunto de preguntas adaptadas al negocio de la organización, que se puede complementar individualmente por caso de uso.

La evaluación de la probabilidad de que ocurra (consulte el paso 2 "Análisis de riesgos" a continuación) es en la práctica bastante desafiante. Aquí es importante que, además de "mirar hacia atrás" (valores empíricos, acontecimientos comparables en otras organizaciones, cifras clave, estadísticas, etc.), también es esencial "mirar hacia adelante" para estar capaz de tener en cuenta hallazgos y desarrollos previamente "desconocidos" que pueden estar ya en el horizonte (por ejemplo, la aparición de nuevas tecnologías).

11 En ISO 31000:2018, estas actividades se describen en el apartado 6 "Proceso".

12 Véase también IEC 31010:2019.

En otras palabras: "En la gestión de riesgos, el éxito depende de los preparativos realizados.

Establecer criterios de aceptación de riesgos

La definición de criterios de aceptación de riesgos es una tarea central en el proceso de gestión de riesgos, porque es la única manera de lograr el beneficio total para la organización de no tener que tratar "por igual" todos los riesgos identificados y evaluados en términos de costos y recursos.

Los criterios de aceptación de riesgos pueden tomar la forma de niveles de aceptabilidad dependiendo del daño potencial cualitativo y/o cuantitativo (por ejemplo, incumplimiento, daño financiero, daño a la reputación, deterioro del cumplimiento de la tarea).

Los criterios de aceptación de riesgos pueden incluir múltiples niveles de umbral. Cada nivel de umbral puede vincularse a un nivel jerárquico/ de gestión específico, de modo que la aceptación de riesgos por encima de un determinado nivel también sea exclusiva de los gestores designados dentro de este nivel.

Para una mejor comparabilidad, los niveles de estimación cualitativa se pueden convertir en montos cuantitativos (financieros). estar en red. Sin embargo, esto normalmente sólo es posible en estrecha proximidad.

Puede tener sentido, especialmente para las pequeñas y medianas empresas, utilizar el proceso de evaluación de riesgos con un modelo simplificado y luego desarrollarlo de forma iterativa. Por ejemplo, en un primer paso, los riesgos se pueden recopilar y evaluar inicialmente junto con los expertos en la materia de los departamentos de TI y de los departamentos comerciales, incluso sin un modelo completamente elaborado. Los criterios de aceptación de riesgos pueden derivarse gradualmente de los resultados y convertirse en criterios formales en una fase posterior, tras su aceptación por parte de la dirección de la empresa.

A la hora de definir los criterios de aceptación del riesgo, es necesario proceder con prudencia y previsión para garantizar que, por un lado, el apetito de riesgo15 de la empresa (ni demasiado alto ni demasiado bajo) y al mismo tiempo asegurar la eficiencia y eficacia del SGSI minimizando los riesgos. pueden identificarse "en todos los ámbitos" y tratarse de forma coherente según su evaluación y, por ejemplo, de acuerdo con los requisitos legales o reglamentarios (no se puede dar prioridad a todos los riesgos).

Un sistema de gestión de riesgos verdaderamente integral que cubra todos los riesgos de la consolidación en cualquier momento. En la práctica, la identificación y análisis detallado del texto de seguridad de la información en todas las áreas de la empresa y en todos los procesos es un gran desafío.

Orientación a un proceso de gestión de riesgos establecido

Una vez definida la evaluación de riesgos, siguen los pasos del proceso de gestión de riesgos, cada uno de los cuales debe realizarse de forma iterativa. Seguir un proceso establecido sirve a la transparencia y la trazabilidad y hace más fiables los resultados de todo el proceso. ISO 31000 se centra en los siguientes pasos (ver Figura 3):

1. Identificación de riesgos
2. Análisis de riesgos
3. Evaluación/valoración de riesgos
4. Tratamiento de riesgos

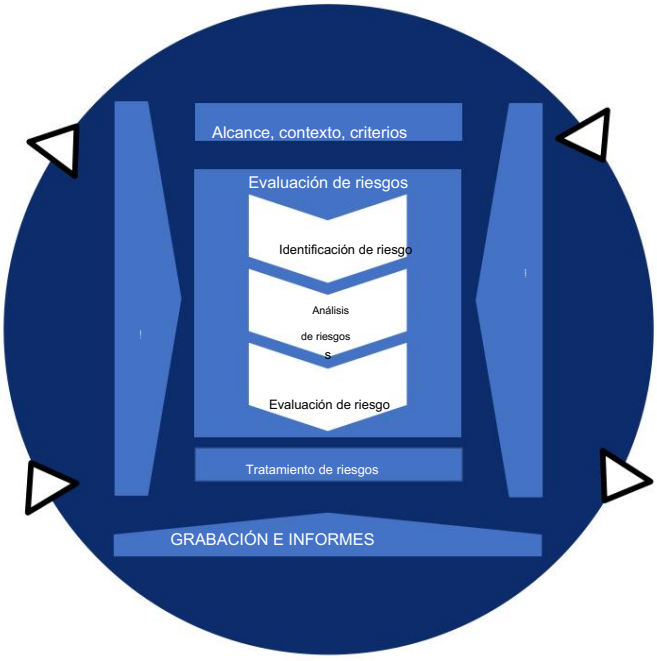


Figura 3: Proceso de gestión de riesgos según ISO 3100016

Paso 1: Identificación de riesgos

La identificación de riesgos siempre se basa en información dentro del alcance del SGSI (ver Sección 6.1.2 c).

13 Por ejemplo, a través de APT o vulnerabilidades de día cero.

14 Adaptado de Confucio, filósofo chino, *551 a.C. †479 a.C.

15 Cuanto mayor sea el apetito por el riesgo, más margen de maniobra y Las oportunidades generalmente están disponibles.

16 Véase ISO 31000:2018.

La identificación de riesgos específicos se puede derivar de los siguientes escenarios, por ejemplo:

Análisis de riesgos
- Para procesos, aplicaciones y procesos críticos para el negocio.
  Para los procesos y sistemas en cuestión se llevan a cabo análisis y evaluaciones de riesgos explícitos, con ayuda de los cuales se pueden hacer declaraciones claras sobre la situación de riesgo y la exposición al riesgo de los procesos o aplicaciones/sistemas en cuestión.
- Dentro de la gestión de proyectos, se deberían incluir como elemento obligatorio los análisis de riesgos (con un alcance adaptado en cada caso).

Auditorías
- Las auditorías realizadas muestran que se están mejorando los estados de seguridad.
  El riesgo de que los responsables o los sistemas no cumplan o no cumplan suficientemente las normas y las mejores prácticas conocidas.
- El requisito previo para esto es, por supuesto, que también se lleven a cabo auditorías (ver capítulo 3.12 Auditoría interna) y que el proceso de auditoría incluya un procedimiento claro para el manejo de los resultados de la auditoría (documentación de los resultados, transferencia de los resultados al auditado, etc.). .).

Operacional
- A través de hallazgos en el contexto de la operación "normal".
  Durante el curso de la operación en curso, pueden salir a la luz nuevos riesgos previamente desconocidos, que deben informarse (con prontitud) al equipo de gestión de riesgos o al empleado, según el proceso de gestión de riesgos seleccionado.

Incidentes de seguridad
- Por incidentes de seguridad (sin importar
  La definición de "incidente de seguridad") puede, por un lado, identificar riesgos previamente desconocidos que se vuelven visibles como resultado del incidente. Por otro lado, pueden ocurrir riesgos que ya se conocen pero que no se han abordado o aceptado adecuadamente hasta el momento (por ejemplo, mediante la explotación activa de una vulnerabilidad ya conocida por parte de un atacante o mediante la falla de un sistema debido a una insuficiencia de datos). dimensionamiento técnico).

Paso 2: Análisis de riesgos

Al analizar los riesgos identificados, tanto la probabilidad como las posibles consecuencias/consecuencias deben resolverse claramente y presentarse a los tomadores de decisiones de una manera comprensible.

En la formulación lingüística de las consecuencias
Se debe tener cuidado para evitar las consecuencias para la ge-La atención debe centrarse en los procesos y actividades comerciales en lugar de en los detalles técnicos.

Se pueden utilizar matrices de evaluación estandarizadas para el análisis de riesgos, aunque dependiendo de la organización, puede tener sentido utilizar matrices con un número par de columnas (por ejemplo, 4x4). Cuando se utilizan matrices con un número impar de columnas/filas (p. ej. 3x3 o 5x5), existe el riesgo básico de que la decisión recaiga a menudo en "el medio".

Paso 3: Evaluación/valoración de riesgos

La decisión (final) sobre el tratamiento de los riesgos identificados debe recaer en el propietario del riesgo respectivo, ya que él puede evaluar el impacto de la ocurrencia del riesgo y tiene la responsabilidad final de los procesos de negocio afectados por el riesgo. Por regla general, el propietario del riesgo también decide sobre la provisión de recursos (por ejemplo, recursos financieros).

En este punto, queda claro cuán importante es la identificación y definición del propietario del riesgo para la ge-proceso de gestión de riesgos.

En la práctica, el papel de propietario del riesgo debe ser desempeñado por las partes responsables o directivos de la empresa debidamente designados (por ejemplo, consejo de administración, director general, director comercial, director de división, director de departamento o director de grupo). En los proyectos, el director del proyecto suele desempeñar el papel de propietario del riesgo, al menos para los riesgos específicos del proyecto.

Paso 4: tratamiento de riesgos

Los riesgos se manejan de acuerdo al mapa de riesgos de la respectiva organización. En el contexto de la seguridad de la información, los modelos ISO/IEC 2700517 son particularmente adecuados como punto de partida para modelar opciones de tratamiento de riesgos (ver Figura 4).

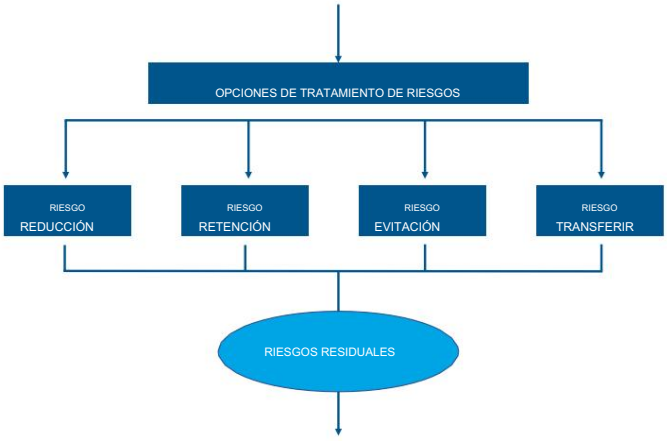


Figura 4: Opciones de tratamiento de riesgos según ISO/IEC 27005

17 Véase, entre otros, la sección 8 de ISO/IEC 27005:2022 - "Información tratamiento de riesgos de seguridad".

En principio, las medidas para el tratamiento de riesgos pueden tomarse de todas las fuentes,
pero deben estar alineadas con el Anexo A del estándar y el SoA del SGSI.

Los riesgos deben asignarse a los propietarios de riesgos asociados. Sin responsables dedicados La falta de
una evaluación "correcta" y de un tratamiento exitoso a largo plazo de los riesgos identificados se hace más difícil por la falta de una evaluación "correcta" y la falta de un tratamiento exitoso y sostenible de los riesgos identificados.

El propietario del riesgo es generalmente la entidad que soporta el impacto económico cuando ocurre el riesgo.
debe. En muchos casos, este es el propietario del proceso, pero dependiendo de la evaluación de impacto y riesgo, también puede ser la alta dirección.

Incluso si los riesgos son causados, por ejemplo, por sistemas informáticos, las respectivas partes interesadas son en última instancia

responsables del riesgo. unidades de negocio los efectos. Esto significa que, aunque los riesgos (de TI) deben ser manejados por el departamento de TI respectivo18 (responsabilidad), la propiedad del riesgo y la responsabilidad general siguen siendo de las unidades de negocios involucradas, que también deben decidir sobre la provisión de recursos (responsabilidad).

La identificación de riesgos y la identificación de los propietarios de los riesgos asociados podrán realizarse de forma separada o en el momento oportuno.
están compensados entre sí.

Documentación e informes

Es aconsejable mantener los resultados de todas las evaluaciones de riesgos en un lugar central, por ejemplo en
forma de un registro de riesgos. Aunque este no es un requisito estándar, ayuda a evaluar y gestionar los riesgos conocidos y su estado de procesamiento.

Dependiendo del tamaño de la organización se requieren herramientas con diferentes funcionalidades (número de riesgos, número de usuarios, concepto de autorización, capacidad de gestión, disponibilidad online, opciones de evaluación, etc.).

La norma no exige un registro central de riesgos.
Sin embargo, sí requiere que el proceso de evaluación de riesgos de

Los riesgos de seguridad de la información conducen a resultados consistentes, válidos y comparables (ver Sección 6.1.2 b). Por tanto, según el tipo y el uso de las herramientas utilizadas, la creación de un registro es una consecuencia lógica.

Dado que el registro de riesgos suele contener información sensible y (estrictamente) confidencial, se debe crear e
implementar un concepto adaptado de derechos y roles para el acceso a los datos.

Factores de éxito de la práctica.

Si ya existe un sistema general de gestión de riesgos en la empresa o en el grupo de empresas. Si la gestión de riesgos no
forma parte de la gestión del riesgo operativo, la gestión del riesgo de SI debe integrarse en ella (por ejemplo, como parte de la gestión del riesgo operativo) o al menos al menos tienen interfaces definidas.

Siempre que sea posible, la gestión de riesgos debe estar orientada a los procesos, en lugar de centrarse en activos
individuales en primer plano. Por un lado, esto garantiza que los riesgos y peligros se formulen de manera orientada a los procesos (de negocio) y, por lo tanto, sean más fácilmente comprendidos por los propietarios del riesgo, es decir, normalmente los propietarios del proceso, y por otro lado, los riesgos potenciales (dañinos).) los impactos se pueden determinar con mucha precisión.

Se debe adaptar y ampliar el modelo de procesos para la implementación de proyectos en la empresa.
El equipo del proyecto debe documentar los resultados del análisis y, según el diseño del sistema de gestión de riesgos, informar sobre los riesgos que superen un valor umbral definido. El equipo del proyecto debe documentar los resultados del análisis y, según el diseño del sistema de gestión de riesgos, se deben informar los riesgos que superen un valor umbral definido. También debe realizarse una aceptación formal del riesgo por parte del respectivo propietario del riesgo y documentarse en caso de que falten medidas o de la aceptación del riesgo.

Incluso en el caso de cambios (extensos) en procesos, aplicaciones o sistemas, se recomienda que el riesgo introduzca análisis
y evaluaciones como parte obligatoria de la gestión de cambios.

Si se identifican no conformidades o vulnerabilidades (por ejemplo, mediante monitoreo u otros procesos operativos
de TI, como gestión de cambios, problemas o incidentes) que no se pueden remediar dentro de las operaciones regulares o no se pueden remediar de manera oportuna, estas deben evaluarse en la gestión de riesgos y tratados por el propietario del riesgo.

Los análisis y evaluaciones de riesgos siempre implican el conocimiento especializado del propietario del proceso respectivo.
Los responsables de SI de la organización pueden brindar apoyo durante la implementación. Los responsables de SI de la organización pueden apoyar la implementación y, por ejemplo, registrar los riesgos en entrevistas o talleres y hacer sugerencias para la evaluación. A

18 Esto también incluye departamentos especializados y departamentos de desarrollo de software, que pueden estar ubicados fuera de TI, tienen sus propios riesgos de TI de los que responder y son responsables de su manejo de riesgos.

Otro método es el uso de cuestionarios/autoevaluaciones. Dependiendo del enfoque elegido, estas autoevaluaciones pueden ser evaluadas adicionalmente por un "segundo par de ojos". Es crucial que exista un proceso formal y pragmático que apoye de manera óptima a los departamentos y gerentes de proyectos en su trabajo y al mismo tiempo garantice que los riesgos se identifiquen en una etapa temprana y se traten adecuadamente.

La norma BSI 200-3 - Análisis de riesgos sobre la base de IT-Grundschutz - proporciona puntos de partida sobre cómo utilizar la información proporcionada en IT-Grundschutz-
Kompendium, se puede realizar un análisis de riesgos para el procesamiento de la información. Sin embargo, la metodología BSI requiere que primero se hayan llevado a cabo los pasos del procedimiento IT-Grundschutz (incluyendo redes de información, análisis estructural, identificación de requisitos de protección, modelado, verificación IT-Grundschutz, análisis de seguridad complementario) antes de que se pueda decidir por Por el contrario, esto no es necesario para qué objetos objetivo se debe realizar un análisis de riesgos y para qué objetos objetivo.

El activo que vale la pena proteger en el contexto de un SGSI siempre sigue siendo la información misma. Es tarea de los respectivos responsables (dirección de la empresa, dirección, propietarios del proceso) evaluar este activo en relación con su "valor" para la empresa o el proceso respectivo. El activo de información se convierte así en el valor de la información. La tarea de los propietarios del riesgo es establecer medidas apropiadas, efectivas y eficientes en todos los pasos del proceso. Los responsables del SGSI son los "vigilantes" de la implementación de la estrategia de seguridad de la información y son responsables, entre otras cosas, de informar verazmente sobre la exposición a riesgos e incidentes de seguridad.

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

- Proceso de evaluación de riesgos (sección 6.1.2)
- Proceso de tratamiento de riesgos (sección 6.1.3)
- Registros y resultados de evaluaciones de riesgos o análisis de riesgos (sección 8.2)
- Registros y resultados de tratamientos de riesgo (Sección 8.3)

Además, los siguientes documentos han demostrado ser útiles en la práctica:

- Registros y resultados de evaluaciones de riesgos y análisis de riesgos.

Referencias

ISO/IEC 27001:2022 - Secciones 6.1, 8.2, 8.3

ISO/CEI 27005:2022

ISO 31000:2018

Área de enfoque de COBIT 2019: Seguridad de la información

Normas BSI 200-2 y 200-3

3.7 Monitoreo de desempeño/riesgo/cumplimiento

En el contexto del SGSI se definen una serie de especificaciones, p. Por ejemplo, objetivos de seguridad de la información o directrices y conceptos para su implementación en la práctica. Se espera que se garantice continuamente el cumplimiento de estos requisitos, lo que debe garantizarse mediante un seguimiento adecuado.

Por lo tanto, "supervisión del rendimiento/riesgo/cumplimiento" también se refiere a la supervisión y mejora continua del sistema de gestión de seguridad de la información (SGSI).

El seguimiento del desempeño comprende la evaluación de la eficacia del SGSI en términos de consecución de los objetivos de seguridad y cumplimiento de los requisitos de la norma ISO/IEC 27001.

El seguimiento de riesgos se refiere a la evaluación y seguimiento de los riesgos de seguridad en la empresa y en el SGSI (ver también el Capítulo 3.6).

El seguimiento del cumplimiento se refiere al seguimiento del cumplimiento de los requisitos legales y reglamentarios, pero también de las directrices y normas internas.

El monitoreo del desempeño, el riesgo y el cumplimiento está diseñado para ayudar a las organizaciones a garantizar que su SGSI esté funcionando de manera efectiva y eficiente y que cumpla con los requisitos de ISO/IEC 27001, así como con los requisitos legales y reglamentarios. Implica revisar periódicamente los procesos, procedimientos y controles del SGSI para garantizar que cumplan con los requisitos pertinentes.

Para establecer comparabilidad, continuidad y trazabilidad, todos los objetivos cuyo logro deba medirse mediante indicadores clave de desempeño deben cumplir con los
Criterios INTELIGENTES:

- Específico
- Medible
- Atractivo/Aceptado
- Realista
- Terminado

Esto garantiza que estos objetivos se describan con precisión, claridad y de una manera que todos puedan entender.

El responsable de seguridad de la información ahora está en condiciones de evaluar y controlar la seguridad de la información sobre la base de la varios ratios, por ejemplo con ayuda de una vista de panel.
De la gran cantidad de métricas, nos centramos en las siguientes clases de métricas con respecto a la seguridad de la información:

Indicadores clave de desempeño/riesgo/control (KxI)

KPI: indicadores clave de rendimiento
Un indicador clave de desempeño es un valor (objetivo/real). comparación) que muestra el éxito de una empresa implementa las medidas pertinentes y la información procesos de seguridad en relación con la obtención de la información objetivos de seguridad. Una medida es exitosa si lo deseado El nivel de rendimiento se logra dentro del tiempo especificado. y con el menor esfuerzo posible.

KRI - Indicadores clave de riesgo
Un indicador de riesgo clave es un valor (comparación objetivo/real) que muestra si los cambios en el perfil de riesgo potencialmente exceden los límites de tolerancia deseados y, por lo tanto, poner en peligro la logro de objetivos. Por lo tanto es una medida de cómo orientada al riesgo que tiene una empresa al implementar las medidas.

e implementa los procesos de seguridad de la información. A Se plantea una situación que supera el apetito de riesgo de la empresa. volver al rango de riesgo aceptable tomando contramedidas.

KCI - Indicadores clave de control
Un indicador de control clave es un valor (comparación objetivo/real) que muestra la eficacia con la que una empresa implementa medidas relevantes y procesos de seguridad de la información en relación con el logro de objetivos. Una medida es eficaz si Los objetivos de control se logran de manera confiable dentro de los límites deseados. límites de tolerancia.

Con el fin de monitorear continuamente la efectividad y eficiencia de los procesos del SGSI y de los establecidos medidas, estos indicadores deben usarse en la práctica (ver Fig. 5). Proporcionan información sobre el estado de rendimiento de todo el SGSI y sirven como desencadenantes de las acciones necesarias. intervención de gestión.

Esto significa registrar la situación real en relación con el situación objetivo descrita por las especificaciones y, si necesario, interviniendo de manera controladora. Estos Los indicadores de desempeño se resumen en relación con el objetivos corporativos a alcanzar, requisitos legales y necesidades de protección.

El valor añadido de los KxI radica en su capacidad de proporcionar servicios básicos declaraciones sobre el sistema de protección. ellos sirven el

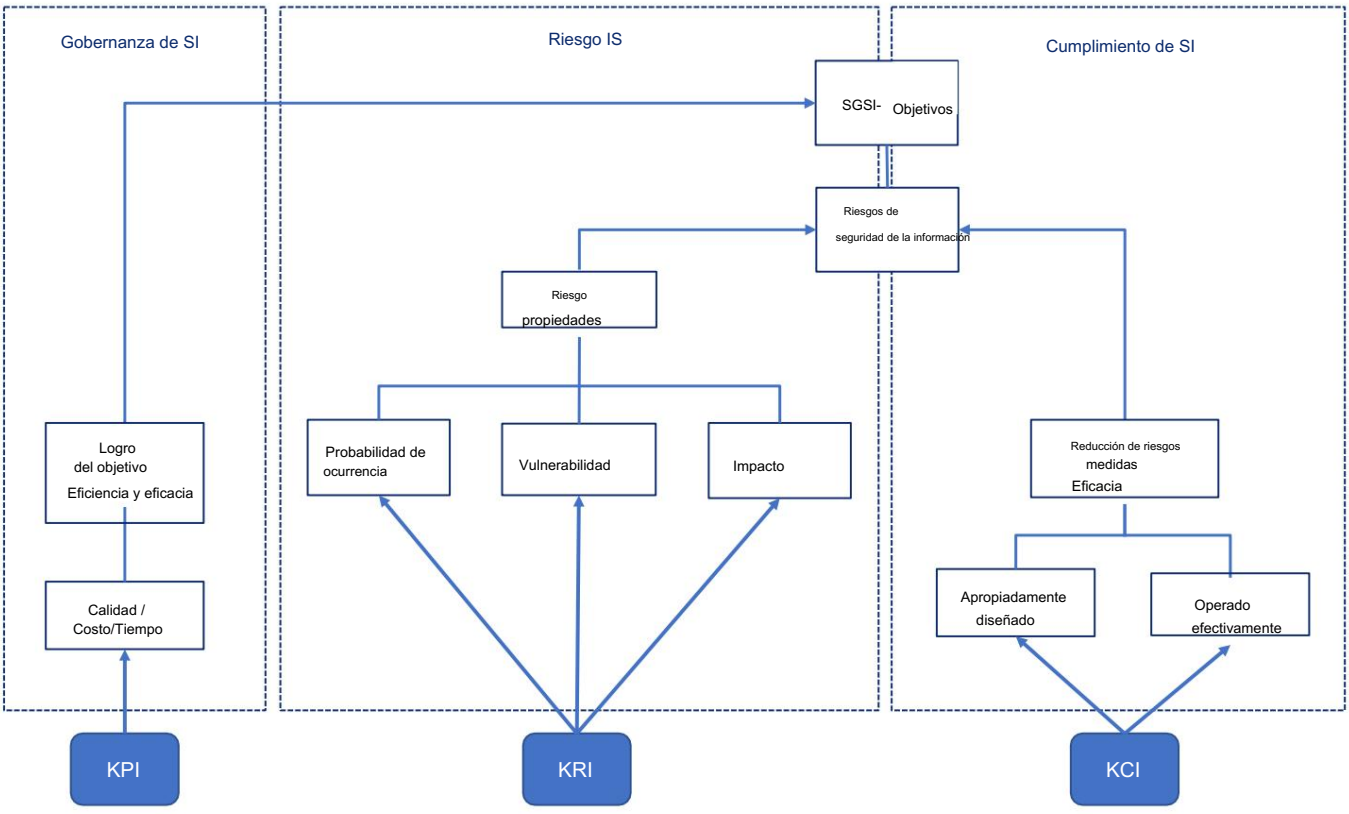


Figura 5: Estructura y relación de KPI, KRI y KCI

gestión como base comprensible y comprensible para decisiones fundamentadas sobre la gestión de la seguridad de la información. Además de los análisis de rendimiento clásicos, los KxI se pueden utilizar para revelar indicaciones de (nuevos) riesgos o cambios dentro del panorama de riesgos, así como no conformidades con respecto a la implementación de requisitos y directrices de seguridad.

Factores de éxito de la práctica.

Los indicadores clave sólo pueden usarse de manera significativa para representar la situación actual y controlarla si cumplen ciertos requisitos:

- Cada indicador clave debe ser mensurable, repetible y comparable, tanto a lo largo del cronograma como entre industrias o al menos organizaciones.
- Los indicadores deben estructurarse sistemáticamente y basarse en fundamentos estadístico-matemáticos sólidos y apropiados con mediciones confiables basadas en un alcance suficiente.
- Los indicadores deben ser oportunos y reflejar la información actual. La frecuencia de la recopilación de datos El procesamiento y la duración del procesamiento hasta la presentación a la gerencia deben permitir el control, similar a las pantallas en el tablero de un automóvil, que indican a la "dirección" del sistema si todos los parámetros "importantes" están en el rango ordenado y deseado.
- Los indicadores de desempeño deben ser relevantes para los objetivos de la gestión de la seguridad de la información, tener un efecto de control y brindar apoyo práctico para la toma de decisiones.
- La selección de indicadores debe basarse en el riesgo y debe tenerse en cuenta la rentabilidad de la recopilación de datos.
- Los resultados deben compararse con el valor informativo y la usabilidad para la toma de decisiones.
- La selección de KxI debería permitir una evaluación del SGSI en su conjunto. Es decir, no es suficiente, sólo subaspectos e indicadores individuales. Más bien, deben combinarse en un todo significativo y capturar el desempeño de todo el SGSI.
- Los indicadores de desempeño también pueden usarse para evaluar y gestionar las relaciones con los proveedores de servicios e incluirse, por ejemplo, como parte de un contrato o en un SLA (de seguridad).

Ver también Anexo 8.3 Salvaguardia integral de la cadena de valor, página 66

KxI relevantes para el SGSI

Hay muchas fuentes de métricas de desempeño de seguridad de la información que ofrecen una gran selección, como COBIT 2019 para la seguridad de la información19 o la Guía de medición del desempeño para la seguridad de la CIS20 , "La seguridad de la información21 , por nombrar algunas.

Por supuesto, también nos gustaría aprovechar esta oportunidad para hacer referencia a la guía práctica de ISACA "Evaluación del desempeño de un SGSI utilizando indicadores clave de desempeño (para un sistema de indicadores clave de desempeño de SI orientado a objetivos según ISO/IEC 27004:2016)" .

La selección específica de KxI debe basarse en las circunstancias de la organización respectiva, cumplir con los criterios de calidad ya descritos y optimizarse continuamente.

A continuación se muestran algunos ejemplos de indicadores clave de la Guía de prácticas de ISACA para evaluar el desempeño de una SGSI por indicadores clave:

Indicadores clave de rendimiento

- Tiempo requerido en comparación con el tiempo planificado a la tasa de implementación dada (por ejemplo, 80% de los empleados) de una campaña de sensibilización.
- Presupuesto requerido en comparación con el presupuesto previsto para la implementación de una campaña de sensibilización

Indicadores clave de riesgo

- Porcentaje de empleados que hacen clic en un enlace de phishing preparado durante una campaña de concientización
- Porcentaje de sistemas de TI con vulnerabilidades que no se cerraron en el plazo designado
- Porcentaje de sistemas informáticos productivos para los que existe ya no hay soporte del fabricante

Indicadores clave de control :

- proporción de empleados capacitados hasta la fecha en comparación con el número planificado de empleados que se capacitarán en una campaña de concientización.
- Número de empleados que superaron la prueba de aprendizaje al final de la campaña de sensibilización, en comparación con el número de empleados ya formados durante una campaña de sensibilización.

19 ISACA, COBIT 2019 para Seguridad de la Información, 2019.

20 Centro para la Seguridad de Internet, "The CIS Security Metrics".

21 "Guía de medición del rendimiento para la seguridad de la información", especial del NIST Publicación SP 800-55.

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

Documentación de la estructura de medición de todos los KxI. Responde a las siguientes preguntas:

– ¿ Qué se midió y evaluó?

– ¿ Qué métodos se utilizaron para la medición, el análisis y la evaluación? ¿Conducen a resultados reproducibles?

–¿Cuándo fue medido por quién?

– ¿ Cuándo fue analizado y evaluado por quién?

Resultados de las mediciones y de los informes de gestión derivados de ellos para la escalada

Además, los siguientes documentos han demostrado ser útiles en la práctica:

Todos los registros y evidencias que proporcionen información relevante para el contexto del monitoreo de la efectividad, ya que la organización debe mantener evidencia documentada del monitoreo y los resultados medidos.

Referencias

ISO/IEC 27001:2022 - Sección 9.1

ISO/IEC 27004:2009 - Secciones 5, 6, 7, 8, 9, 10 y Anexo A

Área de enfoque de COBIT 2019: Seguridad de la información

3.8 Documentación

En el contexto de la documentación, se debe asegurar como requisito central dentro del sistema de gestión que (al menos) estén regulados los siguientes aspectos para la documentación del SGSI:

La creación y actualización, así como la aprobación y, en su caso, la comunicación de documentos deben realizarse según un procedimiento definido (workflow).

Los documentos deben estar claramente identificados, por ejemplo, título, fecha, autor, versión, número de versión, número de versión, número de versión, número de versión, número de versión, número de versión, número de versión, número de versión, número de versión, número de versión, número de versión, número de versión, número de versión.

y una prueba de idoneidad y aptitud para el propósito (QA) adecuada y una liberación final.

Clasificación de los documentos o de su contenido en términos de confidencialidad

Elaboración de registros suficientes y relevantes en el marco de las actividades operativas para la Garantizar la trazabilidad

Los contenidos y el nivel de detalle de los documentos requeridos por la norma están influenciados por el alcance seleccionado del SGSI, el tamaño de la organización, las tecnologías utilizadas y la estructura organizacional, entre otros factores, y por lo tanto difieren de una organización a otra.

El número y tipo de documentos también varían. Desde una perspectiva práctica, puede tener sentido que una organización cree un conjunto de (muchos) documentos individuales y los mantenga granulares. Para otra organización, por otro lado, puede ser más apropiado utilizar un medio de almacenamiento central al que pueda acceder toda la organización. En la práctica, esto también puede significar utilizar una wiki u otro sistema en línea como base de documentación.

Si no se requieren documentos específicos, la norma ISO/IEC 27001:2022 utiliza el término "información documentada" en relación con la documentación y los registros.

En este caso, la empresa es libre de decidir en qué documentos asociados se conserva esta información, comprendiendo el término "documento" cualquier formato.

La documentación requerida dentro del SGSI será monitoreada continuamente para garantizar lo siguiente:

Disponibilidad e idoneidad para su uso, independientemente del lugar y tiempo

Protección adecuada, por ejemplo contra pérdida de confidencialidad, uso indebido o acceso no autorizado.

Manipulación/pérdida de integridad

Factores de éxito de la práctica.

En la práctica, el cumplimiento del requisito de control de documentos generalmente puede estar respaldado por una directriz documental.
Sin embargo, el factor decisivo para una implementación exitosa no es la cantidad de documentación, sino su calidad, aceptación y disponibilidad, así como su control eficaz (palabra clave: control de documentos).

Los aspectos prácticos para la evaluación de la calidad de la documentación y el control de los mismos resultan de las siguientes preguntas:

¿ Cómo se comunican los contenidos y modificaciones de la documentación a los empleados o ge-trains afectados?

¿ En qué medida conocen los empleados el contenido y cómo "viven" en la vida cotidiana los requisitos de los documentos?

¿ Quién conoce los lugares de presentación y los medios de presentación donde ¿Se pueden encontrar los documentos actuales?

¿ El contenido está preparado de manera orientada al grupo objetivo y formulado con claridad?

¿ Qué tan fácil les resulta a los nuevos empleados comprender el contenido de los documentos e implementarlos en su propio entorno de trabajo? ¿colocar? ¿Qué tipo de demandas hay?

¿ Se actualizan los documentos periódicamente o según sea necesario? ¿Qué tan bien funcionan las actualizaciones? y la liberación de los documentos?

¿ Hay propietarios de documentos dedicados por documento?

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación (secciones 4-10):

- Alcance del SGSI (Sección 4.3)
- Política de seguridad de la información, apartado 5.2 e)
- Descripción del proceso de evaluación de riesgos (Proceso de evaluación de riesgos de seguridad de la información, apartado 6.1.2)
- Descripción del proceso de tratamiento de riesgos (Proceso de tratamiento de riesgos de seguridad de la información, apartado 6.1.3)
- Declaración de Aplicabilidad (Sección 6.1.3 d)
- Plan de tratamiento de riesgos de seguridad de la información (Sección 6.1.3 mi)
- Objetivos de seguridad (Objetivos de seguridad de la información y planificación para alcanzarlos, Sección 6.2)
- Seguimiento para la consecución de los objetivos de seguridad (información objetivos de seguridad y planificación para alcanzarlos, Ab-secciones 6.2 d, 6.2 g)
- Prueba de competencia (sección 7.2 d)
- Evidencia de ejecución correcta, así como cambios en los procesos del SGSI22 (Planificación y control operativo, Sección 8.1 d; Planificación de cambios, Sección 6.3)
- Resultados de la evaluación de riesgos de seguridad de la información (Sección 8.2)
- Resultados del tratamiento de riesgos (Resultados de la Información tratamiento de seguridad, Sección 8.3)
- Evidencia de los resultados de seguimiento y medición del SGSI, apartado 9.1)
- Evidencia de la implementación de las auditorías y sus resultados (Evidencia del programa(s) de auditoría y los resultados de la auditoría, sección 9.2)
- Evidencia de los resultados de las revisiones por la dirección (Apartado 9.3)
- Desviaciones identificadas de los requisitos del SGSI y medidas para corregirlas (Evidencia de la naturaleza de las no conformidades y cualquier acción posterior tomada, Sección 10.1 f)
- Evidencia de los resultados de cualquier acción correctiva (Apartado 10.1 g)

Además, la organización debe determinar por sí misma qué documentación y registros son necesarios además de lo requerido por la normativa para tener "confianza suficiente en que los procesos se han llevado a cabo según lo planeado" (ver Sección 8.1).

Los procesos del SGSI para la gestión de riesgos, la gestión de incidentes y la mejora continua del SGSI deben visualizarse utilizando representaciones de procesos adecuadas (por ejemplo, cadenas de procesos impulsadas por eventos, EPC) y comunicarse a los empleados de manera comprensible mediante descripciones de procesos e instrucciones de trabajo concretas.

Además, se encuentran los documentos y registros del Anexo A, siempre que estas medidas se apliquen de conformidad con la "Declaración de Aplicabilidad".

Referencias

ISO/CEI 27001:2022

3.9 Comunicación

Cuando se opera un SGSI, se requiere la cooperación con otras organizaciones y departamentos (por ejemplo, proveedores, departamento de recursos humanos, departamento legal, auditoría). La tarea principal del módulo "Comunicación" es determinar y describir la
Necesidad de comunicación interna y externa.

La comunicación externa se refiere a la comunicación con las partes interesadas (externas) y otras organizaciones (ver también el análisis del entorno en el capítulo 3.1 Contexto de la organización). La comunicación interna se refiere a la necesidad de comunicación dentro del sistema de gestión y dentro de la organización, por ejemplo, con las partes interesadas internas como la junta ejecutiva, los gerentes y los empleados.

Un análisis debe determinar qué información debe comunicarse en el contexto del SGSI (Sección 7.4 a del estándar), por quién (Sección 7.4 d) y a quién (Sección 7.4 c). Además, se debe determinar cuándo se realizará la comunicación (Sección 7.4 b), y

22 En este contexto, la norma habla de "información documentada en la medida necesario".

a través de qué canales/procesos de comunicación (sección 7.4 e) esto hay que hacerlo.

Idealmente, los resultados del análisis se resumen en un Plan de comunicación. Esto suele desarrollarse formalmente en cinco pasos concretos (ver Figura 6):

Figura 6: Desarrollo de un plan de comunicación

Las interfaces de proceso y comunicación deben estar claramente definido en términos de eficiencia e integrado en el o-La información debe integrarse en el sistema organizacional y procesos operativos. Debe estar claramente definido qué información debe entregarse a quién y por quién y en qué momento, por ejemplo como parte del cambio o gestión de incidencias.

La norma requiere que la organización determine comunicación interna y externa en el contexto de la Sismo.

No requiere explícitamente que esto se haga como parte de un análisis. Sin embargo, el beneficio práctico de una análisis es que se puede utilizar para identificar claramente qué existen requisitos para un ajuste preciso estructura de comunicación.

Factores de éxito de la práctica.

Un plan de comunicación, también conocido como comunicación. matriz, puede parecerse a las tablas 1 y 2.

Comunicación interna				
Razón de comunicación	Iniciador	Receptor	Frecuencia	Medio
Revisión de gestión	CISO	Alta Gerencia	anual	Informe de gestión según plantilla por correo + presentación
Informes	CISO	Alta Gerencia	trimestral	Informe de KPI según plantilla vía correo electrónico + presentación
Entrenamiento de conciencia	CISO	Todos los empleados en el alcance anual.		Formación (presencial/online)
Boletín IS	CISO	Todos los empleados en el alcance trimestralmente y caso por caso en caso de una amenaza aguda.		Correo electrónico
Gestión de riesgos	CISO	Alta Gerencia	trimestralmente, relacionado con el caso en caso de amenaza grave, relacionado con el proyecto	Informe de cuadro de mando integral, vía correo electrónico si corresponde.
Incidente de seguridad	Apoyo	CISO (si es necesario más según SIRP)	relacionado con el caso	Escalada según SIRP (Respuesta a incidentes de seguridad Proceso)
Incidente de seguridad	CISO	Alta Gerencia	relacionado con el caso	Correo electrónico, si es necesario verbalmente
Incidente de seguridad con datos personales	CISO	Delegado de protección de datos	relacionado con el caso	Correo electrónico, si es necesario por teléfono o verbalmente
Incidente de seguridad con referencia de cumplimiento	CISO	Departamento legal	relacionado con el caso	Correo electrónico, si es necesario por teléfono o verbalmente

Tabla 1: Plan de comunicación - comunicación interna

Comunicacion externa				
Razón de comunicación	Iniciador	Receptor	Frecuencia	Medio
Informe de servicio operativo Proveedor	Proveedor de servicios operativos	CISO	trimestral	Informe SLA según plantilla vía correo electrónico
Encargado externo CERT/Vulnerabilidad Análisis	CERTIFICADO	CISO/Gerente de TI	semanal/relacionado con el caso	Informe según contrato por correo electrónico
Incidente de seguridad	CISO, si es necesario alta dirección	Clientes/socios afectados	relacionado con el caso	según SIRP, en sitio web, carta, correo electrónico, teléfono
Incidente de seguridad con criminal fondo	CISO	Agencias de investigación	relacionado con el caso	según SIRP

Tabla 2: Plan de comunicación - comunicación externa

Una vez elaborada la matriz de comunicación, En la práctica se ha demostrado que ya existen varias interfaces entre interlocutores y/o departamentos. Identificarlos es un éxito importante. factor para diseñar eficientemente la comunicación en el contexto del SGSI en la organización. puede hacer sentido integrar el plan de comunicación de SI en un plan general de comunicación.

Para poder comunicarnos con todos los niveles de la organización, se debe proporcionar una plataforma con la que se pueda acceder a la información de seguridad integral de la ISMS es accesible para diferentes grupos objetivo. Plataformas de colaboración para una mejor comunicación o Los informes podrían ser, por ejemplo, intranet, Confluence, Wiki o similar.

Requisitos de documentación

Según ISO/IEC 27001:2022, no existen normas requisitos para la documentación del SGSI con respecto a la comunicación.

Además, los siguientes documentos han demostrado ser útiles en la práctica:

Procedimientos de comunicación interna y externa

Matriz de comunicación

Plan de comunicación

Referencias

ISO/IEC 27001:2022 - Sección 7.4

3.10 Conciencia

"La seguridad de la información es el funcionamiento de cortafuegos y antivirus": este es uno de los principales y frecuentes conceptos erróneos que ponen en peligro la seguridad de la información y sistemas informáticos de una empresa, porque un gran número de de eventos relevantes para la seguridad e incidentes de seguridad en las operaciones cae en las categorías de "falta de sentido de responsabilidad", "falta de procesos o procesos inmaduros" y "empleados inadecuados". entrenamiento y/o sensibilidad."

La creación de una conciencia de riesgo "sana" es, por tanto, una componente esencial de un SGSI práctico que genere beneficios para la organización al identificar las amenazas a tiempo etapa, evitando incidentes de seguridad y "ahorrando" el esfuerzo que sería necesario ocuparse de ellos.

La concienciación sobre la seguridad no es algo natural, sino que debe serlo. promovidos y demandados activamente por la empresa a través de campañas de concientización apropiadas, incluidas las siguientes aspectos importantes (ver Sección 7.3):

Conocimiento de la guía de seguridad de la información y del usuario. guía así como la información relevante Las pautas de seguridad por parte de los destinatarios del especificaciones (empleados, gerentes, socios externos) debe garantizarse.

La aportación de cada empleado en el ámbito del El SGSI debe estar alineado con los requisitos establecidos en la guía del usuario. Lo ideal es que los materiales utilizados para las medidas de sensibilización apoyar la comunicación de este contenido. Los materiales utilizado para medidas de sensibilización idealmente apoya la comunicación de este contenido. Se recomienda demostrar una comunicación exitosa mediante pruebas.

Efectos y, en su caso, sanciones por incumplimiento con las normas de seguridad debe derivarse de la materia- La información debe proporcionarse en forma de datos. utilizado en el contexto de una medida de sensibilización. Al mismo tiempo, el informe de un usuario sobre una violación de seguridad (p. ej., denunciante) debido a su propia mala conducta debe generalmente no dan lugar a sanciones.

Factores de éxito de la práctica.

En la práctica, las campañas de concientización sobre la seguridad de la información generalmente se pueden dividir en diferentes fases. En primer lugar, se realiza una evaluación de las necesidades y luego se planifica e implementa una campaña de sensibilización en línea con el grupo objetivo y en función de amenazas potenciales específicas. La concientización sobre la seguridad de la información no debe verse como un proyecto aislado, sino que debe establecerse de manera sostenible a través de mecanismos planificados en la campaña. El análisis de la eficacia de una campaña debe considerarse previamente. En la práctica, las siguientes fases han demostrado ser útiles para una campaña de concientización sobre seguridad (ver Figura 7):

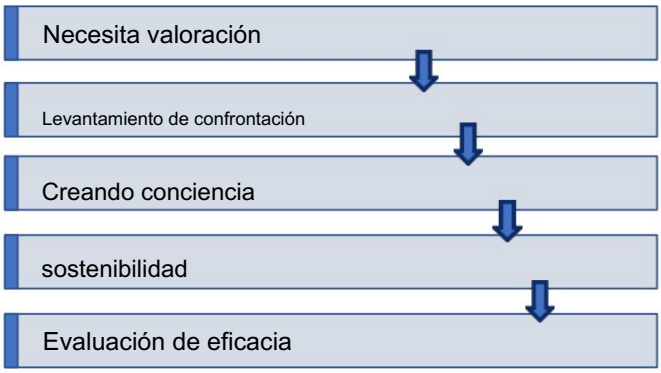


Figura 7: Modelo de fase para campañas de concientización sobre seguridad

Fase 1: Evaluación de necesidades (basada en los peligros potenciales)

La implementación exitosa de campañas de concientización sobre seguridad requiere conocimiento del grupo objetivo y sus necesidades. Por este motivo, las campañas de sensibilización siempre deben comenzar con una evaluación de las necesidades.

La concienciación sobre la seguridad es útil en todas las áreas de una empresa, pero sólo en una de ellas. peligro y en la medida apropiada para el grupo objetivo.

El conocimiento de los requisitos de seguridad se puede aumentar, por ejemplo, mediante medidas de sensibilización con participación activa y participación. La evidencia debe proporcionarse en forma de un registro de las actividades del cliente.

Por lo tanto, antes de comenzar a definir y planificar medidas de sensibilización, una empresa debería pensar en sus peligros (riesgos) potenciales individuales en relación con los usuarios. No es muy útil confrontar a los usuarios con peligros y situaciones que no se aplican a su área.

Fase 2: Confrontación con el tema

En la fase de "confrontación" se debe despertar la atención de los empleados sobre el tema, generar consternación y promover la aceptación para la fase 3, es decir, la sensibilización propiamente dicha. Por lo general, esto se logra mejor confrontando directamente a los empleados con el tema ("aprendizaje basado en la experiencia").

A través de la experiencia personal, los empleados toman conciencia de su importancia para la seguridad de la información. Sibilizados y posteriormente normalmente agradecidos y abiertos a nuevas medidas de formación sobre el tema.

A continuación se muestran algunas simulaciones de ataques para confrontar a los empleados con el tema:

Ataques de ingeniería social a empleados, por ejemplo, utilizando información falsa. llamadas para obtener información confidencial. (como contraseñas) y correos electrónicos falsos (por ejemplo, solicitando el ingreso de una contraseña en un sistema en línea con el aparente propósito de verificar la seguridad de la contraseña para una próxima auditoría).

Debe haber memorias USB preparadas en la empresa (aparcamiento, sala de reuniones, aseos, etc.).
El sistema puede generar mensajes de advertencia que pueden registrarse de forma anónima y utilizarse para evaluación ("Podría haber sido un virus").

Busque en los cubos de basura o en las papeleras documentos confidenciales ("buceo en contenedores de basura").

La práctica ha demostrado que los escenarios de ataque mencionados anteriormente conducen, en este contexto, a incidentes de seguridad "valiosos" e información utilizable en la mayoría de las empresas. La resolución "anónima" de la acción, junto con la presentación de posibles consecuencias para la empresa, suele provocar un "efecto Hola-despertar" entre los empleados, que puede utilizarse como introducción a la propia campaña del EI (" transferencia de conocimiento"). También por razones éticas se recomienda realizar "ataques" simulados a los empleados sólo previo aviso y en estrecha coordinación con la empresa.

Consejo, si existe, para evitar resentimientos entre los afectados, que podrían contrarrestar el efecto de aprendizaje deseado.

Como alternativa a este tipo de campañas, el "enfrentamiento" también puede tener lugar de forma pasiva, por ejemplo al comienzo de una formación en el aula. Las demostraciones podrían incluir sesiones de piratería en vivo, pruebas anónimas de la seguridad de las contraseñas o juegos de roles.

Un aspecto esencial en esta fase es crear un ambiente positivo punto de entrada diseñado para el tema y, por lo tanto, el contacto con los empleados "a la altura de los ojos

para establecer. A pesar de toda confrontación, la dirección básica siempre debe ser "recoger" a los empleados donde se encuentran en este momento (¿Qué requisitos de SI existen ya? ¿Cómo se han comunicado hasta ahora? ¿Qué incidentes han ocurrido ya? etc.), y involucrarlos activamente.

También es importante tener claro el marco e identificar cualquier laguna de información que pueda existir. Puedo saberlo. El alcance de las actividades realizadas y la información proporcionada deben ser coherentes con la La campaña debe equilibrarse con la "capacidad de absorción" de los destinatarios. Sólo así la campaña podrá desarrollar todo su efecto y no ser percibida como demasiado banal ni demasiado excesiva/ sobrecargada.

Fase 3: Sensibilización

La sensibilización real es, en el mejor de los casos, una combinación de transferencia de conocimientos, demostración y participación activa de los empleados. Se pueden utilizar varios métodos para impartir conocimientos (formación previa al servicio, aprendizaje electrónico, etc.).

La clasificación de las actividades de sensibilización en áreas o medidas temáticas ha resultado eficaz, en particular las siguientes:

Seguridad física/seguridad en el lugar de trabajo – ¿Qué se debe tener en cuenta al entrar en los edificios y locales?

– ¿Cómo se puede impedir el acceso de personas no autorizadas, por ejemplo, entregas erróneas o que un desconocido se una a un grupo de empleados y entre en el edificio sin ser visto ("piggybacking")?

Privacidad

- El apartado de protección de datos debe cumplir con los requisitos legales.

Los datos deben mantenerse en secreto, deben existir procedimientos de eliminación y los empleados deben estar obligados a cumplirlos.

Seguridad de TI : lo que es importante cuando se trata de sistemas de TI y computadoras. tern, por ejemplo, manejo de correo electrónico, navegación por Internet, manejo de medios extraíbles (CD, memorias USB), protección y herramientas contra malware?

Telefonía

- ¿Qué puede suceder cuando se pierde información digna de protección?

ciones o procesos se divulgan por teléfono?

Notificación y gestión de incidentes de seguridad : ¿qué puntos de contacto (centrales) existen?

– ¿ Cuáles son las acciones iniciales relevantes?

Además, para sopesar se deben tener en cuenta grupos destinatarios especialmente vulnerables (p. ej., administradores de TI, empleados y directivos con amplios derechos de acceso y de información, empleados móviles, pero también empleados de centros de llamadas u otros grupos con contacto externo) . si necesitan formación especial.

Se deben crear y distribuir materiales de concientización según sea necesario para apoyar la capacitación. Puede tratarse, por ejemplo, de folletos de una o varias páginas o de boletines informativos con contenidos formativos, pero también de carteles, pegatinas u otros soportes con un alto efecto de reconocimiento (pósteres, folletos, vídeos, etc.).

Lo ideal es que los materiales de concientización sean creados por los propios empleados de la empresa como parte de la campaña de SI. Se puede lograr una motivación adicional para cooperar mediante un sistema de incentivos23. Un vídeo guía de la alta dirección puede enfatizar la importancia del tema con la correspondiente solicitud al co-El objetivo es enfatizar la importancia de que los empleados manejen la información de manera consciente.

Fase 4: Crear sostenibilidad

Las medidas puntuales de sensibilización no son suficientes para lograr un cambio sostenible en el comportamiento de los empleados. Aunque es necesario llevar a cabo una sensibilización inicial exhaustiva, sólo la repetición regular de los temas sobre la base de un plan de formación y la comunicación regular de los mensajes clave de la vida cotidiana pueden garantizar una sensibilización duradera. Las formas de crear una presencia subconsciente del tema en la vida cotidiana incluyen:

Envío regular de correos electrónicos de phishing simulados (por ejemplo, a revelar datos de acceso)

Publicación de noticias de actualidad (p. ej., a través de intranet, periódico de los empleados)

Integración de un cuestionario en línea sobre el tema SI en la intranet o mediante una aplicación (posiblemente con incentivos)

Uso de un salvapantallas con atractivos mensajes de seguridad

Implementación anual de un mes de ciberseguridad con, por ejemplo, presentaciones internas o externas, hackeos en vivo

23 Incentivo = incentivo, incentivo por desempeño.

Fase 5: Evaluación de la eficacia

En esta fase se evalúa periódicamente el grado de sensibilización de los empleados. El objetivo es crear transparencia con respecto al nivel de madurez de la sensibilización de los empleados.
Los posibles KPI para medir son, por ejemplo:

- Número de incidentes de seguridad denunciados debido a malas conductas como proporción de todos los incidentes de seguridad. caer
- Número/proporción de clics o entradas de contraseña a correos electrónicos de phishing simulados.
- Resultados de un cuestionario o prueba sobre el tema de la información. seguridad
- Net Promoter Score (NPS) para contenido de capacitación

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

- Evidencia de la competencia de los empleados en el área de aplicación del SGSI (Sección 7.2)

Además, los siguientes documentos se han consolidado en la práctica como orientados a objetivos:

- Concepto de sensibilización/formación
  - ¿ Qué temas se tratan?
  - ¿ Cómo se implementan las medidas de sensibilización?
    ¿Zeg formación presencial y/o formación online?
  - ¿ Cómo son los contenidos de la seguridad de la información?
    ¿Se comunicó la directriz?
- Programa de Concientización/ Capacitación – ¿Cuándo se tratan qué temas?
  - ¿ Están actualizadas las medidas, tal y como exige la norma, proporcionado de forma regular?
- Materiales de capacitación que reflejen de manera concisa los contenidos de la directriz de seguridad de la información; y señalar peligros y debilidades en el procesamiento de la información.
- Comprobante de participación: nombres de las personas participación, contenidos y fecha de la toma de conciencia medida

Referencias

ISO/IEC 27001:2022 - Secciones 7.2 y 7.3

3.11 Relaciones con proveedores

El alto nivel de interconexión y estandarización en el procesamiento de la información ha hecho necesario recurrir a proveedores de servicios externos.

Se recomienda encarecidamente a los proveedores. Por el contrario, los riesgos de seguridad en el proveedor de servicios también tienen un impacto en la propia infraestructura de la empresa. Esto ha quedado demostrado por una serie de incidentes de alto perfil en los últimos años en los que las deficiencias de seguridad en los proveedores de servicios llevaron al robo de datos u otros incidentes de seguridad en empresas conocidas.

El término "proveedor de servicios" o "proveedor

En la imagen propia de la norma ISO/IEC 27001:2022, el término "proveedor" cubre una amplia gama de relaciones comerciales con empresas y socios externos. Incluye relaciones del entorno de TI, como fabricantes de software, proveedores de servicios de TI, socios de subcontratación o proveedores de servicios en la nube, pero también de otras áreas. Estos incluyen, por ejemplo, logística, servicios públicos, gestión de instalaciones, proveedores de servicios de limpieza y muchos otros.

Los requisitos de ISO/IEC 27001:2022 se centran en diversas medidas de protección, como la definición de procesos y procedimientos (sección 5.19) y el acuerdo de regulaciones contractuales con el proveedor (sección 5.20), por ejemplo, conexión con el registro o el registro de seguridad. Conexión CERT, canales de reporte de incidentes de seguridad, integración a un sistema de gestión de identidad existente. También se deben tener en cuenta los riesgos de la infraestructura de TIC del proveedor, las cadenas de suministro y otros subcontratistas (Sección 5.21), así como las regulaciones para monitorear y modificar la prestación de servicios (Sección 5.22).

Se debe establecer una política temática específica para el uso de servicios y procesos en la nube desarrollados para todo el ciclo de vida del servicio (Sección 5.23). De esta forma se abordan aspectos relevantes de la seguridad de la información desde la adquisición, uso, gestión y salida del servicio en la nube.

ISO/IEC 27036 y otras normas relevantes

La norma ISO/IEC 27036 "Seguridad de la información para las relaciones con proveedores" ofrece una visión mucho más detallada. Aborda los procesos necesarios y describe las actividades requeridas en el proceso respectivo. La certificación según esta norma no es posible, pero se crea una terminología común que, entre otras cosas, proporciona muchas ayudas concretas para la implementación.

La Figura 8 muestra una descripción general de los estándares que son relevantes en este contexto, divididos en descripción general, requisitos y directrices, así como documentos complementarios que se centran en procesos y técnicas.

En los sectores regulados es posible que deban tenerse en cuenta otros requisitos específicos, por ejemplo MaRisk AT 9 para bancos. Además, la norma ISO 28001 se utiliza cada vez más.
“Sistemas de Gestión de Seguridad para la Cadena de Suministro” como Be-

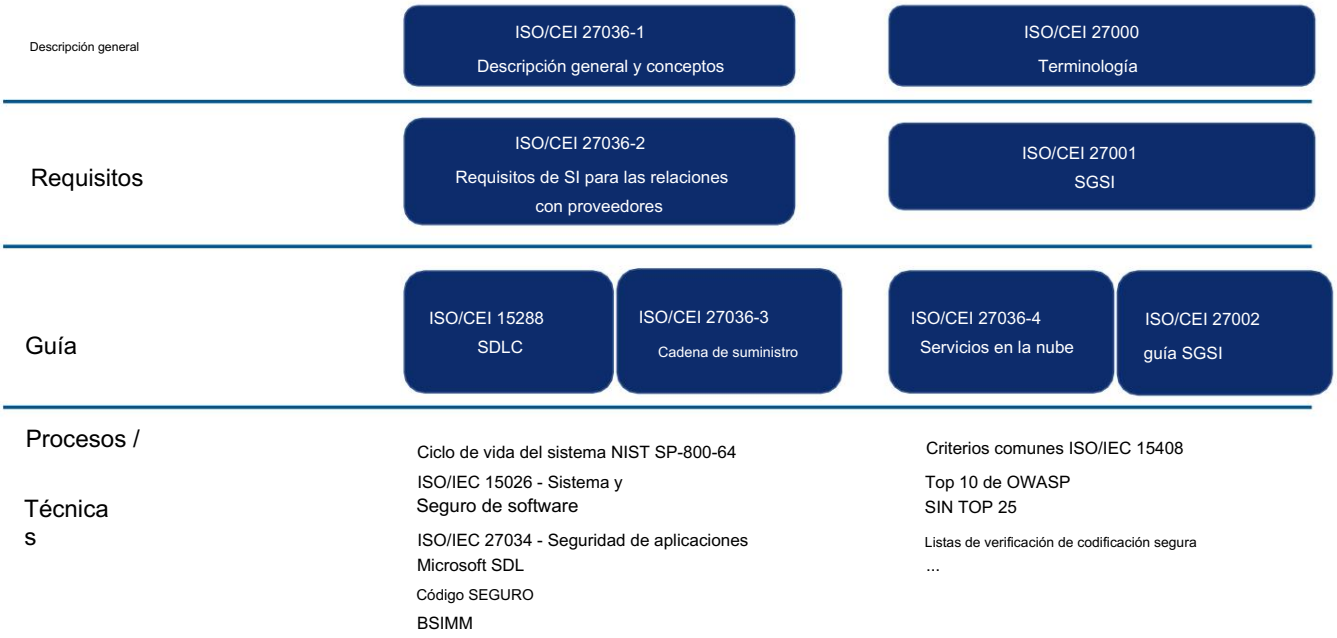


Figura 8: Descripción general de los estándares de SI en las relaciones con los proveedores

parte de los contratos con los clientes. Este estándar también especifica requisitos para la seguridad de la información (por ejemplo, seguridad física, seguridad del personal, seguridad de TI).

Factores de éxito de la práctica.

Evaluación integral de riesgos

Es importante abordar todos los riesgos a los que está expuesta la propia organización mediante la cooperación con proveedores de servicios externos. En este punto, la norma exige que todos los procesos subcontratados estén claramente definidos y controlados de forma sostenible (ver sección 8.1).

Una posible clasificación de las relaciones con los proveedores la proporciona la norma ISO/IEC 27036-1, que distingue entre:

- Relaciones con proveedores de productos
- Relaciones con proveedores de servicios
- Cadena de suministro de tecnología de la información
- Computación en la nube

Uso de software

El uso de software de cualquier tipo también debe evaluarse en el aspecto de gestión de proveedores. Tanto el software de desarrollo propio como los productos y servicios terminados suelen incluir marcos, paquetes u otras bibliotecas. En el pasado, los ataques a estos componentes detrás de la aplicación real condujeron a compromisos exitosos. Procedimientos para identificar y controlar estos

Los componentes deben ser parte de las operaciones de TI o del desarrollo de software.

Derecho a auditar

El derecho de auditoría debe incluirse en cada contrato.

Sin embargo, este derecho no suele concederse en los contratos estándar con proveedores de nube. En este caso se deberán examinar alternativas, como la inclusión de informes de resultados de auditorías externas o la entrega de certificados que incluyan las respectivas áreas de validez.

Certificaciones

Los proveedores responden cada vez más a las exigencias de los clientes en materia de seguridad de la información mediante certificaciones. Para ello son especialmente adecuadas las normas ISO/IEC 27001:2022 o IT-Grundschutz. Sin embargo, para este fin también se utilizan la norma ISO/IEC 27018 para el procesamiento de datos personales en la nube o, en parte, la norma internacional ISAE 3402 "Informes de aseguramiento de los controles en una organización de servicios". se ha consolidado en el sector de la automoción. La base del procedimiento de prueba es la Evaluación de Seguridad de la Información VDA, que se basa en ISO/IEC 27001.

TISAX®

En todos los casos es muy importante un informe completo sobre la auditoría y sus resultados, ya que el alcance de la auditoría y los controles auditados en cada caso pueden variar. Para proveedores clasificados críticamente, se debe solicitar un informe SOC Tipo II de acuerdo con ISAE 3402.

el. Además, las posibles desviaciones deben ser evaluadas por el cliente de acuerdo con su propio apetito de riesgo.

En el caso de datos personales, se debe examinar de forma muy crítica el uso de proveedores de servicios, en particular aquellos que se encuentran fuera del ámbito legal alemán o fuera del EEE24 .

Este contexto también incluye el tema del procesamiento de datos por encargo según el art. 28 UE GDPR25 de forma independiente. del lugar donde se encuentra el proveedor del servicio.

Figuras claves

Las siguientes cifras clave26 pueden utilizarse, por ejemplo, para evaluar la seguridad de la información en relación con los proveedores de servicios:

Número de informes de proveedores de servicios entregados a tiempo en relación con el número total de informes acordados

Tiempo promedio desde la detección hasta el informe de seguridad incidentes por parte de proveedores de servicios

Número de proveedores de servicios que garantizan contractualmente medidas de IS en relación con todos los proveedores de servicios.

Número de incidentes de seguridad en proveedores de servicios en el último período del informe

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

Definición del alcance, teniendo en cuenta la dependencia de socios externos y proveedores de servicios. listas (sección 4.3)

Además, los siguientes documentos se han consolidado en la práctica como orientados a objetivos:

Procesos y procedimientos para las relaciones con proveedores de servicios (cf. ISO/IEC 27001:2022, secciones 5.19- 5.22). Deberán definirse los requisitos resultantes de la estrategia de adquisiciones y de cualquier relación con el proveedor de servicios.
Además, los riesgos de seguridad de la información deben abordarse dentro de la cadena de suministro de productos y servicios de TIC.

Acuerdos sobre requisitos de seguridad de la información con proveedores. Aquí se tienen en cuenta las diferentes categorías de proveedores.

Directrices temáticas específicas para el uso de servicios en la nube (cf. ISO/IEC 27001:2022, apartado 5.23)

Requisitos de seguridad específicos de la industria, como el documento técnico BDEW del sector energético.

Referencias

ISO/IEC 27001:2022 - Secciones 4.3 y 8.1 y 5.19 - 5.23

ISO/IEC 27036-1:2021

Libro blanco de BDEW "Requisitos para sistemas seguros de control y telecomunicaciones".

3.12 Auditoría Interna

Los objetivos principales de las auditorías internas del SGSI son verificar en qué medida el SGSI cumple con los requisitos propios de la organización y los requisitos de ISO/IEC 27001:2022 (verificación de cumplimiento) y verificar la implementación y efectividad de las medidas tomadas (verificación de implementación y efectividad).).

Para ello se debe planificar e implementar un programa de auditoría que regule aspectos como frecuencia, procedimientos, competencias y responsabilidades, requisitos de planificación, seguimiento y presentación de informes. Además, se debe definir cómo se manejan las acciones correctivas y preventivas (es decir, acciones directamente derivadas de las auditorías) y dónde se "guardan" para su posterior procesamiento.

El programa de auditoría tiene como objetivo garantizar que todos los procesos de negocio cubiertos por el SGSI (según el alcance) sean auditados al menos una vez cada tres años con respecto a los requisitos y directrices de seguridad de la información aplicables en el momento de la auditoría y con respecto a la conformidad. con el SGSI. Deberá aportarse prueba de ello.

Las auditorías internas en el sentido de la norma no se refieren a las actividades de la función de auditoría interna en sentido estricto, aunque ésta también puede ser un organismo que lleva a cabo auditorías internas. En la práctica, las auditorías internas de SGSI son una tarea central del gerente de SGSI/CISO, quien planifica y gestiona las auditorías, posiblemente junto con un equipo de auditoría interna o con la ayuda de soporte externo y teniendo en cuenta la norma ISO 19011:2018.

Factores de éxito de la práctica.

Se pueden distinguir dos áreas en la implementación de auditorías internas (ver Figura 9):

El "programa de auditoría" o "marco de auditoría", que sirve como una superestructura organizacional para controlar y

24 EEE: Espacio Económico Europeo.

25 EU-DSGVO: Reglamento general de protección de datos de la UE.

26 Ver también: Evaluación del desempeño de un SGSI utilizando indicadores clave (Capítulo ISACA Alemania).

Figura 9: Estructura para las auditorías internas del SGSI (programa de auditoría versus actividades de auditoría)

El SGSI sirve para monitorear todas las actividades en el contexto de las auditorías internas y forma la interfaz con otros procesos del SGSI.

Se incluyen las "actividades de auditoría" específicas, que implican la planificación y la implementación práctica de auditorías internas individuales.

Las actividades de auditoría sirven para la implementación operativa del programa de auditoría, por lo que tiene sentido la coordinación con la función de auditoría interna de la organización.

En organizaciones más grandes, tiene sentido dividir estas áreas organizacionalmente, con un líder del equipo de auditoría responsable del programa de auditoría y un equipo de auditores que lleva a cabo las auditorías internas en la práctica. Se debe garantizar que tanto el diseño general como la gestión operativa del programa de auditoría funcionen de manera óptima para lograr los objetivos de SI. Esto le da a la organización el mejor retorno de la inversión (ROI) posible para los recursos utilizados en el área de auditoría.

El programa de auditoría

El programa de auditoría consta de un ciclo con los subprocesos de planificación, definición, implementación, seguimiento y revisión y mejora del propio programa de auditoría (ver Figura 10).

En el programa de auditoría y en la planificación basada en riesgos de actividades de auditoría específicas, tanto la importancia

Se tienen en cuenta los procesos afectados (procesos centrales, impacto de los daños, criticidad del negocio) y los sistemas de TI, así como los resultados de auditorías anteriores.

El programa de auditoría debe definir los criterios generales para las auditorías. Dependiendo del tamaño de la organización, del número de auditorías realizadas y del nivel de detalle deseado del programa de auditoría, aquí también se puede definir directamente el alcance específico de las auditorías individuales.

Las auditorías realizadas deben documentarse y la información correspondiente (por ejemplo, en forma de auditoría). El informe de auditoría debe estar disponible como prueba de la implementación del programa de auditoría.

Se deben preparar informes de gestión periódicos con información sobre el desempeño del programa de auditoría y sobre la

sobre las actividades de auditoría y sus resultados.

Subproceso de planificación

El programa de auditoría debe basarse en los requisitos individuales de la respectiva organización (ver secciones 4.2 y 4.3 de la norma y el capítulo 3.1 Contexto de la Organización de esta guía). Además, los objetivos definidos del programa de auditoría deben indicar que

las auditorías están orientadas a los riesgos identificados,

se tiene en cuenta la importancia de los procesos empresariales individuales y

el programa de auditoría cubre el alcance de las actividades asociadas Sismo.

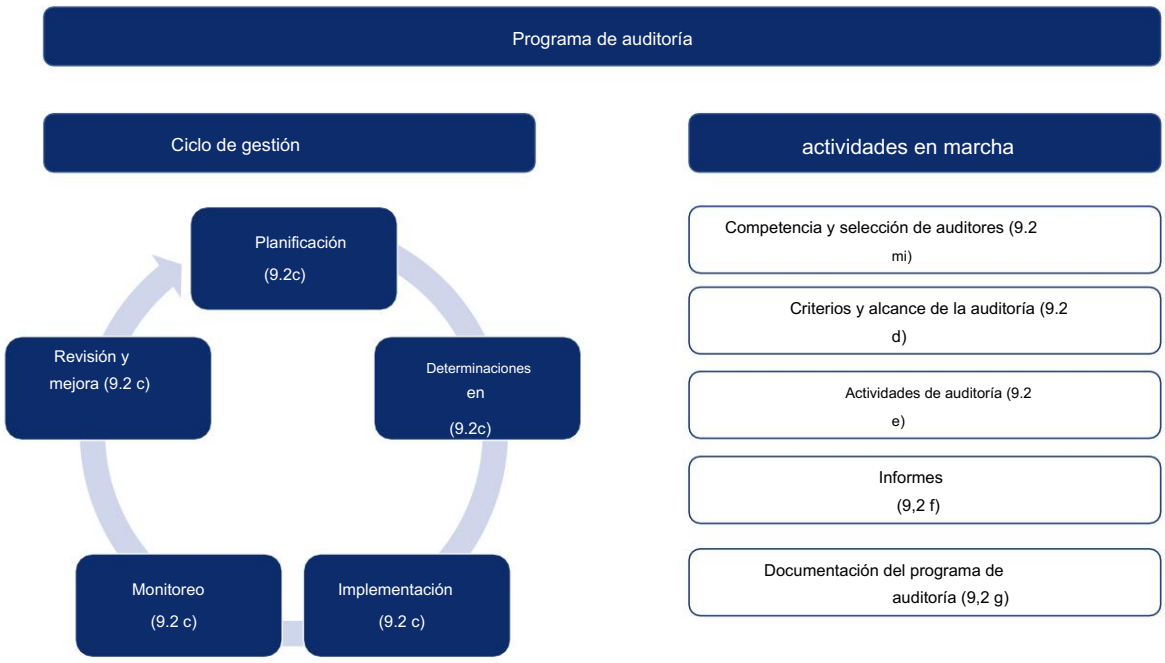


Figura 10 - Programa de auditoría [requisitos27]

Subproceso "Determinación

El empleado responsable del programa de auditoría deberá realizar, entre otras, las siguientes funciones:

- Definición e implementación de todo el programa de auditoría
- Identificar, evaluar y abordar los riesgos que afectan directamente a la programa de auditoría (por ejemplo, recursos demasiado escasos, brechas en las calificaciones de los auditores, áreas de consideración demasiado grandes para auditorías individuales).
- Establecimiento de procesos para la implementación de auditorías
- Determinación y contratación de los recursos necesarios
- Determinación de las auditorías y definición de las áreas y Criterios para las auditorías individuales.
- Determinación de los métodos y herramientas a utilizar
- Selección de auditores asegurando su calificación y experiencia.
- Garantizar que los registros del programa de auditoría se mantengan actualizados en todo momento. veces
- Seguimiento y mejora continuos del propio programa de auditoría

Subproceso "implementación"

Para la implementación y ejecución del programa de auditoría se deben implementar las decisiones tomadas durante la definición.

Que los objetivos y el alcance de las auditorías individuales ya estén definidos aquí depende del diseño respectivo o del nivel de detalle del programa de auditoría. Los objetivos y el alcance de las auditorías generalmente resultan de los requisitos individuales y las necesidades de protección de los sistemas informáticos en cuestión.

Se recomienda encarecidamente seleccionar las áreas a auditar de tal manera que puedan auditarse individualmente y con un esfuerzo manejable. Otros factores para la selección de las áreas a auditar son la criticidad de los procesos comerciales o de servicios y el período tolerable entre dos auditorías. Por supuesto, el número total de áreas auditadas (en un plazo de tres años) debe corresponder al alcance del SGSI.

Subproceso de seguimiento

En el subproceso de "monitoreo", el programa de auditoría en sí debe ser monitoreado continuamente en cuanto a calidad y eficiencia. Entre otras cosas, cabe preguntarse si

- el programa de auditoría sigue alineado con el alcance del ISMS y los requisitos comerciales,
- la planificación del tiempo y los recursos está diseñada adecuadamente,

27 Las referencias entre paréntesis son a la cláusula 9.2 de ISO/IEC 27001:2022.

los procesos/áreas/aplicaciones/sistemas/datos "correctos" son auditados y

la profundidad de las pruebas, así como el tipo de pruebas, son adecuados para respaldar de manera óptima los objetivos.

Es útil documentar el esfuerzo por auditoría. Dado que el esfuerzo requerido puede variar dependiendo de las características del sistema informático y/o de la unidad organizativa en cuestión, los datos se recopilan de esta manera para poder estimar mejor el esfuerzo requerido para futuras auditorías.

Al monitorear el desempeño de los miembros del equipo de auditoría, es importante prestar atención a la calidad, por ejemplo, la objetividad, claridad y comprensibilidad de los resultados de la auditoría. Aquí es relevante, entre otras cosas, si el departamento responsable de un sistema informático ha recibido recomendaciones comprensibles, adecuadas y completas para actuar en respuesta a las deficiencias detectadas. Si las recomendaciones de acción no se entienden porque, por ejemplo, falta información o las recomendaciones de acción no son apropiadas, esto indica que los miembros del equipo de auditoría necesitan apoyo técnico o metodológico adicional.

Este subproceso también incluye la recopilación y evaluación de comentarios de la dirección, las áreas o unidades organizativas auditadas, los auditores y otras partes interesadas.

Subproceso "Revisión y mejora"

En el subproceso "Revisión y Mejora", los responsables del programa de auditoría verifican periódicamente si se siguen cumpliendo las expectativas de las partes interesadas. El punto de partida es que se ha recopilado la información recopilada en el subproceso “Seguimiento”. Además, se debe determinar y controlar el continuo desarrollo profesional y metodológico de los auditores28.

El estado del programa de auditoría debe informarse a la dirección responsable. También es útil introducir KPI para que el nivel de calidad del programa de auditoría y de las auditorías internas en su conjunto sean mensurables y comparables. Las declaraciones de calidad como "Proporción de medidas aceptadas por los departamentos e iniciadas para su implementación" son más importantes que declaraciones puramente basadas en el tiempo como "Calidad del programa de auditoría interna" o "Calidad de la auditoría interna". zeg "tiempo de trabajo empleado por auditoría" es preferible.

Competencia y selección de auditores.

Los auditores del SGSI deben seleccionarse para garantizar la objetividad, experiencia e imparcialidad necesarias.

Los auditores son responsables de garantizar la calidad y confiabilidad del proceso de auditoría.

Deben describirse las competencias necesarias de un auditor interno (por ejemplo, en una descripción de función o puesto). descripción de

la lente).

Planificación y ejecución de auditorías.

Las auditorías se utilizan para identificar tanto las no conformidades con las especificaciones existentes como las posibles debilidades y peligros previamente desconocidos.

Cuando se trata de planificación de auditorías, se aplica lo siguiente: no hay auditoría sin una tarea de auditoría específica. Esto significa que el trabajo real es

La auditoría no debe comenzar hasta que la asignación haya sido asegurada y comunicada formalmente. Además, el área a auditar debe participar activamente en la planificación de la auditoría, por ejemplo, para coordinar el alcance (contra qué se auditará), la programación y la disponibilidad de personas de contacto durante la auditoría.

Si es posible, en la auditoría ya se deberían tomar medidas (inmediatas) para el tratamiento adecuado de los peligros. por derivar. Sin embargo, la implementación debe coordinarse formalmente con los respectivos propietarios del servicio, sistema y/o riesgo.

Si se identifican deficiencias o riesgos inherentes al proceso previamente desconocidos y cuyo tratamiento en el corto plazo no es posible, se incluirán

en el inventario central de riesgos.

Los resultados de la auditoría deben informarse periódicamente al nivel de gestión del SGSI (al menos en forma consolidada). ser

Los informes de auditoría deben indicar claramente qué sistemas y documentos han sido auditados o revisados y utilizados como base para la auditoría. fueron

utilizados para las auditorías.

La comunicación abierta que se mantiene durante toda la duración de una auditoría contribuye significativamente a

Esto ayuda a reducir las reservas por parte del área auditada y así disminuye el riesgo de que se oculte información.

o no presentado de manera realista.29

Para determinar la idoneidad, integridad y eficacia de las medidas implementadas, el En el transcurso de la auditoría, el auditor

interroga directamente a los empleados principales responsables del funcionamiento y seguimiento de estas medidas, examina la documentación y/o organiza y evalúa las medidas prácticas. manifestaciones. Los auditores deben tener amplios conocimientos técnicos y habilidades metodológicas.

Por tanto, procede seleccionar a los auditores en función de los objetivos y contenidos de la auditoría en cuestión.

28 Véase también la sección 7 de ISO/IEC 19011:2018.

29 Véase también "Comunicación - La pieza que falta", ISACA Journal 3/2012 (https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/

ves/journal-volumen-3-2012.pdf).

En el marco de la planificación de auditorías individuales, es decir, antes del inicio de la ejecución, los responsables deben aclarar en todos los niveles de gestión la asunción de los costes incurridos.

A más tardar en la reunión final de una auditoría, los resultados se revisarán junto con el área auditada.

El informe de auditoría debe ser aceptado formalmente por el auditor, quien debe comprender y aceptar los hallazgos y las recomendaciones de acción. Se debe buscar la aceptación formal del informe de auditoría. Los desacuerdos que no puedan resolverse deben documentarse en el informe.

Garantizar que la información relevante y los informes de auditoría se mantengan confidenciales y protegidos del acceso no autorizado.

Los datos deben almacenarse y archivarse de tal manera que estén protegidos contra el acceso no autorizado.

Los requisitos de la sección 9.2 para auditorías internas se pueden cumplir implementando las recomendaciones de la Sección 6.4 de ISO/IEC 19011:2018 e ISO/IEC 27007:2020 (ver Capítulo 8.5 Implementación de auditorías internas de SGSI (diagrama de proceso), página 62) , aunque cabe señalar que los requisitos normativos de ISO/IEC 27001:2022 no son en absoluto tan extensos como los descritos en las mejores prácticas actuales.

Se puede encontrar más información sobre auditorías internas, por ejemplo, en la Guía de TI QAR de ISACA. Esta guía está orientada a la auditoría interna de TI, pero también se puede aplicar mutatis mutandis a las auditorías internas del SGSI.30

Diferenciación de las auditorías internas del SGSI de las auditorías de certificación

Las auditorías internas (SGSI) son un instrumento esencial en el proceso de mejora continua del sistema de gestión.
Se utilizan para comprobar si el sistema de gestión cumple con los requisitos propios de la organización y dónde existe potencial de mejora.
El programa de auditoría garantiza que todas las áreas del alcance estén efectivamente controladas por el sistema de gestión.

Las auditorías de certificación son siempre auditorías externas. Son realizados por auditores externos calificados en nombre de un organismo de certificación. Los auditores externos suelen trabajar sobre la base de las dos normas ISO/IEC 27006:2015 "Requisitos para organismos que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información" e ISO/IEC 17021-1:2015 "Evaluación de la conformidad - Requisitos para organismos que proporcionan auditoría y certificación de sistemas de gestión".

Diferenciación de las auditorías internas del SGSI del sistema de control interno (SCI)

El sistema de control interno (SCI) de una empresa representa un instrumento de control y seguimiento esencial. Algunos aspectos del SGSI pueden ser un componente del sistema de control interno, pero el ICS generalmente va mucho más allá del SGSI y también incluye, sobre todo, controles de procesos especializados.

En un ICS, se hace una distinción entre actividades de control integradas en el proceso y actividades de control independientes del proceso. Las primeras suelen ser medidas de control que resultan del análisis de riesgos, buenas prácticas de gestión o requisitos internos y externos (por ejemplo, principio de control dual para la aprobación de reservas, autenticación multifactor para usuarios críticos, etc.) y, por tanto, pueden tener como referencia las recomendaciones de ISO/IEC 2700x. su origen. Se trata de la denominada "primera línea de distribución", que tiene como objetivo asegurar la regularidad de los procesos y actividades en la empresa y es realizada por el nivel de dirección directa.

La eficacia de las medidas de control también se puede comprobar independientemente del proceso, por ejemplo mediante un SGSI fuera de TI o mediante una función de cumplimiento. En la práctica, esto se suele denominar "segunda línea de defensa". Esta revisión no reemplaza las actividades del departamento de auditoría interna, que a su vez debe revisar la efectividad de todo el ICS como la llamada "tercera línea de defensa".

Si ya se ha establecido un ICS o está en proceso de establecerse o modificarse, vale la pena comprobar si, y en qué medida, los requisitos de control y auditoría del SGSI pueden tenerse en cuenta o incluso integrarse parcialmente en él. En la práctica no será posible una integración completa, ya que los objetivos de ambos sistemas difieren sustancialmente. Sin embargo, en cualquier caso se recomiendan interfaces organizacionales con el ICS y la auditoría interna.

En la práctica, COSO o COBIT, por ejemplo, se utilizan para modelar un ICS.

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

Documentación del programa o programas de auditoría (sección 9.2 g)

Documentación de los resultados de la auditoría (sección 9.2 g)

30 Ver https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_ii_2016_overall_screen.pdf.

Referencias

ISO/IEC 27001:2022 - Sección 9.2

ISO/CEI 19011:2018

ISO/CEI 27006:2015

ISO/IEC 27007:2020

ISO/CEI 17021-1:2015

3.13 Gestión de incidentes

Aunque no se menciona explícitamente en la parte normativa del estándar, la gestión de incidentes de seguridad de la información es otro componente elemental de un SGSI que funcione bien.

Los incidentes relevantes para la seguridad suelen ser no conformidades que, si se investigan sus causas, tienen una influencia decisiva en el proceso de mejora continua (CIP) y en la madurez del SGSI. Después de todo, sólo aquellos que reconozcan los errores y aprendan de ellos, es decir, que reconsideren sus actividades y estrategias y, por ejemplo, eliminen o reemplacen medidas ineficaces, adapten conceptos (de seguridad) existentes o implementen nuevas medidas (de seguridad), también obtendrán la el mejor beneficio posible a largo plazo de un sistema de gestión operado dentro de condiciones marco "impredecibles" (= riesgos).

Factores de éxito de la práctica.

Para mantener la seguridad de la información en las operaciones, es fundamental anticipar el manejo de los incidentes de seguridad de la información de la mejor manera posible,
es decir, definir con anticipación responsabilidades, procedimientos y opciones de tratamiento y también practicarlos.

El objetivo fundamental del proceso de manejo de incidentes de seguridad de la información es garantizar una acción en gran medida coordinada, específica y, por lo tanto, eficiente cuando ocurre una brecha de seguridad real o un ciberataque dirigido (consulte la Figura 11).

En este capítulo se aborda "únicamente" el tema de "incidentes de seguridad de la información". Para el desarrollo de un sistema holístico de preparación para emergencias, se hace referencia a la norma ISO 22301:2019 "Seguridad y resiliencia - Requisitos de los sistemas de gestión de la continuidad del negocio".

La organización debe definir una categorización de incidentes que tenga sentido para sí misma y que permita una delimitación practicable y razonable de la
gravedad, por ejemplo, distinguiendo entre incidentes, incidentes de seguridad, emergencias y crisis.

Se debe desarrollar un Plan de Respuesta a Incidentes que identifique los problemas clave que se deben abordar. Se definen los procesos (ver ISO/IEC 27001:2022, Anexo 5.24). Aunque esto no puede cubrir todas las eventualidades, sirve como guía cuando ocurre un incidente y garantiza un enfoque específico.

En caso de emergencia, sólo funcionará lo que ya se ha comunicado y practicado varias veces.
¿Quién? Si se confía en que los empleados afectados (¿quiénes son?) todavía saben "en caso de incidente" dónde deben buscar en su plan de tratamiento (¿dónde se almacenó nuevamente?) para poder seguir las instrucciones allí de forma inmediata y adecuada, y que los responsables responsables según el plan también sepan qué hacer con la información que les llega, usted estará sólo un poco mejor preparado que alguien "sin un plan" cuando se produzca un incidente de seguridad real - al menos al menos durante los primeros minutos u horas. Sin embargo, "en caso de incidente", eso es exactamente lo que importa. Por lo tanto, no basta con tener el plan en el cajón: hay que conocerlo y entrenar el procedimiento.

El proceso de gestión de incidentes de seguridad y su nivel de detalle deben adaptarse al apetito de riesgo de la organización y a las condiciones marco del SGSI.

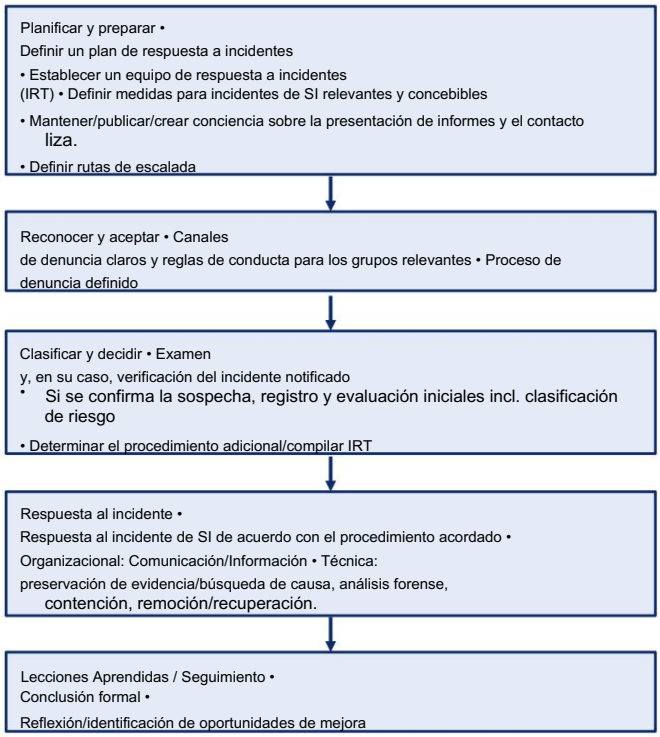


Figura 11: Gestión de respuesta a incidentes: modelo de fase basado en ISO/CEI 27035-1:2023

Planificar y preparar

Para lograr el objetivo fundamental del proceso, se deben tomar medidas preventivas en todas las fases operativas del proceso para preparar a la organización y a los empleados para tal eventualidad de la mejor manera posible. Además de las estrategias genéricas de resolución de problemas, se deben definir de antemano las personas de contacto y las vías de escalada.

Reconocer y aceptar

Los incidentes de seguridad siempre deben recibirse en un punto central de notificación (independientemente del momento de recepción).
Todos Se debe ofrecer un canal de denuncia claro a los grupos relevantes donde puedan ocurrir incidentes de SI, como empleados, proveedores de TI, clientes y socios.

Las normas de conducta en caso de irregularidades relevantes para la seguridad, incluidos los puntos de contacto/planes de notificación, deben estar orientadas a objetivos.
proporcionarse de manera específica.

Clasifica y decide

La oficina de informes decide si el evento notificado constituye realmente un evento de seguridad o si se trata de un evento que no está relacionado con la seguridad, el llamado "incidente de seguridad".

"Error conocido" ("Problema"), para el cual ya existe una descripción de la solución, o incluso una emergencia para la cual puede existir un plan de emergencia. En caso de duda, la derivación debe realizarse aquí (si es necesario a través de un "Gerente de turno"). La oficina de informes debe recibir la formación correspondiente.

Todos los informes de incidentes entrantes deben documentarse. Como mínimo, se registra la siguiente información:

- Número de identificación único
- Fecha de aceptación e ingreso del Incidente de Seguridad
- Nombre(s) del(los) informante(s), nombre(s) de la(s) persona(s) interesada(s) e identificación(es) de los sistemas de información/TI
- Descripción del incidente de seguridad (¿Cómo procedió el atacante, qué vulnerabilidades aprovechó? Daños causados hasta el momento)
- Medidas inmediatas ya adoptadas, si procede.

Todos los incidentes de seguridad deben clasificarse según un esquema de clasificación predefinido (inicial). para
que se pueda derivar una prioridad. Dependiendo de la prioridad, se deben iniciar medidas inmediatas predefinidas e informar a las personas responsables (p. ej., responsable de seguridad de la información, CISO).

Las incidencias de seguridad documentadas en el sistema (tickets) deberán ser objeto de seguimiento, si fuera necesario, para que se garantiza que también se procesen los eventos de baja clasificación.

Respuesta al incidente

En lo que respecta a la respuesta a incidentes, el siguiente procedimiento ha demostrado ser eficaz en la práctica:

1. Contención y preservación (inicial) de pruebas: Análisis del alcance y contención del incidente de seguridad, así como preservación (inicial) de posibles indicios y pruebas, si es necesario mediante análisis forenses y procedimientos predefinidos y practicados (!) (ver también Control 5.28).

Ejemplos de medidas de mitigación locales:

- Bloqueo de cuentas de usuario comprometidas
- Cierre de servicios atacados o comprometidos
- Uso de herramientas de malware (escáneres de virus, anti-spyware o programas similares) para limpiar los sistemas superficialmente
- Ejemplos en la red:
  - Aislar los sistemas comprometidos del resto de la red y restringir el acceso a una red en cuarentena.
  - Bloqueo de ciertos servicios y/o protocolos y direcciones IP seleccionadas

2. Eliminación y restauración: Medidas para restaurar el estado objetivo de un sistema de información/TI: En muchos casos, esto se puede hacer restaurando la copia de seguridad. En este caso, los datos y el software se restauran desde archivos de copia de seguridad "limpios" a sistemas "nuevos", por lo que se debe tener cuidado para garantizar que todas las vulnerabilidades (que aún puedan estar presentes en la copia de seguridad) estén cerradas (si es necesario, cargas y se deben aplicar parches) y que los archivos de respaldo estén libres de cambios realizados por un atacante.

Otra medida puede ser, por ejemplo, actualizar el software del sistema y reforzar los sistemas afectados.

3. Identificación de la causa raíz y preservación (ampliada) de la evidencia: Determinación de la causa raíz del evento y
preservación de posibles pistas y pruebas, si es necesario mediante análisis forenses adicionales.

Lecciones aprendidas/Seguimiento

La trazabilidad de un incidente de seguridad debe garantizarse en todo el tiempo. Esto significa que para cada
incidente debe ser evidente,

- cuál es el estado actual del procesamiento (por ejemplo, Nuevo, Aceptado, En curso, Detenido, Resuelto, Cerrado),

- quiénes son los empleados encargados del procesamiento, si cualquier,
- qué medidas están (actualmente) previstas para resolver el problema,
- cuando la implementación de las medidas requeridas es planificado.

Todos los incidentes de seguridad documentados deben (después del procesamiento) someterse a un examen para determinar si mediante la optimización del plan de respuesta a incidentes o cambios en la estructura y los procesos organizacionales (incluida la creación o adaptación de instrucciones de acción) se puede mejorar el manejo de incidentes similares. incidentes en el futuro.

En la tramitación de incidencias de seguridad siempre se debe documentado al final cómo tales

Se deben evitar incidentes en el futuro o minimizar su impacto. Si es necesario, de esto se pueden derivar otras medidas que se trasladarán al funcionamiento normal.

Requisitos de documentación

Según ISO/IEC 27001:2022, no existen requisitos mínimos de documentación.

Sin embargo, en la práctica, los siguientes documentos se han consolidado como líderes en objetivos:

Plan de respuesta a incidentes (IRP), incluidos los controles actuales (!). listas de tácticas y planes de escalada.

Normas de conducta en caso de irregularidades relacionadas con la seguridad

Descripciones de procesos e instrucciones de trabajo para asegurar evidencia

Informes de incidentes IS

Referencias

ISO/IEC 27001:2022 - cláusulas 5.24 - 5.28 y 6.8

ISO/CEI 27035-1:2023

ISO/CEI 27035-2:2023

ISO 22301:2019

3.14 Mejora Continua

Independientemente de cuántas guías y libros haya disponibles sobre el tema.
La razón por la que no se escriben sistemas de gestión "óptimos" es que probablemente nunca existirán en la práctica, ya que las organizaciones son demasiado diferentes para poder gestionarlas con un sistema de gestión uniforme. "receta" para servir. Además,
las condiciones generales cambian constantemente, por lo que nunca podrá haber una "mejor solución para siempre".

Por lo tanto, las organizaciones están llamadas a analizar las mejores prácticas existentes y aplicarlas de manera que se adapten constantemente a sus necesidades. En particular, están llamados a extraer potencial de mejora de sus no conformidades y así mejorar continuamente su SGSI. Este proceso se llama proceso de mejora continua (CIP).

Por lo tanto, una organización que quiera operar un SGSI que cumpla con los estándares debe definir medidas organizativas sobre cuya base se lleve a cabo la mejora continua de manera específica y planificada. La implementación de estas medidas y los respectivos resultados deben ser monitoreados y documentados adecuadamente. Además, la organización debe demostrar cómo garantiza que las deficiencias identificadas no se repitan.

Ciclo PDCA (Planificar-Hacer-Verificar-Actuar)

El enfoque recomendado para garantizar de manera sostenible la mejora continua del SGSI aún puede seguir el ciclo PDCA, que es la base de muchos sistemas de gestión.

Plan

- Establecimiento de objetivos de SI y responsabilidades para su consecución –

Establecimiento de las medidas de seguridad para alcanzar los objetivos de SI y el proceso operativo responsable de estas medidas.

- Definir los indicadores de desempeño que permitan medir el desempeño frente a los objetivos de SI y las medidas de seguimiento asociadas.
- Definición del proceso de medida de potencia incluyendo los puntos de medida, método de cálculo del indicador y los rangos estándar y de tolerancia.
- Definición de medidas correctoras para regular la seguridad medir en el rango estándar.

Hacer

- Medición continua del logro de objetivos de SI
- Inicio de acciones correctivas en caso de detectarse defectos o no conformidades

Verificar

- Seguimiento de las medidas de seguridad individuales en indicadores y comparaciones de las capacidades de desempeño individual con los objetivos de SI.
- Seguimiento de las medidas introducidas en cuanto a su implementación y eficacia.
- Crear informes de seguridad con indicadores clave de desempeño para la gestión basados en objetivos de SI.
  Estos informes deben incluir opciones de acción para las decisiones de gestión necesarias para fortalecer las medidas de seguridad que regularmente alcanzan el rango de tolerancia o exceden el umbral de ineficacia.

Actuar : tomar las decisiones de gestión necesarias para restablecer la eficacia de las medidas de seguridad. Las decisiones se transmiten a las operaciones para su implementación.

– Las decisiones tomadas se documentan adecuadamente y con sus motivos, por ejemplo mediante controles de seguridad.

Factores de éxito de la práctica.

El SGSI suele mejorarse identificando las desviaciones de los requisitos y las medidas correctoras que de ellos se derivan. Sin embargo, también es posible que las sugerencias de mejora se evalúen y apliquen directamente, es decir, sin que exista ninguna desviación.

Posibles fuentes de desviaciones y sugerencias de mejora.

Conclusiones de KPIs - análisis y mediciones Seguimiento de incidentes de seguridad Resultados de auditorías (internas) Revisión y control de la gestión por parte de la dirección Esquema de sugerencias de la empresa (sugerencia de mejora) Medidas derivadas del tratamiento de riesgos

Las medidas del PIC deben incluirse en un plan general de implementación, de modo que exista una lista central consolidada o al menos una lista de medidas para toda el área de negocio.

Además, los análisis de riesgos periódicos conducen a una mejora continua del SGSI.

Los resultados del tratamiento de riesgos son una parte importante de la mejora del SGSI, ya que se identifican e incluyen medidas de minimización de riesgos en el tratamiento de riesgos.

planes para su implementación.

El plan general de implementación facilita el seguimiento del estado de implementación y la fecha límite de implementación.

El objetivo del proyecto es garantizar que las medidas se apliquen antes de finales de año.

Acción correctiva versus acción correctiva: cuando se identifican deficiencias y no conformidades, la organización debe corregirlas o detenerlas (ver secciones 10.1 a y b).

Las correcciones se utilizan para rectificar o eliminar situaciones de incumplimiento. Para evitar que se repita el mismo error, es necesario realizar un análisis de causa raíz sostenible y definir acciones correctivas (ver secciones 10.1 c a g).

Requisitos de documentación

Según ISO/IEC 27001:2022, existen los siguientes requisitos mínimos de documentación:

Evidencia sobre la naturaleza de las no conformidades, así como sobre las medidas implementadas (sección 10.1 f)

Evidencia de la efectividad de la implementación de una medida (sección 10.1 d)

Evidencia de resultados de todas las acciones correctivas (Sección 10.1 gramo).

Además, los siguientes documentos han demostrado ser útiles en la práctica:

Procedimientos para acciones correctivas (de la sección 10.1 c)

Descripción de la gestión de incidentes y seguimiento de acciones correctivas

Herramienta de documentación para el seguimiento del estado de implementación. y verificar la efectividad de Medidas

Referencias

ISO/IEC 27001:2022 - Sección 10

Directivas ISO/IEC, Parte 1, Suplemento ISO consolidado, 2021 - Anexo SL

4 Integración y operacionalización de sistemas de gestión

Integración de sistemas de gestión existentes.

La directriz anterior contempla la implementación de un SGSI, pero sólo se centra en considera marginalmente la integración del sistema de gestión en las estructuras de gobernanza existentes, lo que a menudo es útil en este contexto, junto con las oportunidades y desafíos asociados, como el uso de efectos de sinergia al agrupar medidas. o conjuntos de control.

En la práctica, normalmente no es posible, o más bien no necesario, introducir un SGSI de forma aislada como una isla. Además de otros sistemas de gestión ya establecidos en la organización, incluidas sus medidas y procesos, también deben tenerse en cuenta otras circunstancias operativas u organizativas.

Todos los sistemas de gestión tienen grandes superposiciones en estructura, requisitos internos y externos y, por tanto, también oportunidades para utilizar sinergias. Al armonizar los requisitos de los sistemas de gestión, se pueden implementar medidas individuales en todos los sistemas de gestión, como el control de documentos o el uso integrado de evaluaciones de riesgos. Esto reduce el esfuerzo y el riesgo que implica la introducción, operación y verificación del sistema de gestión.[1]

En este capítulo se describen algunos de los desafíos que frecuentemente enfrentan las empresas y los enfoques asociados. Aborda explícitamente no sólo los nuevos sistemas de gestión que se introducirán, sino también las posibles mejoras de los sistemas establecidos. Debido al inmenso aumento de las amenazas a la seguridad cibernética en los últimos años y a los requisitos de cumplimiento en rápido aumento, especialmente para las organizaciones activas a nivel internacional, los sistemas establecidos también deben preguntarse si las regulaciones/procesos actuales todavía están actualizados para poder cumplir con las crecientes tareas que no sólo de forma eficaz sino también eficiente.

Las consultas del siguiente tipo son ahora comunes en Departamentos de SGSI:

- Compruebe si cumplimos con la "Ley de seguridad cibernética de China".
- ¿ Qué medidas de seguridad son relevantes para la seguridad de OT? [2]
- Una parte interesada/un cliente importante desearía un autoevaluación de su propia evaluación. seguridad según ISO/NIST/BSI/VDA-ISA/UE-
- Haga que se lleve a cabo DSGVO.

Por lo tanto, un nuevo desafío es la necesidad de responder con prontitud a un número creciente de requisitos de cumplimiento, que a menudo implican esencialmente las mismas medidas o al menos similares a las normas que conocemos.

Como resultado, como una especie de ola de listas de requisitos de cumplimiento, también están creciendo las tablas de mapeo en las que los respectivos controles, puntos de referencia, etc. se correlacionan entre sí para poder utilizar implementaciones ya evaluadas en otros sistemas de gestión. como el SCI o el sistema de gestión de protección de datos.

Mientras tanto, algunos proveedores de herramientas de gestión de riesgos/ cumplimiento/SGSI han adaptado sus soluciones para que sus propios objetivos de control puedan definirse y vincularse a los objetivos de control de las distintas normas.

Esto permite comprobar en cualquier momento el grado de madurez o cumplimiento de una norma y reconocer inmediatamente qué controles de la norma seleccionada todavía tienen puntos abiertos o riesgos.

1 Véase el Anexo SL.

2 Véase https://www.isaca.de/sites/default/files/isaca_leitfaden_cyber-sicherheits-check_ot.pdf, página 17 y siguientes.

Operacionalización mediante el establecimiento de un "Base de datos de control corporativo"

Basado en el enfoque del capítulo anterior, la introducción de una "base de datos de control corporativo" mantenida centralmente representa un área de acción en términos de mejora continua de todos los sistemas de gestión existentes.

En la mayoría de las organizaciones, los responsables de un sistema de gestión todavía tienen definidas sus propias medidas, lo que lleva al hecho de que muchas medidas de control, por ejemplo el borrado seguro de información, se mantienen dos o tres veces en diferentes lugares de la organización, incluyendo todas las medidas de seguimiento, como, por ejemplo, comprobar el estado de ejecución, realizar auditorías, comprobar la eficacia, etc. Esto, sin duda, conduce a un esfuerzo adicional y, en particular, a una falta de comprensión por parte de la persona técnicamente responsable del tema. Esto conduce inevitablemente a un trabajo adicional y, en particular, a una falta de comprensión por parte de los responsables técnicos del tema, ya que varios revisores/auditores formulan las mismas preguntas.

Los responsables también se ven afectados por normas, estándares y mejores prácticas específicas de la industria, productos y servicios, que a menudo entran en conflicto entre sí. Cumplir estos requisitos resulta especialmente difícil debido a la gran cantidad de procesos diferentes, manuales y aislados.

La estructura armonizada de los sistemas de gestión (según el Anexo SL) ha hecho que muchos sistemas de gestión ISO sean aptos para la integración. Ejemplos destacados son ISO/IEC 27001, ISO/IEC 27701 e ISO 22301. Otros sistemas de gestión que no son directamente relevantes para TI, como la gestión de calidad, la salud y seguridad en el trabajo y la protección ambiental, también siguen la nueva estructura y, por lo tanto, permiten que una organización -Amplio sistema de gestión integrado en el contexto de GRC.

Una base de datos de control corporativo armoniza las reglas de diferentes especificaciones y directrices para el usuario sobre la base de un marco común. Esto también va acompañado de un cambio de enfoque en el que las medidas de control ya no están alineadas con estándares sino con temas. La alineación con dominios (ver más abajo) es útil para este propósito.

Los estándares se asignan y mantienen con la ayuda de un metanivel. Este metanivel permite así medidas consolidadas para toda la organización[3] . Esto tiene la ventaja de que las respuestas a otras "normas/leyes/mejores prácticas" no consideradas anteriormente se vuelven evidentes, incluso si uno nunca antes ha estado involucrado con el nuevos requisitos de cumplimiento. Al mismo tiempo, esto permite a los usuarios recopilar los requisitos de forma individualizada en términos de industria, producto y rendimiento, y controlar su cumplimiento.

Además, contienen flujos de trabajo e interfaces correspondientes para que los cambios se puedan integrar automáticamente. De esta manera, los requisitos de gobernanza se consolidan e integran en un sistema holístico de gestión de riesgos y cumplimiento. La calidad de la base de datos crece con cada nueva evaluación de un estándar o norma.

Operacionalización a través de la alineación de "Central Controles Corporativos" con dominios

En la práctica, ha resultado útil agrupar y alinear los aspectos que deben gestionarse en la organización en dominios para crear una tarea y una responsabilidad temáticamente claras.
Estos dominios deben integrarse en el modelo de nivel superior de la organización en relación con sus sistemas de gestión, siendo COBIT una orientación adecuada.

Los dominios subyacentes en el ámbito de la seguridad de la información se podrían tomar, por ejemplo, de ISO/IEC 27002. En la nueva versión, por ejemplo, se podría agrupar según la nueva propiedad "Cybersecurity Concepts".
Alternativamente, sería posible agruparlos según el BSI IT-Grundschutz-Kompendium o la publicación especial NIST 800-53. Es importante que se cubran todas las áreas de interés.

La elección de los marcos de control tiene una importancia secundaria y la organización debe seleccionarlos adecuadamente para sus fines, que en última instancia también pueden variar debido a requisitos externos o al modelo de negocio. Es más probable que un fabricante de automóviles utilice TISAX, mientras que la Matriz de Control en la Nube (CCM) de Cloud Security Alliance (CSA) es más adecuada para un proveedor de SaaS, por ejemplo, mientras que el Compendio BSI será principalmente útil en el entorno regulatorio.

Independientemente de lo que decida la organización, con el soporte de software adecuado o con diligencia manual, el estándar finalmente seleccionado se puede mantener a través de un metanivel, de modo que muchos estándares se pueden tener en cuenta en gran medida. En este enfoque, el administrador de dominio es responsable de resolver innovaciones, conflictos de requisitos o ambigüedades en un punto central. La calidad de la base de datos crece así cada vez más con cada nueva evaluación de un estándar o norma.

3 Véanse, por ejemplo, los controles de las normas IDW PS 951, EU-DSGVO (ISO/IEC 27701:2019), ISMS (ISO/IEC 27002:2022), BCMS (ISO 22301:2019), QMS (ISO 9001: 2015) a Controles de Operaciones de TI/OT.

5 Glosario

ADV Procesamiento de datos por encargo: el procesamiento de datos personales por parte de proveedores de servicios (externo o interno por entidades legalmente independientes de un grupo de empresas) de conformidad con el art. 28 UE-DSGVO.

Amenaza persistente avanzada APT

Activo Cualquier cosa que tenga valor para la organización, también llamado activo de información o activo de información. Hay muchos tipos de activos, como por ejemplo: información, software, hardware, servicios, personas y sus calificaciones, habilidades y experiencia, y activos intangibles como la reputación y la imagen. ISO/IEC 27005:2022 distingue entre activos primarios y secundarios, donde los activos primarios incluyen procesos de negocio y actividades de negocio, así como información. Los activos secundarios respaldan los activos primarios, como instalaciones, salas, hardware, software, redes, personal y sitios web.

Sistema de gestión de continuidad del negocio BCMS

Cuadro de mando de criticidad empresarial de BCS

BDEW Asociación Alemana de Industrias de Energía y Agua

Análisis de impacto empresarial de BIA

BO Organización operativa

BSI Oficina Federal de Seguridad de la Información

Modelo de seguridad en madurez del edificio BSIMM

Matriz de control de la nube de CCM

Equipo de respuesta a emergencias informáticas del CERT

Director de Información CIO

Centro CIS para la seguridad de Internet

CISO Director de Seguridad de la Información

Objetivos de control de COBIT para la información y tecnologías relacionadas: un marco reconocido internacionalmente para el gobierno de TI con un enfoque en los procesos de TI y los objetivos de control.

Comité COSO de Organizaciones Patrocinadoras de la Comisión Tread-way, una organización estadounidense que, entre otras cosas, desarrolló el estándar reconocido para controles internos conocido como modelo COSO.

Alianza de seguridad en la nube CSA

Delegado de Protección de Datos del DPO

DSGVO ver EU-DSGVO

UE Unión Europea

EU-DSGVO Reglamento general de protección de datos de la UE

EEE Espacio Económico Europeo

Gobernanza, riesgo y cumplimiento de GRC

TIC Tecnología de la Información y las Comunicaciones

Comisión Electrotécnica Internacional IEC - una organización inter-
organización nacional de normalización que, entre otras cosas, desarrolló el estándar ISO/IEC 2700x junto con ISO.

Sistema de control interno del ICS

Plan de respuesta a incidentes del IRP

Equipo de respuesta a incidentes IRT

Seguridad de la información SI

Evaluaciones de seguridad de la información de ISA

Norma internacional ISAE sobre encargos de aseguramiento

Oficial de seguridad de la información de la JIS

Sistema de gestión de seguridad de la información SGSI : parte del sistema de gestión general, basado en un enfoque de riesgo empresarial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procesos y recursos.

Organización Internacional de Normalización ISO : editor de normas internacionales, incluida la familia ISO/IEC 2700x.

Oficial de Seguridad de la Información ISO , sinónimo de ISB

Indicador de control clave KCI

Indicador clave de rendimiento KPI : un indicador de rendimiento

Indicador clave de riesgo KRI

CIP Proceso de mejora continua

Requisitos mínimos de MaRisk para la gestión de riesgos: una instrucción administrativa sobre el diseño de la gestión de riesgos en las instituciones de crédito alemanas del alemán
Autoridad de Supervisión Financiera (BaFin)

Instituto Nacional de Estándares y Tecnología NIST

NPS (Net Promoter Score) Indicador que mide en qué medida los consumidores recomendarían un producto o servicio a otros.

Tecnología operativa OT

Proyecto de seguridad de aplicaciones web abiertas OWASP

Ciclo PDCA Planificar-Hacer-Verificar-Actuar: una mejora continua proceso

QAR-IT Guía ISACA para realizar un aseguramiento de la calidad Revisión de la Auditoría Interna de TI (QAR-IT)

Representante de Gestión de Calidad QMB

Sistema de gestión de calidad QMS

Garantía de calidad

Matriz RACI Las organizaciones utilizan la categorización según RACI para describir qué rol es responsable de qué actividades y qué roles deben estar involucrados. De esta manera se puede lograr una descripción clara de responsabilidades y competencias. Los términos se interpretan de la siguiente manera:

Responsable : responsable de la implementación real (responsabilidad de implementación). La persona que toma la iniciativa para la implementación ante los
demás. También interpretado como responsabilidad en el sentido disciplinar y cualitativo.

Responsable - responsable (responsabilidad general), responsable en el sentido de "aprobar", "bil-ligen" o "firmar". La persona que
soporta la responsabilidad en el sentido jurídico o comercial. También interpretado como responsabilidad desde la perspectiva del centro de costos.

Consultado - consultado (experiencia profesional). Una persona cuyo consejo debe o debe buscarse. También referido
como
Responsabilidad interpretada desde un punto de vista profesional.

estar informado - estar informado (derecho a la información). Una persona que recibe información sobre el curso o la La persona recibe el resultado de la actividad o tiene derecho a recibir información.

Como regla general, sólo una persona (rol) debe ser responsable por actividad. Sin embargo, varias personas pueden ser responsables, consultadas o informadas de una actividad. También es posible que una persona sea responsable y responsable de una actividad al mismo tiempo.

Riesgo Efecto de la incertidumbre sobre los objetivos (definición según ISO 31000:2018)

Objetivo del punto de recuperación de RPO

Objetivo de tiempo de recuperación de RTO

Software SaaS como servicio

Alcance Alcance

Ciclo de vida del desarrollo de software SDLC

Proceso de respuesta a incidentes de seguridad SIRP

Acuerdo de nivel de servicio SLA : acuerdo entre el cliente y proveedor de servicios

SMART Específico, mensurable, aceptado, realista, programado

Declaración de aplicabilidad de SoA : declaración documentada de objetivos y medidas de control relevantes y aplicables en el SGSI de la organización.

Matriz SoD Matriz de segregación de funciones: descripción general de las segregaciones funcionales que se deben considerar entre roles dentro de la organización.

Intercambio de evaluación de seguridad de la información confiable de TISAX

Ley de Telemedios TMG

Ley de competencia desleal de la UWG

Asociación VDA de la Industria Automotriz eV

Vulnerabilidad de día cero Una vulnerabilidad no revelada ni corregida previamente que podría explotarse para manipular o atacar aplicaciones informáticas, datos u otros servicios de red.

6 referencias

Normas y estándares

ISO 9001:2015 Sistemas de gestión de calidad - Requisitos

ISO 19011:2018 Directrices para la auditoría de sistemas de gestión.

ISO 22301:2019 Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio - Requisitos

ISO 31000:2018 Gestión de riesgos - Directrices

IEC 31010:2018 Gestión de riesgos: técnicas de evaluación de riesgos

Guía ISO 73:2009 Gestión de riesgos - Vocabulario

ISO/IEC 17021-1:2015 Evaluación de la conformidad - Requisitos para los organismos que proporcionan auditoría y certificación de sistemas de gestión - Parte 1: Requisitos

ISO/IEC 17021-2:2016 Evaluación de la conformidad - Requisitos para los organismos que proporcionan auditoría y certificación de sistemas de gestión - Parte 2: Requisitos de competencia para la auditoría y certificación de sistemas de gestión ambiental

ISO/IEC 27000:2018 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario

ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de seguridad de la información - Requisitos

ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información

ISO/IEC 27003:2017 Tecnología de la información - Técnicas de seguridad - Sistema de gestión de seguridad de la información - Orientación

ISO/IEC 27004:2016 Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Monitoreo, medición, análisis y evaluación

ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de riesgos de seguridad de la información

ISO/IEC 27006:2015 Tecnología de la información - Técnicas de seguridad - Requisitos para los organismos que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información

ISO/IEC 27007:2020 Seguridad de la información, ciberseguridad y protección de la privacidad: Directrices para la auditoría de sistemas de gestión de seguridad de la información

ISO/IEC 27014:2020 Seguridad de la información, ciberseguridad y protección de la privacidad - Gobernanza de la seguridad de la información

ISO/IEC 27017:2015 Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube

ISO/IEC 27018:2019 Tecnología de la información - Técnicas de seguridad - Código de prácticas para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII

ISO/IEC 27032:2012 Tecnología de la información - Técnicas de seguridad - Directrices para la ciberseguridad

ISO/IEC 27035-1:2023 Tecnología de la información - Gestión de incidentes de seguridad de la información - Parte 1: Principios y proceso

ISO/IEC 27035-2:2023 Tecnología de la información. Gestión de incidentes de seguridad de la información. Parte 2: Directrices para planificar y preparar la respuesta a incidentes.

ISO/IEC 27036-1:2021 Ciberseguridad - Relaciones con proveedores - Parte 1: Descripción general y conceptos

ISO/IEC 27036-2:2022 Ciberseguridad - Relaciones con proveedores - Parte 2: Requisitos

ISO/IEC 27036-3:2014 Tecnología de la información - Técnicas de seguridad - Seguridad de la información para las relaciones con proveedores - Parte 3: Directrices para la seguridad de la cadena de suministro de tecnologías de la información y las comunicaciones

Directivas ISO/IEC, Parte 1, Suplemento ISO consolidado - Procedimiento para el trabajo técnico - Procedimientos específicos de ISO -, Anexo SL, 2021

ISO/IEC TR 27023:2015 Tecnología de la información - Técnicas de seguridad - Mapeo de las ediciones revisadas de ISO/IEC 27001 e ISO/IEC 27002

Más fuentes

COBIT 2019 para Seguridad de la Información, ISACA 2019

Documento técnico de BDEW, Requisitos para sistemas seguros de control y telecomunicaciones, versión 2.0, mayo de 2018

Estándar BSI 200-2, Procedimiento IT-Grundschutz, Versión 1.0, 2017

Estándar BSI 200-3, Análisis de riesgos basado en IT-Grundschutz, Versión 1.0, 2017

IT-Grundschutz-Kompendium 2022, BSI, 2022

Guía de verificación de seguridad cibernética, versión 2, BSI/ISACA, 2020

SC27 Platinum Book - Veinte años de ISO/IEC JTC1/SC27

enlaces web

www.bsi.bund.de

www.enisa.europa.eu

www.esma.europa.eu

www.isaca.de

www.isaca.org

www.iso27001security.com

www.iso.org

www.jtc1sc27.din.de

7 Lista de figuras/tablas

Imágenes

Mesas

8 archivos adjuntos

8.1 Mapeo del Anexo ISO/IEC 27001:2022 vs. Anexo ISO/IEC 27001:2013

La siguiente tabla muestra la coherencia de las medidas de ISO/IEC 27001:2022 con ISO/IEC 27001:2013.

Mapeo: ISO/IEC 27001:2022 frente a ISO/IEC 27001:2013		
ISO/CEI 27001:2022		ISO/CEI 27001:2013
5	Controles organizacionales	
5.1	Políticas de seguridad de la información.	A.5.1.1, A.5.1.2
5.2	Funciones y responsabilidades de seguridad de la información	A.6.1.1
5.3	Segregación de deberes	A.6.1.2
5.4	Responsabilidades de gestión	A.7.2.1
5.5	Contacto con autoridades	A.6.1.3
5.6	Contacto con grupos de intereses especiales	A.6.1.4
5.7	Inteligencia de amenazas	Nuevo
5.8	Seguridad de la información en la gestión de proyectos.	A.6.1.5, A.14.1.1
5.9	Inventario de información y otros activos asociados	A.8.1.1, A.8.1.2
5.10	Uso aceptable de la información y otros activos asociados	A.8.1.3, A.8.2.3
5.11	Devolución de activos	A.8.1.4
5.12	Clasificación de la información	A.8.2.1
5.13	Etiquetado de información	A.8.2.2
5.14	Transferencia de información	A.13.2.1, A.13.2.2, A.13.2.3
5.15	Control de acceso	A.9.1.1, A.9.1.2
5.16	Gestión de identidad	A.9.2.1
5.17	Información de autenticación	A.9.2.4, A.9.3.1, A.9.4.3
5.18	Derechos de acceso	A.9.2.2, A.9.2.5, A.9.2.6
5.19	Seguridad de la información en las relaciones con proveedores	A.15.1.1
5.20	Abordar la seguridad de la información en los acuerdos con proveedores	A.15.1.2
5.21	Gestión de la seguridad de la información en la cadena de suministro de TIC	A.15.1.3
5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores.	A.15.2.1, A.15.2.2
5.23	Seguridad de la información para el uso de servicios en la nube.	Nuevo
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información.	A.16.1.1
5.25	Evaluación y decisión sobre eventos de seguridad de la información.	A.16.1.4
5.26	Respuesta a incidentes de seguridad de la información	A.16.1.5
5.27	Aprender de los incidentes de seguridad de la información	A.16.1.6
5.28	Recopilación de pruebas	A.16.1.7
5.29	Seguridad de la información durante la interrupción	A.17.1.1, A.17.1.2, A.17.1.3
5.30	Preparación de las TIC para la continuidad del negocio	Nuevo
5.31	Identificación de requisitos legales, estatutarios, reglamentarios y contractuales.	A.18.1.1, A.18.1.5

5	Controles organizacionales (continuación)	
5.32	Derechos de propiedad intelectual	A.18.1.2
5.33	Protección de registros	A.18.1.3
5.34	Privacidad y protección de la PII	A.18.1.4
5.35	Revisión independiente de la seguridad de la información.	A.18.2.1
5.36	Cumplimiento de políticas y estándares de seguridad de la información	A.18.2.2, A.18.2.3
5.37	Procedimientos operativos documentados	A.12.1.1
6	controles de personas	
6.1	Poner en pantalla	A.7.1.1
6.2	Términos y condiciones de empleo	A.7.1.2
6.3	Concientización, educación y capacitación sobre seguridad de la información.	A.7.2.2
6.4	Proceso Disciplinario	A.7.2.3
6.5	Responsabilidades tras el despido o cambio de empleo	A.7.3.1
6.6	Acuerdos de confidencialidad o no divulgación	A.13.2.4
6.7	Trabajo remoto	A.6.2.2
6.8	Informes de eventos de seguridad de la información	A.16.1.2, A.16.1.3
7	Controles físicos	
7.1	Perímetro de seguridad física	A.11.1.1
7.2	Controles de entrada física	A.11.1.2, A.11.1.6
7.3	Seguridad de oficinas, habitaciones e instalaciones.	A.11.1.3
7.4	Monitoreo de seguridad física	Nuevo
7.5	Protección contra amenazas físicas y ambientales.	A.11.1.4
7.6	Trabajar en áreas seguras	A.11.1.5
7.7	Escritorio claro y pantalla clara	A.11.2.9
7.8	Ubicación y protección de equipos.	A.11.2.1
7.9	Seguridad de los activos fuera de las instalaciones	A.11.2.6
7.10	Medios de almacenamiento	A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5
7.11	Servicios públicos de apoyo	A.11.2.2
7.12	Seguridad del cableado	A.11.2.3
7.13	Mantenimiento de equipo	A.11.2.4
7.14	Eliminación segura o reutilización del equipo	A.11.2.7
8	Controles tecnológicos	
8.1	Dispositivos terminales de usuario	A.6.2.1, A.11.2.8
8.2	Derechos de acceso privilegiados	A.9.2.3
8.3	Restricción de acceso a la información	A.9.4.1
8.4	Acceso al código fuente	A.9.4.5
8.5	Autenticación segura	A.9.4.2
8.6	Gestión de capacidad	A.12.1.3
8.7	Protección contra malware	A.12.2.1
8.8	Gestión de vulnerabilidades técnicas.	A.12.6.1, A.18.2.3
8.9	Gestión de configuración	Nuevo
8.10	Eliminación de información	Nuevo

8	Controles tecnológicos (continuación)	
8.11	Enmascaramiento de datos	Nuevo
8.12	Prevención de fuga de datos	Nuevo
8.13	Copia de seguridad de la información	A.12.3.1
8.14	Redundancia de instalaciones de procesamiento de información.	A.17.2.1
8.15	Inicio sesión	A.12.4.1, A.12.4.2, A.12.4.3
8.16	Actividades de seguimiento	Nuevo
8.17	Sincronización del reloj	A.12.4.4
8.18	Uso de programas de utilidad privilegiados.	A.9.4.4
8.19	Instalación de software en sistemas operativos.	A.12.5.1, A.12.6.2
8.20	Controles de red	A.13.1.1
8.21	Seguridad de los servicios de red.	A.13.1.2
8.22	Segregación en redes	A.13.1.3
8.23	Filtrado web	Nuevo
8.24	Uso de criptografía	A.10.1.1, A.10.1.2
8.25	Ciclo de vida de desarrollo seguro	A.14.2.1
8.26	Requisitos de seguridad de la aplicación	A.14.1.2, A.14.1.3
8.27	Principios de ingeniería y arquitectura de sistemas seguros	A.14.2.5
8.28	Codificación segura	Nuevo
8.29	Pruebas de seguridad en desarrollo y aceptación.	A.14.2.8, A.14.2.9
8.30	Desarrollo subcontratado	A.14.2.7
8.31	Separación de los entornos de desarrollo, prueba y producción.	A.12.1.4, A.14.2.6
8.32	Gestión del cambio	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
8.33	Información de prueba	A.14.3.1
8.34	Protección de los sistemas de información durante la auditoría y las pruebas.	A.12.7.1

La siguiente tabla muestra la coherencia de las medidas de ISO/IEC 27001:2013 con ISO/IEC 27001:2022.

Mapeo: ISO/IEC 27001:2013 frente a ISO/IEC 27001:2022		
ISO/CEI 27001:2013		ISO/CEI 27001:2022
A.5	Políticas de seguridad de la información	
A.5.1.1	Políticas de seguridad de la información.	5.1
A.5.1.2	Revisión de las políticas de seguridad de la información.	5.1
A.6	Organización de la seguridad de la información.	
A.6.1.1	Funciones y responsabilidades de seguridad de la información	5.2
A.6.1.2	Segregación de deberes	5.3
A.6.1.3	Contacto con autoridades	5.5
A.6.1.4	Contacto con grupos de intereses especiales	5.6
A.6.1.5	Seguridad de la información en la gestión de proyectos.	5.8
A.6.2.1	Política de dispositivos móviles	8.1
A.6.2.2	Teletrabajo	6.7
A.7	Seguridad de los recursos humanos	
A.7.1.1	Poner en pantalla	6.1
A.7.1.2	Términos y condiciones de empleo	6.2
A.7.2.1	Responsabilidades de gestión	5.4
A.7.2.2	Concientización, educación y capacitación sobre seguridad de la información	6.3
A.7.2.3	Proceso Disciplinario	6.4
A.7.3.1	Terminación o cambio de responsabilidades laborales	6.5
A.8	Gestión de activos	
A.8.1.1	Inventario de activos	5.9
A.8.1.2	Propiedad de activos	5.9
A.8.1.3	Uso aceptable de los activos	5.10
A.8.1.4	Devolución de activos	5.11
A.8.2.1	Clasificación de la información	5.12
A.8.2.2	Etiquetado de información	5.13
A.8.2.3	Manejo de activos	5.10
A.8.3.1	Gestión de medios extraíbles.	7.10
A.8.3.2	Eliminación de medios	7.10
A.8.3.3	Transferencia de medios físicos	7.10
A.9	Control de acceso	
A.9.1.1	Política de control de acceso	5.15
A.9.1.2	Acceso a redes y servicios de red	5.15
A.9.2.1	Alta y Baja de Usuario	5.16
A.9.2.2	Aprovisionamiento de acceso de usuario	5.18
A.9.2.3	Gestión de derechos de acceso privilegiado	8.2
A.9.2.4	Gestión de información secreta de autenticación de usuarios	5.17
A.9.2.5	Revisión de los derechos de acceso de los usuarios	5.18
A.9.2.6	Eliminación o ajuste de derechos de acceso	5.18

A.9	Control de acceso (continuación)	
A.9.3.1	Uso de información de autenticación secreta	5.17
A.9.4.1	Restricción de acceso a la información	8.3
A.9.4.2	Procedimientos de inicio de sesión seguro	8.5
A.9.4.3	Sistema de gestión de contraseñas	5.17
A.9.4.4	Uso de programas de utilidad privilegiados	8.18
A.9.4.5	Control de acceso al código fuente del programa	8.4
A.10	Criptografía	
A.10.1.1	Política sobre el uso de controles criptográficos	8.24
A.10.1.2	Gestión de claves	8.24
A.11	Seguridad física y ambiental	
A.11.1.1	Perímetro de seguridad física	7.1
A.11.1.2	Controles de entrada física	7.2
A.11.1.3	Seguridad de oficinas, habitaciones e instalaciones	7.3
A.11.1.4	Protección contra amenazas externas y ambientales	7.5
A.11.1.5	Trabajar en áreas seguras	7.6
A.11.1.6	Áreas de entrega y carga	7.2
A.11.2.1	Ubicación y protección de equipos	7.8
A.11.2.2	Servicios públicos de apoyo	7.11
A.11.2.3	Seguridad del cableado	7.12
A.11.2.4	Mantenimiento de equipo	7.13
A.11.2.5	Eliminación de activos	7.10
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	7.9
A.11.2.7	Eliminación segura o reutilización del equipo	7.14
A.11.2.8	Equipo de usuario desatendido	8.1
A.11.2.9	Política de escritorio limpio y pantalla limpia	7.7
A.12	Seguridad de las operaciones	
A.12.1.1	Procedimientos operativos documentados	5.37
A.12.1.2	Gestión del cambio	8.32
A.12.1.3	Gestión de capacidad	8.6
A.12.1.4	Separación de entornos operativos, de prueba y de desarrollo.	8.31
A.12.2.1	Controles contra malware	8.7
A.12.3.1	Copia de seguridad de la información	8.13
A.12.4.1	El registro de eventos	8.15
A.12.4.2	Protección de la información de registro	8.15
A.12.4.3	Registros de administrador y operador	8.15
A.12.4.4	Sincronización del reloj	8.17
A.12.5.1	Instalación de software en sistemas operativos.	8.19
A.12.6.1	Gestión de vulnerabilidades técnicas.	8.8
A.12.6.2	Restricciones en la instalación de software	8.19
A.12.7.1	Controles de auditoría de sistemas de información.	8.34

A.13	Seguridad de las comunicaciones	
A.13.1.1	Controles de red	8.20
A.13.1.2	Seguridad de los servicios de red.	8.21
A.13.1.3	Segregación en redes	8.22
A.13.2.1	Políticas y procedimientos de transferencia de información.	5.14
A.13.2.2	Acuerdos sobre transferencia de información.	5.14
A.13.2.3	mensajería electrónica	5.14
A.13.2.4	Acuerdos de confidencialidad o no divulgación	6.6
A.14	Adquisición, desarrollo y mantenimiento de sistemas	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	5.8
A.14.1.2	Protección de servicios de aplicaciones en redes públicas	8.26
A.14.1.3	Protección de transacciones de servicios de aplicaciones	8.26
A.14.2.1	Política de desarrollo seguro	8.25
A.14.2.2	Procedimientos de control de cambios del sistema	8.32
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma operativa	8.32
A.14.2.4	Restricciones sobre cambios en paquetes de software	8.32
A.14.2.5	Principios de ingeniería de sistemas seguros	8.27
A.14.2.6	Entorno de desarrollo seguro	8.31
A.14.2.7	Desarrollo subcontratado	8.30
A.14.2.8	Pruebas de seguridad del sistema	8.29
A.14.2.9	Pruebas de aceptación del sistema	8.29
A.14.3.1	Protección de datos de prueba	8.33
A.15	Relaciones con proveedores	
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	5.19
A.15.1.2	Abordar la seguridad en los acuerdos con proveedores	5.20
A.15.1.3	Cadena de suministro de tecnologías de la información y las comunicaciones	5.21
A.15.2.1	Seguimiento y revisión de servicios de proveedores.	5.22
A.15.2.2	Gestión de cambios en los servicios de los proveedores.	5.22
A.16	Gestión de Incidentes de Seguridad de la Información	
A.16.1.1	Responsabilidades y procedimientos	5.24
A.16.1.2	Notificación de eventos de seguridad de la información	6.8
A.16.1.3	Informar las debilidades de la seguridad de la información	6.8
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	5.25
A.16.1.5	Respuesta a incidentes de seguridad de la información	5.26
A.16.1.6	Aprender de los incidentes de seguridad de la información	5.27
A.16.1.7	Recopilación de pruebas	5.28
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	5.29
A.17.1.2	Implementación de la continuidad de la seguridad de la información	5.29
A.17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información	5.29
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	8.14

A.18	Cumplimiento	
A.18.1.1	Identificación de la legislación aplicable y requisitos contractuales.	5.31
A.18.1.2	Derechos de propiedad intelectual	5.32
A.18.1.3	Protección de registros	5.33
A.18.1.4	Privacidad y protección de la información de identificación personal	5.34
A.18.1.5	Regulación de controles criptográficos	5.31
A.18.2.1	Revisión independiente de la seguridad de la información	5.35
A.18.2.2	Cumplimiento de políticas y estándares de seguridad	5.36
A.18.2.3	Revisión de cumplimiento técnico	5,36, 8,8

8.2 Comparación de versiones ISO/IEC 27001/2:2022 vs. ISO/IEC 27001/2:2013

A continuación encontrará una breve descripción de los principales cambios en el contenido de ISO/IEC 27001:2022 e ISO/IEC 27002:2022 en comparación con las versiones anteriores de 2013.

ISO/IEC 27001:2022 frente a ISO/IEC 27001:2013

En octubre de 2022 se publicó la tercera edición de ISO/IEC 27001. Al igual que otras normas ISO/IEC que describen los requisitos para un sistema de gestión (por ejemplo, ISO 9001, ISO 14001, ISO 22301), la ISO/IEC 27001 sigue una estructura uniforme, la denominada "Estructura Armonizada" del Anexo SL de las Directivas ISO/IEC, Parte 1. Dado que esta estructura cambió en 2021, los capítulos principales de ISO/IEC 27001:2022 se han adaptado en consecuencia. Esto ha resultado en los siguientes cambios en los capítulos principales[1]:

- La organización (Capítulo 4 "Contexto de la organización") ahora, además de definir requisitos relevantes de las partes interesadas, también es necesario definir cuáles de estos requisitos se abordan en el marco del SGSI (Sección 4.2c).
- La gestión del cambio (Capítulo 6 "Planificación") se ha añadido a la Sección 6.2 "Objetivos de seguridad de la información y planificación para alcanzarlos" para incluir el aspecto de que, además de los requisitos para definir e implementar objetivos de seguridad de la información, estos también deben ser monitoreado. El capítulo se amplió aún más con la sección 6.3 "Planificación de cambios" para la implementación de cambios planificados en el SGSI. Las circunstancias que requieren un cambio en el SGSI pueden ser planificadas o no (como se describe en la Sección 6.1 "Acciones para abordar riesgos y oportunidades"), pero los cambios en sí deben planificarse.
- En el capítulo 8 "Operación", la nueva versión añade que se deben establecer criterios explícitos para la implementación de los procesos del Capítulo 6 "Planificación" y la implementación debe realizarse de acuerdo con estos criterios.
- En el Capítulo 9 "Evaluación del desempeño", las secciones 9.2 "Auditoría interna" y 9.3 "Revisión de la gestión" se dividen en subsecciones adicionales, pero su contenido sigue siendo idéntico.
- La Sección 9.3 "Revisión por la Gestión" se ha dividido en tres subsecciones. Aquí se agregó que ma- revisiones de la gestión, los cambios en las necesidades y expectativas de las partes interesadas que son necesarios para el Los SGSI son relevantes (sección 9.3.2. "Aportes de revisión por la dirección", (c).
- Mejora Continua: El Capítulo 10 se ha reorganizado para que la declaración, idoneidad, adecuación y eficacia del SGSI de forma continua, preceda a la sección de no conformidades, con el objetivo de fomentar la mejora en lugar de la acción correctiva.
- La nueva versión de ISO/IEC 27001:2022 contiene en esencia un reemplazo completo del Anexo A, que refleja los controles de ISO/IEC 27002:2022. La única diferencia entre la información del anexo de ISO/IEC 27001 y los controles de ISO/IEC 27002 radica en la redacción de los requisitos: El anexo de ISO/IEC 27001:2022 utiliza la palabra "deberá", lo que significa que el Los controles son obligatorios, mientras que ISO/IEC 27002 utiliza la palabra "debería", lo que significa que los requisitos deben entenderse como recomendaciones.
- Los controles enumerados en el anexo todavía no pretenden ser completa y es posible que se requieran medidas adicionales. Las empresas también son libres, como antes, de utilizar medidas de otras fuentes (por ejemplo, NIST Cybersecurity Framework, BSI IT-Grundschutz, ISF Standard of Good Practice, etc.) para mitigar sus riesgos de seguridad de la información. En este caso, todo lo que se requiere es una declaración de aplicabilidad que incluya una correlación de las medidas seleccionadas con los controles del Anexo de ISO/IEC 27001:2022, así como la justificación requerida para la selección. Esto confirma que no se ha descuidado ningún requisito que sea realmente aplicable y necesario para mitigar los riesgos existentes (cf. ISO/IEC 27001:2022, cláusula 6.1.3. “Tratamiento de riesgos de seguridad de la información”, (b) y Nota 2 de la Sección 6.1.3; (c) se ha modificado ligeramente para aclarar aún más este aspecto).

ISO/IEC 27002:2022 frente a ISO/IEC 27002:2013

En la nueva versión de ISO/IEC 27002:2022 ya se nota el cambio de título de "Tecnologías de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información" a "Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información". El término "Código de prácticas" se eliminó para reflejar mejor su propósito como referencia para las medidas de seguridad de la información.
Además de la palabra
Se enfatizan los términos "Seguridad de la Información", "Ciberseguridad" y "Protección de la Privacidad" . Como resultado, la nueva versión aborda explícitamente las medidas de seguridad cibernética como un subconjunto de medidas de seguridad de la información y medidas de protección de la privacidad.

[1] A continuación, el término "capítulo" también se utiliza para ISO/IEC 27001:2013.

El contenido de ISO/IEC 27002:2013 se ha ampliado significativamente: la norma de 2013 consta de un total de 80 páginas (más 10 páginas de tabla de contenidos y prólogo), mientras que la versión actualizada comprende 131 páginas (más 10 páginas de tabla de contenidos). contenido y prólogo, así como 17 páginas del anexo). La norma de 2013 contiene referencias a otras 27 normas ISO, mientras que la nueva versión contiene más del doble. En total, se hace referencia a otras 56 fuentes.

También se ha añadido un capítulo/glosario de términos, definiciones y abreviaturas, en lugar de una referencia exclusiva a ISO/IEC 27000, como era el caso en la versión anterior.

La estructura de la nueva ISO/IEC 27002:2022 ha sido completamente revisado. Como estructura temática, la nueva versión ahora contiene 4 temas en lugar de 14 capítulos/dominios ("Cláusulas de control de seguridad") (ver más abajo con más detalle).
Directamente detrás de éstas se encuentran las 93 medidas ("Controles"). Por lo tanto, por el momento se omite la integración original en los "Objetivos de control". En el futuro, esto se presentará como un objetivo para cada medida. En total, las medidas de la nueva versión comprenden los siguientes contenidos:

una breve descripción de la medida ("Título de control"), atributos adicionales ("Tabla de atributos"), una descripción del control, una descripción del propósito del control ("Propósito"), una guía de implementación para el control ("Guía") como así como

texto explicativo o referencias a otros documentos relacionados ("Otra Información").

Como se mencionó anteriormente, las medidas en la nueva versión se dividen en 4 temas:

"Controles de personas", capítulo 6, para medidas que se centran en las personas, como el "cribado" o el "trabajo a distancia";

"Controles físicos", Capítulo 7, cuando los elementos físicos sean involucrados, como el control de acceso;

"Controles tecnológicos", capítulo 8, cuando se trate de tecnología; y

todas las demás medidas se asignan a "Controles organizativos", capítulo 5.

Una adición útil en la nueva versión son los atributos ("Tabla de atributos"), que se puede asignar a cinco categorías diferentes:

"Tipos de control (valores posibles: preventivo, detectivo, correctivo),

"Propiedades de seguridad de la información" (valores posibles: confidencialidad, integridad, disponibilidad),

“Conceptos de ciberseguridad” (posibles valores: identificar, prodetectar, detectar, responder, recuperar),

"Capacidades operativas (posibles valores: por ejemplo, seguridad física, gobernanza) y

"Dominios de seguridad" (valores posibles: p. ej. protección, cerca).

Con la ayuda de estos nuevos atributos, se puede centrar mucho mejor el enfoque en ciertos aspectos, por ejemplo, se pueden crear diferentes vistas para diferentes grupos objetivo, se pueden clasificar los requisitos y las medidas se pueden filtrar fácilmente.

La reestructuración a nivel de medida tiene el siguiente efecto: en la nueva versión, se agregaron 11 controles nuevos , se dividió un control, se fusionaron 57 controles en 24 controles y se reformularon 58 controles.

Por lo tanto, la nueva versión contiene 93 medidas/controles en 4 temas, en comparación con 114 medidas/controles en 14 cláusulas de control de seguridad en la versión anterior.

Nuevas medidas

Como se mencionó anteriormente, hay 11 nuevas medidas en la nueva norma:

La "inteligencia sobre amenazas" (Sección 5.7) es definitivamente nueva en esta forma. Esto implica, entre otras cosas, la recopilación y evaluación de información sobre el entorno de amenazas específico de la organización para poder tomar las medidas reactivas adecuadas: se distingue entre inteligencia de amenazas estratégica, táctica y operativa.

“Seguridad de la información para el uso de servicios en la nube” (art. 5.23), esta medida no estaba disponible en la versión 2013. implícitamente anclado en las relaciones con los proveedores. La medida cubre la seguridad de la información de los servicios en la nube desde el punto de vista del cliente. Por ejemplo, se requiere una guía sobre computación en la nube en la empresa.

"Preparación de las TIC para la continuidad del negocio" (sección 5.30); Aquí TIC significa "Información y Comunicaciones". Tecnologías" y la medida va más allá de los antiguos aspectos de seguridad de la información de la gestión de la continuidad del negocio (versión antigua, cláusula 17): como base se describe, por ejemplo, la realización de análisis de impacto en el negocio (BIA).

"Enmascaramiento de datos" (Sección 8.11) trata no sólo el tema del enmascaramiento de datos (relacionados con personas)
El estudio también analiza las propiedades de la seudonimización y la anonimización de datos y aborda aspectos legales.

"Prevención de fuga de datos" (Sección 8.12) amplía el requisito original de clasificación de información y ofrece
una amplia gama de medidas para proteger contra la fuga de datos, incluidos los aspectos de monitoreo y su implementación técnica.

Las otras nuevas medidas son:

"Monitoreo de seguridad física" (sección 7.4)
"Gestión de la configuración" (sección 8.9)
"Eliminación de información" (sección
8.10) "Actividades de seguimiento" (Sección
8.16) "Filtrado web" (Sección
8.23) "Codificación segura " (sección 8.28)

Medida dividida

Una medida se ha dividido en dos medidas separadas en la nueva norma:

La medida “Revisión de cumplimiento técnico” (versión antigua, Cláusula de Control de Seguridad 18.2.3) se divide en dos partes: en primer lugar, la parte organizativa “Cumplimiento de políticas y estándares de seguridad de la información” (Sección 5.36), con explicaciones de cómo verificar cumplimiento de las directrices, y en segundo lugar, la parte técnica "Gestión de vulnerabilidades técnicas" (Sección 8.8), que se ha ampliado mucho y se describe en detalle. Por ejemplo, se analiza en detalle la identificación y evaluación de vulnerabilidades técnicas y se recomienda explícitamente la realización de pentests.

Medidas resumidas

Un total de 57 compases se combinaron en 24 compases, lo que representa una compresión significativa. Llegados a este punto, nos limitaremos a dos ejemplos seleccionados:

"Seguridad de la información en la gestión de proyectos" (Sección 5.8) se desarrolló a partir de 2 dominios/convenciones de seguridad originales. Se han fusionado las cláusulas de control. Por un lado, el contenido de la medida “Seguridad de la información en la gestión de proyectos” (versión antigua, Cláusula de Control de Seguridad 6.1.5), y por otro lado, el contenido de “Análisis y especificación de requisitos de seguridad de la información” (versión antigua, Se ha incluido la Cláusula de Control de Seguridad 14.1.1).

"Dispositivos terminales de usuario" (Sección 8.1) también se creó a partir de 2 Cláusulas de control de seguridad/
dominios originales para-. fusionado. Por un lado, el contenido de la medida “Política de dispositivos móviles” (versión antigua, Cláusula de Control de Seguridad 6.2.1), y por otro lado, el contenido de “Equipos de usuario desatendidos” (versión antigua, Cláusula de Control de Seguridad 11.2.1). 8) han sido incorporados. Esto reúne todos los aspectos que deben tenerse en cuenta en la protección de los dispositivos del usuario final.

Evaluación

La nueva versión representa un desarrollo significativo y una actualización en cuanto a las medidas de seguridad de la información reconocidas, como prometía la norma en su introducción.
En la nueva versión se han tenido en cuenta importantes prácticas y tendencias importantes en el sector de la seguridad de la información, aunque no se han realizado ampliaciones temáticas masivas con 11 nuevas medidas.

La división en medidas organizativas, personales, físicas y técnicas ofrece una mejora significativa en la estructura desde el punto de vista de los autores. En comparación con la versión 2013, se incluye amplia información adicional y se proporciona ayuda más detallada. Los textos y las definiciones se han perfeccionado y los atributos brindan coherencia en la interpretación. Los atributos de la categoría "Conceptos de ciberseguridad" , por ejemplo, corresponden a las funciones del marco de ciberseguridad del NIST, creando así un vínculo directo con otro marco de gestión.

Con estas y otras adiciones formales, se puede crear una variedad de vistas de diferentes subaspectos. Estas opciones y el mayor nivel de detalle pueden simplificar la creación de directrices específicas para la empresa.

panorama

Seguirá la actualización de otras normas existentes y de las normas de la serie ISO/IEC 27000, que han adoptado la estructura de ISO/ IEC 27002:2013, y se espera que esté completa en 2024.

Las organizaciones ya tienen la opción de utilizar las nuevas medidas del Anexo A como medidas. Con las tablas de mapeo disponibles, también se pueden crear declaraciones de aplicabilidad para empresas certificadas, que aún corresponden a la versión anterior de 2013 si es necesario. Con la publicación de la versión ISO/IEC 27001:2022, este paso solo debería ser necesario para obtener la certificación si la certificación aún debe realizarse explícitamente según la versión 2013. Esto podría ser necesario, por ejemplo, si el organismo de certificación aún no ha sido acreditado para la certificación según la versión 2022.

tiene. El documento "Requisitos de transición para ISO/IEC 27001:2022" del Foro Internacional de Acreditación2 regula la transición de la versión 2013 a la versión 2022. De este modo, las medidas existentes de un SGSI certificado pueden adaptarse a la nueva ISO/IEC 27002:2022 y, por tanto, a el nuevo anexo en el marco de un período transitorio de tres años (a más tardar el 31.10.2025). Debido a las asignaciones proporcionadas, el esfuerzo para dicha adaptación debería poder centrarse esencialmente en las nuevas medidas, así como en las mejoras de las medidas existentes de la norma.

Los organismos de certificación deben comenzar a certificar según el nuevo estándar a más tardar el 31 de octubre de 2023.

8.3 Protección integral de la cadena de valor

Uno de los aspectos centrales de la introducción o adaptación de la estrategia de SGSI/seguridad cibernética debería ser la introducción de un proceso para asegurar la cadena de valor de la organización que será protegida por el SGSI. Con esta medida se pueden sentar las bases para una gestión de seguridad de extremo a extremo, que garantiza una protección básica en toda la empresa y determina otras actividades en función del riesgo.

En la práctica, se ha establecido un "Cuadro de Mando de Criticidad Empresarial (BCS)" para este fin.

Con ellos se documenta, por ejemplo, una clasificación basada en escenarios del nivel de riesgo básico del proceso o de las aplicaciones utilizadas en él.

Para una protección de extremo a extremo, es útil que la organización evalúe la criticidad del proceso y la necesidad de protección de la información procesada en él sobre la base de una política para al menos cada proceso principal y para cada aplicación operada para el proceso por el propietario del proceso respectivo en dicho cuadro de mando.

Además, es importante que la metodología de proyectos de una organización garantice que se cree dicho cuadro de mando para nuevos proyectos (análogo a la protección de datos y/o la notificación al comité de empresa) para que los requisitos de seguridad de la información puedan coordinarse en una etapa temprana.

Priorización basada en escenarios de los procesos de negocio a proteger

El cuadro de mando de criticidad empresarial se utiliza para realizar una identificación de alto nivel de los riesgos de seguridad de la información resultantes del proceso o las aplicaciones con el fin de determinar el esfuerzo necesario para proteger el activo considerado. En este caso, la identificación basada en preguntas y escenarios fundamentales específicos de la organización en el contexto de los objetivos de seguridad de la información, que se ilustran a continuación como ejemplos (consulte la Figura 12), es un enfoque adecuado.

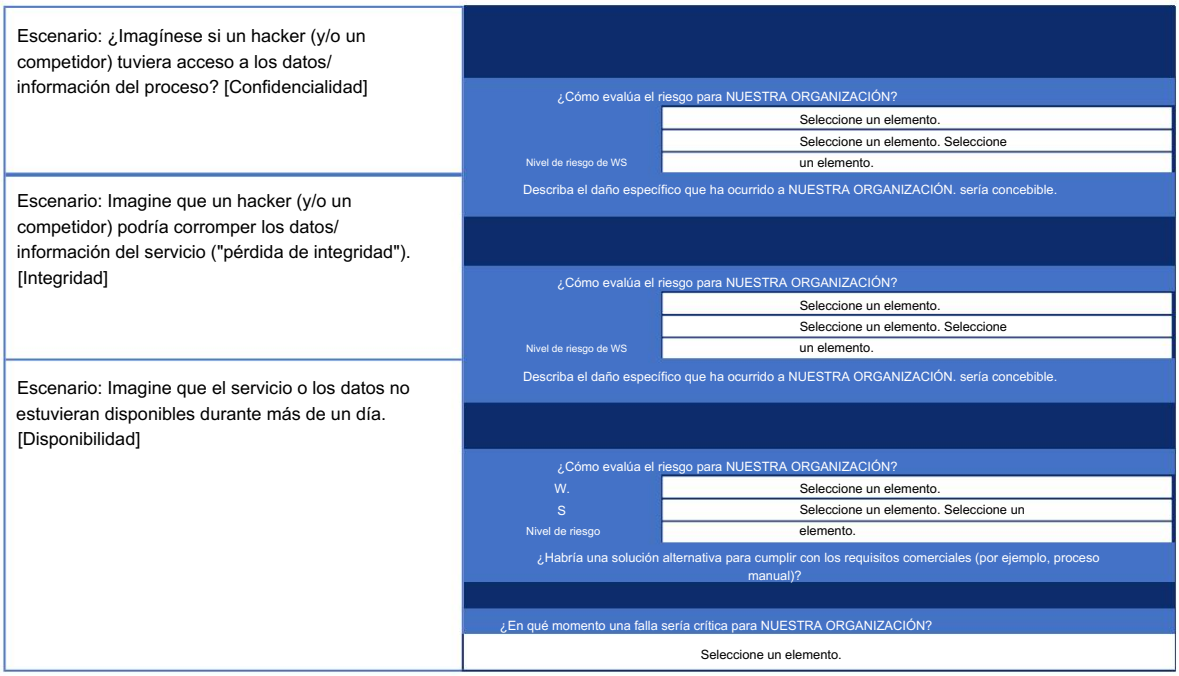


Figura 12: Determinación del nivel de riesgo basada en escenarios

2 Foro Internacional de Acreditación, Inc, Requisitos de transición para ISO/IEC 27001:2022, Edición 1 (IAF MD 26:2022).

Además de la criticidad y la evaluación de riesgos, también se pueden recopilar otros datos, por ejemplo, sobre el RTO/RPO o sobre procesos relevantes para las operaciones. Un cuadro de mando debe incluir al menos una descripción del proceso principal considerado o de las aplicaciones operadas para él, así como un identificador único.

Con base en la información recopilada, por ejemplo, la implementación del nivel de madurez de los requisitos básicos y los requisitos de documentación, y en particular con base en la criticidad y la evaluación de riesgos recopilada, el oficial de seguridad de la información (ISO) en BCS decide qué esfuerzo se debe invertir en una mayor seguridad. análisis (del proceso) con el fin de alcanzar un nivel de seguridad adecuado para la organización.

Para sistemas menos críticos, por ejemplo, se puede aplicar una protección estándar a definir, y para procesos con mayor potencial de riesgo, conceptos de seguridad específicos o controles técnicos, como por ejemplo, la realización de una prueba de penetración. Las posibles etapas de decisión podrían definirse como se ejemplifica en la Tabla 3.

Análisis de seguridad del esfuerzo de etapa	
0	No es necesario realizar más análisis
1	Medidas estándar Realizar un análisis GAP de las medidas estándar de la organización o, alternativamente, si es operado por el propio TI del Grupo, confirmación por parte del departamento de TI de que las medidas se han implementado.
2	Análisis de seguridad avanzado Realice una evaluación de vulnerabilidad específica utilizando modelos de amenazas (por ejemplo, STRIDE3).
3	Análisis técnico de seguridad. Realización de una prueba de penetración o análisis del código fuente por parte de un tercero independiente

Tabla 3: Análisis de seguridad del esfuerzo

El BCS representa así una especie de "prefiltro" para la gestión de riesgos, ya que sólo se pueden realizar análisis exhaustivos si el debe llevarse a cabo si la evaluación inicial de la criticidad identifica una necesidad correspondiente, pero la metodología garantiza, no obstante, que cada proceso esté sujeto al menos a un análisis de alto nivel y que se garantice una garantía básica adecuada, lo que conduce automáticamente a una evaluación sistemática. aseguró la garantía del "eslabón más débil".

Otra ventaja de una solución de cuadro de mando es que también se puede utilizar para consultar otros aspectos (para que los procesos se controlen operativamente), por ejemplo, requisitos de cumplimiento, verificaciones de procesos operativos documentados, responsabilidades para la gestión de parches y vulnerabilidades, evaluación de registros, respaldo de datos, concepto de autorización y otros. Esto puede incluir aspectos fuera de la seguridad de la información que son necesarios para otros sistemas de gestión, por ejemplo, de protección de datos, cumplimiento o gestión de calidad.

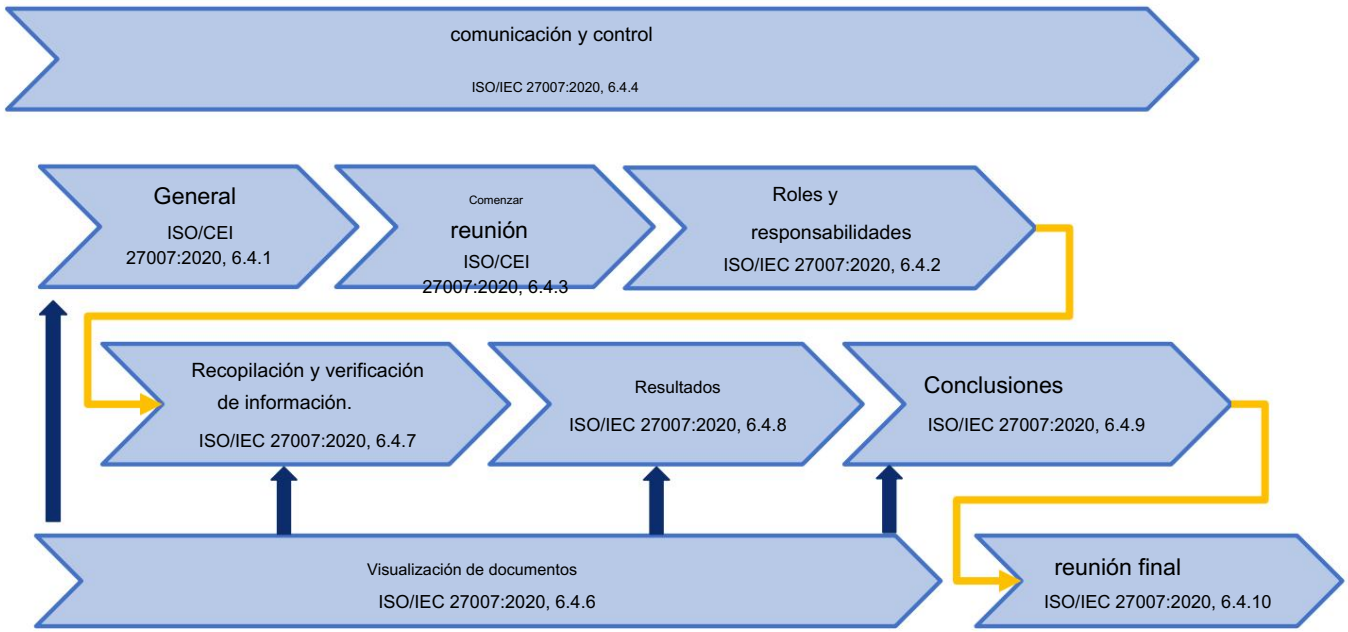
3 Ver sección 3.6

8.4 Auditorías internas del SGSI: correspondencia con ISO/IEC 19011 e ISO/IEC 27007

Requisitos para auditorías internas de SGSI de ISO/IEC 27001:2022 vs. ISO/IEC 19011:2018 e ISO/IEC 27007:2020

Subproceso/actividad	ISO/CEI 27001:2022	ISO/CEI 19011:2018 ISO/IEC 27007:2020
Planificación del programa de auditoría.	9.2a 9,2 b 9,2 litros	5.1 Generalidades 5.2 Establecimiento de los objetivos del programa de auditoría
Determinación del programa de auditoría.	9,2 litros	A.5.4 Establecimiento del programa de auditoría
Implementación del programa de auditoría.	9,2 litros	A.5.5 Implementación del programa de auditoría
Seguimiento del programa de auditoría	9,2 litros	A.5.6 Seguimiento del programa de auditoría
Revisión y mejora del programa de auditoría.	9,2 litros	A.5.7 Revisión y mejora del programa de auditoría
Competencia y selección de auditores.	9.2e	7 Competencia y evaluación de los auditores
Documentación y evidencia	9,2 gramos	A.5.5.7 Gestión y mantenimiento de registros del programa de auditoría
Definir criterios de auditoría y alcance por auditoría.	9,2 días	A.5.5.2 Definir los objetivos, alcance y criterios de una auditoría individual
Implementación de auditorías del SGSI	9.2e	6 Realización de una auditoría
Informes de resultados de auditoría	9,2 f	A.5.5.6 Gestión de los resultados del programa de auditoría

8.5 Implementación de auditorías internas del SGSI (diagrama de procesos)



Su socio para la educación continua: El Capítulo de ISACA Alemania e. v.

La asociación profesional alemana de auditores de TI, administradores de seguridad de TI y expertos en gobierno de TI promueve su desarrollo profesional a través de cursos de preparación para los exámenes de las certificaciones profesionales internacionales CISA, CISM, CRISC y CDPSE.

Para ayudarlo, ofrecemos un programa de certificación temáticamente amplio basado en el marco COBIT 2019.

Puede encontrar nuestra gama completa de cursos en nuestro sitio web www.isaca.de/seminare view. Además de los seminarios presenciales, también ofrecemos todos los cursos como seminarios en línea. Para todos los cursos recibirá un certificado de desarrollo profesional reconocido (las llamadas horas CPE).