ISO/IEC 27005:2022

Seguridad de la información, ciberseguridad y protección de la privacidad

Traducción propia exclusiva con fines académicos

ISO/IEC 27005:2022

SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

Contenido

0. INTRODUCCIÓN

Este documento proporciona orientación sobre:

- La aplicación de los requisitos de riesgo de seguridad de la información especificados en la norma ISO/IEC 27001;
- Referencias esenciales dentro de las normas desarrolladas por ISO/IEC JTC 1/SC 27 para apoyar las actividades de gestión de riesgos de seguridad de la información
- Las acciones que abordan los riesgos relacionados con la seguridad de la información (véase ISO/IEC 27001:2022, 6.1 y cláusula 8)
- Aplicación de las orientaciones sobre gestión de riesgos de la norma ISO 31000 en el contexto de la seguridad de la información.

Este documento contiene orientaciones detalladas sobre la gestión de riesgos y complementa las orientaciones de la norma ISO/IEC 27003.

Este documento está destinado a ser utilizado por:

- Organizaciones que pretenden establecer e implementar un sistema de gestión de la seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001;
- Personas que realizan o están involucradas en la gestión de riesgos de seguridad de la información (por ejemplo, profesionales del SGSI, propietarios de riesgos y otras partes interesadas);
- Organizaciones que pretenden mejorar su proceso de gestión de riesgos de seguridad de la información.

1. ALCANCE

Este documento proporciona orientación para ayudar a las organizaciones a:

- Cumplir los requisitos de la norma ISO/IEC 27001 relativos a las acciones para tratar los riesgos de seguridad de la información;
- Realizar actividades de gestión de riesgos de seguridad de la información, específicamente la evaluación y el tratamiento de los riesgos de seguridad de la información.

Este documento es aplicable a todas las organizaciones, independientemente de su tipo, tamaño o sector.

2. REFERENCIAS NORMATIVAS

En el texto se hace referencia a los siguientes documentos de manera que parte o la totalidad de su contenido constituye requisitos de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento referenciado (incluyendo cualquier enmienda).

ISO/IEC 27000, *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario*

3. TERMINOS Y DEFINICIONES

A los efectos de este documento, se aplican los términos y definiciones que figuran en la norma ISO/IEC 27000 y los siguientes.

La ISO y la IEC mantienen bases de datos terminológicas para su uso en la normalización en las siguientes direcciones

- Plataforma de navegación en línea de ISO: disponible en: https://www.iso.org/obp
- IEC Electropedia: disponible en: https://www.electropedia.org/

3.1. Términos relacionados con el riesgo para la seguridad de la información

3.1.1. Contexto externo

Entorno externo en el que la organización pretende alcanzar sus objetivos

Nota 1 a la entrada: El contexto externo puede incluir lo siguiente

- El entorno social, cultural, político, jurídico, normativo, financiero, tecnológico, económico y geológico, ya sea internacional, nacional, regional o local
- Los principales factores y tendencias que afectan a los objetivos de la organización
- Las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas
- Las relaciones y compromisos contractuales
- La complejidad de las redes y dependencias

[FUENTE: ISO Guía 73:2009, 3.3.1.1, modificada — Nota 1 A la entrada ha sido modificada.]

3.1.2. Contexto Interno

Entorno interno en el que la organización trata de alcanzar sus objetivos

Nota 1 a la entrada: El contexto interno puede incluir:

- Visión, misión y valores;
- Gobernanza, estructura organizativa, funciones y responsabilidades
- La estrategia, los objetivos y las políticas
- La cultura de la organización
- Las normas, directrices y modelos adoptados por la organización
- Las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías)
- Los datos, los sistemas de información y los flujos de información
- Las relaciones con las partes interesadas internas, teniendo en cuenta sus percepciones y valores
- Relaciones y compromisos contractuales;
- Interdependencias e interconexiones internas.

[FUENTE: ISO Guía 73:2009, 3.3.1.2, modificada — Nota 1 A la entrada ha sido modificada.]

3.1.3. Riesgo

Efecto de la incertidumbre en los objetivos

Nota 1 a la entrada: Un efecto es una desviación de lo esperado, positiva o negativa.

Nota 2 a la entrada: Los objetivos pueden tener diferentes aspectos y categorías, y pueden aplicarse a diferentes niveles.

Nota 3 a la entrada: La incertidumbre es el estado, incluso parcial, de falta de información relacionada con la comprensión o el conocimiento de un acontecimiento (3.1.11), su consecuencia (3.1.14) o su probabilidad (3.1.13).

Nota 4 de la entrada: El riesgo suele expresarse en términos de fuentes de riesgo (3.1.6), eventos potenciales, sus consecuencias y su probabilidad.

Nota 5 de la entrada: En el contexto de los sistemas de gestión de la seguridad de la información, los riesgos de seguridad de la información pueden expresarse como efecto de la incertidumbre sobre los objetivos de seguridad de la información.

Nota 6 a la entrada: Los riesgos de seguridad de la información suelen estar asociados a un

efecto negativo de la incertidumbre sobre los objetivos de seguridad de la información.

Nota 7 a la entrada: Los riesgos de seguridad de la información pueden asociarse con la posibilidad de que las amenazas (3.1.9) exploten las vulnerabilidades (3.1.10) de un activo de información o grupo de activos de información y, por tanto, causen daños a una organización.

[FUENTE: ISO 31000:2018 3.1, modificada — la frase: "Puede ser positiva, negativa o ambas, y puede abordar, crear o dar lugar a oportunidades y amenazas" ha sido sustituida por "positiva o negativa" en la Nota 1 de la entrada; la Nota 3 original de la entrada ha sido renumerada como Nota 4 de la entrada; y se han añadido las Notas 3, 5, 6 y 7 de la entrada]

3.1.4. Escenario de Riesgo

Secuencia o combinación de eventos (3.1.11) que llevan de la causa inicial a la consecuencia no deseada (3.1.14)

[FUENTE: ISO 17666:2016, 3.3.13, modificada — Nota 1 A la entrada ha sido eliminada.]

3.1.5. Propietario del Riesgo

Persona o entidad con responsabilidad y autoridad para gestionar un riesgo (3.1.3)

[FUENTE: ISO Guía 73:2009, 3.5.15]

3.1.6. Fuente del Riesgo

Elemento que por sí solo o en combinación tiene el potencial de dar lugar a un riesgo

Nota 1 a la entrada: Una fuente de riesgo puede ser uno de estos tres tipos

- Humana;
- Ambiental;
- Técnica.

Nota 2 a la entrada: Un tipo de fuente de riesgo humano puede ser intencional o no intencional.

[FUENTE: ISO 31000:2018, 3.4 modificada — Notas 1 y 2 A la entrada han sido adicionadas]

3.1.7. Criterio de Riesgo

Términos de referencia con los que se evalúa la importancia de un riesgo (3.1.3)

Nota 1 a la entrada: Los criterios de riesgo se basan en los objetivos de la organización y en el contexto externo (3.1.1) e interno (3.1.2).

Nota 2 a la entrada: Los criterios de riesgo pueden derivarse de normas, leyes, políticas y otros

requisitos.

[FUENTE: ISO Guía 73:2009, 3.3.1.3]

3.1.8. Apetito de Riesgo

Cantidad y tipo de riesgo (3.1.3) que una organización está dispuesta a perseguir o retener

[FUENTE: ISO Guía 73:2009, 3.7.1.2]

3.1.9. Amenaza

Causa potencial de un incidente de seguridad de la información (3.1.12) que puede provocar daños en un sistema o en una organización.

3.1.10. Vulnerabilidad

Debilidad de un activo o control (3.1.16) que puede ser explotada para que ocurra un evento (3.1.11) con una consecuencia negativa (3.1.14)

3.1.11. Evento

Ocurrencia o cambio de un conjunto particular de circunstancias

Nota 1 de la entrada: Un acontecimiento puede tener uno o varios sucesos y puede tener varias causas y varias consecuencias (3.1.14).

Nota 2 de la entrada: Un evento también puede ser algo que se espera que no ocurra, o algo que no se espera que ocurra**.**

[FUENTE: ISO 31000:2018, 3.5, modificado - Se ha eliminado la nota 3 de la entrada].

3.1.12. Incidente de seguridad de la información

Un evento único o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la empresa y amenazar la seguridad de la información

3.1.13. Probabilidad

Posibilidad de que algo ocurra

Nota 1 de la entrada: En la terminología de la gestión de riesgos, la palabra "probabilidad" se utiliza para referirse a la posibilidad de que algo ocurra, ya sea definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos (como una probabilidad o una frecuencia en un período de tiempo determinado).

Nota 2 de la entrada: El término inglés "likelihood" no tiene un equivalente directo en algunos idiomas; en su lugar, se suele utilizar el equivalente del término "probability". Sin embargo, en inglés, "probability" suele interpretarse de forma restringida como un término matemático. Por lo tanto, en la terminología de la gestión de riesgos, "likelihood" se utiliza con la intención de que tenga la misma interpretación amplia que tiene el término "probability" en muchos idiomas distintos del inglés.

[FUENTE: ISO 31000:2018, 3.7]

3.1.14.Consecuencia

Resultado de un evento (3.1.11) que afecta a los objetivos

Nota 1 a la entrada: Una consecuencia puede ser cierta o incierta y puede tener efectos directos o indirectos positivos o negativos sobre los objetivos.

Nota 2 de la entrada: Las consecuencias pueden expresarse cualitativa o cuantitativamente.

Nota 3 a la entrada: Cualquier consecuencia puede escalar a través de efectos en cascada y acumulativos.

[FUENTE: ISO 31000:2018, 3.6]

3.1.15.Nivel de Riesgo

Importancia de un riesgo (3.1.3), expresada en términos de la combinación de consecuencias (3.1.14) y su probabilidad (3.1.13)

[FUENTE: Guía ISO 73:2009, 3.6.1.8, modificada - la frase: "magnitud de un riesgo o combinación de riesgos" se ha sustituido por "importancia de un riesgo"].

3.1.16.Control

Medida que mantiene y/o modifica el riesgo (3.1.3)

Nota 1 a la entrada: Los controles incluyen, pero no se limitan a, cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantienen y/o modifican el riesgo.

Nota 2 a la entrada: Los controles pueden no ejercer siempre el efecto modificador previsto o asumido.

[FUENTE: ISO 31000:2018, 3.8]

3.1.17.Riesgo Residual

Riesgo (3.1.3) que queda después del tratamiento del riesgo (3.2.7)

Nota 1 a la entrada: El riesgo residual puede contener riesgo no identificado. Nota 2 a la entrada:

Los riesgos residuales también pueden contener riesgo retenido.

[FUENTE: Guía ISO 73:2009, 3.8.1.6, modificada - Se ha modificado la nota 2 de la entrada].

3.2. Términos relacionados con la gestión de riesgos de la seguridad de la información

3.2.1. Proceso de gestión de riesgos

Aplicación sistemática de las políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo (3.1.3)

[FUENTE: Guía ISO 73:2009, 3.1]

3.2.2. Comunicación y consulta de riesgos

Conjunto de procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información, y para entablar un diálogo con las partes interesadas en relación con la gestión del riesgo (3.1.3)

Nota 1 a la entrada: La información puede referirse a la existencia, naturaleza, forma, probabilidad (3.1.13), importancia, evaluación, aceptación y tratamiento del riesgo.

Nota 2 de la entrada: La consulta es un proceso bidireccional de comunicación informada entre una organización y sus partes interesadas sobre una cuestión antes de tomar una decisión o determinar una dirección sobre dicha cuestión. La consulta es

- Un proceso que influye en una decisión mediante la influencia y no el poder;
- Una aportación a la toma de decisiones, no una decisión conjunta

3.2.3. Evaluación de riesgos

Proceso global de identificación del riesgo (3.2.4), análisis del riesgo (3.2.5) y evaluación del riesgo (3.2.6)

[FUENTE: Guía ISO 73:2009, 3.4.1]

3.2.4. Identificación de riesgos

Proceso de encontrar, reconocer y describir los riesgos (3.1.3)

Nota 1 a la entrada: La identificación de riesgos implica la identificación de las fuentes de riesgo (3.1.6), los eventos (3.1.11), sus causas y sus posibles consecuencias (3.1.14).

Nota 2 a la entrada: La identificación del riesgo puede implicar datos históricos, análisis teóricos,

opiniones informadas y de expertos, y necesidades de las partes interesadas.

[FUENTE: Guía ISO 73:2009, 3.5.1, modificada - "parte interesadas" ha sustituido a "parte interesada" en la Nota 2 de la entrada].

3.2.5. Análisis del riesgo

Proceso para comprender la naturaleza del riesgo (3.1.3) y determinar el nivel de riesgo (3.1.15)

Nota 1 a la entrada: El análisis del riesgo proporciona la base para la evaluación del riesgo (3.2.6) y las decisiones sobre su tratamiento (3.2.7).

Nota 2 de la entrada: El análisis de riesgos incluye la estimación del riesgo.

[FUENTE: Guía ISO 73:2009, 3.6.1]

3.2.6. Valoración del riesgo

Proceso de comparación de los resultados del análisis de riesgos (3.2.5) con los criterios de riesgo (3.1.7) para determinar si el riesgo (3.1.3) y/o su importancia son aceptables o tolerables

Nota 1 de la entrada: La evaluación del riesgo ayuda a decidir el tratamiento del riesgo (3.2.7).

[FUENTE: Guía ISO 73:2009, 3.7.1, modificada - "importancia" ha sustituido a "magnitud"].

3.2.7. Tratamiento del riesgo

Proceso para modificar el riesgo (3.1.3)

Nota 1 a la entrada: El tratamiento del riesgo puede consistir en

- Evitar el riesgo decidiendo no iniciar o continuar con la actividad que lo origina;
- Asumir o aumentar el riesgo para perseguir una oportunidad
- Eliminar la fuente de riesgo (3.1.6);
- Cambiar la probabilidad (3.1.13);
- Cambiar las consecuencias (3.1.14);
- Compartir el riesgo con otra u otras partes (incluidos los contratos y la financiación del riesgo); y
- Conservar el riesgo mediante una decisión informada.

Nota 2 de la entrada: El tratamiento del riesgo de la seguridad de la información no incluye

"asumir o aumentar el riesgo para perseguir una oportunidad", pero la organización puede tener esta opción para la gestión general del riesgo.

Nota 3 a la entrada: Los tratamientos de riesgos que tratan las consecuencias negativas se denominan a veces "mitigación de riesgos", "eliminación de riesgos", "prevención de riesgos" y "reducción de riesgos".

Nota 4 de la entrada: El tratamiento del riesgo puede crear nuevos riesgos o modificar los existentes.

[FUENTE: Guía ISO 73:2009, 3.8.1, modificada — Se ha añadido la Nota 1 a la entrada y las Notas 1 y 2 originales a la entrada se han renumerado como Nota 2 y 3 a la entrada].

3.2.8. Aceptación del riesgo

Decisión informada de asumir un determinado riesgo (3.1.3)

Nota 1 a la entrada: La aceptación del riesgo puede producirse sin tratamiento del riesgo (3.2.7) o durante el proceso de tratamiento del riesgo.

Nota 2 a la entrada: Los riesgos aceptados están sujetos a seguimiento y revisión.

[FUENTE: Guía ISO 73:2009, 3.7.1.6]

3.2.9. Distribución del riesgo

Forma de tratamiento del riesgo (3.2.7) que implica la distribución acordada del riesgo (3.1.3) con otras partes

Nota 1 a la entrada: Los requisitos legales o reglamentarios pueden limitar, prohibir u obligar a compartir el riesgo.

Nota 2 a la entrada: El reparto de riesgos puede llevarse a cabo a través de seguros u otras formas de contrato.

Nota 3 de la entrada: El grado de distribución del riesgo puede depender de la fiabilidad y claridad de los acuerdos de distribución.

Nota 4 de la entrada: La transferencia del riesgo es una forma de compartir el riesgo.

[FUENTE: Guía ISO 73:2009, 3.8.1.3]

3.2.10. Retención del riesgo

Aceptación temporal del beneficio potencial de ganancia, o de la carga de pérdida, de un riesgo particular (3.1.3)

Nota 1 a la entrada: La retención puede limitarse a un determinado período de tiempo.

Nota 2 a la entrada: El nivel de riesgo (3.1.15) retenido puede depender de los criterios de riesgo (3.1.7).

[FUENTE: Guía ISO 73:2009, 3.8.1.5, modificada - se ha añadido la palabra "temporal" al principio de la definición y la frase; "La retención de riesgos incluye la aceptación de los riesgos residuales" ha sustituido a "La retención puede limitarse a un determinado periodo de tiempo" en la nota 1 de la entrada].

4. ESTRUCTURA DEL DOCUMENTO

Este documento está estructurado de la siguiente manera:

- Cláusula 5: Gestión de los riesgos para la seguridad de la información;
- Cláusula 6: Establecimiento del contexto;
- Cláusula 7: Proceso de evaluación de riesgos para la seguridad de la información;
- Cláusula 8: Proceso de tratamiento de los riesgos para la seguridad de la información;
- Cláusula 9: Operación;
- Cláusula 10: Aprovechamiento de los procesos relacionados del SGSI.

A excepción de las descripciones dadas en las subcláusulas generales, todas las actividades de gestión de riesgos presentadas desde la Cláusula 7 hasta la Cláusula 10 están estructuradas como sigue:

Entrada: Identifica cualquier información necesaria para realizar la actividad.

Acción: Describe la actividad.

Activación: Proporciona orientación sobre el momento de iniciar la actividad, por ejemplo, debido a un cambio dentro de la organización o de acuerdo con un plan o un cambio en el contexto externo de la organización.

Resultado: Identifica cualquier información derivada después de realizar la actividad, así como cualquier criterio que dicho resultado deba satisfacer.

Orientación: Proporciona orientación sobre la realización de la actividad, la palabra clave y el concepto clave.

5. GESTION DE RIESGOS PARA LA SEGURIDAD DE LA INFORMACION

5.1. Proceso de gestión de riesgos para la seguridad de la información

El proceso de gestión de riesgos para la seguridad de la información se presenta en la figura 1.

NOTA Este proceso se basa en el proceso general de gestión de riesgos definido en la norma ISO 31000.

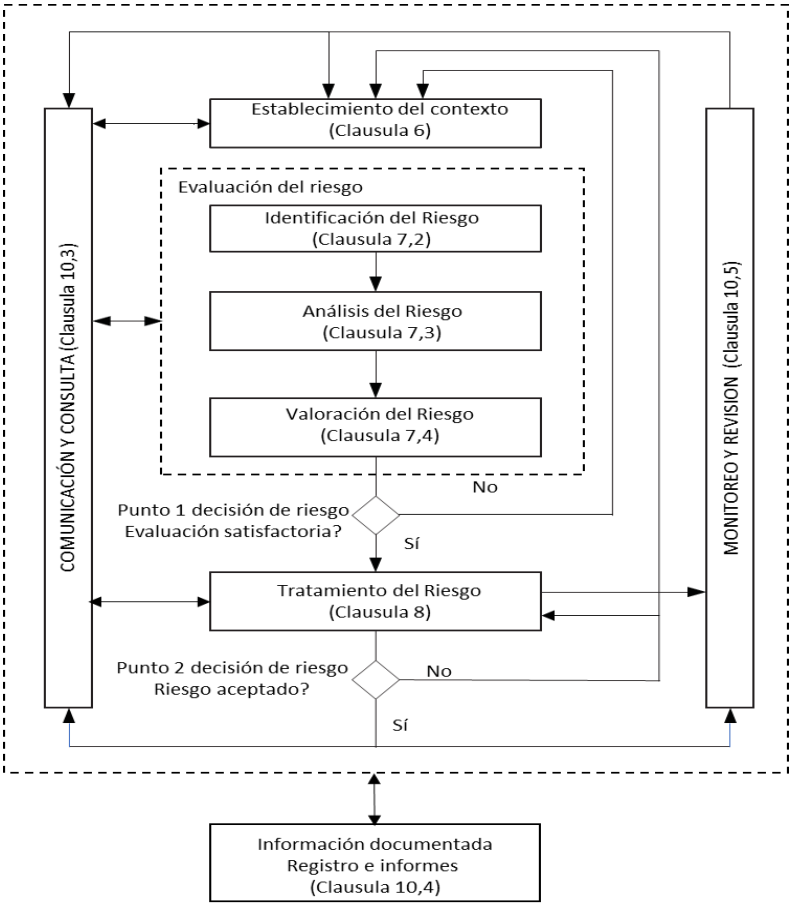

Figura 1 - Proceso de gestión de riesgos para la seguridad de la información

Como ilustra la figura 1, el proceso de gestión de riesgos de seguridad de la información puede ser iterativo para las actividades de evaluación y/o tratamiento de riesgos. Un enfoque iterativo para llevar a cabo la evaluación de riesgos puede aumentar la profundidad y el detalle de la evaluación en cada iteración. El enfoque iterativo proporciona un buen equilibrio entre la minimización del tiempo y el esfuerzo dedicado a la identificación de los controles, al tiempo que garantiza que los riesgos se evalúan adecuadamente.

Establecer el contexto significa reunir el contexto interno y externo para la gestión de riesgos de seguridad de la información o una evaluación de riesgos de seguridad de la información.

Si la evaluación de riesgos proporciona información suficiente para determinar eficazmente las acciones necesarias para modificar los riesgos hasta un nivel aceptable, la tarea está completa y el tratamiento de los riesgos sigue. Si la información es insuficiente, debe realizarse otra iteración de la evaluación de riesgos. Esto puede implicar un cambio de contexto de la evaluación

de riesgos (por ejemplo, la revisión del alcance), la participación de expertos en el campo correspondiente, u otras formas de recoger la información necesaria para permitir la modificación del riesgo hasta un nivel aceptable (véase el "punto de decisión de riesgo 1" en la figura 1).

El tratamiento del riesgo implica un proceso iterativo de

- Formular y seleccionar las opciones de tratamiento del riesgo
- Planificar y aplicar el tratamiento del riesgo
- Evaluar la eficacia de dicho tratamiento
- Decidir si el riesgo restante es aceptable
- Adoptar un nuevo tratamiento en caso de que no sea aceptable.

Es posible que el tratamiento del riesgo no conduzca inmediatamente a un nivel aceptable de riesgos residuales. En esta situación, se puede realizar otro intento de encontrar un tratamiento adicional del riesgo, o puede haber otra iteración de la evaluación del riesgo, ya sea en su conjunto o por partes.

Esto puede implicar un cambio de contexto de la evaluación de riesgos (por ejemplo, mediante una revisión del alcance) y la participación de expertos en el campo correspondiente. El conocimiento de las amenazas o vulnerabilidades pertinentes puede llevar a tomar mejores decisiones sobre las actividades de tratamiento del riesgo adecuadas en la siguiente iteración de la evaluación del riesgo (véase el "punto de decisión del riesgo 2" en la figura 1).

El establecimiento del contexto se trata en detalle en la cláusula 6, las actividades de evaluación del riesgo en la cláusula 7 y las actividades de tratamiento del riesgo en la cláusula 8.

Otras actividades necesarias para la gestión de los riesgos de seguridad de la información se tratan en la cláusula 10.

5.2. Ciclos de gestión de riesgos para la seguridad de la información

La evaluación y el tratamiento de los riesgos deben actualizarse periódicamente y en función de los cambios. Esto debe aplicarse a toda la evaluación de riesgos y las actualizaciones pueden dividirse en dos ciclos de gestión de riesgos:

- ciclo estratégico, en el que los activos de la empresa, las fuentes de riesgo y las amenazas, los objetivos o las consecuencias de los eventos de seguridad de la información evolucionan a partir de los cambios en el contexto general de la organización. Esto puede resultar como insumos para una actualización general de la evaluación de riesgos o de las evaluaciones de riesgos y los tratamientos de riesgos. También puede servir como insumo para identificar nuevos riesgos e iniciar evaluaciones de riesgo completamente nuevas;

- ciclo operativo, en el que los elementos mencionados anteriormente sirven como información de entrada o criterios modificados que afectarán a una evaluación o evaluación de riesgos en la que los escenarios deben ser revisados y actualizados. La revisión debe incluir la actualización del tratamiento del riesgo correspondiente, según proceda.

El ciclo estratégico debe realizarse a más largo plazo o cuando se produzcan cambios importantes, mientras que el ciclo operativo debe ser más corto en función de los riesgos detallados que se identifiquen y evalúen, así como del tratamiento del riesgo correspondiente.

El ciclo estratégico se aplica al entorno en el que la organización pretende alcanzar sus objetivos, mientras que el ciclo operativo se aplica a todas las evaluaciones de riesgos teniendo en cuenta el contexto del proceso de gestión de riesgos. En ambos ciclos, puede haber muchas evaluaciones de riesgos con diferentes contextos y alcance en cada evaluación.

6. ESTABLECIMIENTO DEL CONTEXTO

6.1. Consideraciones Organizacionales

NOTA: Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 4.1.

Una organización se define como una persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos. Una organización no es necesariamente una empresa.

Otra entidad corporativa o jurídica, también puede ser un subconjunto de una entidad jurídica (por ejemplo, el departamento de TI de una empresa), y puede considerarse como la "organización" en el contexto del SGSI.

Es importante entender que el apetito de riesgo, definido como la cantidad de riesgo que una organización está dispuesta a perseguir o aceptar, puede variar considerablemente de una organización a otra. Por ejemplo, los factores que afectan al apetito de riesgo de una organización incluyen el tamaño, la complejidad y el sector. El apetito de riesgo debe ser establecido y revisado regularmente por la alta dirección.

La organización debe asegurarse de que el papel del propietario del riesgo se determina en términos de las actividades de gestión de los riesgos identificados. Los propietarios de los riesgos deben tener la responsabilidad y la autoridad adecuadas para gestionar los riesgos identificados.

6.2. Identificación de los requisitos básicos de las partes interesadas

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 4.2.

Deben identificarse los requisitos básicos de las partes interesadas pertinentes, así como el estado de cumplimiento de estos requisitos. Esto incluye la identificación de todos los documentos de referencia que definen las normas y controles de seguridad y que se aplican en

el ámbito de la evaluación de riesgos de seguridad de la información.

Estos documentos de referencia pueden incluir, entre otros, los siguientes

a) ISO/IEC 27001:2022, Anexo A;

b) normas adicionales que cubren el SGSI;

c) normas adicionales aplicables a un sector específico (por ejemplo, financiero, sanitario)

d) normas internacionales y/o nacionales específicas;

e) las normas de seguridad internas de la organización;

f) las normas y controles de seguridad de los contratos o acuerdos;

g) los controles de seguridad aplicados sobre la base de actividades anteriores de tratamiento de riesgos.

Cualquier incumplimiento de los requisitos básicos debe explicarse y justificarse. Estos requisitos básicos y su cumplimiento deben ser la entrada para la evaluación de la probabilidad y para el tratamiento del riesgo.

6.3. Aplicación de la evaluación de riesgos

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 4.3.

Las organizaciones pueden realizar evaluaciones de riesgos integradas en muchos procesos diferentes, como la gestión de proyectos, la gestión de vulnerabilidades, la gestión de incidentes, la gestión de problemas, o incluso de forma improvisada para un tema específico identificado. Independientemente de cómo se realicen las evaluaciones de riesgos, deben cubrir colectivamente todos los temas relevantes para la organización dentro del alcance de un SGSI.

La evaluación de riesgos debe ayudar a la organización a tomar decisiones sobre la gestión de los riesgos que afectan a la consecución de sus objetivos. Por lo tanto, debe dirigirse a aquellos riesgos y controles que, si se gestionan con éxito, mejorarán la probabilidad de que la organización logre sus objetivos.

En la norma ISO/IEC 27003 se ofrece más información sobre el contexto de un SGSI y las cuestiones que deben comprenderse mediante la evaluación de riesgos.

6.4. Establecimiento y mantenimiento de los criterios de riesgo para la seguridad de la información

6.4.1. Generalidades

ISO/IEC 27001:2022, 6.1.2 a), especifica los requisitos para que las organizaciones definan sus

criterios de riesgo, es decir, los términos de referencia mediante los cuales evalúan la importancia de los riesgos que identifican y toman decisiones relativas a los riesgos.

ISO/IEC 27001 especifica los requisitos para que una organización establezca y mantenga los criterios de riesgo de seguridad de la información que incluyen:

a) los criterios de aceptación del riesgo;

b) los criterios para la realización de evaluaciones de riesgos de seguridad de la información.

En general, para establecer los criterios de riesgo, se debe considerar lo siguiente:

- la naturaleza y el tipo de incertidumbres que pueden afectar a los resultados y objetivos (tanto tangibles como intangibles);
- cómo se definirán, predecirán y medirán las consecuencias y la probabilidad
- los factores relacionados con el tiempo
- la coherencia en el uso de las mediciones
- cómo se determinará el nivel de riesgo
- cómo se tendrán en cuenta las combinaciones y secuencias de múltiples riesgos;
- la capacidad de la organización.

En el Anexo A se presentan otras consideraciones sobre los criterios de riesgo.

6.4.2. Criterios de aceptación del riesgo

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.2 a) 1).

En la valoración del riesgo, los criterios de aceptación del riesgo deben utilizarse para determinar si un riesgo es aceptable o no.

En el tratamiento del riesgo, los criterios de aceptación del riesgo pueden utilizarse para determinar si el tratamiento del riesgo propuesto es suficiente para alcanzar un nivel de riesgo aceptable, o si es necesario un tratamiento adicional del riesgo.

Una organización debe definir los niveles de aceptación del riesgo. Durante el desarrollo se debe tener en cuenta lo siguiente

a) la coherencia entre los criterios de aceptación del riesgo para la seguridad de la información y los criterios generales de aceptación del riesgo de la organización;

b) se identifica el nivel de gestión con autoridad delegada para tomar decisiones de aceptación de riesgos

c) los criterios de aceptación de riesgos pueden incluir múltiples umbrales, y la autoridad para la aceptación puede asignarse a diferentes niveles de gestión

d) los criterios de aceptación del riesgo pueden basarse únicamente en la probabilidad y las consecuencias, o pueden ampliarse para considerar también el equilibrio coste/beneficio entre las pérdidas previstas y el coste de los controles

e) pueden aplicarse diferentes criterios de aceptación de riesgos a diferentes clases de riesgo (por ejemplo, los riesgos que pueden dar lugar a un incumplimiento de la normativa o las leyes no siempre se retienen, mientras que la aceptación de riesgos puede permitirse si la aceptación es resultado de un requisito contractual);

Los criterios de aceptación del riesgo deben ser aprobados por el nivel de gestión autorizado.

6.4.3. Criterios para realizar valoraciones de riesgos para la seguridad de la información

6.4.3.1. Generalidades

NOTA Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 6.1.2 a) 2).

Los criterios de valoración de riesgos especifican cómo se determina la importancia de un riesgo en términos de sus consecuencias, probabilidad y nivel de riesgo.

Los criterios de valoración de riesgos para la seguridad de la información deben tener en cuenta la idoneidad de las actividades de gestión de riesgos.

Las consideraciones para lograr esto incluyen

a) el nivel de clasificación de la información

b) la cantidad y, en su caso, la concentración de la información

c) el valor estratégico de los procesos empresariales que hacen uso de la información

d) la criticidad de la información y de los activos relacionados con ella

e) la importancia operativa y empresarial de la disponibilidad, la confidencialidad y la integridad

f) las expectativas y percepciones de las partes interesadas (por ejemplo, la alta dirección)

g) las consecuencias negativas, como la pérdida de la buena voluntad y la reputación

h) la coherencia con los criterios de riesgo de la organización.

Los criterios de evaluación de riesgos, o una base formal para definirlos, deben ser

estandarizados en toda la organización para todos los tipos de evaluación de riesgos, ya que esto puede facilitar la comunicación, la comparación y la agregación de los riesgos asociados a múltiples ámbitos empresariales.

Los criterios de evaluación de riesgos para la seguridad de la información suelen incluir

- consecuencias;
- probabilidad;
- nivel de riesgo.

6.4.3.2. Criterios de consecuencias

NOTA Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 6.1.2 a) 2).

ISO/IEC 27001 se ocupa de las consecuencias que se ven afectadas directa o indirectamente por la preservación o la pérdida de la confidencialidad, la integridad y la disponibilidad de la información en el ámbito del SGSI. Los criterios de consecuencia deben desarrollarse y especificarse en términos de la magnitud del daño o pérdida, o del perjuicio para una organización o individuo resultante de la pérdida de confidencialidad, integridad y disponibilidad de la información. Al definir los criterios de consecuencia, se debe considerar especialmente lo siguiente:

a) la pérdida de vidas o el daño a individuos o grupos;

b) pérdida de la libertad, la dignidad o el derecho a la intimidad

c) pérdida de personal y de capital intelectual (habilidades y conocimientos);

d) el deterioro de las operaciones internas o de terceros (por ejemplo, el daño a una función o proceso empresarial)

e) efectos sobre los planes y los plazos;

f) Pérdida de valor empresarial y financiero;

g) pérdida de ventaja comercial o de cuota de mercado;

h) daños a la confianza o reputación del público

i) incumplimientos de requisitos legales, reglamentarios o estatutarios

j) incumplimientos de contratos o niveles de servicio;

k) Impacto negativo en las partes interesadas;

l) impacto negativo en el medio ambiente, contaminación

Los criterios de consecuencia definen cómo una organización categoriza la importancia de los posibles eventos de seguridad de la información para la organización. Es esencial determinar cuántas categorías de consecuencias se utilizan, cómo se definen y qué consecuencias se asocian a cada categoría.

Normalmente, los criterios de consecuencias son diferentes para las distintas organizaciones, dependiendo del contexto interno y externo de la organización.

EJEMPLO 1 La cantidad máxima que la organización está dispuesta a cancelar en un ejercicio fiscal y la cantidad mínima en el mismo periodo que la obligaría a liquidar pueden crear límites superiores e inferiores realistas de la escala de consecuencias de una organización expresada en términos monetarios.

Esta escala, que depende del contexto, puede dividirse en varias categorías de consecuencias, cuyo número y distribución deben depender de la percepción y el apetito de riesgo de la organización. Las escalas de consecuencias monetarias suelen expresarse en una escala logarítmica, como en décadas o potencias de 10 (por ejemplo, de 100 a 1.000; de 1 a 10.000, etc.), pero pueden utilizarse esquemas de cuantificación alternativos cuando se ajusten mejor al contexto de la organización.

Dado que las consecuencias en los distintos ámbitos o departamentos de una organización pueden expresarse inicialmente de diversas maneras en lugar de estrictamente en términos monetarios, es útil que estas diversas expresiones puedan cruzarse con una escala de anclaje común para garantizar que los niveles aproximadamente equivalentes de consecuencias en los distintos ámbitos se comparen correctamente entre sí. Esto debería permitir realizar una agregación de riesgos entre dominios.

EJEMPLO 2 Una violación de datos, además de afectar a la privacidad individual, puede provocar la pérdida de confidencialidad, integridad o disponibilidad de la información en el ámbito del SGSI. También puede provocar el incumplimiento de la legislación aplicable en materia de protección de datos. Las consecuencias potenciales van desde la pérdida de información, la pérdida de activos relacionados con la información y el proceso de información, hasta la pérdida de los objetivos operativos del negocio y la proyección de este.

6.4.3.3. Criterios de probabilidad

NOTA Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 6.1.2 a) 2).

La determinación de los criterios de probabilidad depende de aspectos tales como

a) los acontecimientos accidentales o naturales;

b) el grado de exposición de la información relevante o del activo relacionado con la información a la amenaza;

c) el grado de explotación de la vulnerabilidad de la organización

d) el fallo de la tecnología;

e) actos u omisiones humanas.

La probabilidad puede expresarse en términos probabilísticos (la posibilidad de que un evento ocurra en un plazo determinado) o en términos frecuentistas (el número medio nocional de ocurrencias en un plazo determinado). La probabilidad expresada en términos frecuenciales suele utilizarse cuando se comunica, aunque sólo puede utilizarse la probabilidad expresada en términos probabilísticos cuando se realiza la agregación de probabilidades.

Los criterios de probabilidad deben abarcar la gama previsiblemente manejable de probabilidades de sucesos previstos. Más allá de los límites de la manejabilidad practicable, normalmente sólo es necesario reconocer que se ha superado uno u otro límite para tomar una decisión adecuada de gestión del riesgo (designación como caso extremo). Si las escalas finitas son demasiado amplias, esto suele dar lugar a una cuantificación excesivamente gruesa y puede conducir a un error en la evaluación. Esto ocurre especialmente cuando las probabilidades se sitúan en el extremo superior de las escalas representadas exponencialmente, ya que los incrementos en los rangos superiores son intrínsecamente muy amplios.

Aunque casi todo es "posible", las fuentes de riesgo a las que se debe prestar atención primordial son aquellas con probabilidades más relevantes para el contexto de la organización y el alcance de su SGSI.

6.4.3.4. Criterios para determinar el nivel de riesgo

NOTA Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 6.1.2 a) 2).

El propósito de las escalas para el nivel de riesgo es ayudar a los propietarios del riesgo a decidir sobre la retención o el tratamiento de los riesgos y priorizarlos para su tratamiento. El nivel evaluado de un riesgo concreto debe ayudar a la organización a determinar la urgencia de tratar ese riesgo.

Dependiendo de la situación, se recomienda considerar el nivel de riesgo inherente (sin tener en cuenta ningún control), o el nivel de riesgo actual (teniendo en cuenta la eficacia de cualquier control ya implementado). La organización debe elaborar una clasificación de los riesgos, teniendo en cuenta lo siguiente

a) los criterios de consecuencia y de probabilidad;

b) las consecuencias que pueden tener los eventos de seguridad de la información a nivel estratégico, táctico y operativo (esto puede definirse como el peor caso o en otros términos, siempre que se utilice la misma base de forma coherente)

c) los requisitos legales y reglamentarios, y las obligaciones contractuales

d) los riesgos que aparecen más allá de los límites del ámbito de la organización, incluidos los efectos imprevistos sobre terceros.

Los criterios de nivel de riesgo son necesarios para evaluar los riesgos analizados.

Los criterios de nivel de riesgo pueden ser cualitativos (por ejemplo, muy alto, alto, medio, bajo) o cuantitativos (por ejemplo, expresados en términos de valor esperado de pérdida monetaria, pérdida de vidas o cuota de mercado en un periodo de tiempo determinado).

EJEMPLO Los riesgos pueden cuantificarse en forma de expectativa de pérdida anual, es decir, el valor monetario medio de la consecuencia por año tomado durante el año siguiente.

Independientemente de que se utilicen criterios cuantitativos o cualitativos, las escalas de valoración deberían, en última instancia, estar ancladas a una escala de referencia que sea comprendida por todas las partes interesadas, y tanto el análisis como la valoración de riesgos deberían incluir al menos una calibración formal periódica con respecto a la escala de referencia para garantizar la validez, la coherencia y la comparabilidad de los resultados.

Si se utiliza un enfoque cualitativo, los niveles de cualquier escala cualitativa deben ser inequívocos, sus incrementos deben estar claramente definidos, las descripciones cualitativas de cada nivel deben expresarse en un lenguaje objetivo y los niveles no deben solaparse. Cuando se utilicen diferentes escalas (por ejemplo, para abordar los riesgos en diferentes ámbitos empresariales), debe haber una equivalencia que permita obtener resultados comparables.

6.5. Elección de un método adecuado

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.2 b).

En general, el enfoque y los métodos de gestión de los riesgos de seguridad de la información deberían estar alineados con el enfoque y los métodos utilizados para gestionar los demás riesgos de la organización.

El enfoque elegido debe estar documentado.

Según la norma ISO/IEC 27001:2022, 6.1.2 b), la organización en el ámbito del SGSI debe garantizar que las evaluaciones repetidas de los riesgos para la seguridad de la información producen resultados coherentes, válidos y comparables. Esto significa que el método elegido debe garantizar las siguientes propiedades de los resultados

- consistencia: las evaluaciones de los mismos riesgos realizadas por diferentes personas, o por las mismas personas en diferentes ocasiones, en el mismo contexto, deben producir resultados similares;

- comparabilidad: los criterios de evaluación del riesgo deben definirse para garantizar que las evaluaciones realizadas para diferentes riesgos produzcan resultados comparables

cuando representen niveles de riesgo equivalentes

- validez: las evaluaciones deben producir resultados que se ajusten lo más posible a la realidad.

Para la gestión de los riesgos de seguridad de la información se suelen utilizar métodos de gestión de riesgos operativos. El método elegido puede utilizar cualquier enfoque apropiado con respecto al uso del riesgo residual. Los enfoques más utilizados para la gestión de riesgos de seguridad de la información utilizan el riesgo actual al evaluar la probabilidad y la consecuencia de los riesgos.

7. PROCESO DE EVALUACIÓN DE LOS RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN

7.1. Generalidades

La organización debe utilizar el proceso de evaluación de riesgos de la organización (si está establecido) para evaluar los riesgos para la información o para definir un proceso de evaluación de riesgos para la seguridad de la información.

La evaluación de riesgos permite a los propietarios de los riesgos priorizarlos de acuerdo con la perspectiva del tratamiento, basándose principalmente en sus consecuencias y probabilidad u otros criterios establecidos.

Debe determinarse el contexto de la evaluación de riesgos, incluyendo una descripción del alcance y el propósito, así como las cuestiones internas y externas que afectan a la evaluación de riesgos.

La evaluación de riesgos consiste en las siguientes actividades:

a) la identificación del riesgo, que es un proceso para encontrar, reconocer y describir los riesgos (en el apartado 7.2 se ofrecen más detalles sobre la identificación del riesgo)

b) el análisis de riesgos, que es un proceso para comprender los tipos de riesgo y determinar el nivel de riesgo. El análisis de riesgos implica la consideración de las causas y fuentes de riesgo, la probabilidad de que se produzca un evento específico, la probabilidad de que este evento tenga consecuencias y la gravedad de las mismas (en el apartado 7.3 se ofrecen más detalles sobre el análisis de riesgos);

c) la valoración del riesgo, que es un proceso para comparar los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su importancia son aceptables y para priorizar los riesgos analizados para su tratamiento. Sobre la base de esta comparación, se puede considerar la necesidad de tratamiento (en el apartado 7.4 se ofrecen más detalles sobre la valoración de riesgos).

El proceso de evaluación de riesgos debe basarse en métodos (véase el apartado 6.5) e

instrumentos diseñados con el suficiente detalle para garantizar, en la medida de lo posible, resultados coherentes, válidos y reproducibles. Además, el resultado debe ser comparable, por ejemplo, para determinar si el nivel de riesgo aumentó o disminuyó.

La organización debe asegurarse de que su enfoque de gestión de riesgos de seguridad de la información se alinea con el enfoque de gestión de riesgos de la organización, de modo que cualquier riesgo de seguridad de la información pueda ser comparado con otros riesgos de la organización y no sólo considerado de forma aislada.

La norma ISO/IEC 27001 no obliga a utilizar un enfoque concreto para cumplir los requisitos de la norma ISO/IEC 27001:2022, 6.1.2. Sin embargo, hay dos enfoques principales para la evaluación: un enfoque basado en eventos y un enfoque basado en activos. Estos enfoques se analizan con más detalle en el apartado 7.2.1.

7.2. Identificación de los riesgos para la seguridad de la información

7.2.1. Identificación y descripción de los riesgos para la seguridad de la información

NOTA Esta subcláusula está relacionada con ISO/IEC 27001:2022, 6.1.2 c) 1).

Entrada: Eventos que pueden influir negativamente en la consecución de los objetivos de seguridad de la información en la organización o en otras organizaciones.

Acción: Se deben identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información.

Activación: Los propietarios del riesgo, las partes interesadas y/o los expertos detectan, o tienen la necesidad de buscar, eventos o situaciones nuevas o modificadas que pueden afectar a la consecución de los objetivos de seguridad de la información.

Resultado: Una lista de los riesgos identificados.

Guía de implementación:

La identificación de riesgos es el proceso de encontrar, reconocer y describir los riesgos. Implica la identificación de las fuentes y eventos de riesgo.

El objetivo de la identificación de riesgos es generar una lista de riesgos basada en aquellos eventos que pueden impedir, afectar o retrasar la consecución de los objetivos de seguridad de la información.

Los riesgos identificados deben ser aquellos que, si se materializan, pueden tener un efecto sobre la consecución de los objetivos.

ISO/IEC 27001:2022, 6.1.2 c), requiere que la organización defina y aplique un proceso de evaluación de riesgos de seguridad de la información que identifique los riesgos de seguridad de

la información. Existen dos enfoques comúnmente utilizados para realizar la identificación de riesgos.

a) Enfoque basado en eventos: identificar los escenarios estratégicos a través de una consideración de las fuentes de riesgo, y cómo utilizan o impactan a las partes interesadas para alcanzar el objetivo deseado de esos riesgos.

b) Enfoque basado en activos: identificar escenarios operativos, que se detallan en términos de activos, amenazas y vulnerabilidades.

En un enfoque basado en eventos, el concepto subyacente es que los riesgos pueden identificarse y evaluarse a través de una evaluación de eventos y consecuencias. Los eventos y las consecuencias pueden determinarse a menudo mediante un descubrimiento de las preocupaciones de la alta dirección, los propietarios de los riesgos y los requisitos identificados al determinar el contexto de la organización (ISO/IEC 27001:2022, cláusula 4). Las entrevistas con la alta dirección y las personas de la organización que tienen una responsabilidad en un proceso de negocio pueden ayudar a identificar no sólo los eventos y consecuencias relevantes, sino también los propietarios de los riesgos.

Un enfoque basado en eventos puede establecer escenarios de alto nivel o estratégicos sin dedicar una cantidad de tiempo considerable a la identificación de activos a nivel detallado. Esto permite a la organización centrar sus esfuerzos de tratamiento de riesgos en los riesgos críticos. La evaluación de los eventos mediante este enfoque puede aprovechar los datos históricos en los que los riesgos permanecen invariables durante largos periodos, y permite a las partes interesadas implicadas alcanzar sus objetivos.

Sin embargo, en el caso de los riesgos para los que no se dispone de datos históricos o no son fiables, el asesoramiento basado en el conocimiento y la experiencia de los expertos o la investigación de las fuentes de riesgo puede ayudar a la evaluación.

Con un enfoque basado en los activos, el concepto subyacente es que los riesgos pueden identificarse y evaluarse mediante una inspección de los activos, las amenazas y las vulnerabilidades. Un activo es cualquier cosa que tenga valor para la organización y que, por tanto, requiera protección. Los activos deben ser identificados, teniendo en cuenta que un sistema de información se compone de actividades, procesos e información que debe ser protegida. Los activos pueden identificarse como primarios y de apoyo según su tipo y prioridad, destacando sus dependencias, así como sus interacciones con sus fuentes de riesgo y las partes interesadas de la organización. Una amenaza explota una vulnerabilidad de un activo para comprometer la confidencialidad, integridad y/o disponibilidad de la información correspondiente. Si todas las combinaciones válidas de activos, amenazas y vulnerabilidades pueden enumerarse en el ámbito del SGSI, entonces, en teoría, se identificarían todos los riesgos. Para los siguientes pasos de la evaluación de riesgos, debe elaborarse una lista de activos asociados a la información y a las instalaciones de procesamiento de la información.

El enfoque basado en los activos puede identificar las amenazas y vulnerabilidades específicas

de los activos y permite a la organización determinar el tratamiento específico de los riesgos a un nivel detallado.

En el anexo A se ofrece más información sobre ambos enfoques.

En principio, los dos enfoques sólo difieren en cuanto al nivel en el que se inicia la identificación. Ambos enfoques pueden describir el mismo escenario de riesgo, por ejemplo, cuando un activo de información está en el nivel de detalle y una exposición empresarial está en el nivel general. La identificación de las fuentes de riesgo que contribuyen a la situación mediante una evaluación basada en eventos suele requerir una búsqueda descendente desde el nivel general del escenario hasta el nivel de detalle, pero una evaluación basada en activos suele buscar hacia arriba desde el activo hasta el escenario, con el fin de proporcionar visibilidad sobre cómo se acumulan las consecuencias.

La identificación del riesgo es fundamental, porque un riesgo para la seguridad de la información que no se identifique en esta fase no se incluirá en el análisis posterior.

La identificación de riesgos debe considerar los riesgos independientemente de si su fuente está bajo el control de la organización, incluso si no se evidencian fuentes de riesgo específicas. Especialmente cuando se evalúan escenarios de riesgo complejos, debe realizarse una evaluación de riesgos iterativa.

La primera ronda debe concentrarse en las observaciones de alto nivel y las rondas sucesivas deben abordar niveles adicionales de detalle hasta que puedan identificarse las causas fundamentales de los riesgos.

Se puede utilizar cualquier otro enfoque de identificación de riesgos siempre que garantice la producción de resultados coherentes, válidos y comparables, cumpliendo el requisito de la norma ISO/IEC 27001:2022, 6.1.2 b).

La gestión de los riesgos de la seguridad de la información no debe estar limitada por puntos de vista arbitrarios o restrictivos sobre cómo deben estructurarse, agruparse, agregarse, dividirse o describirse los riesgos. Los riesgos pueden parecer superpuestos o ser subconjuntos o instancias específicas de otros riesgos. Sin embargo, los controles de los riesgos individuales deben considerarse e identificarse por separado de los riesgos más amplios o de los riesgos agregados a efectos del tratamiento de los riesgos.

EJEMPLO 1 Un ejemplo de dos riesgos que se solapan: (1) existe el riesgo de incendio en la sede central; (2) existe el riesgo de que un incendio afecte al funcionamiento del departamento de contabilidad cuando éste se encuentra en la sede central pero también en otros edificios.

Un ejemplo de casos específicos de un riesgo: (1) hay un incidente de pérdida de datos; (2) hay un incidente de pérdida de datos personales.

El segundo riesgo es una instancia específica del primer riesgo, pero es probable que tenga atributos y controles diferentes a los del primer riesgo, y puede ser importante gestionarlo por

separado del primer riesgo, mucho más amplio.

La agregación de riesgos no debe llevarse a cabo a menos que sean relevantes entre sí en el nivel en el que se está considerando el contexto de la organización. Puede ser necesario considerar por separado los riesgos que se fusionan a efectos de la presupuestación de la gestión global de los riesgos, cuando se planifican las opciones de tratamiento, ya que pueden ser necesarios diferentes controles para gestionarlos.

EJEMPLO 2 Un centro de datos puede estar sometido a varios riesgos independientes: inundación, incendio, picos de energía eléctrica y vandalismo.

Para estimar el nivel global de riesgo corporativo, los riesgos individuales de estos eventos pueden combinarse en un nivel global de riesgo, pero como cada uno de estos eventos requiere diferentes controles para gestionar el riesgo, deben considerarse e identificarse por separado a efectos del tratamiento del riesgo. Los riesgos (combinaciones de probabilidades y consecuencias) no siempre pueden agregarse directamente.

7.2.2. Identificación de los propietarios del riesgo

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.2 c) 2).

Entrada: Lista de riesgos identificados.

Acción: Los riesgos deben asociarse a los propietarios de los mismos.

Activación: La identificación de los propietarios de los riesgos se hace necesaria cuando

- no se ha hecho antes;
- hay un cambio de personal en el área de negocio correspondiente donde residen los riesgos;

Resultado: Lista de propietarios de riesgos con los riesgos asociados.

Orientación para la aplicación:

La alta dirección, el comité de seguridad, los propietarios de los procesos, los propietarios funcionales, los directores de departamento y los propietarios de los activos pueden ser los propietarios de los riesgos.

Una organización debe utilizar el proceso de evaluación de riesgos de la organización (si está establecido) en lo que respecta a la identificación de los propietarios de los riesgos, o bien debe definir los criterios para identificar a los propietarios de los riesgos. Estos criterios deben tener en cuenta que los propietarios de los riesgos

- sean responsables y tengan autoridad para gestionar los riesgos que poseen, es decir,

deben tener una posición en la organización que les permita ejercer realmente esta autoridad;

- comprendan los problemas que se plantean y estén en condiciones de tomar decisiones con conocimiento de causa (por ejemplo, sobre cómo tratar los riesgos).

El nivel de riesgo y a qué activo debe aplicarse el riesgo puede servir de base para identificar a los propietarios del riesgo.

La asignación debe tener lugar como parte del proceso de evaluación de riesgos.

7.3. Análisis de los riesgos para la seguridad de la información

7.3.1. Generalidades

El análisis de riesgos tiene como objetivo determinar el nivel de riesgo.

La norma ISO 31000 está referenciada en la norma ISO/IEC 27001 como modelo general. ISO/IEC 27001:2022, 6.1.2, requiere que, para cada riesgo identificado, el análisis de riesgos se base en la evaluación de las consecuencias resultantes del riesgo y la evaluación de la probabilidad del riesgo para determinar un nivel de riesgo.

Las técnicas de análisis de riesgos basadas en las consecuencias y la probabilidad pueden ser

a) cualitativas, utilizando una escala de atributos calificativos (por ejemplo, alto, medio, bajo); o

b) cuantitativas, utilizando una escala con valores numéricos (por ejemplo, coste monetario, frecuencia o probabilidad de ocurrencia);

c) semicuantitativo, utilizando escalas cualitativas con valores asignados.

El análisis de riesgos debe centrarse en aquellos riesgos y controles que, si se gestionan con éxito, mejoran la probabilidad de que la organización alcance sus objetivos. Es fácil dedicar mucho tiempo a una evaluación de riesgos, sobre todo a la evaluación de probabilidades y consecuencias. Para permitir una toma de decisiones eficaz sobre la gestión de los riesgos, puede ser suficiente utilizar estimaciones iniciales y aproximadas de la probabilidad y las consecuencias.

7.3.2. Evaluación de las consecuencias potenciales

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.2 d) 1).

Entrada: Una lista de escenarios de eventos o riesgos relevantes identificados, incluyendo la identificación de las fuentes de riesgo, y los procesos de negocio, los objetivos de negocio y los criterios de consecuencia. Además, una lista de todos los controles existentes, su eficacia, estado de implementación y uso.

Acción: Deben identificarse y evaluarse las consecuencias derivadas de no preservar adecuadamente la confidencialidad, la integridad o la disponibilidad de la información.

Activación: La evaluación de las consecuencias se hace necesaria cuando

- no se ha hecho antes
- la lista elaborada por la "identificación de riesgos" se modifica
- los propietarios del riesgo o las partes interesadas han cambiado las unidades en las que quieren que se especifiquen las consecuencias; o
- se determinan cambios en el ámbito o el contexto que afectan a las consecuencias.

Resultado: Una lista de consecuencias potenciales relacionadas con los escenarios de riesgo con sus consecuencias relacionadas con los activos o eventos, dependiendo del enfoque aplicado.

Orientación para la aplicación:

No preservar adecuadamente la seguridad de la información puede conducir a la pérdida de su confidencialidad, integridad o disponibilidad. La pérdida de la confidencialidad, la integridad o la disponibilidad puede tener otras consecuencias para la organización y sus objetivos. El análisis de consecuencias puede realizarse de forma ascendente a partir de las consecuencias de la seguridad de la información, considerando lo que puede ocurrir si se produce una pérdida de confidencialidad, integridad o disponibilidad de la información en cuestión. Normalmente, el propietario del riesgo puede estimar la consecuencia si se produce el evento. Deben tenerse en cuenta los siguientes elementos

- Estimación (o medida basada en la experiencia) de las pérdidas (de tiempo o de datos) debidas al evento como resultado de la interrupción o perturbación de las operaciones;
- Estimación/percepción de la gravedad de la consecuencia (por ejemplo, expresada en dinero)
- Los costes de recuperación, en función de si la recuperación puede realizarse internamente (por el equipo propietario del riesgo), o si es necesario llamar a una entidad externa.

7.3.3. Evaluación de la probabilidad

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.2 d) 2).

Entrada: Una lista de escenarios de eventos o riesgos relevantes identificados, incluyendo la

identificación de las fuentes de riesgo, y los procesos de negocio, los objetivos de negocio y los criterios de probabilidad.

Además, una lista de todos los controles existentes, su eficacia, su implementación y su estado de uso.

Acción: La probabilidad de ocurrencia de los escenarios posibles o reales debe ser evaluada y expresada utilizando los criterios de probabilidad establecidos.

Activación: Junto con la consecuencia, la evaluación de la probabilidad es una actividad clave del proceso de evaluación de riesgos a la hora de determinar el nivel de riesgo.

La evaluación de la probabilidad se hace necesaria cuando:

- no se ha hecho antes;
- se determinan cambios en el alcance o el contexto que pueden afectar a la probabilidad
- se descubren vulnerabilidades en los controles implementados
- las pruebas/auditorías de eficacia de los controles arrojan resultados inesperados
- se descubren cambios en el entorno de la amenaza (por ejemplo, nuevos actores/fuentes de amenaza).

Resultado: Una lista de eventos o escenarios de riesgo complementada con las probabilidades de que estos ocurran.

Orientación para la aplicación:

Una vez identificados los escenarios de riesgo, es necesario analizar la probabilidad de que se produzca cada escenario y consecuencia, utilizando técnicas de análisis cualitativo o cuantitativo. La evaluación de la probabilidad no siempre es fácil y debe expresarse de diferentes maneras. Debe tenerse en cuenta la frecuencia con la que se producen las fuentes de riesgo o la facilidad con la que se pueden explotar algunas de ellas (por ejemplo, las vulnerabilidades), teniendo en cuenta:

- la experiencia y las estadísticas aplicables a la probabilidad de las fuentes de riesgo;
- para las fuentes de riesgo deliberadas: el grado de motivación [por ejemplo, la viabilidad (coste/beneficio) del ataque] y las capacidades (por ejemplo, el nivel de destreza de los posibles atacantes), que cambian con el tiempo, los recursos de que disponen los posibles atacantes, y las influencias sobre los posibles atacantes, como la delincuencia grave, las organizaciones terroristas o la inteligencia extranjera, así como la percepción del atractivo y la vulnerabilidad de la información para un posible atacante;
- para las fuentes de riesgo accidentales: factores geográficos (por ejemplo, la proximidad

a instalaciones o actividades peligrosas), la posibilidad de que se produzcan catástrofes naturales como condiciones meteorológicas extremas, actividad volcánica, terremotos, inundaciones, tsunamis y factores que puedan influir en los errores humanos y el mal funcionamiento de los equipos;

- los puntos débiles conocidos y cualquier control compensatorio, tanto individualmente como en conjunto

- los controles existentes y su eficacia para reducir las debilidades conocidas.

La estimación de la probabilidad es intrínsecamente incierta, no sólo porque tiene en cuenta cosas que aún no han sucedido y, por tanto, no se conocen del todo, sino también porque la probabilidad es una medida estadística y no es directamente representativa de los acontecimientos individuales. Las tres fuentes básicas de incertidumbre en la evaluación son:

- la incertidumbre personal, que se origina en el juicio del evaluador y que se deriva de la variabilidad de la heurística mental de la toma de decisiones

- la incertidumbre metodológica, que se deriva del uso de herramientas que inevitablemente modelan los sucesos de forma simplista

- la incertidumbre sistémica sobre el propio acontecimiento previsto, que se deriva de un conocimiento insuficiente (en particular, si las pruebas son limitadas o una fuente de riesgo cambia con el tiempo).

Para aumentar la fiabilidad de la estimación de la probabilidad, las organizaciones deberían considerar el uso de:

a) evaluaciones en equipo en lugar de evaluaciones individuales;

b) fuentes externas, como los informes sobre violaciones de la seguridad de la información

c) escalas con rango y resolución adecuados al enfoque de la organización;

d) categorías inequívocas, como "una vez al año", en lugar de "infrecuente"

Al evaluar la probabilidad de los sucesos, es importante reconocer la diferencia entre sucesos independientes y dependientes. La probabilidad de los sucesos que dependen unos de otros está condicionados por la relación entre ellos (por ejemplo, un segundo suceso puede ser inevitable si se produce un primer suceso), de modo que no es necesario evaluar por separado la probabilidad de ambos.

Las probabilidades de los sucesos independientes relevantes contribuyen de forma esencial a la probabilidad de una consecuencia a la que contribuyen.

EJEMPLO La probabilidad de un ataque de denegación de servicio a un servidor depende del panorama actual de amenazas y de la vulnerabilidad y accesibilidad del servidor. Sin embargo,

la probabilidad de paquetes maliciosos puede ser del 100 % una vez que el ataque ha comenzado y su evaluación no ayuda a la evaluación de la probabilidad del ataque de denegación de servicio.

Para evitar la complejidad innecesaria de la evaluación, es importante identificar cualquier dependencia entre los eventos que contribuyen a un escenario de riesgo y, en primer lugar, evaluar las probabilidades de aquellos eventos que son independientes entre sí.

La probabilidad global de las consecuencias empresariales de un evento de seguridad de la información suele depender de la probabilidad de varios eventos contribuyentes de menor nivel y de sus consecuencias. En lugar de intentar estimar la probabilidad de las consecuencias para el negocio en una única evaluación de alto nivel, puede ser más válido empezar agregando las probabilidades de los eventos de nivel inferior evaluados individualmente que contribuyen a ello.

7.3.4. Determinación de los niveles de riesgo

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.2 d) 3).

Entrada: Una lista de escenarios de riesgo con sus consecuencias relacionadas con los activos o eventos y su probabilidad (cuantitativa o cualitativa).

Acción: El nivel de riesgo debe determinarse como una combinación de la probabilidad y las consecuencias evaluadas para todos los escenarios de riesgo relevantes.

Activación: La determinación de los niveles de riesgo se hace necesaria si se van a evaluar los riesgos de seguridad de la información.

Resultado: Una lista de riesgos con valores de nivel asignados.

Guía de implementación:

El nivel de riesgo puede determinarse de muchas maneras posibles. Normalmente se determina como una combinación de la probabilidad evaluada y las consecuencias evaluadas para todos los escenarios de riesgo relevantes. Los cálculos alternativos pueden incluir un valor del activo además de la probabilidad y las consecuencias. Además, el cálculo no es necesariamente lineal, por ejemplo, puede ser la probabilidad al cuadrado combinada con la consecuencia. En cualquier caso, el nivel de riesgo debe determinarse utilizando los criterios establecidos según lo descrito en el apartado 6.4.3.4.

7.4. Valoración de los riesgos para la seguridad de la información

7.4.1. Comparación de los resultados del análisis de riesgos con los criterios de riesgo

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.2 e) 1).

Entrada: Una lista de criterios de riesgo y riesgos con valores de nivel asignados.

Acción: El nivel de los riesgos debe compararse con los criterios de valoración de riesgos, en particular con los criterios de aceptación de riesgos.

Activación: La comparación de los resultados del análisis de riesgos con los criterios de riesgo se hace necesaria si los riesgos de seguridad de la información deben ser priorizados para su tratamiento.

Resultado: Una lista de sugerencias para la toma de decisiones sobre las acciones adicionales relativas a la gestión de los riesgos.

Orientación para la aplicación:

Una vez identificados los riesgos y asignados los valores de probabilidad y gravedad de las consecuencias, las organizaciones deben aplicar sus criterios de aceptación de los riesgos para determinar si pueden aceptarse o no. Si no se pueden aceptar, se debe dar prioridad a su tratamiento.

Para valorar los riesgos, las organizaciones deben comparar los riesgos evaluados con los criterios de riesgo definidos durante el establecimiento del contexto.

Las decisiones de valoración de los riesgos deben basarse en la comparación del riesgo evaluado con los criterios de aceptación definidos, teniendo en cuenta idealmente el grado de confianza en la evaluación.

En algunos casos, como la ocurrencia frecuente de sucesos de consecuencias relativamente bajas, puede ser útil considerar su efecto acumulativo a lo largo de una escala temporal de interés, en lugar del riesgo de cada suceso considerado individualmente, ya que esto puede proporcionar una representación más realista de los riesgos globales.

Puede haber incertidumbres a la hora de definir el límite entre los riesgos que requieren tratamiento y los que no. En determinadas circunstancias, utilizar un único nivel como nivel de riesgo aceptable que divide los riesgos que requieren tratamiento de los que no lo requieren no siempre es apropiado. En algunos casos, puede ser más eficaz incluir un elemento de flexibilidad en los criterios, incorporando parámetros adicionales como el coste y la eficacia de los posibles controles.

Los niveles de riesgo pueden validarse sobre la base de un consenso entre los propietarios de los riesgos y los especialistas empresariales y técnicos. Es importante que los propietarios de los riesgos tengan una buena comprensión de los riesgos de los que son responsables que coincida con los resultados de la valoración objetiva. En consecuencia, cualquier disparidad entre los niveles de riesgo valorados y los percibidos por los propietarios de los riesgos debe investigarse para determinar cuál se aproxima más a la realidad.

7.4.2. Priorización de los riesgos analizados para su tratamiento

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.2 e) 2).

Entrada: Una lista de los resultados de los riesgos comparados con los criterios de riesgo.

Acción: Los riesgos de la lista deben ser priorizados para el tratamiento de riesgos, considerando los niveles de riesgo valorados.

Activación: La priorización de los riesgos analizados para el tratamiento de los riesgos se hace necesaria si se quieren tratar los riesgos de seguridad de la información.

Resultado: Una lista de riesgos priorizados con los escenarios de riesgo que conducen a esos riesgos.

Guía de aplicación

La valoración de riesgos utiliza la comprensión del riesgo obtenida por el análisis de riesgos para hacer propuestas para decidir sobre el siguiente paso a dar. Éstas deben referirse a:

- si es necesario un tratamiento del riesgo;
- las prioridades para el tratamiento del riesgo teniendo en cuenta los niveles de riesgo valorados

Los criterios de riesgo utilizados para priorizar los riesgos deben tener en cuenta los objetivos de la organización, los requisitos contractuales, legales y reglamentarios y las opiniones de las partes interesadas pertinentes. La priorización adoptada en la actividad de valoración de riesgos se basa principalmente en los criterios de aceptación.

8. PROCESO DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

8.1. Generalidades

La entrada del tratamiento de los riesgos para la seguridad de la información se basa en los resultados del proceso de evaluación de riesgos en forma de un conjunto priorizado de riesgos a tratar, basado en criterios de riesgo.

El resultado de este proceso es un conjunto de controles de seguridad de la información necesarios [véase ISO/IEC 27001:2022, 6.1.3 b)] que deben desplegarse o mejorarse entre sí, de acuerdo con el plan de tratamiento de riesgos [véase ISO/IEC 27001:2022, 6.1.3 e)]. Desplegado de esta manera, la eficacia del plan de tratamiento de riesgos es modificar el riesgo de seguridad de la información al que se enfrenta la organización para que cumpla con los criterios de aceptación de la organización.

8.2. Selección de las opciones de tratamiento de riesgos de seguridad de la información adecuadas

NOTA Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 6.1.3 a).

Entrada: Una lista de riesgos priorizados con escenarios de eventos o riesgos que conducen a esos riesgos.

Acción: Se deben elegir las opciones de tratamiento de los riesgos.

Activación: La selección de las opciones de tratamiento de los riesgos de seguridad de la información es necesaria si no existe un plan de tratamiento de los riesgos o si el plan está incompleto.

Resultado: Una lista de riesgos priorizados con las opciones de tratamiento de riesgos seleccionadas.

Orientación para la aplicación:

Varias opciones para el tratamiento del riesgo incluyen:

- Evitar el riesgo, decidiendo no iniciar o continuar con la actividad que da lugar al riesgo;
- modificar el riesgo, cambiando la probabilidad de que se produzca un suceso o una consecuencia o cambiando la gravedad de la consecuencia
- Retener del riesgo, mediante una elección informada;
- Compartir el riesgo, repartiendo las responsabilidades con otras partes, ya sea interna o externamente (por ejemplo, compartiendo las consecuencias a través de un seguro);

EJEMPLO 1 Un ejemplo de evitar el riesgo es la ubicación de una oficina situada en una zona inundable, donde existe la posibilidad de que se produzca una inundación y los consiguientes daños a la oficina y restricciones a la disponibilidad y/o acceso a la misma. Los controles físicos pertinentes pueden resultar insuficientes para reducir este riesgo, en cuyo caso, la opción de tratamiento para evitar el riesgo puede ser la mejor opción disponible. Esto puede implicar el cierre o la interrupción del funcionamiento de esa oficina.

EJEMPLO 2 Otro ejemplo de evitar el riesgo consiste en optar por no recoger determinada información de los individuos, de modo que no sea necesario que la organización gestione, almacene y transmita la información en sus sistemas de información.

En el caso de compartir el riesgo, se requiere al menos un control para modificar la probabilidad o la consecuencia, pero la organización delega la responsabilidad de aplicar el control a otra parte.

Las opciones de tratamiento del riesgo deben seleccionarse en función del resultado de la evaluación del riesgo, los costes previstos para la aplicación de estas opciones y los beneficios esperados de estas opciones, tanto individualmente como en el contexto de otros controles. El

tratamiento del riesgo debe priorizarse en función de los niveles de riesgo definidos, las limitaciones de tiempo y la secuencia necesaria de implementaciones, y los resultados de la valoración del riesgo establecidos en el punto 7.4. A la hora de elegir la opción, se puede considerar cómo perciben un riesgo concreto las partes afectadas, y las formas más adecuadas de comunicar el riesgo a estas partes.

8.3. Determinación de todos los controles necesarios para implementar las opciones de tratamiento de riesgos de seguridad de la información

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.3 b).

Entrada: Una lista de riesgos priorizados con las opciones de tratamiento de riesgos seleccionadas.

Acción: Determinar todos los controles, a partir de los conjuntos de control seleccionados de una fuente apropiada, que son necesarios para tratar los riesgos en base a las opciones de tratamiento de riesgos elegidas, tales como modificar, retener, evitar o compartir los riesgos.

Activación: Conformidad con el SGSI; gestión de los riesgos de seguridad de la información.

Resultado: Todos los controles necesarios.

Orientación para la aplicación:

Se debe prestar especial atención a la determinación de los controles necesarios. Debe comprobarse cada control para determinar si es necesario preguntando

- qué efecto tiene este control sobre la probabilidad o la consecuencia de este riesgo;
- de qué manera el control mantiene el nivel de riesgo.

Sólo los controles que tengan un efecto más que insignificante sobre el riesgo deben ser designados como "necesarios". Deben aplicarse uno o más controles a cada riesgo evaluado como necesario.

Hay muchas fuentes de conjuntos de control. Pueden encontrarse en la norma ISO/IEC 27001:2022, Anexo A, en códigos de prácticas específicos del sector (por ejemplo, ISO/IEC 27017) y en otros conjuntos de control nacionales, regionales e industriales. Una organización también puede determinar uno o varios controles "personalizados" (véase ISO/IEC 27003).

Si se define un control personalizado, la redacción del control debe describir de forma precisa y justa qué es el control y cómo funciona. Según sea aplicable y apropiado, esta redacción puede incluir útilmente aspectos tales como:

- si se trata de un control documentado

- a quién pertenece el control;
- cómo se supervisa;
- cómo se puede demostrar;
- cualquier excepción;
- la frecuencia de funcionamiento del control
- la tolerancia del control;
- si no es evidente, la razón por la que existe el control.

Si el control está fuera de la tolerancia, el control no está funcionando con la suficiente eficacia para gestionar el riesgo identificado.

EJEMPLO 1 "Existe un proceso documentado de gestión de malware, propiedad del responsable de seguridad informática.

Esto excluye a los Macs y se supervisa a través de la consola del proveedor con informes sobre el rendimiento enviados semanalmente al CIO".

Un enfoque tan detallado de la redacción de los controles puede ser útil si los controles personalizados también están destinados a apoyar a la organización en la elaboración de informes de garantía de control.

Sin embargo, es más importante que la redacción de los controles tenga significado para las personas de la organización y les ayude a tomar decisiones sobre la gestión de esos controles y los riesgos asociados.

La determinación de los controles puede incluir nuevos controles aún no implementados, o puede incluir el uso de controles que existen en la organización. Sin embargo, un control que ya está en funcionamiento no debe incluirse automáticamente en la evaluación de riesgos porque:

- el control no es necesario para gestionar uno o más riesgos de seguridad de la información;
- puede ser un control que ayude de alguna manera a gestionar uno o más riesgos para la seguridad de la información, pero que no sea lo suficientemente eficaz como para ser incluido en la evaluación de riesgos o gestionado por el SGSI, o
- puede estar operando actualmente por razones no relacionadas con la seguridad de la información (por ejemplo, calidad, eficiencia, eficacia o cumplimiento), o;
- está actualmente en funcionamiento, pero, desde el punto de vista de la seguridad de la información, puede suprimirse por no tener un efecto suficiente que justifique su

continuidad como control esencial.

Si un control se utiliza para fines distintos de la gestión de los riesgos para la seguridad de la información, hay que asegurarse de que el control se gestiona para alcanzar los objetivos de seguridad de la información, así como los objetivos no relacionados con la seguridad de la información.

EJEMPLO 2 CCTV interno para controlar la calidad del proceso de producción, así como por razones de seguridad de la información (para proteger del fraude).

Cuando se determinan los controles a partir de un conjunto de controles existentes (por ejemplo, ISO/IEC 27001:2022, Anexo A, o una lista de controles específicos del sector), la redacción del control debe coincidir con lo necesario para gestionar el riesgo y reflejar con exactitud lo que es o debería ser el control.

Si el enfoque general es utilizar un conjunto de controles existentes (por ejemplo, ISO/IEC 27001:2022, Anexo A, o una lista de controles específicos del sector) y el conjunto de controles no contiene un control que describa con precisión el control necesario, entonces se debe considerar la posibilidad de definir un control personalizado que describa con precisión el control.

Los controles pueden clasificarse en preventivos, detectivos y correctivos:

a) control preventivo: control destinado a evitar que se produzca un evento de seguridad de la información que pueda conducir a la aparición de una o varias consecuencias;

b) control de detección: control destinado a detectar la ocurrencia de un evento de seguridad de la información;

c) control correctivo: control destinado a limitar las consecuencias de un evento de seguridad de la información

El tipo de control describe si un control actúa, o pretende actuar, para prevenir o detectar un evento o reaccionar ante sus consecuencias.

EJEMPLO 3 Una política de seguridad de la información es un control que mantiene el riesgo, pero el cumplimiento de la política pretende reducir la probabilidad de que se produzca el riesgo y, por lo tanto, puede clasificarse como preventivo.

La utilidad de categorizar los controles como preventivos, detectivos y correctivos radica en su uso, para asegurar que la construcción de los planes de tratamiento del riesgo sea resistente a los fallos de control.

Siempre que haya una combinación adecuada de controles preventivos, detectivos y correctivos:

- los controles detectivos deben mitigar el riesgo si los controles preventivos fallan;
- los controles correctivos deben mitigar el riesgo si fallan los controles detectivos;

- los controles preventivos deben reducir la probabilidad de que los controles correctivos tengan que ser utilizados.

Al utilizar los controles, las organizaciones deben decidir primero si es posible detectar la ocurrencia de un evento. Si es así, deben aplicarse los controles de detección. Si no es posible detectar un suceso, los controles de detección pueden ser ineficaces, sin que haya forma de saber si un control preventivo está funcionando.

EJEMPLO 4 Si no está claro si un ordenador ha pasado a formar parte de una "botnet", no se puede saber si los controles que se utilizan para evitar que forme parte de una botnet funcionan como se pretende.

Los controles de detección pueden funcionar como es debido, pero pueden seguir siendo ineficaces.

EJEMPLO 5 La implantación de sistemas de detección/prevención de intrusiones puede ser una forma eficaz de evitar que el malware atraviese la red, pero no sirven de nada si no hay una supervisión de los sistemas/alertas para actuar en caso de que se produzca un brote que no esté contenido.

En general, los controles detectivos son en última instancia ineficaces en los casos en los que se pueden eludir o en los que su notificación no da lugar a una acción adecuada. Los controles correctivos deben ser el siguiente paso. Si los controles de detección fallan, es probable que se produzcan una o más consecuencias indeseables. La aplicación de los controles correctivos puede ayudar a limitar esas consecuencias. Aunque los controles correctivos surten efecto después de la aparición de la consecuencia, a menudo es necesario desplegarlos con bastante antelación a la aparición de cualquier evento.

EJEMPLO 6 La encriptación del disco duro no evita el robo de un ordenador portátil ni los intentos posteriores de extraer los datos. Sin embargo, reduce la gravedad de las consecuencias vinculadas a una revelación. El control, por supuesto, debe desplegarse antes de que el portátil sea robado.

La categorización de los controles no es absoluta y depende del contexto en el que se describe el uso de un control.

EJEMPLO 7 La copia de seguridad no evita que se produzca un evento que, de otro modo, provocaría la pérdida de datos (por ejemplo, la caída de un disco o la pérdida de un portátil), pero ayuda a reducir las consecuencias. Por lo tanto, algunas organizaciones pueden considerarlo un control correctivo más que un control preventivo. Del mismo modo, el cifrado no evita la pérdida de información, pero si el suceso se describe como "datos personales revelados al atacante", entonces el cifrado es un control preventivo, más que correctivo.

El orden en que se organizan los controles que abordan los riesgos depende de varios factores. Se pueden utilizar muchas técnicas. Es responsabilidad de los respectivos propietarios de los riesgos decidir el equilibrio entre los costes de invertir en controles y asumir las consecuencias

en caso de que los riesgos se materialicen.

La identificación de los controles existentes puede determinar que estos controles superan las necesidades actuales. Antes de eliminar los controles redundantes o innecesarios (sobre todo si los controles tienen un alto coste de mantenimiento) debe realizarse un análisis coste-beneficio. Dado que los controles pueden influirse mutuamente, la eliminación de controles redundantes puede reducir la seguridad global existente. Los controles no deben incluirse en el tratamiento del riesgo a menos que sean controles necesarios para gestionar uno o más de los riesgos de seguridad de la información identificados.

Un control debe tener un efecto sobre la consecuencia o la probabilidad de los riesgos de seguridad de la información identificados. Los controles no deben incluirse en el tratamiento del riesgo si funcionan por razones no relacionadas con la seguridad de la información.

Deben tenerse en cuenta los controles que están implantados pero que se sabe que presentan algunas deficiencias. Si la evaluación de todos los riesgos que gestiona un control con debilidades está dentro de los criterios de aceptación, no es necesario mejorar el control. Aunque el control no funcione con plena eficacia, no siempre es necesario mejorarlo para que sea totalmente eficaz. No hay que suponer que todos los controles deben funcionar con plena eficacia para que la organización gestione sus riesgos con éxito.

Es posible especificar que cada control individual tiene un nivel de tolerancia al fallo por debajo del cual se puede considerar que el control no funciona con suficiente eficacia para gestionar los riesgos identificados. Mientras el control funcione dentro de la tolerancia, no necesita ninguna mejora.

8.4. Comparación de los controles determinados con los de la norma ISO/IEC 27001:2022, Anexo A

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.3 c).

Entrada: Todos los controles necesarios (véase 8.3).

Acción: Comparar todos los controles necesarios con los enumerados en la norma ISO/IEC 27001:2022, anexo A.

Activación: La identificación de los controles que faltan se hace necesaria si se formulan planes de tratamiento de riesgos.

Resultado: Todos los controles aplicables al tratamiento del riesgo.

Guía de implementación:

ISO/IEC 27001:2022, 6.1.3 c), requiere que una organización compare los controles que ha determinado como necesarios para implementar sus opciones de tratamiento de riesgos elegidas con los controles enumerados en ISO/IEC 27001:2022, Anexo A. El propósito de esto es actuar

como una comprobación de seguridad para verificar que no se han omitido controles necesarios en la evaluación de riesgos. Esta comprobación de seguridad no se realiza para identificar cualquier control omitido de la norma ISO/IEC 27001:2022, Anexo A, en la evaluación de riesgos. Es una comprobación de seguridad para identificar cualquier control necesario omitido de cualquier fuente, comparando los controles con otras normas y listas de controles. Los controles omitidos identificados durante esta comprobación pueden ser controles específicos del sector o personalizados, o bien de la norma ISO/IEC 27001:2022, Anexo A. Deben seguirse las directrices para determinar los controles que figuran en el apartado 8.3 cuando se considere si deben añadirse a la evaluación de riesgos los controles que faltan.

EJEMPLO Es importante que un control que ya está en funcionamiento en la organización no se añada automáticamente a la evaluación de riesgos sin más consideración.

Es importante recordar que esta comparación de los controles se realiza mediante la evaluación de riesgos y no mediante la declaración de aplicabilidad. El principio consiste en examinar cada uno de los riesgos y comparar los controles determinados como necesarios para el riesgo con los controles del Anexo A de la norma ISO/IEC 27001:2022, para ayudar a identificar si faltan controles necesarios para cada riesgo.

8.5. Elaboración de una declaración de aplicabilidad

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.3 d).

Entrada: Todos los controles aplicables al tratamiento del riesgo (véase 8.4).

Acción: Elaborar una declaración de aplicabilidad.

Activación: Documentación de todos los controles necesarios, su justificación y el estado de implementación.

Resultado: Declaración de aplicabilidad.

Guía de implementación:

De conformidad con la norma ISO/IEC 27001:2022, 6.1.3 d), la declaración de aplicabilidad (SOA) debe contener, como mínimo

a) los controles necesarios;

b) la justificación de su inclusión

c) sí están implementados o no;

d) la justificación de la exclusión de los controles de la norma ISO/IEC 27001:2022, Anexo A.

El SOA puede elaborarse fácilmente examinando la evaluación de riesgos para identificar los

controles necesarios y el plan de tratamiento de riesgos para identificar los que se prevé implantar. Sólo los controles identificados en la evaluación de riesgos pueden incluirse en la SOA. Los controles no pueden añadirse a el SOA independientemente de la evaluación de riesgos. Debe haber coherencia entre los controles necesarios para realizar las opciones de tratamiento del riesgo seleccionadas y el SOA. El SOA puede declarar que la justificación para la inclusión de un control es la misma para todos los controles y que han sido identificados en la evaluación de riesgos como necesarios para tratar uno o más riesgos a un nivel aceptable. No se necesita ninguna otra justificación para la inclusión de un control para ninguno de los controles. El estado de implementación de todos los controles contenidos en la SOA puede declararse como "implementado", "parcialmente implementado" o "no implementado". Esto puede ser individualmente para cada control o como una declaración global.

EJEMPLO El SOA contiene la declaración "Todos los controles se han implantado". No se requiere ningún análisis o información adicional para completar el SOA.

8.6. Plan de tratamiento de riesgos de seguridad de la información

8.6.1. Formulación del plan de tratamiento de riesgos

NOTA Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 6.1.3 e).

Entrada: Resultados de las evaluaciones de riesgos.

Acción: Formular el plan de tratamiento de riesgos.

Activación: La necesidad de la organización de tratar los riesgos.

Resultado: Plan de tratamiento de riesgos.

Guía de implementación:

El propósito de esta actividad es crear plan(es) para tratar conjuntos específicos de los riesgos que están en la lista de riesgos priorizados (ver Cláusula 7). Un plan de tratamiento de riesgos es un plan para modificar el riesgo de manera que cumpla los criterios de aceptación de riesgos de la organización (véase 6.4.2). Hay dos interpretaciones posibles del término "plan" en el contexto del tratamiento de riesgos. La primera es un plan de proyecto, es decir, un plan para implementar los controles necesarios de la organización. La segunda es un plan de diseño, es decir, el plan que no sólo identifica los controles necesarios, sino que también describe cómo los controles interactúan con su entorno y entre sí para modificar los riesgos. En la práctica, pueden utilizarse ambos.

Una vez establecidos los controles, el plan del proyecto deja de tener valor, salvo como registro histórico, mientras que el plan de diseño sigue siendo útil.

Cada riesgo que necesite tratamiento debe ser tratado en uno de los planes de tratamiento de riesgos.

Una organización puede optar por tener varios planes de tratamiento de riesgos, que en conjunto implementan todos los aspectos requeridos del tratamiento de riesgos. Éstos pueden organizarse en función de dónde resida la información (por ejemplo, un plan para el centro de datos, otro para la informática móvil, etc.), por activos (por ejemplo, diferentes planes para diferentes clasificaciones de activos) o por eventos (como los utilizados al evaluar el riesgo mediante el método basado en eventos).

Al crear el plan de tratamiento de riesgos, las organizaciones deben tener en cuenta lo siguiente

- las prioridades en relación con el nivel de riesgo y la urgencia del tratamiento;
- sí son aplicables diferentes tipos de controles (preventivos, detectivos, correctivos) o su composición.
- si es necesario esperar a que se resuelva un control antes de empezar a aplicar uno nuevo en el mismo activo
- sí hay un retraso entre el momento en que se implanta el control y el momento en que es plenamente eficaz y operativo.

Para cada riesgo tratado, el plan de tratamiento debe incluir la siguiente información

- la justificación de la selección de las opciones de tratamiento, incluidos los beneficios que se espera obtener;
- los responsables de aprobar y aplicar el plan;
- las acciones propuestas
- los recursos necesarios, incluidos los imprevistos
- los indicadores de rendimiento
- las limitaciones;
- los informes y el seguimiento necesarios;
- cuando se espera que las acciones se lleven a cabo y se completen;
- el estado de ejecución.

Las acciones del plan de tratamiento de riesgos deben clasificarse por prioridad en relación con el nivel de riesgo y la urgencia del tratamiento. Cuanto mayor sea el nivel de riesgo y, en algunos casos, la frecuencia con la que se produce el riesgo, antes deberá aplicarse el control.

Para cada uno de los riesgos enumerados en el plan de tratamiento de riesgos, se debe hacer

un seguimiento de la información detallada sobre su aplicación, que puede incluir, entre otras cosas

- nombres de los propietarios del riesgo y de las personas responsables de la aplicación
- fechas o plazos de aplicación;
- actividades de control planificadas para probar el resultado de la implementación
- estado de la implementación;
- nivel de coste (inversión, funcionamiento).

8.6.2. Aprobación por parte de los propietarios de los riesgos

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.3 f).

Entrada: Plan(es) de tratamiento de riesgos.

Acción: Aprobación del (de los) plan(es) de tratamiento de riesgos por parte de los propietarios de los riesgos.

Activación: La necesidad de aprobar el/los plan/es de tratamiento de riesgos.

Resultado: Plan(es) de tratamiento de riesgos aprobado(s)

Orientación para la aplicación:

El plan de tratamiento de los riesgos de seguridad de la información debe ser aprobado por los propietarios de los riesgos una vez formulado. Los propietarios de los riesgos también deben decidir sobre la aceptación de los riesgos residuales para la seguridad de la información. Esta decisión debe basarse en criterios de aceptación de riesgos definidos.

Los resultados de la evaluación de los riesgos, el plan de tratamiento de los riesgos y los riesgos restantes deben ser comprensibles para los propietarios de los riesgos, de modo que puedan cumplir con sus responsabilidades adecuadamente.

8.6.3. Aceptación de los riesgos residuales de seguridad de la información

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 6.1.3 f).

Entrada: Plan(es) de tratamiento de riesgos aprobado(s) y criterios de aceptación de riesgos.

Acción: Determinar si los riesgos residuales son aceptables.

Activación: La necesidad de que la organización decida sobre la retención de los riesgos residuales.

Resultado: Riesgos residuales aceptados.

Orientación para la aplicación:

Para determinar los riesgos residuales, los planes de tratamiento de riesgos deben alimentar la evaluación de seguimiento de la probabilidad y las consecuencias residuales. Los controles propuestos en los planes de tratamiento de riesgos y su eficacia deben considerarse a la luz de si reducirán la probabilidad o la consecuencia, o ambas, y si el nivel de riesgos residuales se asigna a los riesgos. El nivel de los riesgos residuales es entonces considerado por el propietario del riesgo para determinar si los riesgos residuales son aceptables.

Los planes de tratamiento de riesgos deben describir cómo se van a tratar los riesgos evaluados para cumplir con los criterios de aceptación del riesgo.

En algunos casos, el nivel de riesgo residual no siempre cumple los criterios de aceptación del riesgo, porque los criterios que se aplican no tienen en cuenta las circunstancias imperantes.

EJEMPLO Se puede argumentar que es necesario conservar los riesgos porque los beneficios que los acompañan son una importante oportunidad de negocio, o porque el coste de la modificación del riesgo es demasiado elevado.

Sin embargo, no siempre es posible revisar los criterios de aceptación del riesgo a tiempo. En estos casos, los propietarios de los riesgos pueden retener los riesgos que no cumplen los criterios normales de aceptación. Si esto es necesario, el propietario del riesgo debe comentar explícitamente los riesgos e incluir una justificación de la decisión de anular los criterios normales de aceptación del riesgo.

La aceptación del riesgo puede implicar un proceso para lograr la aprobación de los tratamientos antes de la decisión final de aceptación del riesgo. Es importante que los propietarios de los riesgos revisen y aprueben los planes de tratamiento de riesgos propuestos y los riesgos residuales resultantes, y registren cualquier condición asociada a dicha aprobación. Dependiendo del proceso de evaluación de riesgos y de los criterios de aceptación del riesgo, esto puede requerir que un gestor con un nivel de autoridad superior al del propietario del riesgo dé su visto bueno a la aceptación del riesgo.

Puede llevar algún tiempo aplicar un plan para tratar los riesgos evaluados. Los criterios de riesgo pueden permitir que los niveles de riesgo superen un umbral deseado en una medida definida si existe un plan para reducir ese riesgo en un tiempo aceptable. Las decisiones de aceptación del riesgo pueden tener en cuenta los plazos de los planes de tratamiento del riesgo y si el progreso de la aplicación del tratamiento del riesgo se ajusta a lo previsto.

Algunos riesgos pueden variar con el tiempo (independientemente de que este cambio se deba a la aplicación de un plan de tratamiento de riesgos). Los criterios de aceptación de riesgos pueden tener en cuenta este aspecto y contar con umbrales de aceptación de riesgos que dependan del tiempo que una organización puede estar expuesta a un riesgo evaluado.

9. OPERACIÓN

9.1. Realización del proceso de evaluación de riesgos para la seguridad de la información

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 8.2.

Entrada: Documentos sobre el proceso de evaluación de riesgos para la seguridad de la información, incluyendo la evaluación de riesgos y los criterios de aceptación de riesgos.

Acción: El proceso de evaluación de riesgos debe realizarse de acuerdo con la cláusula 7.

Activación La necesidad de la organización de evaluar los riesgos, a intervalos planificados o en base a eventos.

Resultado: Los riesgos evaluados.

Guía de implementación:

El proceso de evaluación de riesgos para la seguridad de la información definido y aplicado en la norma ISO/IEC 27001:2022, 6.1, debe integrarse en las operaciones de la organización y debe realizarse a intervalos planificados o cuando se propongan u ocurran cambios significativos. El proceso de evaluación de riesgos para la seguridad de la información debe tener en cuenta los criterios establecidos en la norma ISO/IEC 27001:2022, 6.1.2 a). Los intervalos en los que se realiza la evaluación de riesgos deben ser apropiados para el SGSI. Cuando se produzca un cambio significativo del SGSI (o de su contexto) o un cambio en el panorama de las amenazas (por ejemplo, un nuevo tipo de ataque a la seguridad de la información), la organización debe determinar si este cambio requiere una evaluación adicional de los riesgos para la seguridad de la información.

Al hacer planes para las evaluaciones de riesgo rutinarias, las organizaciones deben tener en cuenta cualquier calendario que se aplique a sus procesos empresariales generales y a los ciclos presupuestarios asociados.

EJEMPLO Si existe un ciclo presupuestario anual, se puede exigir a la organización que presente solicitudes de financiación en un momento determinado del año. Los fondos se conceden (disminuyen o se deniegan) más tarde.

Si se trata de procesos de adquisición, puede haber otro ciclo presupuestario antes de que se puedan aplicar las recomendaciones de tratamiento de riesgos y evaluar su eficacia antes de la siguiente evaluación de riesgos rutinaria. En tales casos, las evaluaciones de riesgos deben programarse:

a) para hacer sus recomendaciones de tratamiento de riesgos a tiempo para la solicitud de financiación;

b) para ser reevaluadas tras los resultados de las asignaciones presupuestarias

c) para realizar la siguiente evaluación rutinaria, una vez aplicadas las recomendaciones, después de cualquier actividad de adquisición.

9.2. Realización del proceso de tratamiento de riesgos de seguridad de la información

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 8.3.

Entrada: Riesgo(s) evaluado(s).

Acción: El proceso de tratamiento de riesgos debe realizarse de acuerdo con la cláusula 8.

Activación: La necesidad de la organización de tratar los riesgos, a intervalos planificados o en base a eventos.

Resultado: Los riesgos residuales retenidos o aceptados.

Guía de implementación:

ISO/IEC 27001:2022, 8.3, especifica los requisitos para que las organizaciones implementen sus planes de tratamiento de riesgos. Las consideraciones incluidas en 8.6 también son relevantes para esta subcláusula.

10. APROVECHAMIENTO DE LOS PROCESOS RELACIONADOS CON EL SGSI

10.1. Contexto de la organización

NOTA Esta subcláusula está relacionada con la ISO/IEC 27001:2022, cláusula 4.

Entrada: Información sobre la organización, su contexto interno y externo.

Acción: Se deben considerar todos los datos relevantes para identificar y describir los aspectos internos y externos que influyen en la gestión de riesgos de seguridad de la información y los requisitos de las partes interesadas.

Activación: La norma ISO/IEC 27001:2022 especifica los requisitos de dicha información para poder establecer los objetivos de seguridad de la información.

Resultado: Cuestiones internas y externas relacionadas con el riesgo que influyen en la gestión del riesgo de la seguridad de la información.

Guía de implementación:

La organización debe tener una comprensión de alto nivel (por ejemplo, estratégica) de las cuestiones importantes que pueden afectar al SGSI, ya sea positiva o negativamente. Además, debe conocer el contexto interno y externo que es relevante para su propósito y que afecta a su capacidad para lograr el resultado previsto de su SGSI. Los resultados previstos deben garantizar la preservación de la confidencialidad, la integridad y la disponibilidad de la información mediante la aplicación del proceso de gestión de riesgos y el conocimiento de los riesgos que se gestionan adecuadamente.

Para identificar los riesgos de forma fiable, la organización debe conocer con suficiente detalle las circunstancias en las que opera. Esto significa que la organización debe reunir información sobre el contexto interno y externo de la organización, sus partes interesadas y sus requisitos (véase ISO/IEC 27001:2022, 4.1 y 4.2). La recopilación de esta información debe hacerse antes de que la organización intente evaluar sus riesgos de seguridad de la información, o cualquier otro riesgo que pueda afectar al resultado previsto del SGSI (véase ISO/IEC 27001:2022, 6.1.1).

La organización debe considerar todas las fuentes de riesgo internas y externas. La comprensión de la organización de las partes interesadas que se oponen a la organización y sus intereses es muy relevante.

EJEMPLO 1 Un ejemplo de parte interesada con intereses opuestos a los objetivos de la organización es el atacante. El atacante desea una organización con un nivel de seguridad débil. La organización tiene en cuenta el interés de esta parte teniendo lo contrario (nivel de seguridad fuerte), es decir, la organización considera los posibles conflictos con los objetivos del SGSI. La organización garantiza, a través de controles eficaces de seguridad de la información, que estos intereses no se cumplan.

Las interfaces con servicios o actividades que no están completamente dentro del alcance del SGSI deben ser consideradas en la evaluación de riesgos de seguridad de la información de la organización.

EJEMPLO 2 Un ejemplo de esta situación es el uso compartido de activos (por ejemplo, instalaciones, sistemas informáticos y bases de datos) con otras organizaciones o la externalización de una función empresarial.

La forma de considerar otros factores relevantes que influyen en la seguridad de la información depende de la elección de la organización de los métodos de identificación y análisis de riesgos.

Los objetivos de seguridad de la información de la organización (véase ISO/IEC 27001:2022, 6.2) pueden restringir los criterios de aceptación del riesgo (por ejemplo, el nivel de riesgo aceptable puede ser una función de las recompensas potenciales asociadas a las diferentes actividades empresariales). Además, la política de seguridad de la información puede restringir el tratamiento del riesgo (por ejemplo, ciertas opciones de tratamiento del riesgo pueden ser excluidas por esa política).

10.2. Liderazgo y compromiso

NOTA Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 5.1.

Entrada: Información sobre los resultados de la evaluación de los riesgos para la seguridad de la información o los resultados del tratamiento de los riesgos para la seguridad de la información que requieren aprobación o respaldo.

Acción: El nivel apropiado de la dirección debe considerar los resultados relacionados con los riesgos de seguridad de la información, para decidir o refrendar las acciones posteriores.

Activación: ISO/IEC 27001 requiere que el nivel apropiado de gestión esté involucrado en todas las actividades relacionadas con los riesgos de seguridad de la información.

Resultado: Decisiones relacionadas con los riesgos de seguridad de la información o su aprobación.

Guía de implementación:

La alta dirección es responsable de la gestión de los riesgos y debe dirigir e impulsar las evaluaciones de riesgos, incluyendo

- Garantizar que se asignan los recursos necesarios para la gestión de los riesgos;
- asignar la autoridad, la responsabilidad y la obligación de rendir cuentas en los niveles apropiados dentro de la organización en lo que respecta a la gestión de riesgos
- la comunicación con las partes interesadas apropiadas.

10.3. Comunicación y consulta

NOTA 1 Esta subcláusula está relacionada con ISO/IEC 27001:2022, 7.4.

NOTA 2 ISO/IEC 27001 se refiere directamente a la parte de comunicación de esta actividad.

Entrada: Información sobre los riesgos, sus causas, consecuencias y su probabilidad, identificada a través de los procesos de gestión de riesgos.

Acción: La información sobre los riesgos, sus causas, consecuencias, su probabilidad y los controles que se están tomando para tratarlos debe ser comunicada a las partes interesadas externas e internas, u obtenida de ellas.

Activación: La norma ISO/IEC 27001 exige dicha comunicación.

Resultado: Las percepciones de las partes interesadas relevantes y la comprensión continua del proceso de gestión de riesgos de seguridad de la información de la organización y sus resultados.

Guía de implementación:

La actividad de comunicación y consulta tiene como objetivo lograr un acuerdo sobre la forma de gestionar los riesgos mediante el intercambio y/o la puesta en común de información sobre el riesgo con los propietarios del riesgo y otras partes interesadas pertinentes. La información incluye, pero no se limita a, la existencia, naturaleza, forma, probabilidad, consecuencia, importancia, tratamiento y aceptación de los riesgos.

La norma ISO/IEC 27001:2022, 6.1.2 c) 2), exige que se identifiquen los propietarios de los riesgos de seguridad de la información. La propiedad de los riesgos puede confundirse u ocultarse deliberadamente. Incluso cuando los propietarios de los riesgos pueden ser

identificados, pueden ser reacios a reconocer que son responsables de los riesgos que poseen, y obtener su participación en el proceso de gestión de riesgos puede ser difícil. Debe haber un procedimiento de comunicación definido para informar a los interesados sobre la propiedad de los riesgos.

La norma ISO/IEC 27001:2022, 6.1.3 f), exige que los propietarios de los riesgos aprueben el plan o los planes de tratamiento de los riesgos y decidan sobre la aceptación de los riesgos residuales. La comunicación entre los propietarios de los riesgos y el personal responsable de la implementación del SGSI es una actividad importante. Debe haber un acuerdo sobre cómo gestionar los riesgos intercambiando y/o compartiendo información sobre el riesgo con los propietarios del riesgo, y quizás con otras partes interesadas y responsables de la toma de decisiones. La información incluye, entre otras cosas, la existencia, naturaleza, forma, probabilidad, importancia, tratamiento y aceptación de los riesgos. La comunicación debe ser bidireccional.

Dependiendo de la naturaleza y la sensibilidad del riesgo o riesgos, puede ser necesario limitar cierta información sobre los riesgos, su evaluación y tratamiento en función de la necesidad de conocerlos a los responsables de su identificación, evaluación y tratamiento. La comunicación de los riesgos debe controlarse en función de la "necesidad de saber", teniendo en cuenta el nivel de detalle requerido por las diferentes partes interesadas, en consulta con los propietarios o posibles propietarios de los riesgos, con el objetivo de evitar la publicidad de los riesgos más sensibles y sus debilidades conocidas asociadas.

Las percepciones del riesgo pueden variar debido a las diferencias en los supuestos, los conceptos, las necesidades, los problemas y las preocupaciones de las partes interesadas correspondientes en relación con el riesgo o las cuestiones que se debaten. Es probable que las partes interesadas emitan juicios sobre la aceptación del riesgo, basándose en su percepción del mismo. Esto es especialmente importante para garantizar que las percepciones del riesgo de las partes interesadas, así como sus percepciones de los beneficios, puedan ser identificadas y documentadas y que las razones subyacentes sean claramente comprendidas y abordadas.

La comunicación y la consulta sobre los riesgos pueden dar lugar a un mayor compromiso de las partes interesadas con lo que se está haciendo y a que las partes interesadas apropiadas se apropien de las decisiones y los resultados. La comunicación y la consulta con las partes interesadas, a medida que se desarrollan los criterios y se seleccionan los métodos de evaluación de riesgos, también pueden mejorar la apropiación de los resultados por parte de las partes interesadas. Es menos probable que las partes interesadas cuestionen los resultados de los procesos que han ayudado a diseñar. En consecuencia, suele aumentar la probabilidad de que acepten los resultados y apoyen los planes de acción. En los casos en que las partes interesadas son directivos, esto puede crear un compromiso para alcanzar los objetivos de la gestión de riesgos y proporcionar los recursos necesarios.

La comunicación de los riesgos debe llevarse a cabo para

- ofrecer garantías sobre el resultado de la gestión de riesgos de la organización

- recopilar información sobre los riesgos
- compartir los resultados de la evaluación de riesgos y presentar el plan de tratamiento de estos;
- evitar o reducir tanto la aparición como las consecuencias de las violaciones de la seguridad de la información debidas a la falta de entendimiento mutuo entre los propietarios de los riesgos y las partes interesadas
- apoyar a los propietarios de los riesgos;
- obtener nuevos conocimientos en materia de seguridad de la información
- coordinar con otras partes y planificar respuestas para reducir las consecuencias de cualquier incidente
- dar un sentido de responsabilidad a los propietarios del riesgo y a otras partes con un interés legítimo en el riesgo;
- mejorar la concienciación

Una organización debe desarrollar planes de comunicación de riesgos tanto para las operaciones normales como para las emergencias. La actividad de comunicación y consulta de riesgos debe realizarse de forma continua.

La coordinación entre los principales propietarios de los riesgos y las partes interesadas pertinentes puede lograrse mediante la formación de un comité en el que se debata sobre los riesgos, su priorización y tratamiento adecuado, y su aceptación.

Las comunicaciones sobre los riesgos pueden remitirse voluntariamente a terceros externos para permitir una mejor coordinación o concienciación de la gestión de los riesgos o de la respuesta, y también pueden ser exigidas por los reguladores o los socios comerciales en determinadas circunstancias.

Es importante cooperar con la unidad de relaciones públicas o de comunicación adecuada dentro de la organización para coordinar todas las tareas relacionadas con la comunicación de riesgos. Esto es crucial en caso de activación de la comunicación de crisis, por ejemplo, en respuesta a determinados incidentes.

10.4. Información documentada

10.4.1. Generalidades

NOTA Esta subcláusula está relacionada con la norma ISO/IEC 27001:2022, 7.5.

ISO/IEC 27001 especifica los requisitos para que las organizaciones conserven información

documentada sobre el proceso de evaluación de riesgos (véase ISO/IEC 27001:2022, 6.1.2) y los resultados (véase ISO/IEC 27001:2022, 8.2); el proceso de tratamiento de riesgos (ISO/IEC 27001:2022, 6.1.3) y los resultados (ISO/IEC 27001:2022, 8.3).

10.4.2. Información documentada sobre los procesos

Entrada: Conocimiento sobre los procesos de evaluación y tratamiento de los riesgos de la seguridad de la información de acuerdo con las cláusulas 7 y 8, definidos por la organización.

Acción: La información sobre los procesos de evaluación y tratamiento de los riesgos para la seguridad de la información debe documentarse y conservarse.

Activación: La norma ISO/IEC 27001 requiere información documentada sobre los procesos de evaluación y tratamiento de los riesgos para la seguridad de la información.

Resultado: Información documentada requerida por las partes interesadas (por ejemplo, el organismo de certificación) o determinada por la organización como necesaria para la eficacia del proceso de evaluación de riesgos de seguridad de la información o del proceso de tratamiento de riesgos de seguridad de la información.

Orientación para la aplicación:

La información documentada sobre el proceso de evaluación de riesgos para la seguridad de la información debe contener

a) Una definición de los criterios de riesgo (incluidos los criterios de aceptación del riesgo y los criterios para realizar las evaluaciones de los riesgos para la seguridad de la información);

b) Un razonamiento sobre la coherencia, la validez y la comparación de los resultados

c) Una descripción del método de identificación del riesgo (incluida la identificación de los propietarios del riesgo)

d) Una descripción del método de análisis de los riesgos para la seguridad de la información (incluida la evaluación de las consecuencias potenciales, la probabilidad realista y el nivel de riesgo resultante)

e) una descripción del método para comparar los resultados con los criterios de riesgo y la priorización de los riesgos para su tratamiento.

La información documentada sobre el proceso de tratamiento de los riesgos para la seguridad de la información debe contener descripciones de

- el método para seleccionar las opciones adecuadas de tratamiento de los riesgos para la seguridad de la información
- el método para determinar los controles necesarios.
- cómo se utiliza la norma ISO/IEC 27001:2022, Anexo A, para determinar que no se han pasado por alto inadvertidamente los controles necesarios;
- cómo se elaboran los planes de tratamiento de riesgos
- cómo se obtiene la aprobación de los propietarios del riesgo.

10.4.3. Información documentada sobre los resultados

Entrada: Los resultados de la evaluación y el tratamiento de los riesgos para la seguridad de la información.

Acción: La información sobre la evaluación de riesgos de seguridad de la información y los resultados del tratamiento deben ser documentados y conservados.

Activación: La norma ISO/IEC 27001 requiere información documentada sobre la evaluación de riesgos de seguridad de la información y los resultados del tratamiento.

Resultado: Información documentada sobre la evaluación de los riesgos para la seguridad de la información y los resultados del tratamiento.

Guía de implementación:

Dado que las organizaciones están obligadas a realizar evaluaciones de riesgos a intervalos planificados o cuando se proponen o se producen cambios significativos, debería haber al menos evidencia de un calendario, y de que las evaluaciones de riesgos se realizan de acuerdo con ese calendario. Si se propone un cambio, o se ha producido, debe haber pruebas de la realización de una evaluación de riesgos asociada. De lo contrario, la organización debe explicar por qué el cambio es significativo o no.

La información documentada sobre los resultados de la evaluación de riesgos para la seguridad de la información debe contener

a) los riesgos identificados, su consecuencia y probabilidad;
b) la identidad del propietario o propietarios del riesgo;
c) los resultados de la aplicación de los criterios de aceptación del riesgo
d) la prioridad del tratamiento del riesgo.

También se recomienda registrar la justificación de las decisiones sobre riesgos, tanto para

aprender de los errores en casos individuales como para facilitar la mejora continua.

La información documentada sobre los resultados del tratamiento de los riesgos para la seguridad de la información debe contener

- la identificación de los controles necesarios
- cuando sea apropiado y esté disponible, pruebas de que estos controles necesarios actúan para modificar los riesgos, de manera que se cumplan los criterios de aceptación de riesgos de la organización.

10.5. Seguimiento y revisión

10.5.1. Generalidades

NOTA Esta subcláusula está relacionada con ISO/IEC 27001:2022, 9.1.

El proceso de seguimiento de la organización (véase ISO/IEC 27001:2022, 9.1) debe abarcar todos los aspectos de los procesos de evaluación y tratamiento de riesgos con el fin de

a) asegurar que los tratamientos de riesgos son efectivos, eficientes y económicos tanto en su diseño como en su operación;

b) obtener información para mejorar las futuras evaluaciones de riesgos

d) analizar y aprender las lecciones de los incidentes (incluidos los cuasi accidentes), los cambios, las tendencias, los éxitos y los fracasos

c) detectar los cambios en el contexto interno y externo, incluidos los cambios en los criterios de riesgo y los propios riesgos, que pueden requerir la revisión de los tratamientos y las prioridades de riesgo

e) identificar los riesgos emergentes.

Los escenarios de riesgo retenidos, procedentes de las actividades de gestión de riesgos, pueden transponerse en escenarios de seguimiento para garantizar un proceso de seguimiento eficaz. En el apartado A.2.7 se ofrecen más detalles sobre los escenarios de seguimiento.

10.5.2. Seguimiento y revisión de los factores que influyen en los riesgos

NOTA Esta subcláusula está relacionada con ISO/IEC 27001:2022, 9.1.

Entrada: Toda la información sobre riesgos obtenida de las actividades de gestión de riesgos.

Acción: Los riesgos y sus factores (es decir, el valor de los activos, las consecuencias, las amenazas, las vulnerabilidades, la probabilidad de ocurrencia) deben ser monitoreados y revisados para identificar cualquier cambio en el contexto de la organización en una etapa

temprana, y para mantener una visión general de la imagen completa del riesgo.

Activación: Revisión de la política de la organización y cualquier detección de cambios en el entorno operativo o de amenazas actual.

Resultado: Alineación continua de la gestión de riesgos con los objetivos empresariales de la organización y con los criterios de aceptación de riesgos.

Guía de implementación:

ISO/IEC 27001:2022, 9.1, requiere que las organizaciones evalúen su desempeño en seguridad de la información (y la efectividad del SGSI). De acuerdo con este requisito, las organizaciones deben utilizar su(s) plan(es) de tratamiento de riesgos como tema para sus evaluaciones de desempeño. Para ello, una organización debe definir primero una o más necesidades de información, por ejemplo, para describir lo que la alta dirección desea saber sobre la capacidad de la organización para defenderse de las amenazas.

A partir de esta especificación de alto nivel, la organización debe determinar las mediciones que debe realizar y cómo deben combinarse para satisfacer la necesidad de información.

Los riesgos no son estáticos. Los escenarios de los eventos, los valores de los activos, las amenazas, las vulnerabilidades, las probabilidades y las consecuencias pueden cambiar abruptamente sin ninguna indicación. Hay que realizar un seguimiento constante para detectar estos cambios. Esto puede ser apoyado por servicios externos que proporcionan información sobre nuevas amenazas o vulnerabilidades.

Las organizaciones deben garantizar el seguimiento continuo de los factores relevantes, como, por ejemplo

a) nuevas fuentes de riesgo, incluyendo las vulnerabilidades recién reportadas en TI;

b) los nuevos activos que se hayan incluido en el ámbito de la gestión de riesgos

c) la modificación necesaria de los valores de los activos (por ejemplo, debido a cambios en los requisitos empresariales)

d) las vulnerabilidades identificadas para determinar las que quedan expuestas a amenazas nuevas o reemergentes

e) los cambios en los patrones de uso de las tecnologías existentes o nuevas que puedan abrir nuevas oportunidades posibles de ataque

f) los cambios en las leyes y reglamentos

g) los cambios en la predisposición al riesgo y la percepción de lo que es aceptable y lo que ya no lo es

h) los incidentes de seguridad de la información, tanto dentro como fuera de la organización.

Las nuevas fuentes de riesgo o los cambios en la probabilidad o las consecuencias pueden aumentar los riesgos previamente evaluados. La revisión de los riesgos bajos y retenidos debe examinar cada riesgo por separado, y también todos esos riesgos en conjunto, para evaluar su potencial consecuencia acumulada. Si los riesgos ya no entran en la categoría de riesgo bajo o aceptable, deben tratarse utilizando una o varias de las opciones del apartado 8.2.

Los factores que afectan a la probabilidad de que se produzcan eventos y sus correspondientes consecuencias pueden cambiar, al igual que los factores que afectan a la idoneidad o al coste de las distintas opciones de tratamiento. Los cambios importantes que afecten a la organización deben ser motivo de una revisión más específica. Las actividades de seguimiento del riesgo deben repetirse regularmente y las opciones seleccionadas para el tratamiento del riesgo deben revisarse periódicamente.

Las nuevas amenazas, las vulnerabilidades o los cambios en la probabilidad o las consecuencias pueden aumentar los riesgos previamente evaluados como bajos. La revisión de los riesgos bajos y retenidos debe considerar cada riesgo por separado, y también todos esos riesgos en conjunto, para evaluar su potencial consecuencia acumulada. Si los riesgos no entran en la categoría de riesgo bajo o aceptable, deben tratarse utilizando una o varias de las opciones consideradas en la cláusula 8.

Los factores que afectan a la probabilidad de que se produzcan las amenazas y sus correspondientes consecuencias pueden cambiar, al igual que los factores que afectan a la idoneidad o al coste de las distintas opciones de tratamiento. Los cambios importantes que afecten a la organización deben ser motivo de una revisión más específica. Las actividades de seguimiento de los riesgos deben repetirse regularmente y las opciones seleccionadas para el tratamiento de los riesgos deben revisarse periódicamente.

El resultado de las actividades de seguimiento del riesgo puede ser una aportación a otras actividades de revisión del riesgo. La organización debe revisar todos los riesgos regularmente, y cuando se propongan o se produzcan cambios importantes, de acuerdo con la norma ISO/IEC 27001:2022, cláusula 8.

10.6. Revisión de la gestión

NOTA Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 9.3.

Entrada: Resultados de la(s) evaluación(es) de riesgos de seguridad de la información, estado del plan de tratamiento de riesgos de seguridad de la información.

Acción: Los resultados de la evaluación de riesgos de seguridad de la información y el estado del plan de tratamiento de riesgos de seguridad de la información deben ser revisados para confirmar que los riesgos residuales cumplen con los criterios de aceptación de riesgos, y que el plan de tratamiento de riesgos aborda todos los riesgos relevantes y sus opciones de tratamiento de riesgos.

Activación: Una parte del calendario programado de actividades de revisión.

Resultado: Cambios de los criterios de aceptación de riesgos y de los criterios para realizar evaluaciones de riesgos de seguridad de la información, plan de tratamiento de riesgos de seguridad de la información actualizado o SOA.

10.7. Acción correctiva

NOTA Esta subcláusula se relaciona con la ISO/IEC 27001:2022, 10.1.

Entrada: El plan de tratamiento de riesgos está resultando ineficaz, lo que significa que el riesgo residual permanecerá en niveles inaceptables después de que el plan de tratamiento se haya completado.

Acción: Revisar el plan de tratamiento de riesgos e implementarlo para modificar el riesgo residual a un nivel aceptable.

Activación: La decisión de revisar el plan de tratamiento de riesgos.

Resultado: Un plan de tratamiento de riesgos revisado y su aplicación.

Orientación para la aplicación:

Las no conformidades relacionadas con la eficacia del plan de tratamiento de riesgos pueden ser planteadas por una auditoría interna o externa, o a través del seguimiento y los indicadores. El plan de tratamiento debe ser revisado para reflejar

- los resultados del proceso de tratamiento de los riesgos para la seguridad de la información;
- la aplicación progresiva del plan (por ejemplo, un control se aplica según lo especificado, según lo diseñado, según lo construido)
- las dificultades identificadas en la aplicación de los controles (por ejemplo, problemas técnicos o financieros, incoherencias con factores internos o externos, como consideraciones de privacidad).

También hay casos en los que, aunque los riesgos residuales sean aceptables una vez completado el plan de tratamiento, los usuarios rechazarán su uso o intentarán eludirlo porque estos controles no son aceptados por los usuarios en términos de facilidad de uso (por ejemplo, no son ergonómicos, son demasiado complicados o largos).

La organización debe revisar la eficacia del plan de tratamiento revisado.

10.8. Mejora continua

NOTA Esta subcláusula está relacionada con ISO/IEC 27001:2022, 10.2

Entrada: Toda la información sobre riesgos obtenida de las actividades de gestión de riesgos.

Acción: El proceso de gestión de riesgos de la seguridad de la información debe ser continuamente monitoreado, revisado y mejorado según sea necesario.

Activación: La organización busca mejorar y madurar a partir de las lecciones aprendidas durante el proceso de gestión de riesgos de seguridad de la información.

Resultado: Pertinencia continua del proceso de gestión de riesgos de seguridad de la información para los objetivos empresariales de la organización o actualización del proceso.

Guía de implementación:

Para garantizar que el proceso de gestión de riesgos de la seguridad de la información sea correcto, es necesario supervisar y revisar continuamente que el contexto, el resultado de la evaluación y el tratamiento de los riesgos, así como los planes de gestión, sigan siendo pertinentes y adecuados a las circunstancias.

La organización debe asegurarse de que el proceso de gestión de riesgos para la seguridad de la información y las actividades relacionadas siguen siendo apropiados en las circunstancias actuales y se siguen. Cualquier mejora acordada en el proceso, o las acciones necesarias para mejorar el cumplimiento del proceso, deben ser notificadas a los gestores responsables. Estos gestores deben tener la seguridad de que no se pasa por alto ni se subestima ningún riesgo o elemento de riesgo y de que se adoptan las medidas y decisiones necesarias para proporcionar una comprensión realista del riesgo y la capacidad de respuesta.

Cabe señalar que el proceso de gestión de cambios debe retroalimentar continuamente el proceso de gestión de riesgos para garantizar que las variaciones en los sistemas de información que puedan modificar los riesgos se tengan en cuenta rápidamente, modificando incluso las actividades de evaluación de riesgos para evaluarlas adecuadamente.

Además, la organización debe verificar regularmente los criterios utilizados para medir el riesgo. Esta verificación debe garantizar que todos los elementos siguen siendo válidos y coherentes con los objetivos, las estrategias y las políticas de la empresa, y que los cambios en el contexto empresarial se tienen en cuenta adecuadamente durante el proceso de gestión de los riesgos de seguridad de la información. Esta actividad de supervisión y revisión debe abordar (pero no limitarse a)

- el contexto legal y medioambiental
- el contexto de la competencia
- el enfoque de la evaluación de riesgos
- el valor y las categorías de los activos

- criterios de consecuencia;
- criterios de probabilidad;
- criterios de valoración de riesgos;
- criterios de aceptación del riesgo;
- coste total de propiedad;
- recursos necesarios.

La organización debe garantizar que los recursos para la evaluación y el tratamiento de los riesgos estén continuamente disponibles para revisar el riesgo, para tratar las amenazas o vulnerabilidades nuevas o modificadas, y para asesorar a la dirección en consecuencia.

El seguimiento de la gestión de riesgos puede dar lugar a la modificación o adición del enfoque, la metodología o las herramientas utilizadas en función de

- la madurez del riesgo de la organización
- los cambios identificados;
- la iteración de la evaluación de riesgos;
- el objetivo del proceso de gestión de riesgos para la seguridad de la información (por ejemplo, la continuidad del negocio, la resistencia a los incidentes, el cumplimiento de la normativa)
- el objeto del proceso de gestión de riesgos para la seguridad de la información (por ejemplo, la organización, la unidad de negocio, el proceso de información, su implementación técnica, la aplicación, la conexión a Internet)

Los ciclos de gestión de riesgos relacionados con el alcance de la evaluación y el tratamiento de los riesgos se presentan en el apartado 5.2.

ANEXO A:

(Informativo)

Ejemplos de técnicas de apoyo al proceso de evaluación de riesgos

A.1. Criterios de riesgo para la seguridad de la información

A.1.1 Criterios relacionados con la evaluación de riesgos

A.1.1.1 Consideraciones generales sobre la evaluación de riesgos

En general, la incertidumbre personal domina la evaluación del riesgo de la información, y los distintos analistas muestran diferentes tendencias a la incertidumbre cuando interpretan los puntos de las escalas de probabilidad y consecuencia. Las escalas de referencia deben relacionar las categorías de consecuencia, probabilidad y riesgo con valores objetivos comunes especificados sin ambigüedad, posiblemente expresados en términos como pérdida financiera en unidades monetarias y frecuencia teórica de ocurrencia en un periodo finito que son específicos para el enfoque cuantitativo.

En particular, cuando se adopta el enfoque cualitativo, los analistas de riesgos deben recibir formación y practicar periódicamente con una escala de referencia de anclaje para mantener la calibración de su juicio.

A.1.1.2 Enfoque cualitativo

A.1.1.2.1 Escala de consecuencias

El cuadro A.1 presenta un ejemplo de escala de consecuencias.

Tabla A1.- Ejemplo de escala de consecuencias

Consecuencias	Descripción
5- Catastrófico	**Consecuencias sectoriales o normativas más allá de la organización** Ecosistema(s) sectorial(es) sustancialmente afectado(s), con consecuencias que pueden ser duraderas. Y/o: dificultad para el Estado, e incluso incapacidad, de asegurar una función reguladora o una de sus misiones de vital importancia. Y/o: consecuencias críticas sobre la seguridad de las personas y los bienes (crisis sanitaria, contaminación ambiental importante, destrucción de infraestructuras esenciales, etc.).
4- Critico	**Consecuencias desastrosas para la organización** Incapacidad de la organización para garantizar toda o parte de su actividad, con posibles consecuencias graves para la seguridad de las personas y los bienes. Lo más probable es que la organización no supere la situación (su

	supervivencia está amenazada), los sectores de actividad o los sectores estatales en los que opera se verán probablemente afectados de forma leve, sin consecuencias duraderas.
3-Serio	**Consecuencias sustanciales para la organización** Alta degradación en el desempeño de la actividad, con posibles consecuencias significativas en la seguridad de las personas y los bienes. La organización superará la situación con serias dificultades (funcionamiento en modo altamente degradado), sin impacto sectorial o estatal.
2-Significante	**Consecuencias significativas pero limitadas para la organización** Degradación del rendimiento de la actividad sin consecuencias para la seguridad de las personas y los bienes. La organización superará la situación a pesar de algunas dificultades (funcionamiento en modo degradado).
1-Menor	**Consecuencias insignificantes para la organización** No hay consecuencias sobre las operaciones o el desempeño de la actividad ni sobre la seguridad de las personas y los bienes. La organización superará la situación sin demasiada dificultad (se consumirán los márgenes).

A.1.1.2.2 Escala de probabilidad

La Tabla A.2 y la Tabla A.4 presentan ejemplos de formas alternativas de representar las escalas de probabilidad. La probabilidad puede expresarse en términos probabilísticos, como en el cuadro A.2, o en términos frecuentistas, como en el cuadro A.4. La representación probabilística indica la probabilidad media de que se produzca un evento de riesgo en un periodo determinado, mientras que la representación frecuentista indica el número de veces que se espera que se produzca de media el evento de riesgo en un periodo de tiempo determinado. Como los dos enfoques se limitan a expresar lo mismo desde dos perspectivas diferentes, se puede utilizar cualquiera de las dos representaciones, según la que la organización considere más conveniente para una determinada categoría de riesgos.

Sin embargo, si ambos enfoques se utilizan como alternativas dentro de la misma organización, es importante que cada rango teóricamente equivalente en ambas escalas represente la misma probabilidad real. De lo contrario, los resultados de la evaluación dependerán de la escala que se utilice, y no de la probabilidad real de la fuente de riesgo que se esté evaluando. Si se utilizan ambos enfoques, el nivel probabilístico de cada rango nocional debe calcularse matemáticamente a partir del valor frecuentista del rango equivalente o viceversa, según el enfoque que se utilice para definir la escala primaria.

Si se utiliza uno de los dos enfoques por separado, no es necesario que los incrementos de la escala estén tan definidos, ya que la priorización de las probabilidades puede seguir realizándose independientemente de los valores absolutos utilizados. Aunque la Tabla A.2 y la Tabla A.4 utilizan incrementos y rangos de probabilidad completamente diferentes, dependiendo del contexto de la organización y de la categoría de riesgo que se esté evaluando, cualquiera de ellas puede ser igualmente eficaz para el análisis si se utilizan exclusivamente. Sin embargo, no podrían utilizarse con seguridad como alternativas en el mismo contexto, ya que los valores asignados a las clasificaciones equivalentes no se correlacionan.

Las categorías y valores utilizados en la Tabla A.2 y la Tabla A.4 son sólo ejemplos. El valor más

apropiado para asignar a cada nivel de probabilidad depende del perfil de riesgo y de la predisposición al riesgo de la organización.

Tabla A2.- Ejemplo de escala de probabilidades

Probabilidad	Descripción
5- Casi seguro	La fuente de riesgo alcanzará con toda seguridad su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy alta.
4 - Muy probable	La fuente de riesgo probablemente alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es alta.
3 - Probable	La fuente de riesgo es capaz de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es significativa.
2 - Bastante improbable	La fuente de riesgo tiene relativamente pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es baja.
1 - Improbable	La fuente de riesgo tiene muy pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy baja.

Las etiquetas verbales como "bajo", "medio" y "alto" pueden adjuntarse a las clasificaciones cuando se utiliza cualquiera de los dos enfoques de la evaluación de la probabilidad. Estas etiquetas pueden ser útiles cuando se discuten los niveles de probabilidad con interesados que no son especialistas en riesgos.

Sin embargo, son subjetivos y, por tanto, inevitablemente ambiguos. En consecuencia, no deben utilizarse como descriptores principales al realizar o informar sobre las evaluaciones.

A.1.1.2.3 Nivel de riesgo

La utilidad de las escalas cualitativas y la coherencia de las evaluaciones de riesgo que se derivan de ellas dependen totalmente de la coherencia con la que las etiquetas de las categorías sean interpretadas por todas las partes interesadas. Los niveles de cualquier escala cualitativa deben ser inequívocos, sus incrementos deben estar claramente definidos, las descripciones cualitativas de cada nivel deben expresarse en un lenguaje objetivo y las categorías no deben solaparse entre sí.

Por lo tanto, cuando se utilicen descriptores verbales de probabilidad, consecuencia o riesgo, éstos deben estar formalmente referenciados a escalas inequívocas ancladas a puntos de referencia numéricos (como en la Tabla A.4) o ratiométricos (como en la Tabla A.2). Todas las partes interesadas deben conocer las escalas de referencia para garantizar que la interpretación de los datos y resultados de la evaluación cualitativa sea coherente.

El cuadro A.3 presenta un ejemplo de enfoque cualitativo.

Tabla A3.- Ejemplo de enfoque cualitativo de los criterios de riesgo

Probabilidad	Consecuencia				
	Catastrófico	**Critico**	**Serio**	**Significante**	**Menor**
Casi seguro	Muy alto	Muy alto	Alto	Alto	Alto
Muy probable	Muy alto	Alto	Alto	Medio	Bajo
Probable	Alto	Alto	Medio	Bajo	Bajo
Bastante improbable	Medio	Medio	Bajo	Bajo	Muy bajo
Improbable	Bajo	Bajo	Bajo	Muy bajo	Muy bajo

El diseño de una matriz de riesgo cualitativo debe guiarse por los criterios de aceptación de riesgos de la organización (véase 6.4.2 y A.1.2).

EJEMPLO Una organización a veces se preocupa más por las consecuencias extremas a pesar de su improbable ocurrencia, o se preocupa principalmente por eventos de alta frecuencia con consecuencias menores.

Cuando se diseña una matriz de riesgos, ya sea cualitativa o cuantitativa, el perfil de riesgo de una organización suele ser asimétrico. Los sucesos triviales suelen ser los más frecuentes y la frecuencia esperada suele reducirse a medida que aumentan las consecuencias, culminando en probabilidades muy bajas de consecuencias extremas. Tampoco es común que la exposición empresarial representada por un evento de alta probabilidad/baja consecuencia sea equivalente a la representada por un evento de baja probabilidad/alta consecuencia. Aunque una matriz de riesgo que es simétrica respecto a su diagonal baja/baja a alta/alta puede parecer fácil de crear e ingenuamente aceptable, es poco probable que represente con exactitud el perfil de riesgo real de cualquier organización y, por lo tanto, puede producir resultados no válidos. Para garantizar que una matriz de riesgo es realista y puede cumplir el requisito de mejora continua (véase ISO/IEC 27001:2022, 10.2), el razonamiento tanto para asignar cada categoría a las escalas de probabilidad y consecuencia como a la matriz de riesgo, y en relación con la forma en que las categorías se ajustan al perfil de riesgo de la organización, debe documentarse cuando se definen o modifican las escalas y la matriz. Como mínimo, las incertidumbres intrínsecas al uso de matrices de escalas incrementales deben describirse con las debidas precauciones para sus usuarios.

La utilidad de las escalas cualitativas y la coherencia de las evaluaciones de riesgo que se derivan de ellas dependen por completo de la coherencia con la que las etiquetas de las categorías sean interpretadas por todas las partes interesadas. Los niveles de cualquier escala cualitativa deben ser inequívocos, sus incrementos deben estar claramente definidos, las descripciones cualitativas de cada nivel deben expresarse en un lenguaje objetivo y las categorías no deben solaparse entre sí.

A.1.1.3. Enfoque Cuantitativo

A.1.1.3.1. Escalas Finitas

El nivel de riesgo puede calcularse utilizando cualquier método y teniendo en cuenta cualquier factor relevante, pero normalmente se muestra multiplicando la probabilidad por la consecuencia.

La probabilidad representa la posibilidad o frecuencia de que se produzca un suceso en un plazo determinado. Este marco temporal suele ser anual (por año), pero puede ser tan grande (por ejemplo, por siglo) o pequeño (por ejemplo, por segundo) como quiera la organización.

Las escalas de probabilidad deben definirse en términos prácticos que reflejen el contexto de la organización, de modo que la ayuden a gestionar el riesgo y sean fáciles de entender para todas las partes interesadas. Esto significa, sobre todo, establecer límites realistas a la gama de probabilidades representadas. Si los límites máximo y mínimo de la escala están demasiado alejados, cada categoría dentro de ella incluye un rango de probabilidades excesivamente amplio, lo que hace que la evaluación sea incierta.

EJEMPLO 1 El punto finito más alto de la escala puede definirse útilmente en términos del tiempo que suele tardar la organización en responder a los acontecimientos, y el punto finito más bajo en términos de la duración de la planificación estratégica a largo plazo de la organización.

Las probabilidades por encima y por debajo de los límites definidos de la escala pueden expresarse útilmente como "mayor que el máximo de la escala" y "menor que el mínimo de la escala", indicando así claramente que las probabilidades más allá de los límites de la escala definida son casos extremos que deben considerarse excepcionalmente (posiblemente utilizando criterios especiales de "fuera de los límites"). Fuera de estos límites, la probabilidad concreta es menos importante que el hecho de que sea una excepción en la dirección dada.

Por lo general, es útil medir las consecuencias mediante una cifra económica, ya que esto permite la agregación para informar del riesgo.

EJEMPLO 2 Las escalas de consecuencias monetarias suelen basarse en factores de 10 (100 a 1 000; 1 000 a 10 000, etc.).

La amplitud de las categorías de una escala de probabilidad debe seleccionarse con referencia a las de la escala de consecuencias elegida para evitar un rango excesivo de riesgo en cada categoría.

EJEMPLO 3 Si la probabilidad y la consecuencia están representadas por los índices de una escala exponencial (es decir, los logaritmos de los valores de la escala), éstos deben sumarse.

El valor del riesgo puede entonces calcularse como sigue: antilog [log (valor de la probabilidad) + log (valor de la consecuencia)].

Tabla A4.- Ejemplo de escala de probabilidad logarítmica

Frecuencia media aproximada	Expresión logarítmica	Escala de valor
Cada hora	(aproximadamente 10^5)	5
Cada 8 horas	(aproximadamente 10^4)	4
Dos veces por semana	(aproximadamente 10^3)	3
Una vez por mes	(aproximadamente 10^2)	2
Una vez por año	(10^1)	1
Una vez en una década	(10^0)	0

EJEMPLO 4 En la Tabla A.4, un ejemplo de evento de alta frecuencia es un ataque con contraseña asistido por ordenador o un ataque distribuido de denegación de servicio de una red de bots. De hecho, la frecuencia de los ataques puede ser mucho mayor.

EJEMPLO 5 En la Tabla A.4, un ejemplo de evento de baja frecuencia son las erupciones volcánicas. Aunque se prevea que un evento sólo ocurra una vez por siglo, eso no significa que no vaya a ocurrir durante la vida de un SGSI.

La tabla A.5 muestra un ejemplo de escala de consecuencias logarítmicas. Uno de los propósitos de considerar la frecuencia es garantizar que las medidas de protección sean lo suficientemente fuertes como para soportar secuencias de ataques de alta frecuencia, incluso cuando la probabilidad de dicha secuencia de ataques es baja.

Tabla A5.- Ejemplo de escala de consecuencia logarítmica

Consecuencia (una pérdida de)	Expresión logarítmica	Escala de valor
£1 000 000	(aproximadamente 10^6)	6
£1 000 00	(aproximadamente 10^5)	5
£1 000 0	(aproximadamente 10^4)	4
£1 000	(aproximadamente 10^3)	3
£1 00	(10^2)	2
Menor que £1 00	(10^1)	1

Si tanto las escalas de probabilidad como las de consecuencias utilizan una base logarítmica 10 para asignar el nivel, los analistas de riesgos pueden acabar con demasiados riesgos en el mismo nivel de riesgo y ser incapaces de tomar una decisión adecuada de priorización o de inversión en seguridad. En ese caso, puede ser útil reducir la base y aumentar el número de niveles considerados. Hay que tener en cuenta que, si se eligen bases diferentes para la probabilidad y las consecuencias, no se puede aplicar una fórmula útil para sumar dos factores.

EJEMPLO 6 Si la probabilidad se duplica al pasar de un nivel al siguiente, mientras que la consecuencia es un factor de 10 más cara, la fórmula dará como resultado los riesgos a) y b), en los que el riesgo b) tiene un nivel de consecuencia 10 veces más caro que el riesgo a), pero sólo la mitad de la probabilidad del riesgo a) que termina en el mismo nivel de riesgo. Esto es económicamente incorrecto.

Las tablas A.4 y A.5 enumeran rangos de probabilidad y consecuencia que cubren la mayoría de las eventualidades en organizaciones muy diferentes. No es probable que una sola organización

se encuentre con la gama de riesgos representada por la totalidad de estas escalas de ejemplo. El contexto de la organización y el alcance del SGSI deben utilizarse para definir límites superiores e inferiores realistas tanto para las probabilidades como para las consecuencias, teniendo en cuenta que la cuantificación de rangos de riesgo superiores a 1 000 a 1 probablemente tenga un valor práctico limitado.

A.1.2 Criterios de aceptación del riesgo

El criterio de aceptación del riesgo puede ser simplemente un valor por encima del cual los riesgos se consideran inaceptables.

EJEMPLO 1 En la tabla A.3, si se elige el valor medio, todos los riesgos con un valor muy bajo, bajo o medio serían considerados aceptables por la organización y todos los riesgos con un valor alto o muy alto serían considerados inaceptables.

Utilizando una matriz de riesgo codificada por colores que refleje las escalas de consecuencia y probabilidad, las organizaciones pueden presentar gráficamente la distribución de riesgos de una o varias evaluaciones de riesgo. Una matriz de riesgo de este tipo también puede utilizarse para señalar la actitud de la organización ante los valores de riesgo e indicar si un riesgo normalmente debe ser aceptado o tratado.

EJEMPLO 2 Una matriz de riesgo que utiliza tres colores, por ejemplo, rojo, ámbar y verde, puede aplicarse para representar tres grados de valoración del riesgo, como se presenta en el cuadro A.6.

Puede ser beneficioso elegir otros modelos que utilicen colores para una matriz de riesgo.

EJEMPLO 3 Si se utiliza una matriz de riesgos para comparar los resultados de una evaluación de riesgos realizada originalmente con los resultados de una reevaluación para los mismos riesgos, la reducción del riesgo puede presentarse más fácilmente si se aplican más colores para presentar los niveles de riesgo.

También es posible añadir a dicho modelo la determinación de qué nivel de gestión está autorizado a aceptar un riesgo con un determinado valor de riesgo.

El cuadro A.6 presenta un ejemplo de escala de valoración.

Tabla A6.- Ejemplo de escala de evaluación combinada con una matriz de riesgo de tres colores

Nivel de Riesgo	Valoración de riesgos	Descripción
Bajo (verde)	Aceptable tal cual	El riesgo puede aceptarse sin más.
Moderado (ámbar)	Tolerable bajo control	Se debe realizar un seguimiento en términos de gestión de riesgos y establecer acciones en el marco de la mejora continua a medio y largo plazo.

Alto (rojo)	Inaceptable	Es absolutamente necesario tomar medidas para reducir el riesgo a corto plazo. En caso contrario, deberá rechazarse toda o parte de la actividad.

A.2 Técnicas prácticas

A.2.1 Componentes del riesgo para la seguridad de la información

A la hora de identificar y evaluar los riesgos de seguridad de la información, deben tenerse en cuenta los siguientes componentes:

- Componentes relacionados con el pasado
- Eventos e incidentes de seguridad (tanto dentro como fuera de la organización);
- Fuentes de riesgo;
- Vulnerabilidades explotadas;
- Consecuencias medibles;
- Componentes relacionados con el futuro:
- Amenazas;
- Vulnerabilidades;
- Consecuencias;
- Escenarios de riesgo.

Las relaciones entre los componentes de riesgo de la seguridad de la información se presentan en la figura A.1 y se analizan en los apartados A.2.2 a A.2.7.

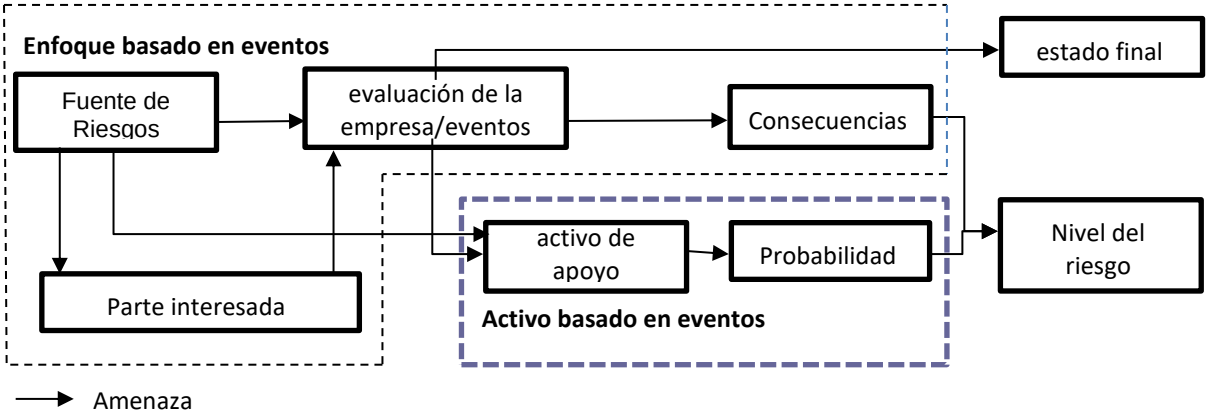

Figura A.1 - Componentes de la evaluación de riesgos para la seguridad de la información

Los detalles sobre el "estado final deseado" se encuentran en A.2.3 b).

A.2.2 Activos

Al aplicar el enfoque basado en los activos a la identificación de los riesgos, deben identificarse los activos.

En el proceso de evaluación de riesgos, dentro del desarrollo de escenarios de riesgo, la identificación de eventos, consecuencias, amenazas, vulnerabilidades, debe estar vinculada a los activos.

En el proceso de tratamiento del riesgo, cada control es aplicable a un subconjunto de los activos. Los activos pueden dividirse en dos categorías

- activos primarios/de negocio - información o procesos de valor para una organización;
- activos de apoyo: componentes del sistema de información en los que se basan uno o varios activos empresariales.

Los activos primarios/de negocio suelen utilizarse en el enfoque basado en eventos (identificación de eventos y sus consecuencias en los activos de negocio).

Los activos de apoyo suelen utilizarse en el enfoque basado en activos (identificación y análisis de las vulnerabilidades y amenazas sobre estos activos) y en el proceso de tratamiento de riesgos (especificación del activo o activos a los que debe aplicarse cada control).

Los activos de negocio y de apoyo están relacionados, por lo que las fuentes de riesgo identificadas para los activos de apoyo pueden afectar a los activos de negocio.

Por esta razón, es importante identificar las relaciones entre los activos y comprender su valor para la organización. Una mala apreciación del valor de los activos puede conducir a una mala apreciación de las consecuencias relacionadas con el riesgo, pero también puede afectar a la comprensión de la probabilidad de las amenazas consideradas.

EJEMPLO 1 Un activo de apoyo alberga un activo empresarial (información en este caso).

Los datos están protegidos por controles internos y externos para evitar que una fuente de riesgo logre su objetivo relacionado con el activo empresarial explotando una vulnerabilidad en el activo de apoyo. Al distinguir los diferentes tipos de activos, se deben documentar las dependencias entre activos y evaluar la propagación del riesgo, de modo que se pueda documentar que el mismo riesgo no se evalúa dos veces, una cuando se produce en el activo de apoyo y otra cuando afecta a los activos primarios. Los gráficos de dependencia de los activos son herramientas útiles para representar dichas dependencias y garantizar que se han tenido en cuenta todas ellas.

EJEMPLO 2 El gráfico de la figura A.2 indica los activos dependientes para el activo de negocio "mostrar el procesamiento de pedidos y facturas" y puede leerse como sigue

- "Administrador" (tipo: recurso humano), que, si no recibe la formación adecuada, propaga un riesgo para el activo.
- "Mantenimiento de TI" (tipo: servicio), que propaga el riesgo al activo.
- "Servidor" (tipo: hardware) o al activo "Red" (tipo conectividad de red). El servidor, si deja de funcionar o la red mal configurada provoca el activo.
- "Portal web" (tipo: aplicación), que deje de funcionar o no esté disponible.

Sin el "portal web", el proceso de negocio "mostrar el procesamiento de pedidos y facturas" no ofrece el proceso previsto a los clientes.

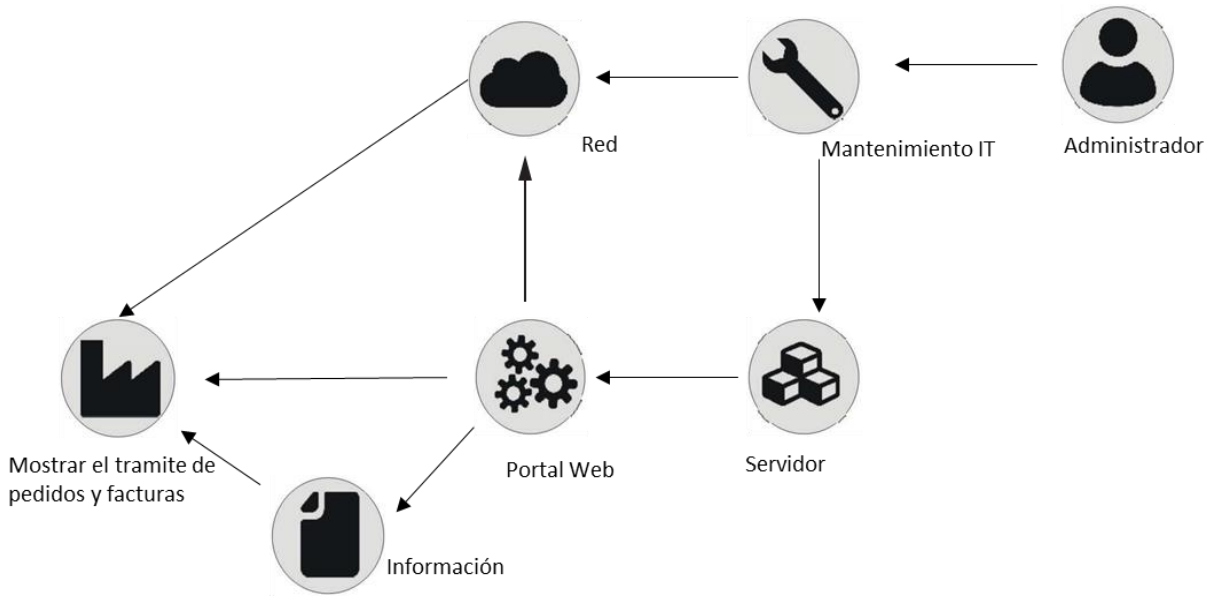

Figura A.2 - Ejemplo de gráfico de dependencia de activos

A.2.3 Fuentes de riesgo y estado final deseado

Este apartado propone caracterizar este tipo de fuentes de riesgo. Dos criterios principales estructuran este enfoque descriptivo

- la motivación;
- la capacidad de actuación.

a) Identificación de las fuentes de riesgo

El cuadro A.7 presenta ejemplos y métodos habituales de ataque.

Cuadro A.7 - Ejemplos y métodos habituales de ataque

Fuente de Riesgo	Ejemplos y métodos habituales de ataque
Relacionados con el Estado	Estados, agencias de inteligencia Método: Ataques generalmente realizados por profesionales, que trabajan con un calendario y un método de ataque predefinidos. Este perfil de atacante se caracteriza por su capacidad de llevar a cabo una operación ofensiva durante un largo periodo de tiempo (recursos estables, procedimientos) y de adaptar sus herramientas y métodos a la topología del objetivo. Por extensión, estos actores disponen de medios para comprar o descubrir vulnerabilidades del Día 0 y algunos son capaces de infiltrarse en redes aisladas y de realizar ataques sucesivos para alcanzar un objetivo o varios (por ejemplo, mediante un ataque dirigido a la cadena de suministro).
Crimen Organizado	Organizaciones cibercriminales (mafias, bandas, grupos criminales) Método: Estafas en línea o en persona, petición de rescate o ataque mediante ransomware, uso de redes de bots, etc. Debido sobre todo a la proliferación de kits de ataque fácilmente disponibles en línea, los ciberdelincuentes realizan operaciones cada vez más sofisticadas y organizadas con fines lucrativos o fraudulentos. Algunos disponen de medios para comprar o descubrir vulnerabilidades de Día 0.
Terrorismo	Ciberterroristas, cibermilicias Método: Ataques que no suelen ser muy sofisticados pero que se llevan a cabo con fines de desestabilización y destrucción: denegación de servicio (destinada, por ejemplo, a dejar fuera de servicio los servicios de urgencia de un centro hospitalario, paradas intempestivas de un sistema industrial de producción de energía), explotación de vulnerabilidades de sitios de Internet
Activismo ideológico	Ciberactivistas, grupos de interés, sectas Método: Los métodos de ataque y la sofisticación de los ataques son relativamente similares a los de los ciberterroristas, pero están motivados por intenciones menos destructivas. Algunos actores realizan estos ataques para transmitir una ideología, un mensaje (por ejemplo, el uso masivo de las redes sociales como caja de resonancia).
Especializado	Perfil de "cibermercenario" con capacidades informáticas generalmente elevadas desde el punto de vista técnico. Por ello, debe distinguirse de los script-kiddies con los que comparte sin embargo el espíritu de desafío y búsqueda de reconocimiento pero con un objetivo lucrativo. Estos grupos pueden organizarse como conjuntos especializados que proponen verdaderos servicios de hacking. Método: Este tipo de hacker experimentado suele estar en el origen del diseño y la creación de kits de ataque y herramientas que están disponibles en línea (posiblemente a cambio de una tarifa) y que luego pueden ser utilizados "llave en mano" por otros grupos de atacantes. No

	hay motivaciones particulares más allá del beneficio económico.
Aficionado	Perfil del hacker script-kiddies o con buenos conocimientos de informática; motivado por la búsqueda del reconocimiento social, la diversión, el desafío. Método: Ataques básicos, pero con la capacidad de utilizar los kits de ataque que están disponibles en línea.
Vengador	Las motivaciones de este perfil de agresor están guiadas por un espíritu de venganza aguda o un sentimiento de injusticia (por ejemplo, empleado despedido por una falta grave, proveedor de servicios descontento tras un contrato no renovado, etc.). Método: Este perfil de atacante se caracteriza por su determinación y su conocimiento interno de los sistemas y procesos organizativos. Esto puede hacerlo formidable y proporcionarle un poder sustancial para hacer daño.
Ataque patológico	Las motivaciones de este perfil de atacante son de naturaleza patológica u oportunista y a veces están guiadas por el motivo de una ganancia (por ejemplo, competidor desleal, cliente deshonesto, estafador y defraudador). Método: En este caso, los atacantes tienen una base de conocimientos en informática que los lleva a intentar comprometer la SI de su objetivo, o bien utilizan los kits de ataque disponibles en línea, o deciden subcontratar el ataque informático recurriendo a un equipo especializado. En algunos casos, los atacantes pueden dirigir su atención a una fuente interna (empleado descontento, proveedor de servicios sin escrúpulos) e intentar corromper a este último.

b) Modelización de la motivación de una fuente de riesgo - estado final deseado

Existe una amplia gama de motivaciones; pueden ser políticas, financieras, ideológicas, pero también sociales o incluso representar una condición psicológica puntual o patológica.

Aunque no es posible expresar directamente una motivación, ésta puede ilustrarse a través de la intención de la fuente de riesgo y expresarse en forma de estado final deseado (EFD): la situación general a la que la fuente de riesgo quiere llegar después de la confrontación. Una clasificación sistemática de las situaciones, asociada a categorías generales de acción, puede guiar el análisis contextualizado.

El cuadro A.8 presenta un ejemplo de clasificación de las motivaciones para expresar el EFD.

Cuadro A.8 - Ejemplo de clasificación de las motivaciones para expresar el EFD

Conquista	Captura a largo plazo de recursos o mercados económicos, obtención de poder político o imposición de valores
Adquirir	Enfoque depredador, decididamente ofensivo, impulsado por la captación de recursos o beneficios
Prevenir	Enfoque ofensivo para limitar las acciones de un tercero
Mantener	Esfuerzos para mantener una situación ideológica, política, económica o social
Defienda	Adoptar una postura de repliegue estrictamente defensiva, o una actitud

	explícitamente amenazante (por ejemplo, la intimidación) para evitar el comportamiento agresivo de un adversario claramente designado o impedir su acción frenándola, etc.
Sobrevivir	Proteger una entidad a toda costa, lo que puede llevar a acciones extremadamente agresivas

c) Objetivos

Para alcanzar el EFD, la fuente de riesgo se centra en uno o varios objetivos que afectan a los activos empresariales del sistema objetivo. Estos son los objetivos de la fuente de riesgo.

El cuadro A.9 presenta ejemplos de objetivos meta.

Cuadro A.9 - Ejemplos de objetivos

Objetivo de la meta	Descripción
Espionaje	Operación de inteligencia (relacionada con el Estado, económica). En muchos casos, el atacante pretende instalarse a largo plazo en el sistema de información y con total discreción. El armamento, el espacio, la aeronáutica, el sector farmacéutico, la energía y ciertas actividades del Estado (economía, finanzas y asuntos exteriores) son objetivos privilegiados.
Pre-proposicionamiento estratégica	Pre-posicionamiento generalmente dirigido a un ataque a largo plazo, sin que el propósito final esté claramente establecido (por ejemplo, comprometer las redes de los operadores de telecomunicaciones, infiltración de sitios de Internet de información masiva con el fin de lanzar una operación de influencia política o económica con un fuerte eco). El compromiso repentino y masivo de ordenadores con el fin de formar una red de bots puede pertenecer a esta categoría.
Influencia	Operación destinada a difundir información falsa o a alterarla, a movilizar a los líderes de opinión en las redes sociales, a destruir reputaciones, a revelar información confidencial, a degradar la imagen de una organización o de un Estado. El objetivo final es generalmente desestabilizar o modificar las percepciones.
Obstáculo para el funcionamiento	Operación de sabotaje destinada, por ejemplo, a hacer que un sitio de Internet no esté disponible, a provocar la saturación de la información, a impedir el uso de un recurso digital, a hacer que una instalación física no esté disponible. Los sistemas industriales pueden estar especialmente expuestos y ser vulnerables a través de las redes informáticas con las que están interconectados (por ejemplo, enviando comandos para generar daños en el hardware o una avería que requiera un mantenimiento exhaustivo). Los ataques de denegación de servicio distribuidos (DDoS) son técnicas comúnmente utilizadas para neutralizar los recursos digitales.
Lucrativo	Operación que tiene como objetivo un beneficio económico, ya sea directo o indirecto. Generalmente vinculadas a la delincuencia organizada, se pueden mencionar: el fraude en Internet, el blanqueo de dinero, la extorsión o la malversación, la manipulación de los mercados financieros, la falsificación de documentos administrativos, el robo de identidad, etc. Algunas operaciones con fines lucrativos

	pueden utilizar un método de ataque que forma parte de las categorías anteriores (por ejemplo, espionaje y robo de datos, ransomware para neutralizar una actividad), pero el objetivo final sigue siendo financiero.
Desafío, diversión	Operación destinada a realizar una hazaña con fines de reconocimiento social, desafío o simplemente por diversión. Aunque el objetivo es principalmente de diversión y sin ningún deseo particular de hacer daño, este tipo de operación puede tener graves consecuencias para la víctima.

La diferencia entre un EDS y un objetivo estratégico puede ilustrarse con el ejemplo de una fuente de riesgo cuyo objetivo es ganar un trato (EFD) que busca robar información confidencial sobre las negociaciones a su competidor (objetivo estratégico). A veces, el objetivo en cuestión (la información deseada) no se traduce finalmente en el EFD.

Se puede considerar que el valor del objetivo desde el punto de vista de la fuente de riesgo se basa en su contribución al EFD.

En términos muy generales, los objetivos del objetivo de la fuente de riesgo se dividen en dos grandes clases

- Explotar los recursos del objetivo en su propio beneficio, por ejemplo, espiar, robar, estafar, fraudar, traficar;
- Impedir que el objetivo utilice sus recursos (la confrontación es siempre relativa), por ejemplo, guerra, terrorismo, sabotaje, subversión, desestabilización.

A.2.4 Enfoque basado en eventos

A.2.4.1 Ecosistema

En un enfoque basado en eventos, los escenarios deben construirse analizando las diferentes vías, relevantes para las interacciones entre la organización y las partes interesadas, que forman un ecosistema que las fuentes de riesgo pueden utilizar para alcanzar los activos de la empresa y sus EFD.

Un número creciente de métodos de ataque utilizan los eslabones más vulnerables de dicho ecosistema para alcanzar sus objetivos.

Las partes interesadas en el ámbito del SGSI que deben tenerse en cuenta al analizar los escenarios de riesgo pueden ser de dos tipos

- partes externas, que incluyen:
  - Clientes;
  - Socios, co-contratistas;

- Proveedores de servicios (subcontratistas, proveedores).

- partes internas, que incluyen:

  - Proveedores de servicios relacionados con la técnica (por ejemplo, servicios de apoyo propuestos por la dirección de TI);

  - Proveedores de servicios relacionados con el negocio (por ejemplo, la entidad comercial que utiliza los datos del negocio);

  - Filiales (en particular, situadas en otros países).

El objetivo de la identificación de las partes interesadas es obtener una visión clara del ecosistema, con el fin de identificar las más vulnerables. El conocimiento del ecosistema debe abordarse como un estudio de riesgo preliminar. La figura A.3 muestra la identificación de las partes interesadas del ecosistema.

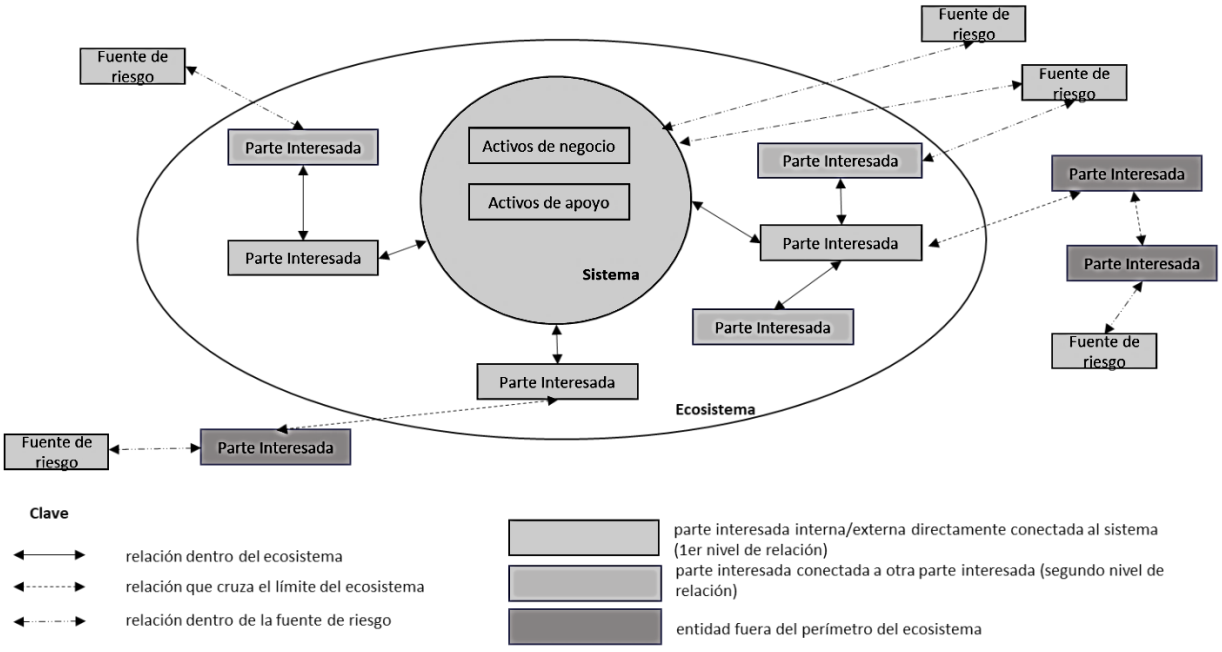

Figura A.3 - Identificación de las partes interesadas del ecosistema

A.2.4.2 Escenarios estratégicos

A partir de la información sobre las fuentes de riesgo y los acontecimientos en cuestión, pueden imaginarse escenarios realistas de alto nivel (escenarios estratégicos) que indiquen de qué manera puede proceder una fuente de riesgo para alcanzar su EFD. Puede, por ejemplo, atravesar el ecosistema o desviar algunos procesos empresariales. Estos escenarios se identifican por deducción, a partir de las fuentes de riesgo y sus EDS: para cada uno de ellos, se pueden plantear las siguientes preguntas, desde el punto de vista de la fuente de riesgo:

- ¿Cuáles son los activos empresariales de la organización a los que las fuentes de riesgo deben apuntar para alcanzar su EFD?

- Para hacer posible su ataque o facilitarlo, ¿es probable que ataquen a los interesados críticos del ecosistema que tienen acceso privilegiado a los activos empresariales?

Una vez identificados los elementos más expuestos, se puede dibujar el escenario estratégico, describiendo la secuencia de los eventos generados por la fuente de riesgo para alcanzar su EFD. La violación de los activos de la empresa corresponde a los eventos finales, mientras que los eventos relativos al ecosistema son eventos intermedios. El escenario estratégico refleja una evaluación de las consecuencias directamente heredadas de los eventos en cuestión.

Estos escenarios pueden representarse en forma de gráficos de ataque o directamente en la vista del ecosistema de la cartografía del sistema de información mediante la superposición de la(s) vía(s) de ataque.

Los escenarios estratégicos requieren una consideración adicional de la probabilidad de los eventos. El enfoque basado en los activos y los escenarios operativos asociados pueden utilizarse para definir la probabilidad de los eventos. Los ejemplos de amenazas presentados en A.2.5.1 pueden utilizarse para obtener las evaluaciones necesarias.

A.2.5 Enfoque basado en los activos

A.2.5.1 Ejemplos de amenazas

La tabla A.10 ofrece ejemplos de amenazas típicas. La lista puede utilizarse durante el proceso de evaluación de amenazas. Las amenazas consideradas como fuentes de riesgo pueden ser deliberadas, accidentales o ambientales (naturales) y pueden provocar, por ejemplo, daños o la pérdida de servicios esenciales. La lista indica, para cada tipo de amenaza, si es pertinente la D (deliberada), la A (accidental) o la E (ambiental). La D se utiliza para todas las acciones deliberadas dirigidas a la información y a los activos relacionados con la información, la A se utiliza para todas las acciones humanas que pueden dañar accidentalmente la información y los activos relacionados con la información, y la E se utiliza para todos los incidentes que no se basan en acciones humanas. Los grupos de amenazas no están en orden de prioridad.

Los controles pueden mitigar las amenazas disuadiendo o impidiendo que esas amenazas actúen o se produzcan. La selección de los controles para reducir el riesgo también requiere la consideración de los controles de detección y respuesta que identifican, responden, contienen y se recuperan de los eventos. Los controles de detección y respuesta están asociados a las consecuencias más que a las amenazas.

EJEMPLO El registro y la supervisión permiten identificar y responder a los eventos de seguridad.

Cuadro A.10 - Ejemplos de amenazas típicas

Categoría	No.	Descripción de Amenaza	Tipo de fuente de riesgo [a]
Amenazas Físicas	AF01	Fuego	A,D,E
	AF02	Agua	A,D,E
	AF03	Contaminación, radiación nociva	A,D,E
	AF04	Accidente grave	A,D,E
	AF05	Explosión	A,D,E
	TP06	Polvo, corrosión, congelación	A,D,E
Amenazas Naturales	AN01	Fenómeno climático	E
	AN02	Fenómeno sísmico	E
	AN03	Fenómeno volcánico	E
	AN04	Fenómeno meteorológico	E
	AN05	Inundación	E
	AN06	Fenómeno pandémico/epidémico	E
Fallos en las infraestructuras	AI01	Fallo de un sistema de suministro	A,D
	AI02	Fallo del sistema de refrigeración o ventilación	A,D
	AI03	Pérdida de suministro eléctrico	A,D,E
	AI04	Fallo de una red de telecomunicaciones	A,D,E
	AI05	Fallo del equipo de telecomunicaciones	A,D
	AI06	Radiación electromagnética	A,D,E
	AI07	Radiación térmica	A,D,E
	AI08	Pulsos electromagnéticos	A,D,E
Fallos técnicos	AT01	Fallo del dispositivo o del sistema	A
	AT02	Saturación del sistema de información	A,D
	AT03	Violación de la mantenibilidad del sistema de información	A,D
Acciones humanas	AH01	Ataque terrorista, sabotaje	D
	AH02	Ingeniería social	D
	AH03	Interceptación de la radiación de un dispositivo	D
	AH04	Espionaje remoto	D
	AH05	Espionaje	D
	AH06	Robo de medios o documentos	D
	AH07	Robo de equipos	D
	AH08	Robo de identidad o credenciales digitales	D
	AH09	Recuperación de soportes reciclados o desechados	D
	AH10	Divulgación de información	A, D
	AH11	Introducción de datos de fuentes no fiables	A, D
	AH12	Manipulación del hardware	D
	AH13	Manipulación del software	A, D
	AH14	Explotación por medio de la comunicación basada en la web	D
	AH15	Ataque de repetición, ataque de hombre en el medio	D
	AH16	Tratamiento no autorizado de datos personales	A, D
	AH17	Entrada no autorizada a las instalaciones	D
	AH18	Uso no autorizado de dispositivos	D
	AH19	Uso incorrecto de los dispositivos	A, D
	AH20	Deterioro de dispositivos o soportes	A, D
	AH21	Copia fraudulenta de software	D
	AH22	Uso de software falsificado o copiado	A, D
	AH23	Corrupción de datos	D

	AH24	Tratamiento ilegal de datos	D
	AH25	Envío o distribución de malware	A, D, E
	AH26	Detección de posiciones	D
Compromiso de funciones o servicios	AC01	Error de uso	A
	AC02	Abuso de derechos o permisos	A, D
	AC03	Falsificación de derechos o permisos	D
	AC04	Denegación de acciones	D
Amenazas para la organización	AO01	Falta de personal	A, E
	AO02	Falta de recursos	A, E
	AO03	Fallo de los proveedores de servicios	A, E
	AO04	Violación de leyes o reglamentos	A, D
[a] D = deliberado; A = accidental; E = ambiental.			

A.2.5.2 Ejemplos de vulnerabilidades

La tabla A.11 da ejemplos de vulnerabilidades en varias áreas de seguridad, incluyendo ejemplos de amenazas que pueden explotar estas vulnerabilidades. Las listas pueden servir de ayuda durante la evaluación de las amenazas y vulnerabilidades, para determinar los escenarios de riesgo relevantes. En algunos casos, otras amenazas pueden explotar también estas vulnerabilidades.

Tabla A.11 - Ejemplos de vulnerabilidades típicas

Categoría	No.	Descripción de Amenaza
Hardware	VH01	Mantenimiento insuficiente/instalación defectuosa de los medios de almacenamiento
	VH02	Insuficientes planes de sustitución periódica de los equipos
	VH03	Susceptibilidad a la humedad, el polvo y la suciedad
	VH04	Sensibilidad a la radiación electromagnética
	VH05	Insuficiente control de los cambios de configuración
	VH06	Susceptibilidad a las variaciones de tensión
	VH07	Susceptibilidad a las variaciones de temperatura
	VH08	Almacenamiento sin protección
	VH09	Falta de cuidado en la eliminación
	VH10	Copia incontrolada
Software	VS01	Ausencia o insuficiencia de pruebas de software
	VS02	Defectos conocidos en el software
	VS03	Ausencia de "cierre de sesión" al abandonar el puesto de trabajo
	VS04	Eliminación o reutilización de los medios de almacenamiento sin un borrado adecuado
	VS05	Configuración insuficiente de los registros con fines de auditoría
	VS06	Asignación incorrecta de los derechos de acceso
	VS07	Software ampliamente distribuido
	VS08	Aplicación de programas de aplicación a los datos erróneos en términos de tiempo
	VS09	Interfaz de usuario complicada
	VS10	Insuficiente o falta de documentación
	VS11	Configuración incorrecta de los parámetros
	VS12	Fechas incorrectas
	VS13	Mecanismos de identificación y autentificación insuficientes (por ejemplo, para la autentificación de los usuarios)
	VS14	Tablas de contraseñas desprotegidas

	VS15	Mala gestión de las contraseñas
	VS16	Servicios innecesarios habilitados
	VS17	Software inmaduro o nuevo
	VS18	Especificaciones poco claras o incompletas para los desarrolladores
	VS19	Control de cambios ineficaz
	VS20	Descarga y uso incontrolado de software
	VS21	Falta de copias de seguridad o copias incompletas
	VS22	Falta de elaboración de informes de gestión
Red	VR01	Mecanismos insuficientes para la prueba de envío o recepción de un mensaje
	VR02	Líneas de comunicación desprotegidas
	VR03	Tráfico sensible desprotegido
	VR04	Cableado conjunto deficiente
	VR05	Punto único de fallo
	VR06	Ineficacia o falta de mecanismos de identificación y autenticación del emisor y el receptor
	VR07	Arquitectura de red insegura
	VR08	Transferencia de contraseñas en claro
	VR09	Gestión inadecuada de la red (resiliencia del enrutamiento)
	VR10	Conexiones de red pública no protegidas
Personal	VP01	Ausencia de personal
	VP02	Procedimientos de contratación inadecuados
	VP03	Formación insuficiente en materia de seguridad
	VP04	Uso incorrecto del software y el hardware
	VP05	Escasa concienciación en materia de seguridad
	VP06	Insuficiencia o falta de mecanismos de supervisión
	VP07	Trabajo no supervisado por personal externo o de limpieza
	VP08	Ineficacia o falta de políticas para el uso correcto de los medios de telecomunicación y mensajería
Sitio	VS01	Uso inadecuado o descuidado del control de acceso físico a edificios y salas
	VS02	Ubicación en una zona susceptible de inundación
	VS03	Red eléctrica inestable
	VS04	Insuficiente protección física del edificio, puertas y ventanas
Organización	VO01	No se ha desarrollado un procedimiento formal para el registro y la cancelación de usuarios, o su aplicación es ineficaz.
	VO02	No se ha desarrollado un proceso formal para la revisión de los derechos de acceso (supervisión), o su aplicación es ineficaz.
	VO03	Disposiciones insuficientes (relativas a la seguridad) en los contratos con clientes y/o terceros
	VO04	No se ha desarrollado un procedimiento de supervisión de las instalaciones de procesamiento de la información, o su aplicación es ineficaz.
	VO05	No se realizan auditorías (supervisión) de forma regular
	VO06	No se han desarrollado procedimientos de identificación y evaluación de riesgos, o su aplicación es ineficaz.
	VO07	Insuficiencia o falta de informes de fallos registrados en los registros de los administradores y operadores
	VO08	Respuesta inadecuada del servicio de mantenimiento
	VO09	Acuerdo de nivel de servicio insuficiente o inexistente
	VO10	No se ha desarrollado un procedimiento de control de cambios, o su aplicación es ineficaz
	VO11	No se ha desarrollado un procedimiento formal para el control de la documentación del SGSI, o su aplicación es ineficaz.
	VO12	No se ha desarrollado un procedimiento formal para la supervisión de los registros del SGSI, o su aplicación es ineficaz.
	VO13	No se ha desarrollado un proceso formal para la autorización de la información

		disponible al público, o su implementación es ineficaz.
	VO14	Asignación inadecuada de las responsabilidades de seguridad de la información
	VO15	No existen planes de continuidad, o son incompletos, o están obsoletos
	VO16	No se ha desarrollado una política de uso del correo electrónico, o su aplicación es ineficaz.
	VO17	No se han elaborado procedimientos para la introducción de programas informáticos en los sistemas operativos, o su aplicación es ineficaz.
	VO18	No se han desarrollado procedimientos para el manejo de información clasificada, o su aplicación es ineficaz.
	VO19	Las responsabilidades de seguridad de la información no están presentes en las descripciones de los puestos de trabajo
	VO20	Insuficiencia o falta de disposiciones (relativas a la seguridad de la información) en los contratos con los empleados
	VO21	El proceso disciplinario en caso de incidente de seguridad de la información no está definido, o no funciona correctamente
	VO22	No se ha desarrollado una política formal sobre el uso de ordenadores móviles, o su aplicación es ineficaz
	VO23	Insuficiente control de los activos fuera de las instalaciones
	VO24	Insuficiente o falta de política de "escritorio y pantalla limpios".
	VO25	Autorización de las instalaciones de procesamiento de la información no implementada o que no funciona correctamente
	VO26	Mecanismos de supervisión de las violaciones de la seguridad no aplicados adecuadamente
	VO27	Procedimientos de notificación de deficiencias de seguridad no desarrollados, o su aplicación es ineficaz
	VO28	No se han desarrollado procedimientos de cumplimiento de las disposiciones en materia de derechos intelectuales, o su aplicación es ineficaz

A.2.5.3 Métodos de evaluación de las vulnerabilidades técnicas

Para identificar las vulnerabilidades se pueden utilizar métodos proactivos, como las pruebas de los sistemas de información, en función de la criticidad del sistema de tecnología de la información y las comunicaciones (TIC) y de los recursos disponibles (por ejemplo, los fondos asignados, la tecnología disponible, las personas con experiencia para realizar la prueba). Los métodos de prueba incluyen

- Herramienta de exploración automatizada de vulnerabilidades;
- Pruebas y evaluaciones de seguridad;
- Pruebas de penetración;
- Revisión del código.

Una herramienta automatizada de escaneo de vulnerabilidades se utiliza para escanear un grupo de hosts o una red en busca de servicios vulnerables conocidos [por ejemplo, el sistema permite el Protocolo de Transferencia de Archivos (FTP) anónimo, la retransmisión de Sendmail]. Sin embargo, algunas de las vulnerabilidades potenciales identificadas por la herramienta de escaneo automático no representan necesariamente vulnerabilidades reales en el contexto del entorno del sistema (por ejemplo, algunas de estas herramientas de escaneo califican las

vulnerabilidades potenciales sin tener en cuenta el entorno y los requisitos del sitio). Algunas de las vulnerabilidades marcadas por el software de escaneo automatizado pueden en realidad no ser vulnerables para un sitio en particular, pero pueden estar configuradas de esa manera porque su entorno lo requiere. Por lo tanto, este método de prueba puede producir falsos positivos.

La prueba y evaluación de la seguridad (PES) es otra técnica que puede utilizarse para identificar las vulnerabilidades de los sistemas TIC durante el proceso de evaluación de riesgos. Incluye el desarrollo y la ejecución de un plan de pruebas (por ejemplo, script de pruebas, procedimientos de pruebas y resultados esperados de las pruebas). La finalidad de las pruebas de seguridad del sistema es comprobar la eficacia de los controles de seguridad de un sistema de TIC tal y como se han aplicado en un entorno operativo. El objetivo es garantizar que los controles aplicados cumplen la especificación de seguridad aprobada para el software y el hardware y que aplican la política de seguridad de la organización o cumplen las normas del sector.

Las pruebas de penetración pueden utilizarse para complementar la revisión de los controles de seguridad y garantizar la seguridad de las distintas facetas del sistema TIC. Las pruebas de penetración, cuando se utilizan en el proceso de evaluación de riesgos, pueden servir para evaluar la capacidad de un sistema TIC para resistir los intentos intencionados de burlar la seguridad del sistema. Su objetivo es probar el sistema de TIC desde el punto de vista de una fuente de amenazas e identificar posibles fallos en los esquemas de protección del sistema de TIC.

La revisión del código es la forma más exhaustiva (pero también más cara) de evaluar la vulnerabilidad. Los resultados de estos tipos de pruebas de seguridad ayudan a identificar las vulnerabilidades de un sistema.

Las herramientas y técnicas de penetración pueden dar resultados falsos a menos que la vulnerabilidad se explote con éxito. Para explotar determinadas vulnerabilidades, es necesario conocer la configuración exacta del sistema/aplicación/parches en el sistema probado. Si esos datos no se conocen en el momento de la prueba, no es necesariamente posible explotar una vulnerabilidad concreta con éxito (por ejemplo, obtener un shell inverso remoto). Sin embargo, sigue siendo posible que un proceso o sistema probado se bloquee o se reinicie. En tal caso, el objeto probado debe considerarse también vulnerable.

Los métodos pueden incluir las siguientes actividades

- Entrevistas a personas y usuarios;
- Cuestionarios;
- Inspección física;
- Análisis de documentos.

A.2.5.4 Escenarios operativos

En un enfoque basado en activos, los escenarios operativos pueden construirse analizando los diferentes caminos, dentro de los activos de apoyo, que las fuentes de riesgo pueden utilizar para llegar a los activos de la empresa y sus EFD.

El análisis de estos escenarios puede ayudar a profundizar en el enfoque basado en eventos.

Un ataque exitoso suele ser el resultado de la explotación de varios fallos. Los ataques intencionados suelen seguir un enfoque secuencial. Estos últimos explotan de forma coordinada varias vulnerabilidades de carácter informático, organizativo o físico. Este enfoque, basado en la explotación simultánea de distintos fallos, puede tener graves consecuencias, aunque las vulnerabilidades explotadas sean insignificantes si se consideran individualmente.

Los escenarios analizados pueden estructurarse según una secuencia de ataque típica. Existen varios modelos que pueden utilizarse (por ejemplo, el modelo de cadena de muerte cibernética1)). El enfoque debe permitir identificar los activos de apoyo críticos que pueden ser utilizados como vectores de entrada o explotación o como relé de propagación del ataque modelado.

Estos escenarios pueden representarse en forma de gráficos o diagramas de ataque, útiles para representar los métodos de ataque del atacante.

A.2.6 Ejemplos de escenarios aplicables en ambos enfoques

Los escenarios de riesgo pueden construirse utilizando un enfoque basado en eventos, un enfoque basado en activos, o ambos. La figura A.4 muestra la evaluación de riesgos basada en escenarios de riesgo.

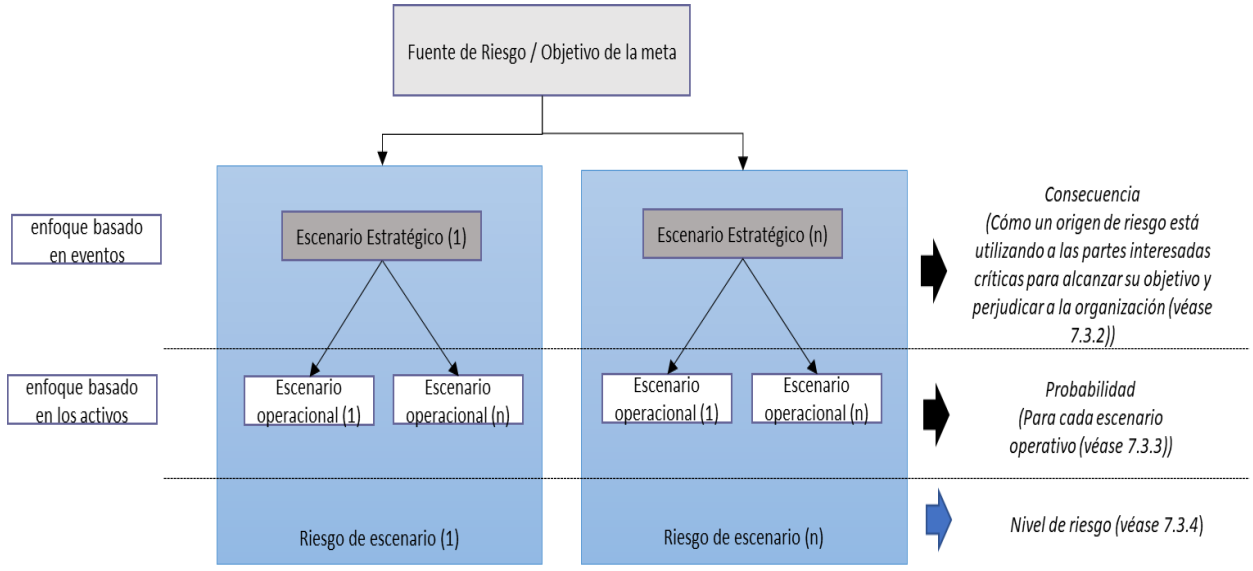

Figura A.4 - Evaluación del riesgo basada en escenarios de riesgo

El cuadro A.12 muestra ejemplos de escenarios de riesgo y los vínculos con los enfoques basados en activos/eventos y las fuentes de riesgo.

Cuadro A.12 - Ejemplos de escenarios de riesgo en ambos enfoques

Fuente del Riesgo	Objetivo de la meta EDS	Escenario de riesgo estratégico (Enfoque basado en eventos)	Escenario de riesgo operacional (Enfoque basado en los activos)
Estado autoritario	Adquisición de un vector estratégico de ataque	Subvertir infraestructuras críticas	Despliegue de malware oculto y persistente en la cadena de suministro
Crimen organizado	Desarrollo de actividades ilegales	Explotación de las infraestructuras portuarias	Infiltración del sindicato de estibadores
			Tomar el control de un sistema informático de gestión de flujos
		Fraude en el carrusel de los impuestos	Creación de empresas ficticias para realizar intercambios falsos en el mercado del impuesto sobre el carbono
		Extorsión	Distribución de ransomware
Negocios agresivos	Obtención de un monopolio de mercado	Influir en el regulador	Corromper a un responsable de la toma de decisiones
		Eliminación de competidores	Campaña de difamación en las redes sociales

A.2.7 Seguimiento de los eventos relacionados con el riesgo

La supervisión de los eventos relacionados con el riesgo consiste en la identificación de los factores que pueden influir en un escenario de riesgo para la seguridad de la información, tal como se define en 10.5.2.

En este contexto, los factores se identifican como un conjunto de elementos que permiten detectar un comportamiento inesperado hacia un activo determinado y que pueden integrarse en las capacidades y herramientas de supervisión de la organización para determinar el desencadenamiento de un escenario de riesgo para la seguridad de la información.

La supervisión de los eventos relacionados con el riesgo puede definirse utilizando varios indicadores procedentes de escenarios operativos o de escenarios estratégicos, ambos introducidos en el apartado 7.2.1. Pueden ser de distinta naturaleza (técnicos, organizativos, de comportamiento, resultados de auditorías, etc.). El seguimiento de los eventos se realiza en función de las prioridades definidas, como la magnitud de las consecuencias y la probabilidad del evento.

El cuadro A.13 ofrece un ejemplo de descripción de un escenario de riesgo para la seguridad de la información con sus eventos asociados relacionados con el seguimiento del riesgo.

Tabla A.13 - Ejemplo de escenario de riesgo y relación de seguimiento de eventos relacionados con el riesgo

Componentes de riesgo	Ejemplo	Eventos por vigilar
Escenario estratégico (basado en eventos)	Los documentos sensibles son destruidos por un administrador	
Acontecimientos que afectan a	Pérdida de documentos críticos	
Gravedad de las consecuencias	Medida descriptiva: alta	
Escenarios operativos (basados en activos)	Uso de los derechos de administrador para destruir los documentos sensibles accediendo directamente a la base de datos	Detección de un acceso directo a la base de datos fuera del horario normal de trabajo
	Acceso a la raíz para modificar la fecha/hora del sistema	
	Infección de malware en la estación de trabajo del administrador con propagación en la base de datos	Detección de operaciones que afectan a un gran volumen de datos (Destrucción)
Probabilidad	Medida descriptiva: media	
Fuente del riesgo	Administrador	
Objetivo de la meta	Compromiso de la disponibilidad de documentos sensibles	
EFD	Compromiso del sistema	
Seguridad de los controles	Aplicación de la estrategia de copias de seguridad	
	Solución antimalware	
	Implementación de NTP	
	Endurecimiento del sistema operativo	
	Restricción de los derechos de acceso a los datos operativos	

- fuente: indica de dónde procede el evento/técnica (¿quién y por qué?) y puede asociarse a recursos A.2.3;
- función: indica el tipo de evento/técnica que realiza el atacante (¿qué?);
- destino: indica sobre qué se realiza la técnica o el evento (¿sobre qué activos primarios de apoyo?)
- activador: indica qué condiciones permiten detectar e identificar el escenario de riesgo (resultados del ataque).

En la figura A.5 se presenta un ejemplo de aplicación del modelo FFDA.

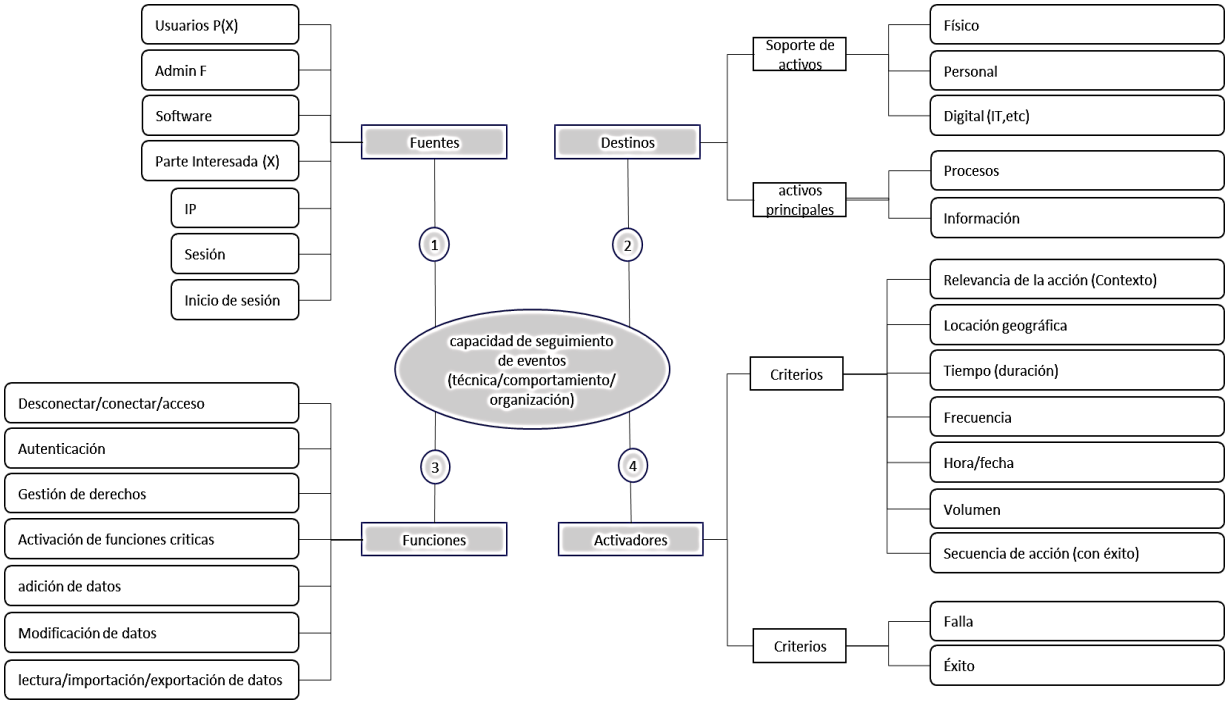

Figura A.5 - Ejemplo de aplicación del modelo FFDA

Para asegurar que un evento relacionado con el riesgo de monitoreo es efectivo y eficiente para monitorear un escenario de riesgo de seguridad de la información, es necesario determinar sus indicadores.

Los indicadores de los eventos relacionados con el riesgo de monitoreo son

- nivel de riesgo del escenario de riesgo que se supervisa;
- eficacia, capacidad de los eventos relacionados con el riesgo para supervisar un escenario de riesgo
- eficiencia, relación entre los verdaderos positivos y los falsos positivos, o el coste de la caracterización.

Bibliografía

[1] ISO 17666:2016, Sistemas espaciales - Gestión de riesgos

[2] ISO/IEC 27001:2022, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos

[3] ISO/IEC 27003, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Guía

[4] ISO/IEC 27004, Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Seguimiento, medición, análisis y evaluación

[5] ISO/IEC 27014, Seguridad de la información, ciberseguridad y protección de la privacidad - Gobierno de la seguridad de la información

[6] ISO/IEC/TR 27016, Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Economía de la organización

[7] ISO/IEC 27017, Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información basados en ISO/IEC 27002 para los servicios en la nube

[8] ISO/IEC 27701, Técnicas de seguridad - Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información sobre la privacidad - Requisitos y directrices

[9] ISO 31000:2018, Gestión de riesgos - Directrices

[10] IEC 31010:2019, Gestión de riesgos - Técnicas de evaluación de riesgos

[11] Guía ISO 73:2009, Gestión de riesgos – Vocabulario