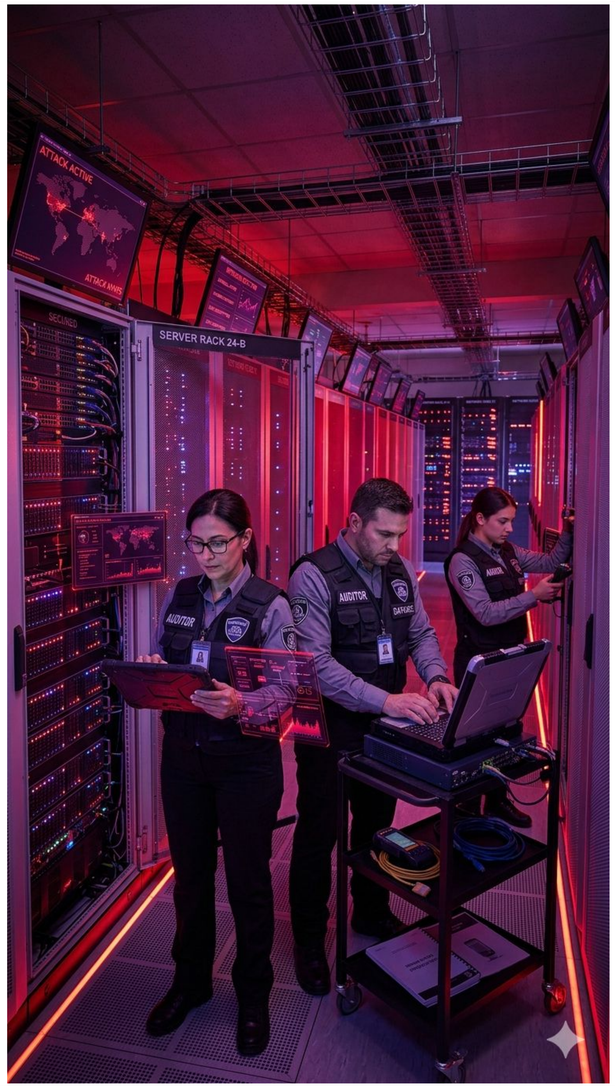
Lead Security Risk Manager 27005:2022
Training Material



Tactical Compliance Badges

Idioma: Español
Ver:2026
Creado por: Valfra It Consulting.

ISO IEC 27005:2022

Quien es Valfra It Consulting

Empresa 100% mexicana, fundada en 2009.

Somos el mejor equipo de profesionales creando un concepto innovador en servicios de consultoría, auditoría, capacitación y certificación, buscando reunir el mejor talento de profesionales para ofrecer servicios de excelencia en las mejores prácticas y sistemas de gestión en México, Canadá, EUA y Latinoamérica.

Líderes en implementación de mejores prácticas y sistemas de gestión, somos asesores reconocidos gracias a la calidad de nuestro servicio.

Miembros de la red de empresas Dun & Bradstreet somos reconocidos internacionalmente por las organizaciones fijadoras de estándares con mayor influencia del mundo, más de 50 asociaciones comerciales e industriales, el Gobierno Federal de Estados Unidos y las Naciones Unidas, entre otras instituciones.

Diamond partners de CERTIPROF LLC® organismo internacional para evaluar y certificar competencias a nivel mundial; VALFRA IT CONSULTING ha capacitado y certificado a cientos de profesionistas en normas internacionales como ISO 27001, ISO 22301, ISO 20000, ISO 9000 y mejores prácticas como Ciberseguridad, ITIL, SCRUM, NIST y NICE.

Valor y Experiencia

Con 17 años de experiencia hemos desarrollado, compartido conocimiento y experiencias en cuanto al conjunto de las prácticas más actuales, con la finalidad que las TI cumplan su propósito y objetivo.

Nuestra misión

Convertirnos en su socio de negocio y aliado estratégico.

Nuestras Afiliaciones

certiprof®

Badge Digital

Los Badges digitales contienen información sobre quién las ha obtenido, las competencias requeridas y la organización que las ha expedido. Algunas insignias incluso están vinculadas a las actividades necesarias para obtenerlas.

Permiten a los profesionales mostrar y verificar sus logros de manera instantánea y global, los perfiles de LinkedIn con insignias digitales reciben más atención por parte de reclutadores y empleadores.

Se reportó que esto mejoró su credibilidad profesional en sus redes. Además, que los Badges digitales les ayudan a identificar rápidamente habilidades específicas.

Se ha demostrado que incluirlos en currículums genera más de probabilidades de contratación en comparación con aquellos que solo mencionan sus habilidades sin verificación digital.

Badge Digital

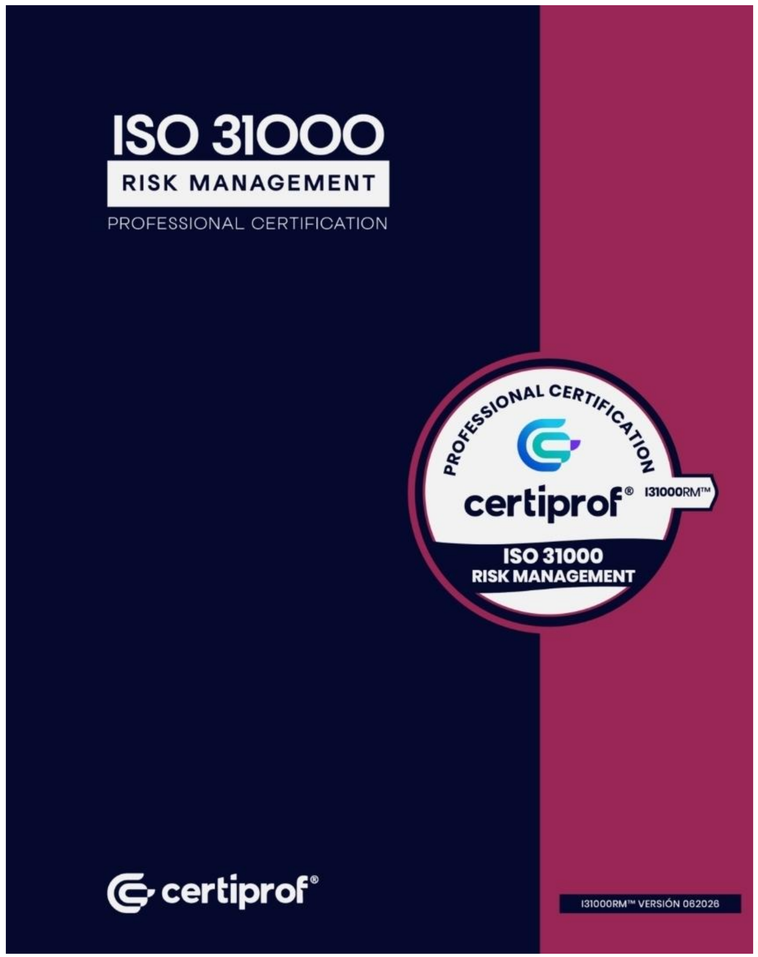
Los Certificados de Cumplimiento Táctico **Lead Security Risk Manager 27005:2022**
(complemento de los Certificados ISO 31000 Risk Management Professional) demuestran que las personas cuentan con las competencias necesarias para establecer, gestionar y mejorar un proceso de evaluación y tratamiento de riesgos de la seguridad de la información y un plan de tratamiento de riesgos dentro de un SGSI en apego a las normas ISO/IEC 27005:2022.

Introducción al curso

Relación ISO 31000:2018 e ISO/IEC 27005:2022

ISO 27001:2022, En su cláusula 6 establece el rol Dueño del Riesgo, el cual debe tener conocimientos básicos sobre la norma ISO 31000:2018 Para el establecimiento del proceso de tratamiento del riesgo, este curso, profundiza en este proceso y lo orienta al tratamiento de riesgos de seguridad de la información en los activos de la organización.

Revisa el manual de autoestudio de Certiprof ISO 31000 RISK MANAGEMENT, para obtener estos conocimientos previos.



Norma ISO/IEC 27005:2022


INTERNATIONAL STANDARD

ISO/IEC 27005

Fourth edition
2022-10

Information technology — Security techniques — Information security risk management

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

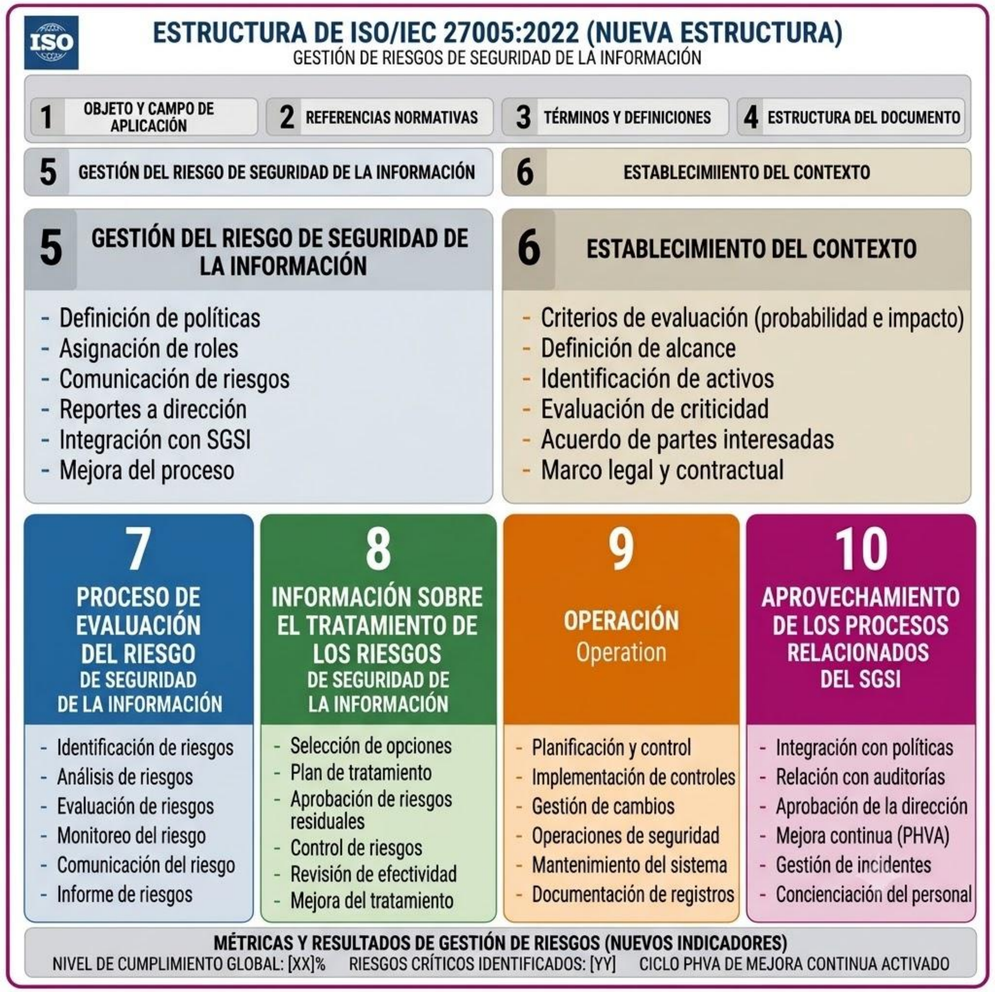
ISO IEC

Reference number
ISO/IEC 27005:2022(E)

Norma internacional que proporciona directrices para la gestión de riesgos de seguridad de la información. Esta edición se alinea con la norma ISO/IEC 27001:2022, integrándose con el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

🎯 Objetivo Principal: Proporcionar un enfoque estructurado para identificar, analizar, evaluar, tratar y comunicar los riesgos de seguridad de la información, permitiendo a las organizaciones tomar decisiones informadas sobre el nivel de riesgo aceptable y los controles necesarios para mitigarlos.

Clausulado Norma ISO/IEC 27005:2022



1. Objeto y campo de aplicación
2. Referencias normativas
3. Términos y definiciones
4. Estructura del documento

5. Gestión del riesgo de seguridad de la información
6. Establecimiento del contexto
7. Proceso de evaluación del riesgo de seguridad de la información
8. Información sobre el tratamiento de los riesgos de seguridad de la información
9. Operación (Operation)
10. Aprovechamiento de los procesos relacionados del SGSI

1. Objeto y campo de aplicación

1. Propósito principal del documento: La norma proporciona directrices (orientación y consejos prácticos) para la gestión de riesgos de seguridad de la información.

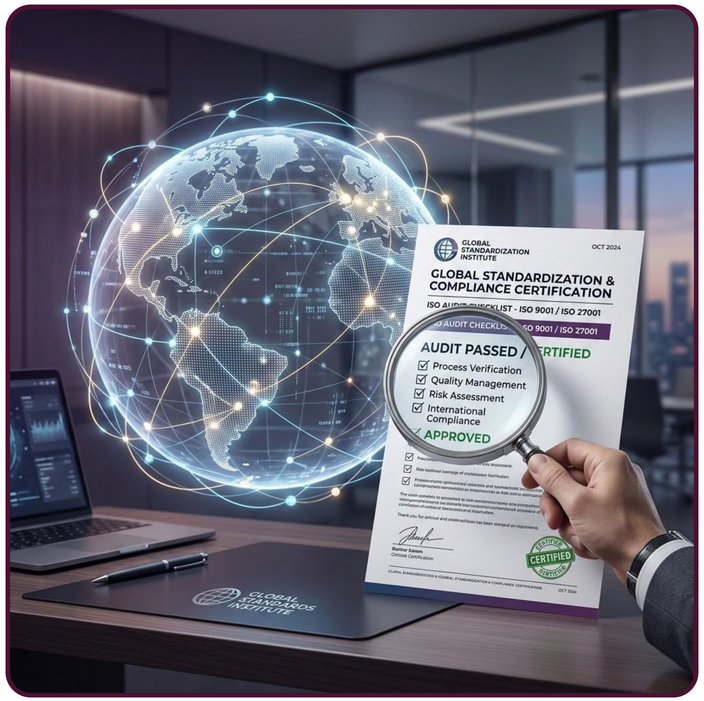
Su objetivo no es darte una receta única, sino ayudarte a implementar un proceso sistemático para identificar, analizar, evaluar y tratar los riesgos que puedan afectar a los activos de información de tu organización.

2. Alineación estratégica con ISO/IEC 27001: La Cláusula 1 deja muy claro que este documento está diseñado específicamente para apoyar los requisitos de seguridad de la información establecidos en la ISO/IEC 27001.

Es el "manual de instrucciones" detallado para cumplir con las cláusulas de planificación y tratamiento de riesgos (específicamente los apartados 6.1.2 y 6.1.3) de un Sistema de Gestión de Seguridad de la Información (SGSI).

3. ¿A quién va dirigida? (Campo de aplicación): El objeto y campo de aplicación es aplicable a:

Todo tipo de organizaciones: Ya sean empresas privadas, entidades públicas, ONGs, corporaciones multinacionales o microempresas; Cualquier sector: Tecnológico, financiero, salud, industrial, educativo, etc.

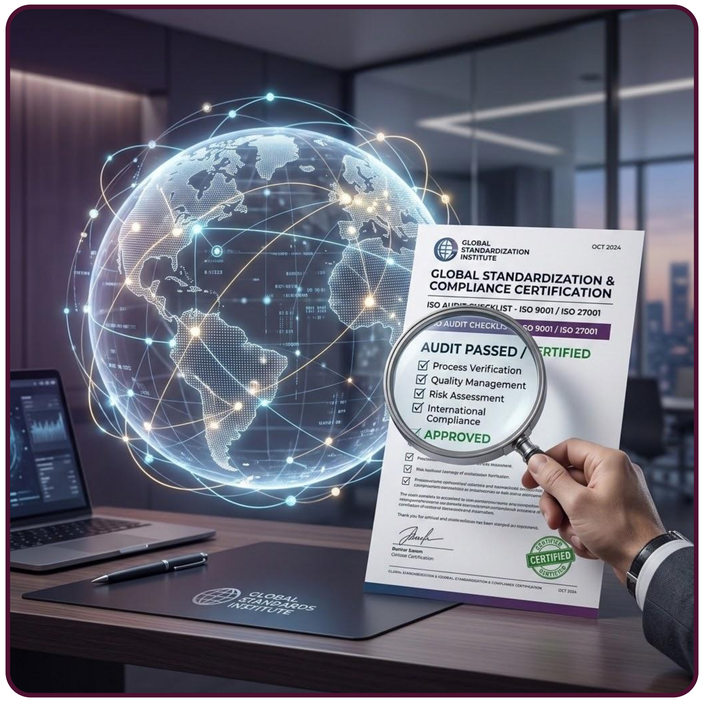


1. Objeto y campo de aplicación

4. Lo que NO es la ISO/IEC 27005:2022: Para entender bien el alcance, la Cláusula 1 (en conjunto con el enfoque general de la norma) delimita sus fronteras:

-No es certificable: Una empresa no puede "certificarse en ISO 27005

-No impone una metodología específica: No te obliga a usar un software o un método de análisis concreto (como Magerit, OCTAVE o NIST). Te da los criterios mínimos que debe cumplir cualquier metodología que decidas usar.



2. Referencias normativas

1. Documentos indispensables: La Cláusula 2 establece formalmente qué otros estándares son estrictamente necesarios para poder entender y aplicar la ISO/IEC 27005. En la versión 2022, se hace referencia explícita a los siguientes documentos:

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary: Es la norma madre del vocabulario. Contiene las definiciones y términos esenciales de todo el ecosistema de seguridad de la información.

2. La regla de la aplicación (Fechado vs. No Fechado): La cláusula incluye una nota legal estándar de ISO muy importante para los auditores y gestores de riesgo:

-Para las referencias con fecha: Sólo se aplica la edición citada (si la norma de vocabulario se actualiza después, teóricamente debes seguir usando la versión del año citado hasta que se revise la 27005).

-Para las referencias sin fecha: Se aplica la última edición del documento de referencia (incluyendo cualquier enmienda). En el caso de la ISO 27005:2022, al citar a la ISO/IEC 27000 de forma general, se entiende que debes usar siempre su versión más reciente y actualizada.

2. Referencias normativas

3. ¿Por qué es crucial esta cláusula en la práctica?: Aunque parece pura burocracia, la Cláusula 2 tiene un impacto directo en cómo gestionas el riesgo:

-Unificación del lenguaje: Al remitirse a la ISO/IEC 27000, la norma se asegura de que cuando hables de "riesgo", "impacto", "vulnerabilidad", "amenaza" o "activo", estés usando exactamente la misma definición que el resto del mundo y que tus auditores de la ISO 27001. Evita malentendidos.

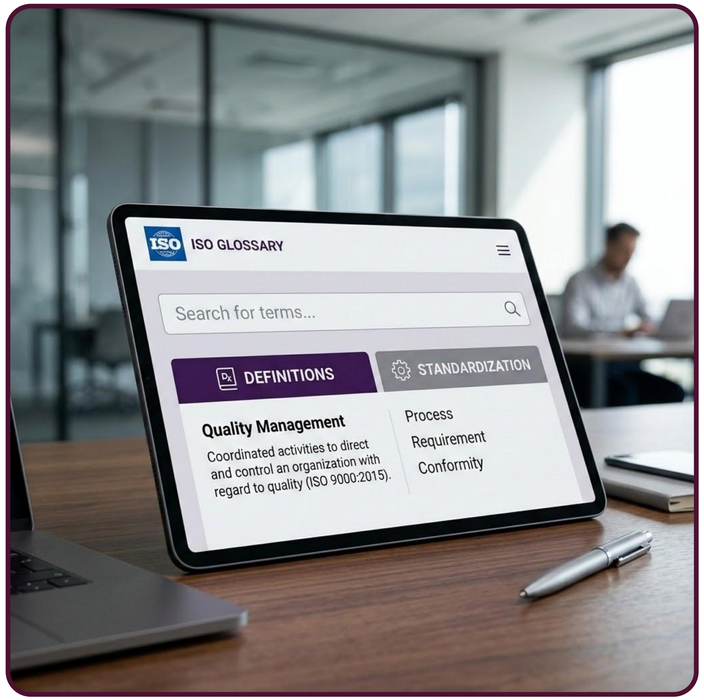
-Evita la redundancia: En lugar de reescribir 50 páginas de definiciones dentro de la ISO 27005, los autores simplemente dicen: "Si tienes dudas con una palabra, ve a buscarla a la ISO 27000".

⚠️ **En resumen:** La Cláusula 2 te dice que no puedes leer la ISO 27005 de forma aislada. Para que tu proceso de gestión de riesgos tenga una base sólida y alineada con los estándares internacionales, debes tener la ISO/IEC 27000 siempre abierta al lado.

3. Términos y definiciones

1. La regla de prioridad del vocabulario: La Cláusula 3 comienza con una aclaración fundamental: para los propósitos de esta norma, se aplican los términos y definiciones dados en la ISO/IEC 27000 (la norma de vocabulario de la familia 27000).

Sin embargo, la 27005:2022 introduce o matiza definiciones específicas y críticas relacionadas directamente con la gestión de riesgos.



2. Conceptos clave desarrollados en la Cláusula 3: La norma desglosa términos específicos bajo el apartado "Términos relacionados con el riesgo para la seguridad de la información". Los conceptos más relevantes que debes dominar son:

-Riesgo (de seguridad de la información): Definido tradicionalmente como el "efecto de la incertidumbre sobre los objetivos". En esta cláusula se especifica que, en el contexto de la seguridad, suele expresarse en términos de la combinación de las consecuencias de un escenario de riesgo y la probabilidad de que ocurra.

-Escenario de Riesgo (Risk Scenario): Una secuencia o combinación de eventos que conducen a una consecuencia no deseada (por ejemplo, un ataque de phishing exitoso que resulta en el cifrado de datos por ransomware).

-Propietario del Riesgo (Risk Owner): Persona o entidad con la responsabilidad y autoridad para gestionar un riesgo. La cláusula enfatiza que esta persona debe tener el poder real para tomar decisiones sobre el tratamiento del riesgo.

3. Términos y definiciones

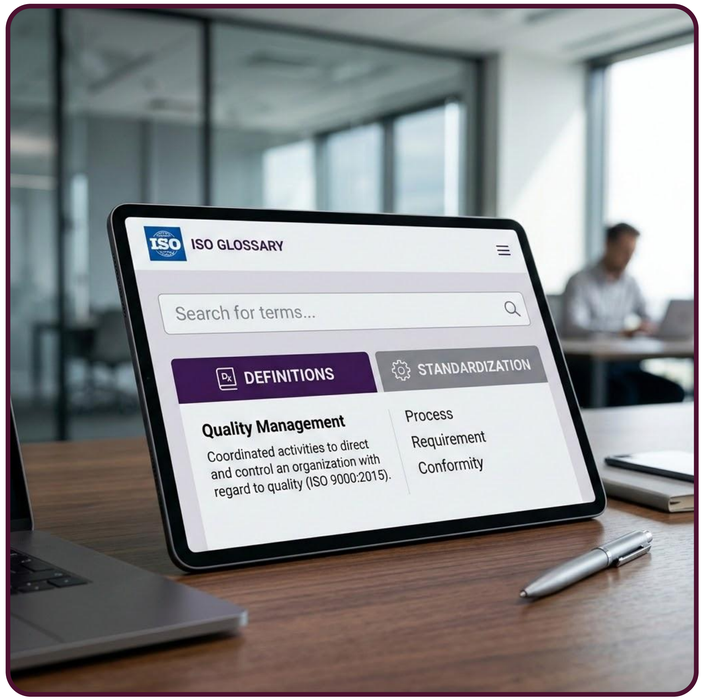
-Fuente de Riesgo (Risk Source): Elemento que, por sí solo o en combinación con otros, tiene el potencial intrínseco de originar un riesgo (puede ser una persona, un factor ambiental, una falla técnica, etc.).

-Criterios de Riesgo (Risk Criteria): Los términos de referencia frente a los cuales se evalúa la importancia de un riesgo (por ejemplo, el impacto financiero, legal o reputacional tolerable).

-Apetito de Riesgo (Risk Appetite): La cantidad y el tipo de riesgo que una organización está dispuesta a buscar o retener para alcanzar sus objetivos estratégicos.

-Amenaza (Threat): Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema u organización.

-Vulnerabilidad (Vulnerability): Debilidad de un activo o control que puede ser explotada por una o más amenazas.



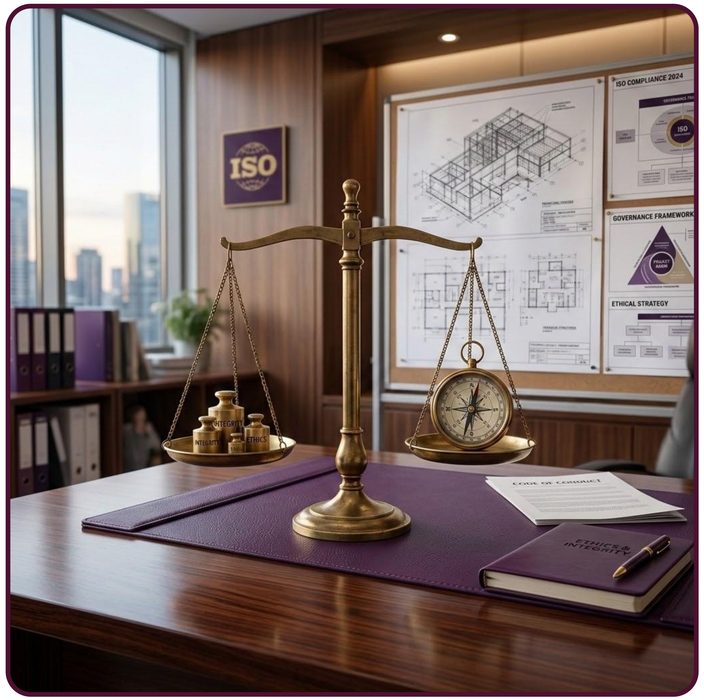
3. ¿Por qué es crucial la Cláusula 3 en la práctica? Esta cláusula no es meramente teórica; tiene un impacto directo en cómo diseñas tu metodología de riesgos:

-Bases para las fórmulas de riesgo: Al definir claramente qué es probabilidad (likelihood), consecuencia e impacto, te da la estructura matemática y lógica para armar tus matrices de riesgo.

-Cambio de enfoque (2022): En esta versión se refuerza mucho la diferencia entre el enfoque basado en activos (tradicional) y el enfoque basado en eventos/escenarios (estratégico), y las definiciones de esta cláusula preparan el terreno para que el usuario entienda cómo estructurar ambos tipos de análisis en las cláusulas siguientes.

4. Estructura del documento

A diferencia de las versiones anteriores (como la de 2018), la actualización de 2022 reestructuró por completo el orden de la norma para alinearla de forma exacta con la ISO 31000 (el estándar global de gestión de riesgos). La Cláusula 4 funciona como el "mapa de carretera" o la guía de navegación que te explica cómo leer y utilizar el resto del documento.



1. El ciclo de la Gestión de Riesgos según la Cláusula 4: Esta sección explica que el cuerpo principal de la norma se divide en 4 bloques fundamentales (Cláusulas 5 a 8) que describen el proceso completo de gestión de riesgos. La estructura se presenta de la siguiente manera:

- **-Cláusula 5:** Contexto (Context): Establece los criterios básicos, los objetivos y el alcance del proceso de riesgos.
- **-Cláusula 6:** Proceso de evaluación del riesgo (Risk assessment process): La parte central que incluye la identificación, el análisis y la valoración del riesgo.
- **-Cláusula 7**: Proceso de tratamiento del riesgo (Risk treatment process): Cómo responder a los riesgos (mitigar, transferir, evitar o aceptar).
- -**Cláusula 8:** Operación (Operation): La ejecución práctica y el día a día del proceso.

Además, detalla los tres procesos transversales (que ocurren al mismo tiempo en todo el ciclo):

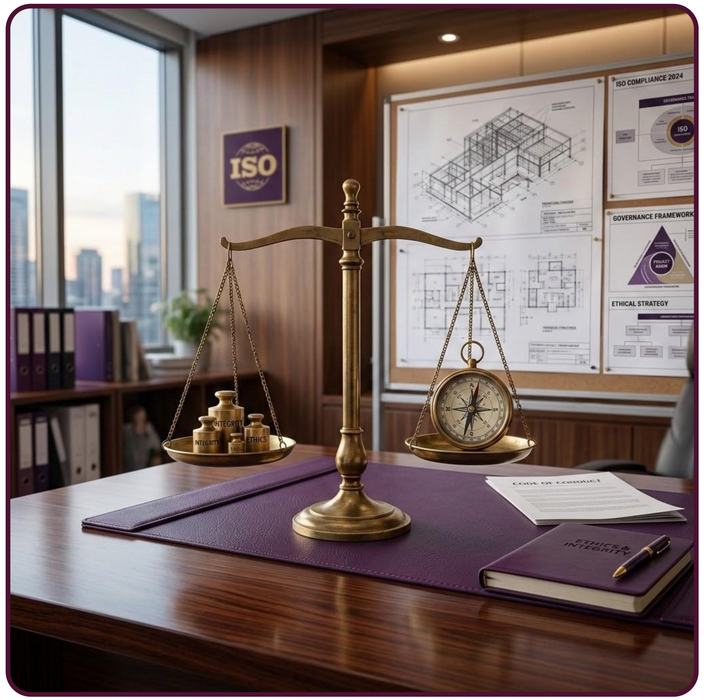
- -Comunicación y consulta
- -Monitoreo y revisión
- -Registro y reporte

4. Estructura del documento

2. La importancia de los Anexos (Los Annexes): La Cláusula 4 hace un énfasis especial en que gran parte del valor práctico de la norma se encuentra en sus anexos (Anexo A y Anexo B). Te explica que están ahí para darte ejemplos y guías metodológicas sobre dos enfoques distintos:

Enfoque basado en activos (Asset-based approach): El método tradicional donde identificas los activos de información (servidores, bases de datos) y analizas sus amenazas y vulnerabilidades.

Enfoque basado en escenarios (Event-based / Scenario-based approach): El método moderno y más estratégico, donde te enfocas en eventos globales (por ejemplo, "un ataque de ransomware paraliza la cadena de suministro") y evalúas su impacto en el negocio.



3. ¿Por qué es útil la Cláusula 4? En la práctica, esta cláusula ayuda al lector a no perderse en la densidad del documento. Te dice explícitamente:

-Qué vas a encontrar en cada sección.

-Cómo se conectan las fases del riesgo entre sí.

-Dónde buscar plantillas o ejemplos prácticos (remitiéndote a los anexos según el enfoque que decida adoptar tu organización).

5. Gestión de la seguridad de la Información

5.1 Proceso de Gestión de Riesgos de Seguridad De La Información

Establece que la gestión de riesgos de seguridad de la información debe ser un proceso integrado en la estrategia global de la organización. Requiere la recopilación y análisis de información tanto del contexto externo (leyes, competidores, entorno social y tecnológico) como del contexto interno (cultura organizacional, objetivos de negocio, estructura y capacidades). El objetivo es asegurar que el proceso de riesgo esté alineado con el propósito de la empresa.

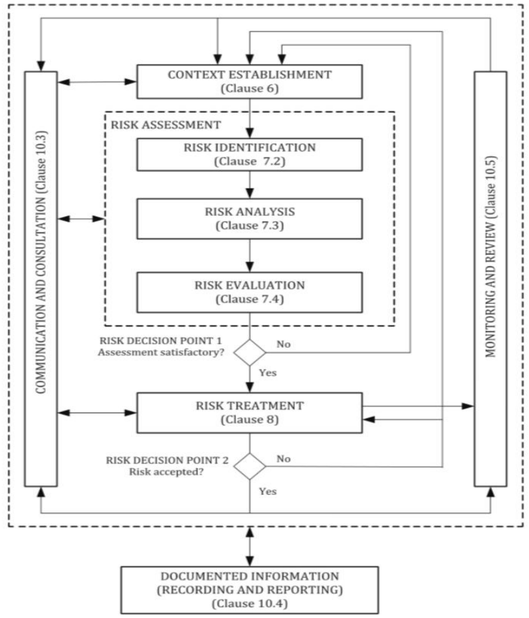


Figure 1 — Information security risk management process

5. Gestión de la seguridad de la Información

5.2 Ciclos de la Gestión de riesgos de Seguridad De La Información

Esta subcláusula establece que las actividades de gestión de riesgos se deben ejecutar de manera iterativa (en ciclos continuos) para aumentar la profundidad, el detalle y la eficacia del análisis a lo largo del tiempo.

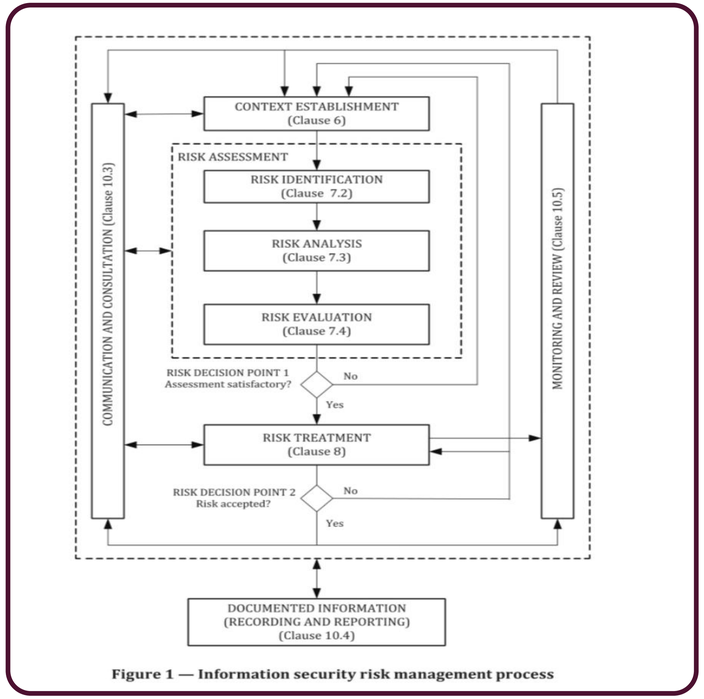


Figure 1 — Information security risk management process

- **5.2.1 El enfoque iterativo (Ciclos de madurez):** La norma reconoce que una organización rara vez puede identificar y mitigar todos los riesgos a la perfección en el primer intento. Por ello, la subcláusula promueve un enfoque por fases u olas:

-Primeros ciclos (Nivel Estratégico): Se realiza una evaluación de riesgos rápida y de alto nivel para identificar los riesgos más evidentes, críticos o sistémicos. Esto permite a la organización concentrar recursos de inmediato donde hay mayor peligro.

-Ciclos posteriores (Nivel Operacional): A medida que el proceso madura, los ciclos se vuelven más profundos. Se analizan sistemas específicos, vulnerabilidades técnicas detalladas o dependencias complejas que en la primera ronda se pasaron por alto.

- **5.2.2 Factores que disparan un nuevo ciclo (Triggers):** La gestión de riesgos en ciclos no sólo responde al calendario (ej. una revisión anual), sino también a eventos del entorno. La subcláusula señala que se debe iniciar una nueva iteración del ciclo de riesgos cuando ocurra:

  Cambios en el contexto de la organización.

  Modificaciones tecnológicas.

  Nuevas amenazas o vulnerabilidades.

  Incidentes de seguridad.

6. Contexto

6.1 Consideraciones Generales

Establece que para que la gestión de riesgos de seguridad de la información sea efectiva, debe alinearse con el contexto interno y externo de la organización, sus objetivos de negocio y los requisitos de las partes interesadas.

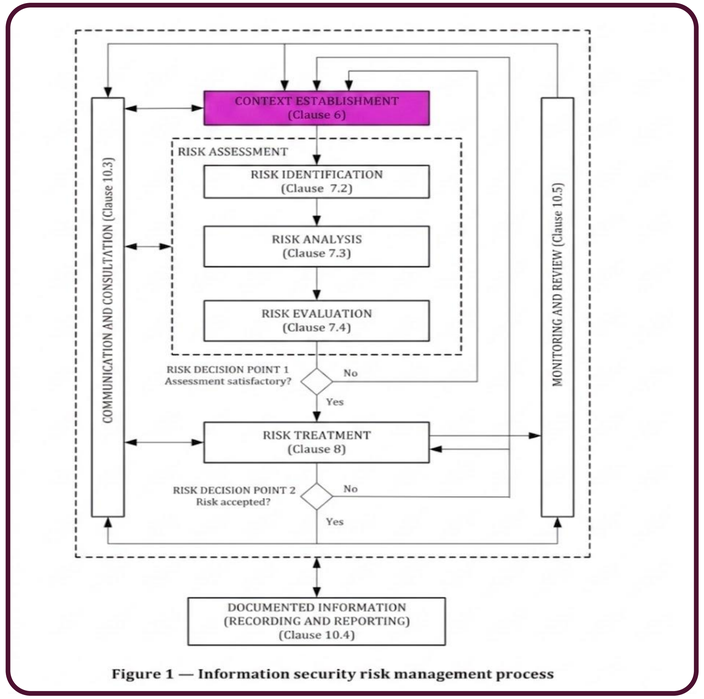


Figure 1 — Information security risk management process

6. Contexto

6.2 Requerimientos de las partes interesadas (Requirements of interested parties)

Ninguna organización opera en el vacío. Esta sub-cláusula obliga a identificar a todos los actores que tienen voz, voto o se ven afectados por la seguridad de la información de la empresa, y a mapear sus expectativas y obligaciones:

-Partes interesadas externas: Reguladores del gobierno (leyes de privacidad, ciberseguridad), clientes (compromisos contractuales de confidencialidad), proveedores y socios comerciales.

-Partes interesadas internas: Empleados, sindicatos, accionistas y la alta dirección.

Objetivo: Asegurar que el proceso de gestión de riesgos identifique y priorice los riesgos que podrían violar leyes (como normativas de protección de datos) o contratos con clientes.

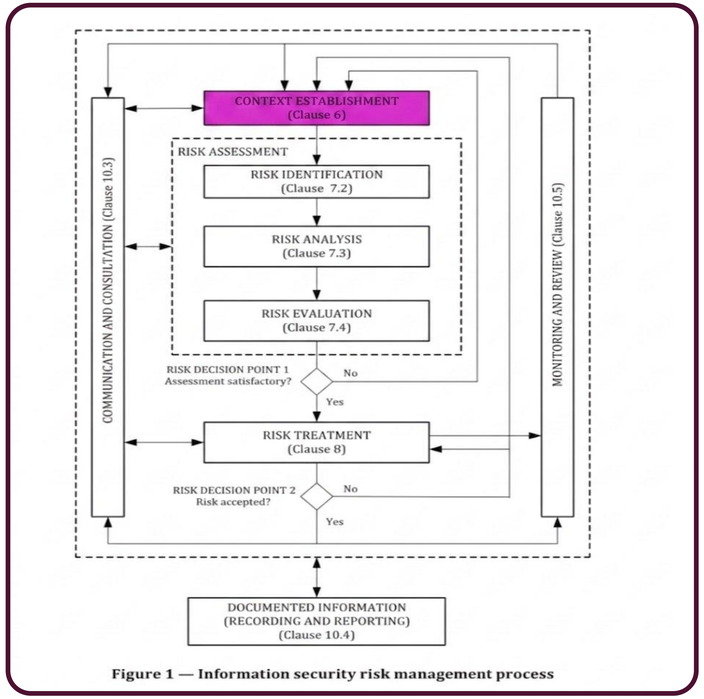


Figure 1 — Information security risk management process

6. Contexto

6.3 Aplicando Criterios De Evaluación de Riesgos

NOTA: Esta subcláusula se relaciona con ISO/IEC 27001:2022, 4.3.

Las organizaciones pueden realizar evaluaciones de riesgos integradas dentro de muchos procesos diferentes, tales como la gestión de proyectos, la gestión de vulnerabilidades, la gestión de incidentes, la gestión de problemas, o incluso de forma improvisada (ad-hoc) para un tema específico identificado. Independientemente de cómo se realicen las evaluaciones de riesgos, estas deben cubrir colectivamente todos los aspectos 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 el logro de sus objetivos. Por lo tanto, esto debe dirigirse a aquellos riesgos y controles que, si se gestionan con éxito, mejorarán la probabilidad de que la organización alcance sus objetivos.

Se proporciona más información sobre el contexto de un SGSI y los aspectos que deben comprenderse a través de la evaluación de riesgos en la norma ISO/IEC 27003.

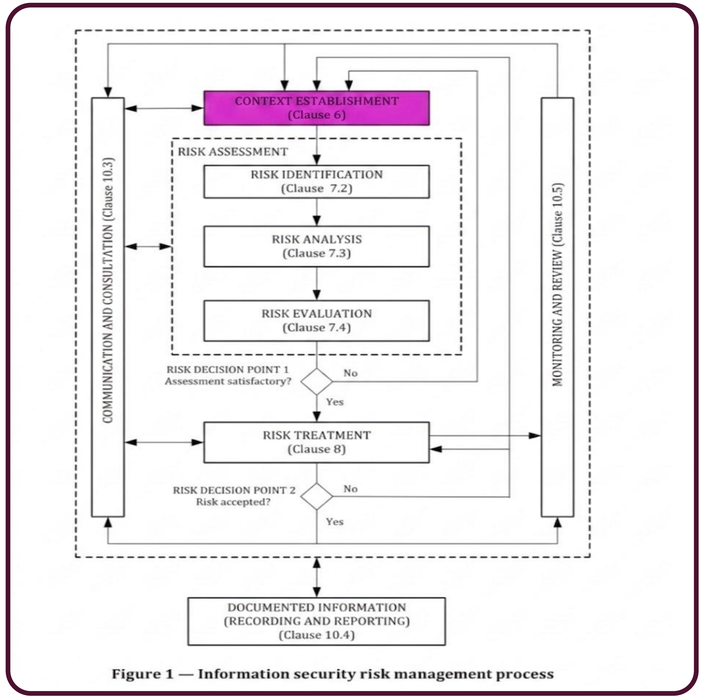


Figure 1 — Information security risk management process

6. Contexto

6.4 Criterios de Riesgo

- **6.4.1 Consideraciones Generales:** Define la necesidad de establecer parámetros claros y homogéneos para que la evaluación del riesgo no sea subjetiva y pueda ser replicable.

- **6.4.2 Criterios de evaluación del riesgo:** Especifica cómo se medirá la importancia del riesgo. Requiere la definición de:
  -Las escalas para evaluar la probabilidad de ocurrencia de los escenarios de riesgo.
  -Las escalas para evaluar las consecuencias o el impacto si el riesgo llega a materializarse.

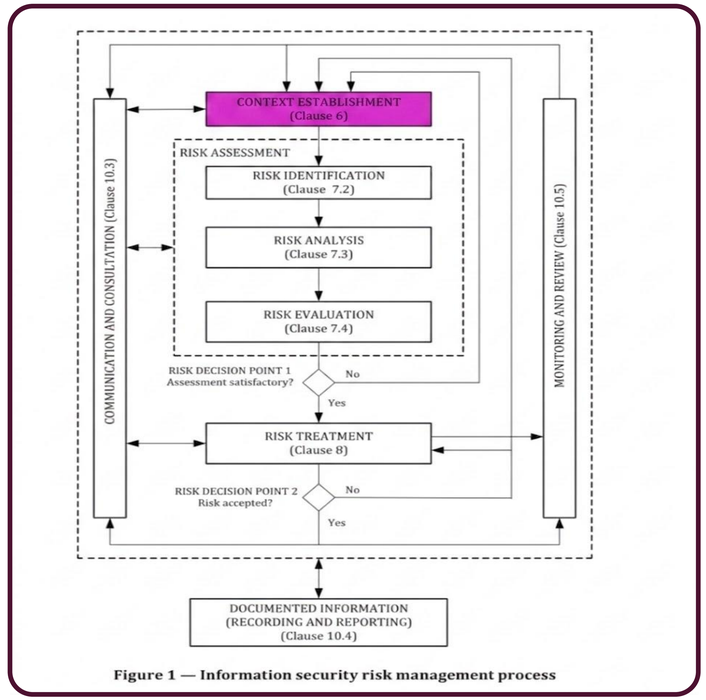


Figure 1 — Information security risk management process

Tabla de Probabilidad / Frecuencia		
Nivel	Rangos	Ejemplo Detallado de la Descripción
1	Muy Poco Probable	Puede ocurrir solo bajo circunstancias excepcionales
2	Poco Probable	Podría ocurrir algunas veces (Pocas veces)
3	Probable	Puede ocurrir en algún momento
4	Bastante Probable	Probabilidad de ocurrencia en la mayoría de las circunstancias
5	Muy Probable	La expectativa de ocurrencia se de en la mayoría de las circunstancias

Tabla de impacto: Prioridad 1 – Impacto en la Operación		
Nivel	Rangos	Ejemplo Detallado de la Descripción
1	Sin Impacto	Hay una indisponibilidad menor o igual a 5 minutos
2	Muy Bajo	Hay una indisponibilidad entre 6 y 15 minutos
3	Bajo	Hay una indisponibilidad entre 15 y 30 minutos
4	Moderado	Hay una indisponibilidad entre 30 y 60 minutos
5	Alto	Hay una indisponibilidad por mayor a 60 minutos. Es necesario un establecer un mecanismo de procesamiento alterno

6. Contexto

6.4 Criterios de riesgo (Risk criteria)

- **6.4.3 Criterios de impacto:** Se centra en determinar qué áreas de la organización se verán afectadas y en qué medida. Los criterios deben considerar, como mínimo:

  El nivel de daño a las **operaciones** del negocio.

  Pérdidas **financieras** o afectación económica directa.

  Incumplimiento de obligaciones **legales**, regulatorias o contractuales.

  Daño a la **reputación**, imagen de marca y confianza de las partes interesadas.

- **6.4.4 Criterios para la aceptación del riesgo:** Establece las reglas para decidir si un riesgo requiere un tratamiento inmediato o si puede ser retenido por la organización.

  -Define el **Apetito de Riesgo** (la cantidad de riesgo que la alta dirección está dispuesta a asumir).

  -Determina los niveles umbral (ej. una matriz de riesgo) que separan los riesgos tolerables de aquellos que son inaceptables y requieren mitigación obligatoria.

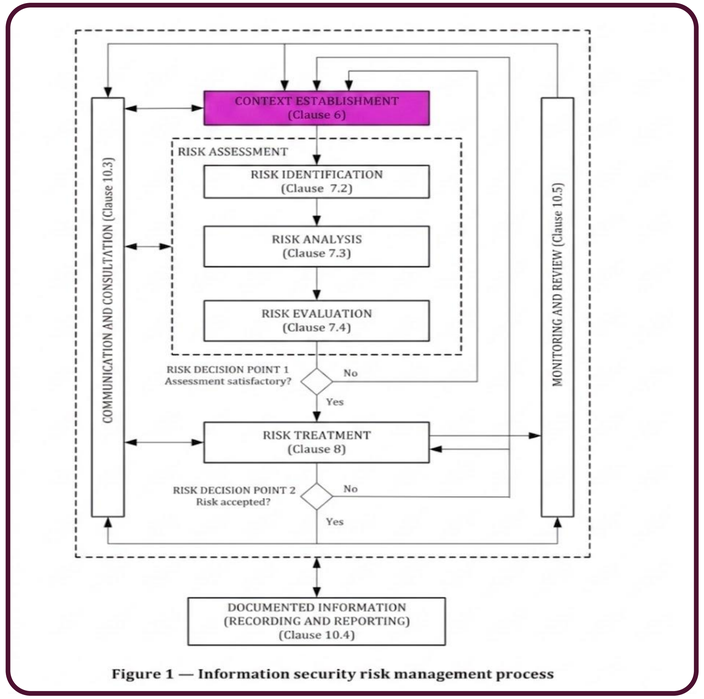


Figure 1 — Information security risk management process

Para definir los criterios de aceptación se hace un cruce de los criterios definidos en base al punto 6.4.2

🧨En la versión 2022, la norma sufrió una reestructuración profunda para alinearse con la ISO 31000 (Gestión de Riesgos General). El comité técnico de ISO decidió eliminar los ejemplos rígidos de matrices de los anexos para evitar que las empresas copiaran y pegaran esta tabla por defecto. La ISO busca que cada organización diseñe sus propios criterios **según su apetito de riesgo.**

6. Contexto

6.4 Criterios de riesgo (Risk criteria)

🧨 Sin embargo puedes utilizar la tabla como esta definida en su predecesora la 27005:2018.

Table E.1 b)

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Resultado de este cruce obtenemos los criterios de aceptación:

Ejemplo: **TODOS LOS RIESGOS CON RESULTADO MAYOR A 1 DEBEN TRATARSE.**

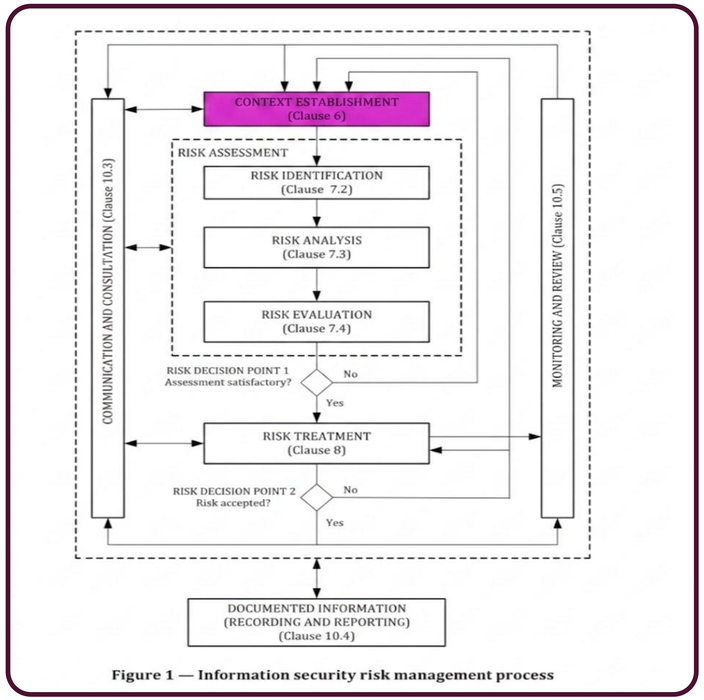


Figure 1 — Information security risk management process

🧨 **¿Dónde se movió o cómo se aborda ahora?** La guía para estructurar esa combinación se movió al cuerpo principal de la norma y a un nuevo enfoque en los anexos:

> **En el cuerpo principal (Cláusula 6.4.2 y 6.4.3):** En lugar de darte la tabla hecha, el clausulado de Criterios de evaluación del riesgo te da las directrices escritas de cómo debes construir tú mismo esa combinación. Te explica qué debes definir escalas para las consecuencias (impacto) y escalas para la probabilidad, y cómo estas deben cruzarse para obtener el nivel de riesgo.

6. Contexto

6.4 Criterios de riesgo (Risk criteria)

En el Anexo A (Estructura para identificar riesgos basados en escenarios): La versión 2022 está fuertemente volcada hacia los escenarios de riesgo. En el Cláusula A.2.1, la norma te explica cómo estimar el riesgo combinando la probabilidad del escenario con el impacto en el negocio, pero delegando el formato de la tabla a la metodología propia de la empresa (como Magerit, NIST o matrices internas).

🧨 **La filosofía actual de la ISO 27005:2022:** La norma actual te da la libertad de combinar la probabilidad y el impacto de tres maneras distintas, y ya no solo con la típica tabla cuadrada:

-Matriz Matricial (La clásica tabla): Sigue siendo válida, pero tú decides si es de 3x3, 4x4 o 5x5.

-Método Multiplicativo o Semicuantitativo: Asignar valores numéricos (ej. Probabilidad 1-5 e Impacto 1-5) y multiplicarlos.

-Enfoque Cualitativo Puro: Mediante reglas lógicas (ej. Si la probabilidad es "Alta" y el impacto es "Medio", el riesgo final es "Alto").

- **6.4.5 Organización para la gestión del riesgo:** Define la gobernanza, quién lidera el proceso, quién ejecuta las evaluaciones y quiénes son los Propietarios del Riesgo (Risk Owner) con poder de decisión y presupuesto.

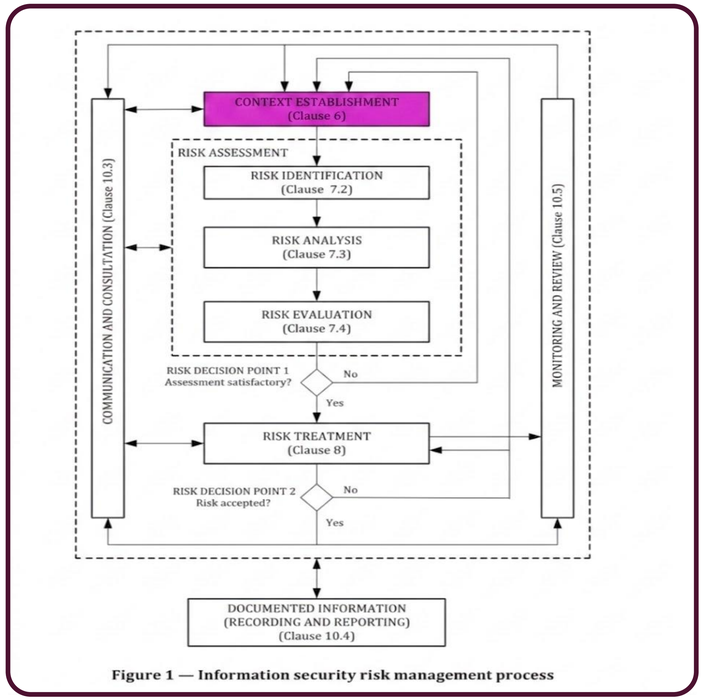


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.1: Generalidades (General)

Esta sección explica que el proceso de evaluación de riesgos consta de tres subprocesos fundamentales e interconectados que deben ejecutarse en orden secuencial o iterativo:

1. Entrada (Input): Para que la evaluación de riesgos pueda dar inicio de manera sólida en la organización, la subcláusula 7.1 establece que se debe contar de antemano con toda la información generada en la etapa previa (la Cláusula 6 - Contexto).

2. Acción (Action): La acción en la 7.1 describe la ejecución sistemática de los tres subprocesos del bloque:

-Identificación: Se busca y reconoce de manera proactiva qué podría pasar para causar una pérdida de confidencialidad, integridad o disponibilidad de la información. La versión 2022 enfatiza que se puede realizar usando dos enfoques válidos:

-Enfoque basado en escenarios: Encontrar secuencias de eventos de amenazas de ciberseguridad.

-Enfoque basado en activos: Mapear los activos (datos, hardware, personas) y cruzarlos con sus respectivas amenazas y vulnerabilidades.

-Análisis: Se determina el valor del riesgo. Se toma la probabilidad de ocurrencia del escenario y se cruza con las consecuencias (el impacto) sobre el negocio.

-Evaluación/Valoración: Se comparan los resultados del análisis de riesgos contra los criterios de aceptación (apetito de riesgo). Aquí se decide si un riesgo es tolerable o si debe ser priorizado obligatoriamente para la fase de tratamiento (Cláusula 8).

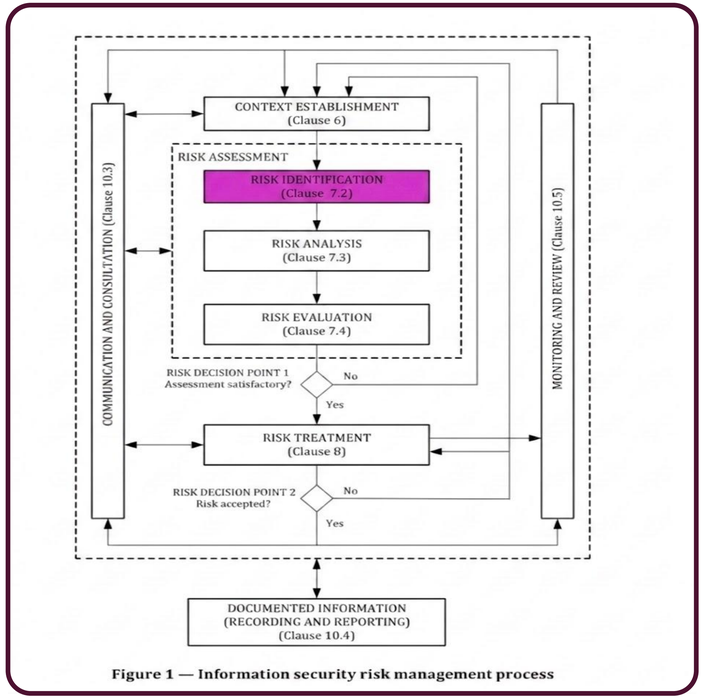


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.1: Generalidades (General)

3. Salida (Output): El resultado final y tangible que debe producir la ejecución completa de este bloque es:

-Un Listado o Registro de Riesgos para la Seguridad de la Información priorizado.

-Este registro debe incluir el escenario de riesgo, su nivel estimado (Bajo, Medio, Alto, Crítico) y la indicación explícita de si el riesgo cumple o no con los criterios de aceptación de la organización.

🎯 En resumen: La subcláusula 7.1 funciona como el manual de introducción técnica del bloque de evaluación. Te dice qué ingredientes necesitas de la fase de contexto (Entradas), los tres pasos lógicos que debes seguir para procesar el riesgo (Acciones) y el entregable formal que debes obtener para poder tomar decisiones en la empresa (Salidas).

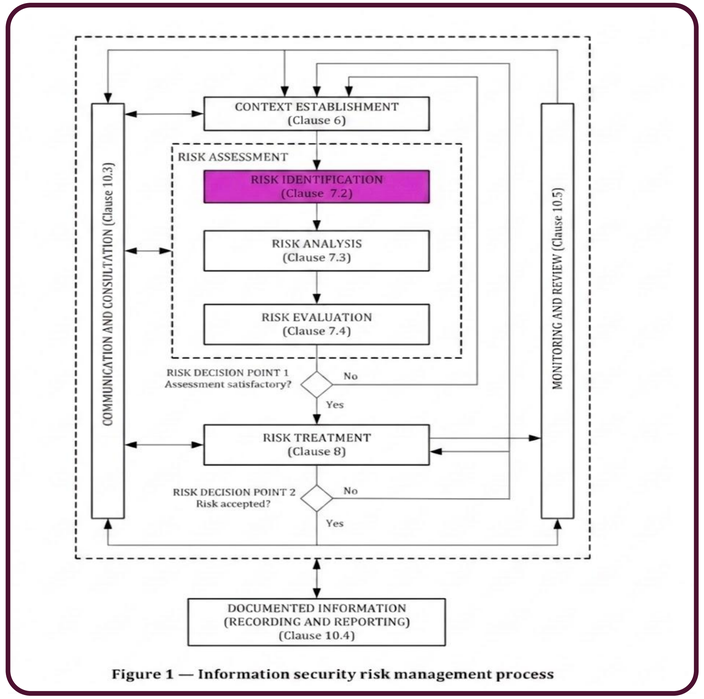


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.2 Identificación del riesgo de seguridad de la información

1. Entrada (Input): Para comenzar la identificación, se requiere la información consolidada en la fase de contexto:

-Los criterios de riesgo establecidos.

-El alcance y los límites del proceso.

-Información sobre los activos de la organización, procesos de negocio, amenazas previas e incidentes de seguridad históricos.

2. Acción (Action): La acción principal consiste en generar una lista exhaustiva de **eventos** que podrían impedir, degradar o retrasar el logro de los objetivos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

La versión 2022 de la norma formaliza que la identificación se puede realizar a través de dos enfoques principales, explicados a detalle en sus anexos:

-Anexo A. Enfoque basado en escenarios.

-Anexo B. Enfoque basado en activos (Asset-based approach)

🧨Es el método detallado. Consiste en realizar una inspección minuciosa de:

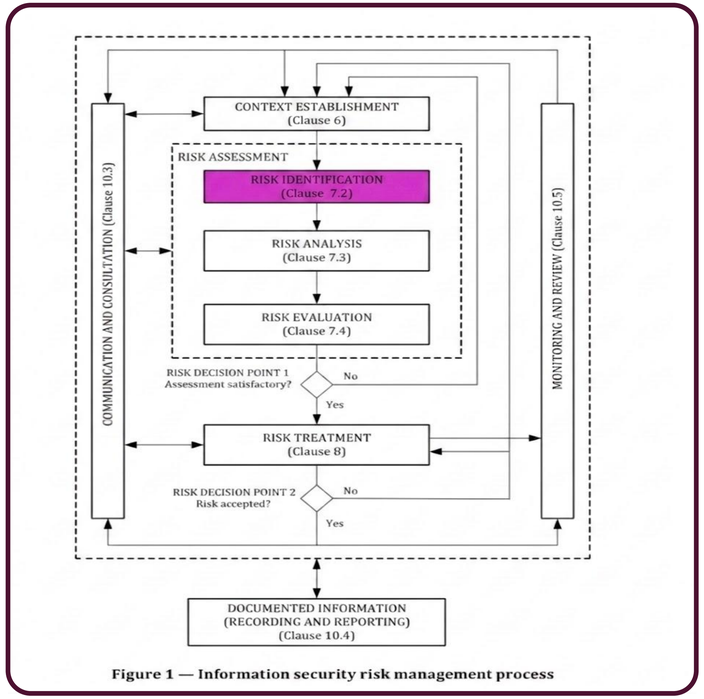


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.2 Identificación del riesgo de seguridad de la información

-Identificación de activos: Inventariar los activos de información (datos, bases de datos) y los activos de soporte (servidores, redes, personal, instalaciones).

Identificación de activos para el enfoque basado en activos, amenazas y vulnerabilidades.

Se requiere identificar los activos para luego realizar la valoración del riesgo. Se identifican dos clases de activos:

- **Primarios**
  - Actividades y procesos misionales, tecnología propietaria, aquellos con requisitos legales y contractuales
  - Información de procesos misionales, de alto costo de procesamiento, almacenamiento, transmisión y recuperación
- **Secundarios**
  - Hardware
  - Software
  - Redes y conectividad
  - Servicios (Subcontratistas/proveedores/fabricantes)
  - Personas a cargo de toma de decisiones (Conocimiento del negocio)

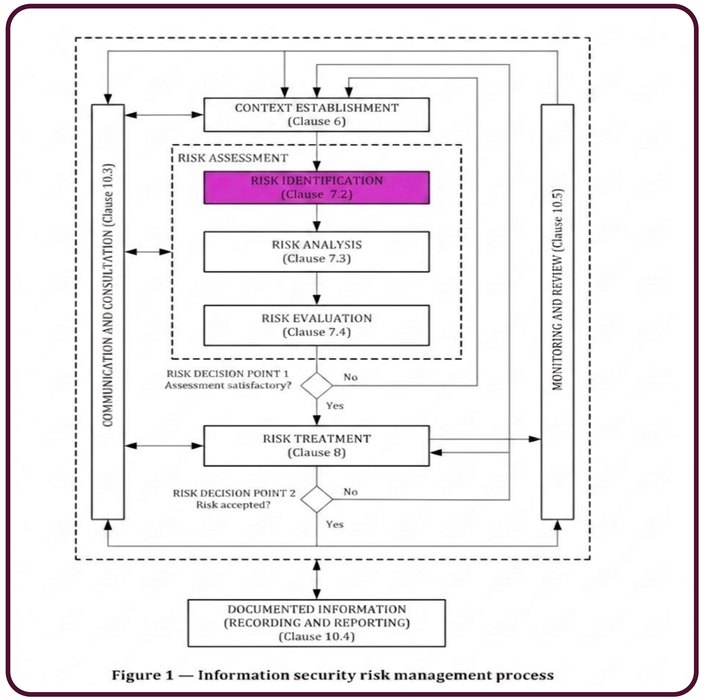


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.2 Identificación del riesgo de seguridad de la información

-Identificación de amenazas: Determinar qué cosas pueden dañar esos activos (ej. software malicioso, incendios, errores humanos).

-Identificación de vulnerabilidades: Encontrar las debilidades existentes en los activos o en los controles actuales (ej. falta de parches de seguridad, ausencia de capacitación).

🧨En las versiones anteriores de la norma, la lista extensa y detallada de amenazas y vulnerabilidades típicas (como fuego, fallos de hardware, malware, espionaje, etc.) se encontraba en el **Anexo C** (específicamente la Tabla C.1). El Anexo B se utilizaba para la identificación de activos.

En la versión actual ISO/IEC 27005:2022, ocurrió un cambio radical con respecto a los anexos: los anexos viejos (de la A a la F) fueron eliminados y condensados en un solo y único anexo llamado Anexo A.

La tabla del anexo C de la versión anterior es totalmente válida y perfectamente utilizable en la práctica, pero con una condición importante: debes usarla como una línea base inicial y no como un catálogo definitivo o cerrado, ¿por qué pasó esto? El comité de la ISO la eliminó de la versión 2022 para evitar que la norma quedará obsoleta ante el rápido avance de la tecnología, metodológicamente esa lista sigue siendo un excelente punto de partida.

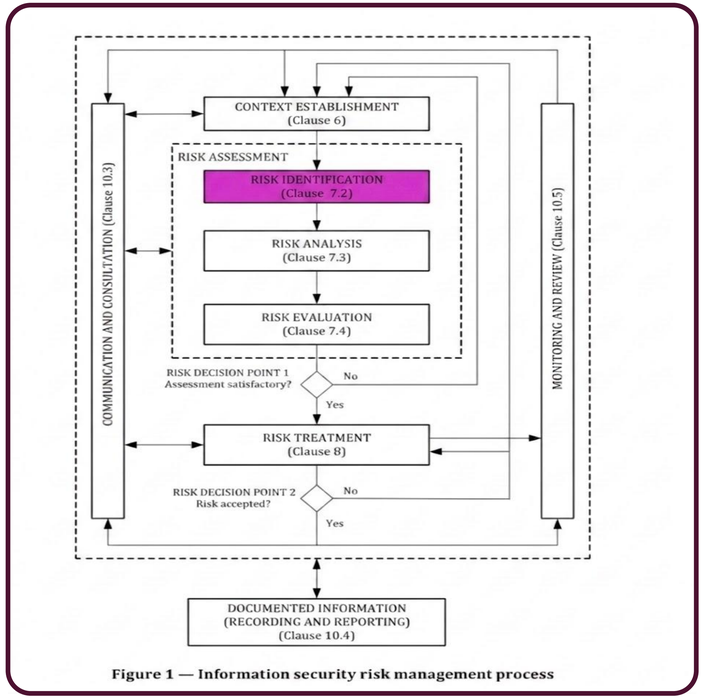


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.2 Identificación del riesgo de seguridad de la información

AMENAZAS TIC	
Interceptación	COMPROMISO DE LA INFORMACIÓN
Espionaje	
Pérdida / Hurto de medios o equipos	
Recuperación de medios	
Divulgación	
Fuentes de datos no confiables	
Incumplimiento obligaciones legales	
Detección de ubicación	
Abuso tecnológico, Operaciones indebidas con los equipos y aplicativos.	ACCIONES NO AUTORIZADAS
Uso no autorizado del equipo	
Copia del software	
Uso de software ilegal	
Corrupción base de los datos	
Procesamiento ILEGAL de datos	
Error en el uso / bloqueo equipo	COMPROMISO DE LAS FUNCIONES
Abuso de los derechos	
Incumpimiento de terceros	
Suplantación de identidad	
Incumpimiento de funciones	
DDOS	ATAQUES INFORMÁTICOS
Cross Site Scripting (XSS)	
Inyección SQL	
Desbordamiento de buffer	
Fuerza Bruta	
Exploits	
Malware	
Puertas traseras	
Ciberestafas	
Energia electrica	PERDIDA DE SERVICIOS ESCENCIALES
Agua o atre acondicionado	
Falla de la RED	

VULNERABILIDADES
Falta de segregación de roles
Configuracion incorrecta de sistemas de información
Falta de capacitacion de usuarios
Vulnerabilidades de dia cero
Fallas por falta de capacitación operadores
Enfermedades
Fallas por actualizaciones
Desconocimiento de herramientas
Falta de compromiso de la alta direccion
Ausencia de estándares para definir criterios o tipología de eventos que podrían generar riesgos a la seguridad de la red del cliente.
La persona no identifica un ataque en la red
Incapacidad de ejecución de tareas por el desequilibrio de carga laboral y/o gestión de capacidad (por tiempo).
Ausencia de un estándar de desarrollo que permita elegir los nuevos comportamientos a detectar por medio del IDS o de escaneo inicial realizado en el proceso de registro.
NO se detectan dispositivos con fallas físicas o de configuración
Errores en configuración que no permiten encendido remoto

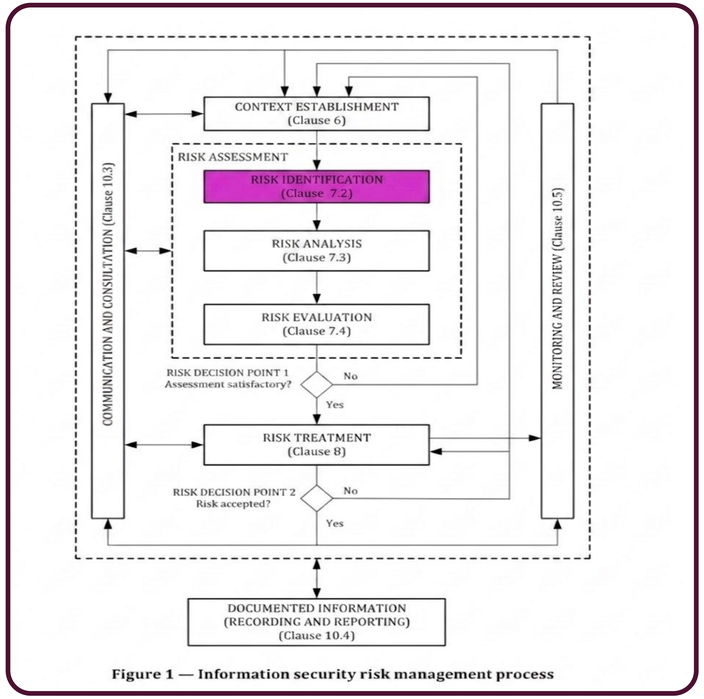


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.2 Identificación del riesgo de seguridad de la información

3. Salida (Output): El resultado directo de esta subcláusula es una lista detallada de los riesgos identificados antes de ser medidos. Para cada riesgo, la salida debe incluir:

-Una descripción clara del escenario de riesgo.

-Los activos involucrados (directa o indirectamente).

-Las consecuencias potenciales o el tipo de impacto en el negocio.

-Las fuentes del riesgo, amenazas o vulnerabilidades asociadas que lo hacen posible.

🔍 En resumen: La Cláusula 7.2 es la fase de "lluvia de ideas técnica e investigación". Su meta es poner sobre la mesa todos los peligros potenciales que acechan a la información de la organización, utilizando ya sea una perspectiva macro (escenarios de eventos) o una perspectiva micro (activos, amenazas y vulnerabilidades), preparando el terreno para calcular qué tan graves son en la siguiente fase (Análisis).

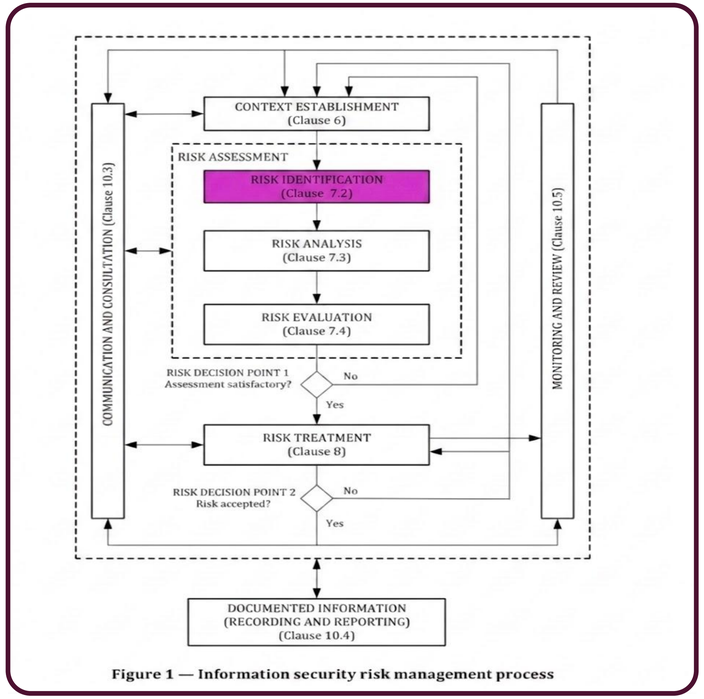


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.2 Identificación del riesgo de seguridad de la información

3. Salida (Output): El resultado directo de esta subcláusula es una lista detallada de los riesgos identificados antes de ser medidos. Para cada riesgo, la salida debe incluir:

-Una descripción clara del escenario de riesgo.

-Los activos involucrados (directa o indirectamente).

-Las consecuencias potenciales o el tipo de impacto en el negocio.

-Las fuentes del riesgo, amenazas o vulnerabilidades asociadas que lo hacen posible.

ESCENARIO	PROBABILIDAD		IMPACTO OPERACIÓN		Riesgo P*Impacto
EVENTO NATURAL -- INFORM. FÍSICA 1	Muy poco probable	1	Sin impacto	1	1
EVENTO NATURAL -- INFORM. FÍSICA 2	Muy poco probable	1	Sin impacto	1	1
EVENTO NATURAL -- REDES	Poco probable	2	Muy bajo	2	4
EVENTO NATURAL -- EQUIPO DE CÓMPUTO	Muy poco probable	1	Muy bajo	2	2
PERDIDA DE SERVICIOS ESCENCIALES -- REDES	Poco probable	3	Muy bajo	2	4
PERDIDA DE SERVICIOS ESCENCIALES -- SERVIDOR LOCAL	Probable	3	Muy bajo	2	6
PERDIDA DE SERVICIOS ESCENCIALES -- EQUIPO DE CÓMPUTO	Probable	3	Muy bajo	2	6
FALLAS TECNICAS -- DOMINA DIGITAL F_E	Poco probable	2	Alto	5	10
FALLAS TECNICAS -- SOFTWARE GESTION F_E	Poco probable	2	Alto	5	10
FALLAS TECNICAS -- REDES	Poco probable	2	Muy bajo	2	4
FALLAS TECNICAS -- SERVIDOR LOCAL	Poco probable	2	Muy bajo	2	4
FALLAS TECNICAS -- EQUIPO DE COMPUTO	Poco probable	2	Muy bajo	2	4
FALLAS TECNICAS -- EQUIPO MÓVIL	Poco probable	2	Muy bajo	2	4
DAÑO FÍSICO -- INFORM. FÍSICA 1	Muy poco probable	1	Sin impacto	1	1
DAÑO FÍSICO -- INFORM. FÍSICA 2	Muy poco probable	1	Sin impacto	1	1
DAÑO FÍSICO -- REDES	Muy poco probable	1	Muy bajo	2	2
DAÑO FÍSICO -- SERVIDOR LOCAL	Poco probable	2	Muy bajo	2	4
DAÑO FÍSICO -- EQUIPO DE COMPUTO	Poco probable	2	Muy bajo	2	4
DAÑO FÍSICO -- EQUIPO MÓVIL	Poco probable	2	Muy bajo	2	4

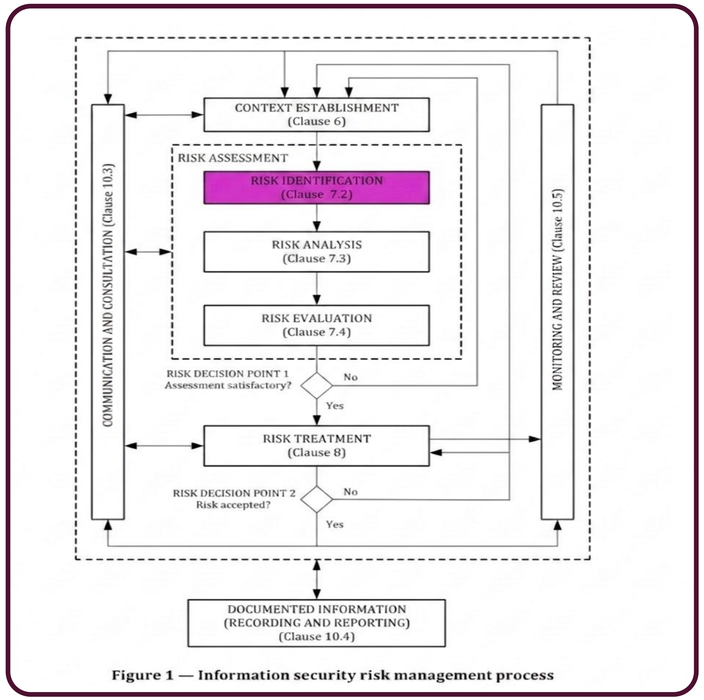


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.3 Análisis del riesgo de seguridad de la información

- **7.3.1 Generalidades (Generalities):** Esta subcláusula establece el marco metodológico para llevar a cabo el análisis. Define los tres elementos rectores del proceso:

  -Entrada (Input): La lista de los riesgos de seguridad de la información identificados (producida en la cláusula 7.2) junto con sus causas y consecuencias potenciales.

  -**Acción (Action):** Consiste en introducir la medición del riesgo. Especifica que la organización debe seleccionar un método de análisis que puede ser cualitativo, semicuantitativo o cuantitativo (o una combinación de estos). El análisis debe enfocarse en modelar cómo interactúan las fuentes de riesgo, las amenazas y las vulnerabilidades para generar un impacto real en el negocio.

  -Salida (Output): Información detallada sobre las consecuencias y probabilidades de los escenarios de riesgo analizados, preparando los datos necesarios para calcular el nivel final.

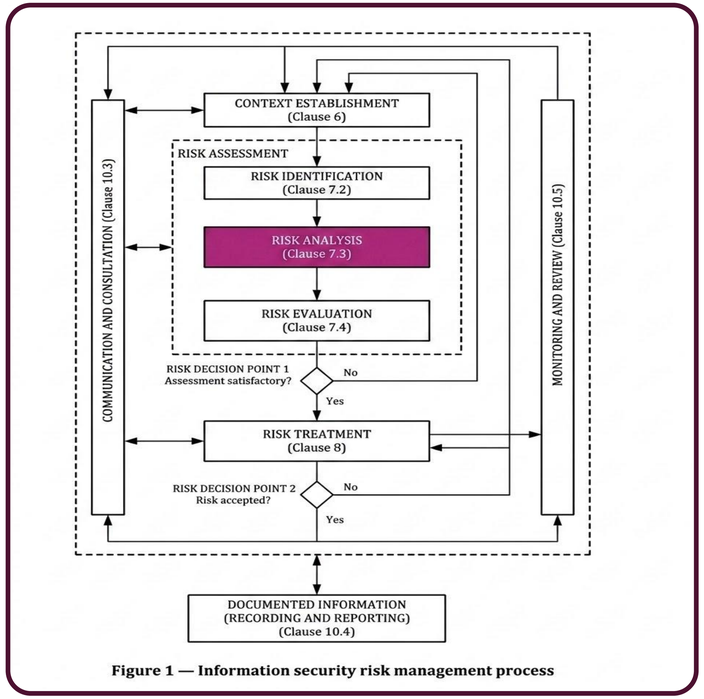


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.3 Análisis del riesgo de seguridad de la información

- **7.3.2 Evaluación de las consecuencias potenciales (Assessment of potential consequences)**

(Relacionada de forma directa con la ISO/IEC 27001:2022, apartado 6.1.2 d) 1)

Entradas (Inputs):

-Escenarios de riesgo identificados.

-Criterios de impacto al negocio preestablecidos.

-Acciones (Actions): Estimar la magnitud del daño que causaría la materialización del escenario sobre la Confidencialidad, Integridad y Disponibilidad (CID) de la información.

-Traducir el daño en impactos específicos del negocio (pérdidas financieras, sanciones legales, interrupción operativa o daño reputacional).

-Desencadenadores (Triggers): La asignación de un nuevo escenario desde la fase de identificación.

-Cambios en la criticidad o valor de los activos de información y procesos de negocio.

-Modificaciones en el entorno regulatorio, legal o contractual (ej. nuevas leyes de privacidad que eleven las multas potenciales).

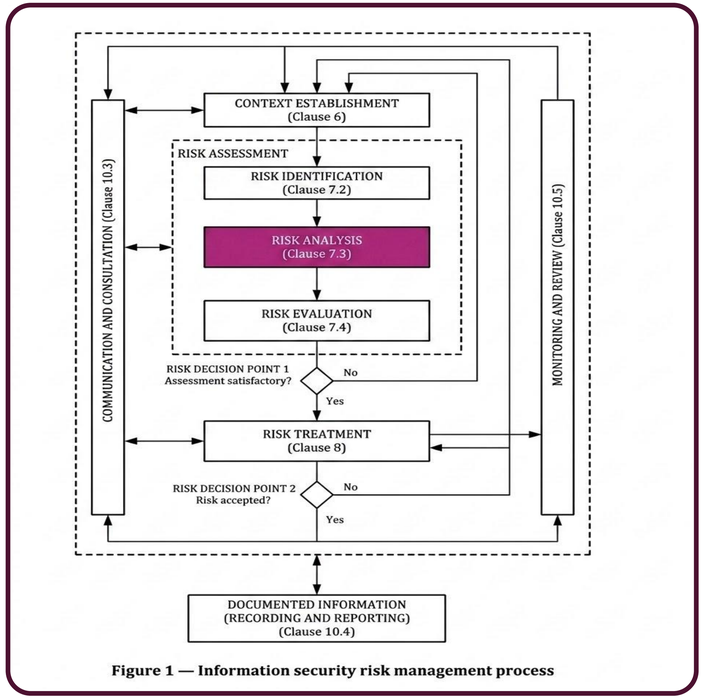


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.3 Análisis del riesgo de seguridad de la información

- **7.3.4 Determinación de los niveles de riesgo (Determination of the level of risk)**

Entradas (Inputs): Los valores específicos de consecuencia (7.3.2) y probabilidad (7.3.3) asignados a cada escenario.

-La matriz, fórmula o regla lógica de combinación definida por la organización.

Acciones (Actions): Combinar formalmente la probabilidad y la consecuencia utilizando la metodología de la organización.

-Asignar un nivel de riesgo definitivo a cada escenario (ej. Crítico, Alto, Medio, Bajo).

Desencadenadores (Triggers): La finalización y actualización de los cálculos de consecuencia y probabilidad para un escenario de riesgo.

-Cambios o recalibraciones estructurales en los criterios de combinación aprobados por la alta dirección (si se modifica la matriz institucional, se dispara este paso para actualizar todo el inventario).

-Salida (Output): El Registro de Riesgos Analizados, el cual actúa como la entrega final lista para ser evaluada contra el apetito de riesgo en la fase de Valoración (7.4).

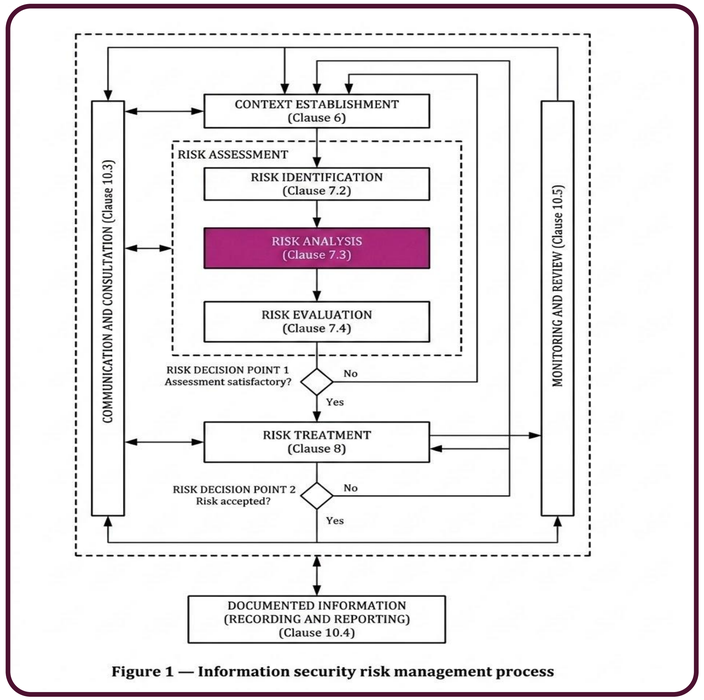


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.4 Valoración del riesgo de seguridad de la información

- **7.4.1 Comparación de los resultados del análisis de riesgos con los criterios de riesgo**

Entradas (Inputs):

-El Registro de Riesgos Analizados (de la Cláusula 7.3.4) con sus respectivos niveles calculados (Crítico, Alto, Medio, Bajo).

-Los Criterios para la aceptación del riesgo establecidos en el contexto (Cláusula 6.4.4) que marcan el Apetito de Riesgo.

Acciones (Actions):

-Contrastar el nivel de cada riesgo estimado contra las líneas umbral de aceptación predefinidas.

-Discriminar de forma preliminar cuáles escenarios caen en la zona "tolerable" (riesgo aceptado) y cuáles entran en la zona "inaceptable" (riesgo que requiere mitigación).

Desencadenadores (Triggers): La obtención o actualización de los niveles de riesgo calculados para uno o más escenarios en la fase de determinación (7.3.4).

Cambios o ajustes en la estrategia del negocio que obliguen a revisar la tolerancia al riesgo de la empresa.

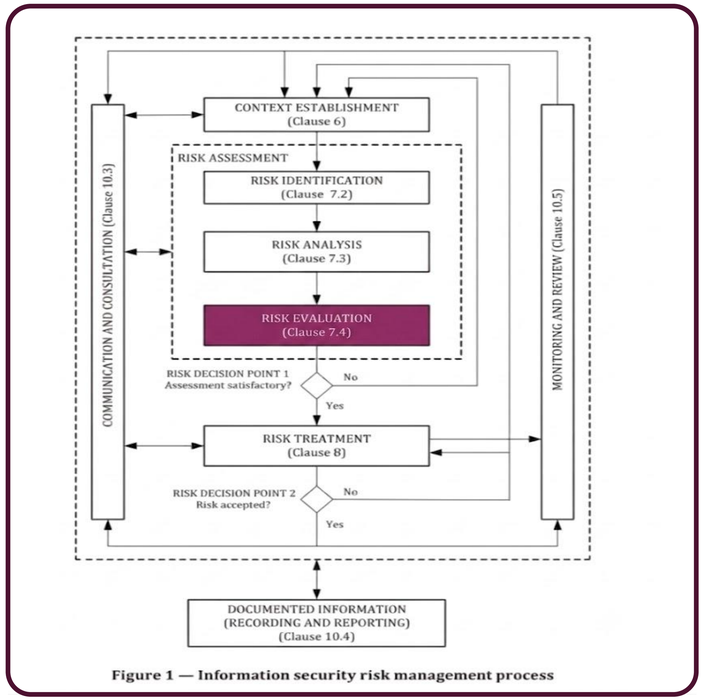


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.4 Valoración del riesgo de seguridad de la información

- **7.4.2 Consideraciones para la toma de decisiones (Decision-making considerations)**

Entradas (Inputs):

-El listado preliminar de riesgos que superan los criterios de aceptación.

-El contexto legal, presupuestario, operativo y los objetivos de negocio de la organización.

Acciones (Actions):

-Analizar las implicaciones estratégicas de cada riesgo. La norma señala que la dirección puede ponderar factores más allá de la fórmula matemática antes de aprobar un gasto, evaluando si el costo de los controles supera el valor del activo o si tratar el riesgo destruye una oportunidad valiosa de negocio.

-Asegurar y documentar la justificación formal de los riesgos que se decida retener (asumir), obteniendo la aprobación y firma explícita del Propietario del Riesgo (Risk Owner).

Desencadenadores (Triggers):

-La presencia de riesgos severos cuya mitigación técnica resulta extremadamente costosa, compleja o paralizante para la operación del negocio, requiriendo un análisis costo-beneficio.

-Presión o cambios en el entorno regulatorio y legal que exijan atención inmediata sobre ciertos riesgos específicos, independientemente de su valor matemático en la matriz.

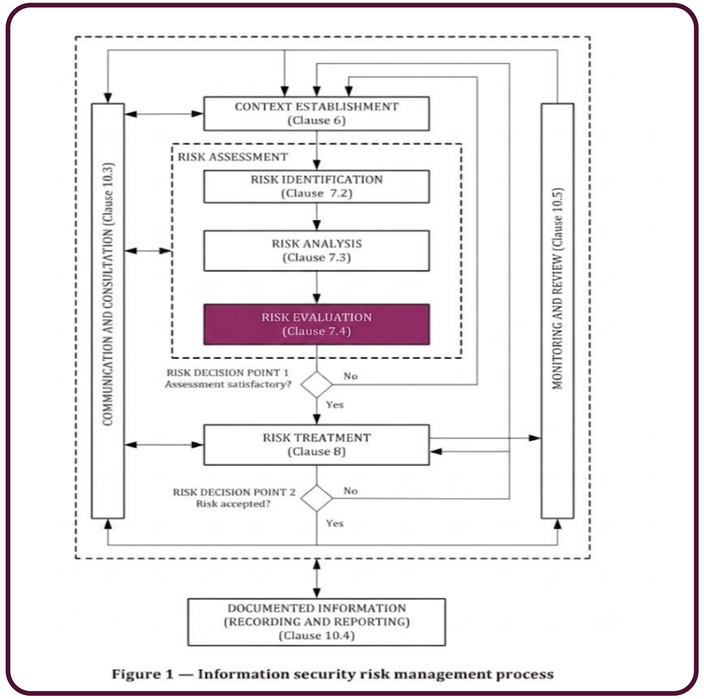


Figure 1 — Information security risk management process

7. Proceso de evaluación del riesgo de S.I.

Cláusula 7.4 Valoración del riesgo de seguridad de la información

Salida del Subproceso 7.4 (Output)

El entregable resultante es la Lista Priorizada de Riesgos de Seguridad de la Información, formalmente aprobada por los tomadores de decisiones. Este documento segmenta con claridad los riesgos que la empresa asume formalmente y aquellos riesgos validados como "inaceptables" que se transfieren en orden de prioridad a la Cláusula 8: Proceso de tratamiento del riesgo.

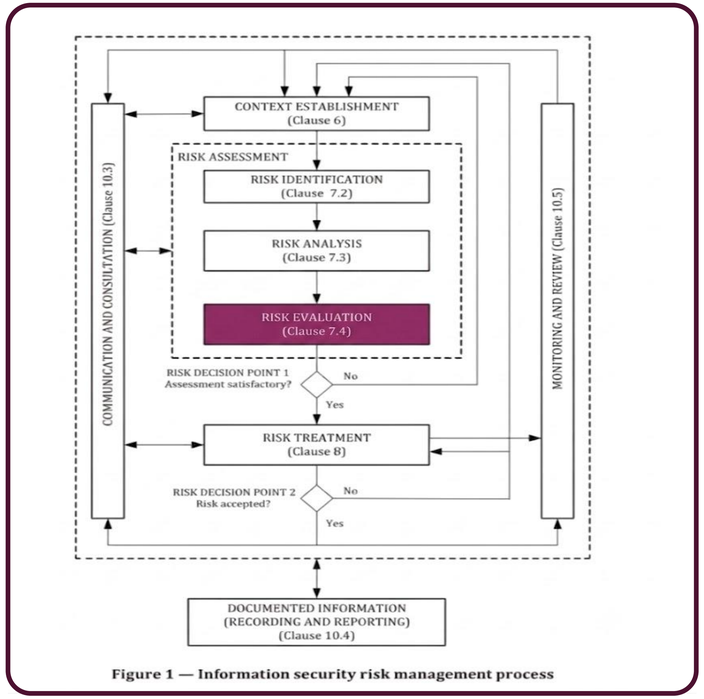


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

8.1 Generalidades

Esta fase se encarga de tomar todos los riesgos que en la etapa de valoración (7.4) fueron declarados como "inaceptables" y definir la estrategia para responder a ellos. Su objetivo es seleccionar e implementar las medidas necesarias para llevar el riesgo a un nivel tolerable para la organización.

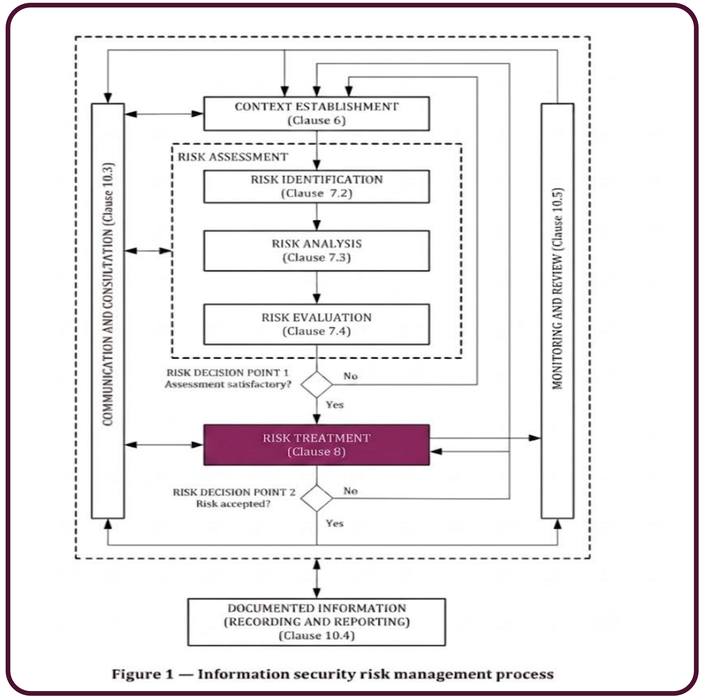


Figure 1 — Information security risk management process

Entradas (Inputs):

-La Lista Priorizada de Riesgos de la etapa de valoración (7.4).

-El inventario de los controles de seguridad de la información existentes y su estado de eficacia.

Acciones (Actions):

-Planificar y ejecutar de manera sistemática los cuatro subprocesos del tratamiento del riesgo: selección de opciones (8.2), diseño del plan (8.3), propuesta de controles (8.4) y aceptación del riesgo residual (8.5).

-Garantizar que el tratamiento esté alineado con los objetivos del negocio y los requisitos de las partes interesadas.

Desencadenadores (Triggers):

-La identificación de uno o más riesgos de seguridad de la información que superan los criterios de aceptación de la organización.

-Cambios en la disponibilidad de recursos (financieros o tecnológicos) que permitan abordar riesgos antes postergados.

8. Proceso de tratamiento del riesgo de S.I.

8.2 Selección de las opciones de tratamiento del riesgo (Selection of risk treatment options)

-**Entradas (Inputs):**

-Los escenarios de riesgo específicos que requieren tratamiento.

-Los criterios de riesgo y las políticas organizacionales.

Acciones (Actions):

-Seleccionar una o más de las siguientes opciones de tratamiento para cada riesgo:

-Reducción del riesgo (Mitigación): Aplicar controles de seguridad para disminuir la probabilidad, el impacto o ambos (ej. instalar un firewall).

-**Retención del riesgo (Asumir):** Aceptar el riesgo si entra en el apetito de riesgo o si su mitigación es inviable, siempre con justificación del Risk Owner.

-Evitación del riesgo: Eliminar la actividad o tecnología que causa el riesgo (ej. cerrar un servicio digital muy vulnerable).

-Compartir el riesgo ~~(Transferir)~~: Pasar parte del riesgo a un tercero mediante seguros de ciberriesgo o subcontratación de proveedores especializados.

⚠️ Nota crítica de alineación con ISO 27001: En seguridad de la información, la responsabilidad última sobre **un riesgo nunca se transfiere ni se externaliza.** El Risk Owner (dueño del riesgo) de la organización siempre sigue siendo el responsable ante el negocio y ante el comité si algo sale mal.

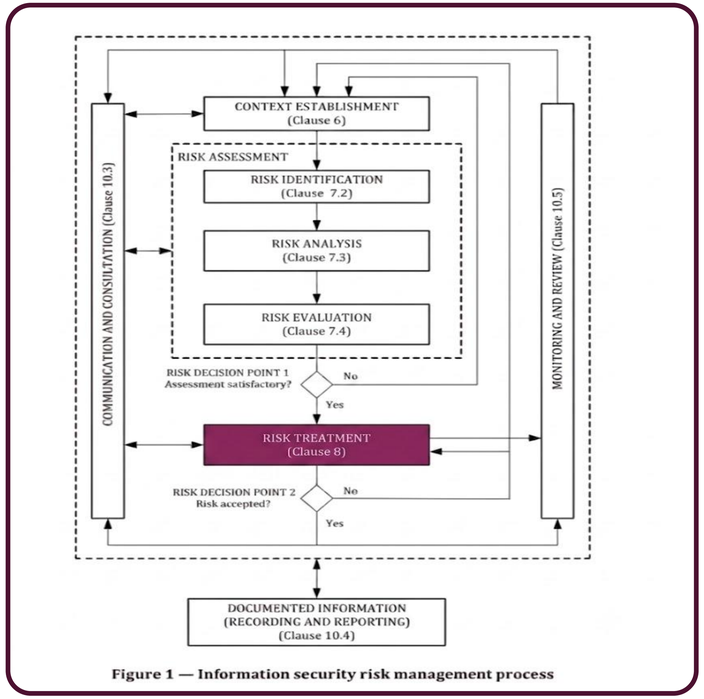


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

8.2 Selección de las opciones de tratamiento del riesgo (Selection of risk treatment options)

⚠️ CUIDADO con el acrónimo 🏁 **META** 🏁: El acrónimo META (originalmente popularizado en marcos como COBIT o la gestión de proyectos) divide las opciones de tratamiento de la siguiente manera:

-Mitigar (Reducir el riesgo mediante controles).

-Evitar (Eliminar la actividad que genera el riesgo).

-Transferir (Tercerizar la operación o el impacto financiero).

-Aceptar (Retener el riesgo residual de forma consciente).

🧨El peligro latente: La trampa de la "T" (Transferir)

La T de Transferir es el punto más crítico y donde fallan la mayoría de las **implementaciones** de ISO 27001 si no se interpreta correctamente:

-El error común: Pensar que "Transferir" significa "Le pago a AWS (Amazon Web Services) o a un tercero, por lo tanto, si hackean el servidor, el problema/riesgo ya no es mío".

-La realidad bajo ISO 27001: En seguridad de la información, la T debería renombrarse internamente como Tercerizar la operación o Compartir el impacto financiero. El Risk Owner sigue estando sentado dentro de tu empresa.

-El efecto en la matriz: Cuando "transfieres" un riesgo a un proveedor (ej. mudando tus servidores locales a la nube), el riesgo original de infraestructura física disminuye, pero nace un nuevo riesgo inmediato en tu matriz: El riesgo de dependencia de terceros (Supply Chain Risk). Ahora debes aplicar controles del Anexo A (Cláusula 5.19 a 5.23 - Seguridad en las relaciones con proveedores) para auditar a ese tercero.

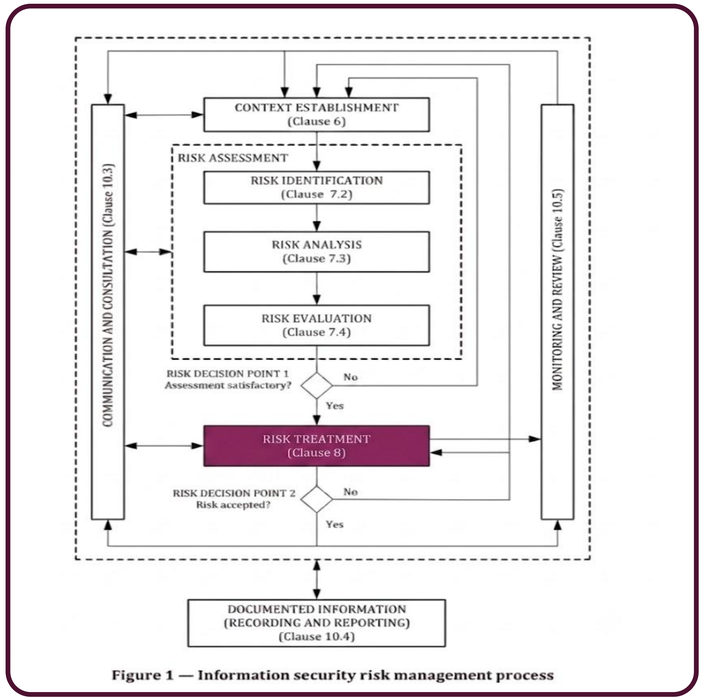


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

8.2 Selección de las opciones de tratamiento del riesgo (Selection of risk treatment options)

💡 La cláusula 6.4 establece los criterios de riesgo, podemos usar la tabla de cruce de impacto contra probabilidad y declarar que tipo de acciones tomar de acuerdo a la calificación asignada

Table E.1 b)

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

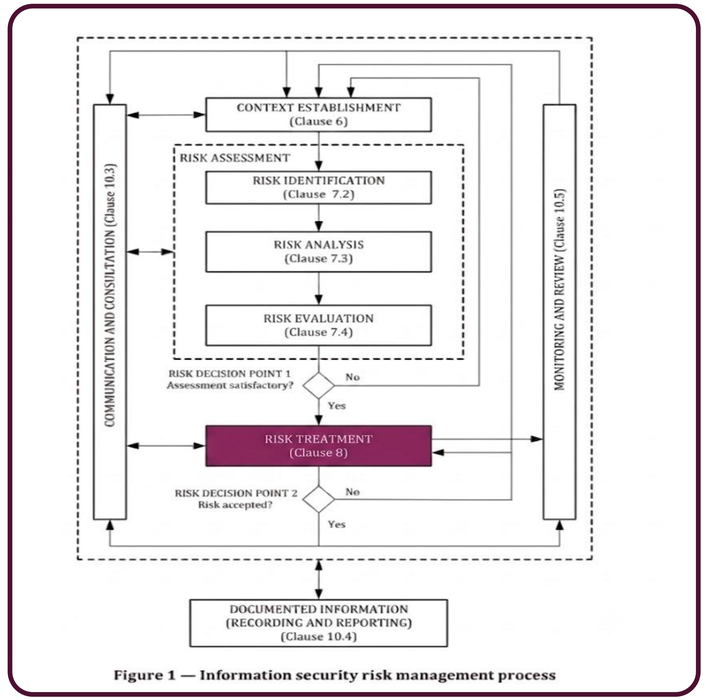


Figure 1 — Information security risk management process

Ejemplo:

De esta manera hacemos más eficientes los recursos asignados (Inversiones).

8. Proceso de tratamiento del riesgo de S.I.

8.3 Determinación de los controles para el tratamiento del riesgo

Una vez que en el subproceso anterior (8.2) se ha elegido la estrategia de Mitigar, la Cláusula 8.3 exige seleccionar las contramedidas específicas que materializan esa decisión. No basta con decir "vamos a mitigar"; aquí se define con qué herramientas, políticas o tecnologías exactas se hará.

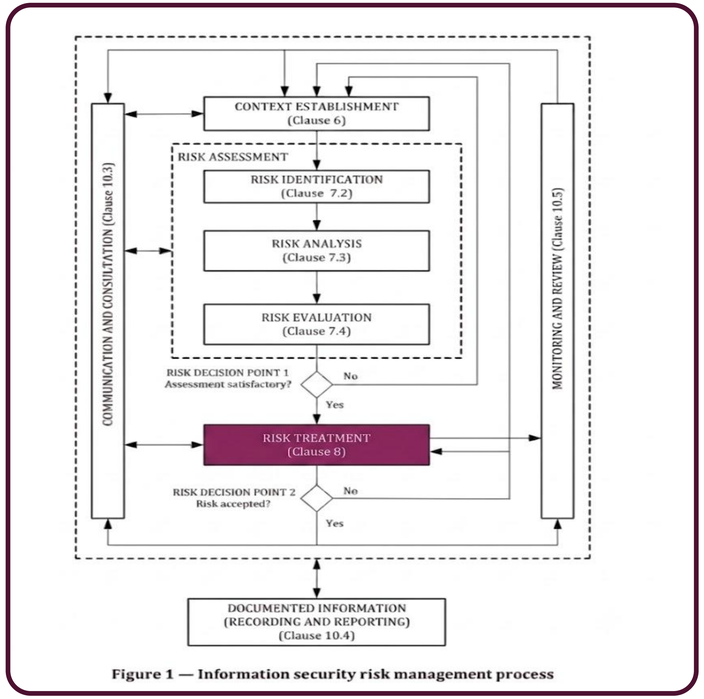


Figure 1 — Information security risk management process

Entradas (Inputs):

-Los escenarios de riesgo específicos cuya opción elegida en la fase 8.2 fue la Mitigación (Reducción del riesgo) o Compartir (Tercerización).

-El conjunto de controles propuestos por el Anexo A de la ISO/IEC 27001:2022 (los 93 controles divididos en las categorías Organizacionales, Personas, Físicos y Tecnológicos).

-Las directrices de implementación detalladas de la ISO/IEC 27002:2022.

Catálogos de controles externos aplicables al sector (ej. NIST SP 800-53, CIS Controls, o normativas legales locales).

Acciones (Actions):

-Selección del set de controles: Determinar qué controles específicos son necesarios para reducir la probabilidad de ocurrencia del escenario de riesgo, mitigar su impacto en el negocio, o ambos.

-Cruce obligatorio con el Anexo A (ISO 27001): La norma exige contrastar los controles seleccionados contra el Anexo A del estándar para asegurar que no se haya omitido ninguna salvaguarda crítica por descuido.

8. Proceso de tratamiento del riesgo de S.I.

8.3 Determinación de los controles para el tratamiento del riesgo

-Consideración de la Inteligencia de Amenazas (Threat Intelligence): Evaluar si los controles seleccionados son realmente efectivos frente a las tácticas modernas que usan los atacantes hoy en día (ligado al control 5.7 de la ISO 27002).

-Análisis de viabilidad técnica y operativa: Asegurar que el control propuesto no altere negativamente la operación del negocio. Un control que vuelve imposible el trabajo diario terminará siendo evadido por los usuarios, anulando su efectividad.

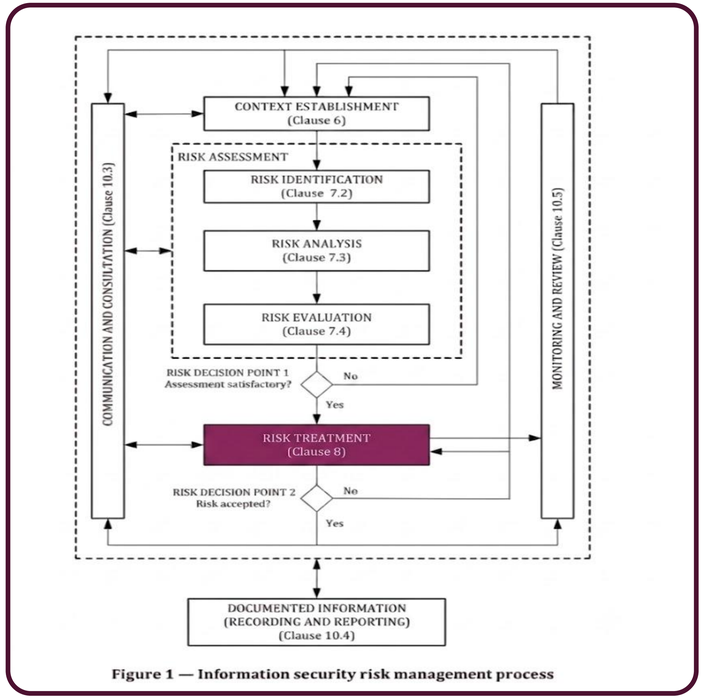


Figure 1 — Information security risk management process

Desencadenadores (Triggers):

-La validación formal y selección de la opción "Mitigar" para un riesgo en el subproceso 8.2.

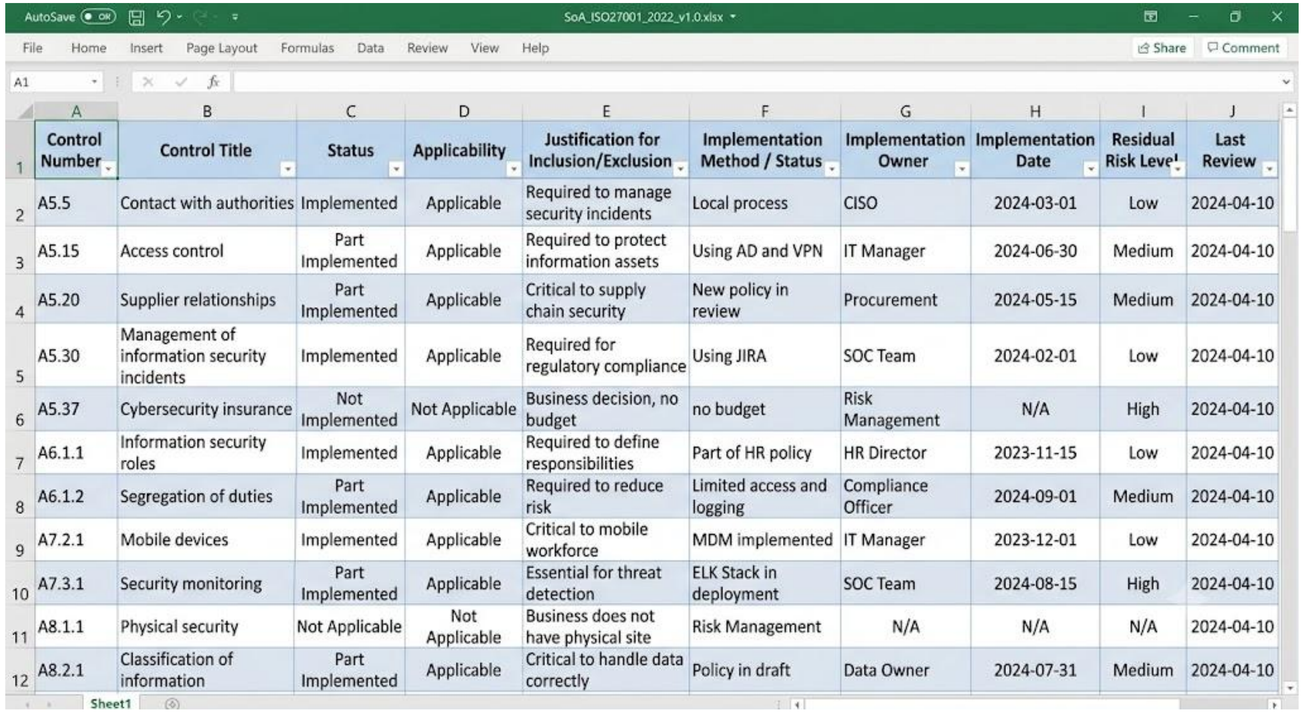
-La identificación de fallos o ineficacia en un control existente durante una auditoría o tras la ocurrencia de un incidente de seguridad, lo que obliga a rediseñar o buscar nuevos controles para ese escenario específico

Salida del Subproceso 8.3 (Output):

El entregable resultante de esta fase es el **Listado de Controles de Seguridad Seleccionados (Puede ser un borrador SOA) para cada riesgo inaceptable.** Este insumo es el que nutrirá directamente la creación del cronograma operativo en la Cláusula 8.4 (Plan de tratamiento del riesgo) y servirá para estructurar la posterior Declaración de Aplicabilidad (SoA) exigida por la certificación ISO 27001.

8. Proceso de tratamiento del riesgo de S.I.

8.3 Determinación de los controles para el tratamiento del riesgo



Control Number	Control Title	Status	Applicability	Justification for Inclusion/Exclusion	Implementation Method / Status	Implementation Owner	Implementation Date	Residual Risk Level	Last Review
A5.5	Contact with authorities	Implemented	Applicable	Required to manage security incidents	Local process	CISO	2024-03-01	Low	2024-04-10
A5.15	Access control	Part Implemented	Applicable	Required to protect information assets	Using AD and VPN	IT Manager	2024-06-30	Medium	2024-04-10
A5.20	Supplier relationships	Part Implemented	Applicable	Critical to supply chain security	New policy in review	Procurement	2024-05-15	Medium	2024-04-10
A5.30	Management of information security incidents	Implemented	Applicable	Required for regulatory compliance	Using JIRA	SOC Team	2024-02-01	Low	2024-04-10
A5.37	Cybersecurity insurance	Not Implemented	Not Applicable	Business decision, no budget	no budget	Risk Management	N/A	High	2024-04-10
A6.1.1	Information security roles	Implemented	Applicable	Required to define responsibilities	Part of HR policy	HR Director	2023-11-15	Low	2024-04-10
A6.1.2	Segregation of duties	Part Implemented	Applicable	Required to reduce risk	Limited access and logging	Compliance Officer	2024-09-01	Medium	2024-04-10
A7.2.1	Mobile devices	Implemented	Applicable	Critical to mobile workforce	MDM implemented	IT Manager	2023-12-01	Low	2024-04-10
A7.3.1	Security monitoring	Part Implemented	Applicable	Essential for threat detection	ELK Stack in deployment	SOC Team	2024-08-15	High	2024-04-10
A8.1.1	Physical security	Not Applicable	Not Applicable	Business does not have physical site	Risk Management	N/A	N/A	N/A	2024-04-10
A8.2.1	Classification of information	Part Implemented	Applicable	Critical to handle data correctly	Policy in draft	Data Owner	2024-07-31	Medium	2024-04-10

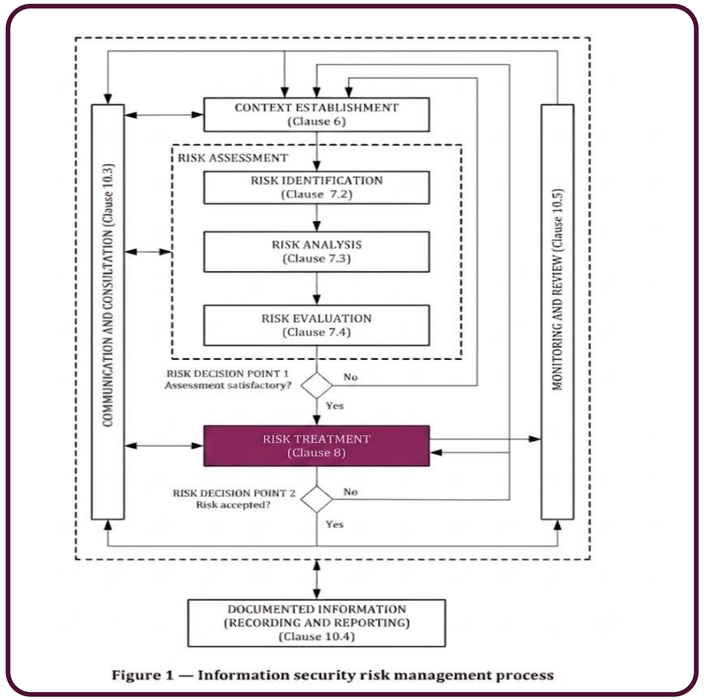


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

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

El propósito de esta subcláusula es actuar como una red de seguridad (sanity check). Asegura que los controles técnicos u operativos que la organización eligió en la 8.3 sean validados contra las mejores prácticas internacionales del Anexo A para garantizar que no se haya olvidado ninguna protección crítica.

Entradas (Inputs):

-La lista de controles específicos determinados en la Cláusula 8.3 (las contramedidas que el equipo técnico propuso para mitigar los riesgos).

-La lista completa y oficial de los 93 controles del Anexo A de la ISO/IEC 27001:2022.

Acciones (Actions):

-Cotejo exhaustivo: Cruzar la lista de controles propios (8.3) contra los 93 controles de la norma para verificar cuáles coinciden y cubren las expectativas del estándar.

-Identificación de brechas (Gap Analysis): Detectar si hay controles del Anexo A que son necesarios para la organización pero que se omitieron durante el análisis de riesgos técnico de la 8.3 (ej. descubrir que se planificó un firewall, pero se olvidó el control del Anexo A para la gestión de bitácoras/logs).

-Validación de exclusiones preliminares: Comenzar a marcar qué controles del Anexo A definitivamente no aplican bajo ninguna circunstancia a los riesgos identificados de la empresa.

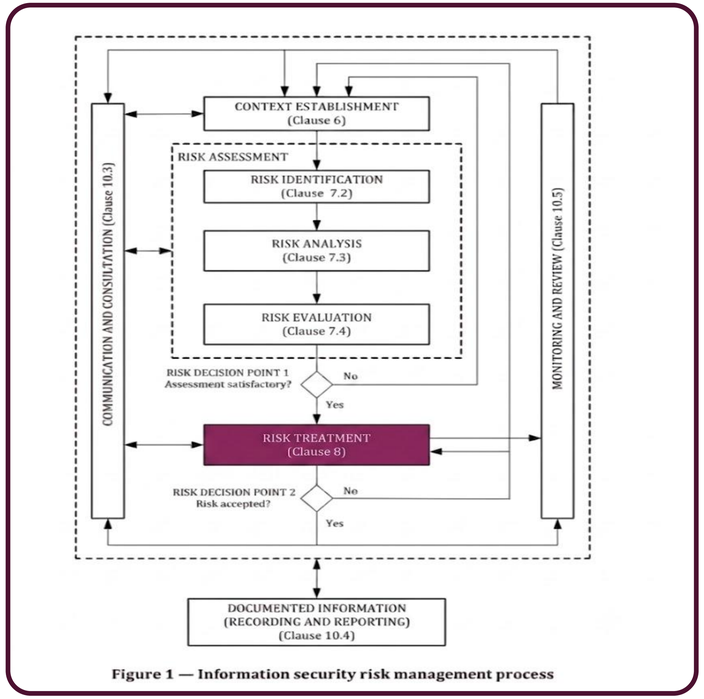


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

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

Desencadenadores (Triggers):

-La finalización de la determinación de controles en la 8.3 (tan pronto tienes tu lista de soluciones técnicas, se dispara esta comparación obligatoria).

-Actualizaciones en el alcance del SGSI o revisiones de la norma que introduzcan nuevos controles de referencia.

Salida (Output):

La Matriz de Conciliación de Controles, que es el mapeo directo entre las necesidades particulares de la empresa y la estructura del Anexo A. Este insumo es la materia prima directa e indispensable que usará la Cláusula 8.5 para poder redactar el SoA.

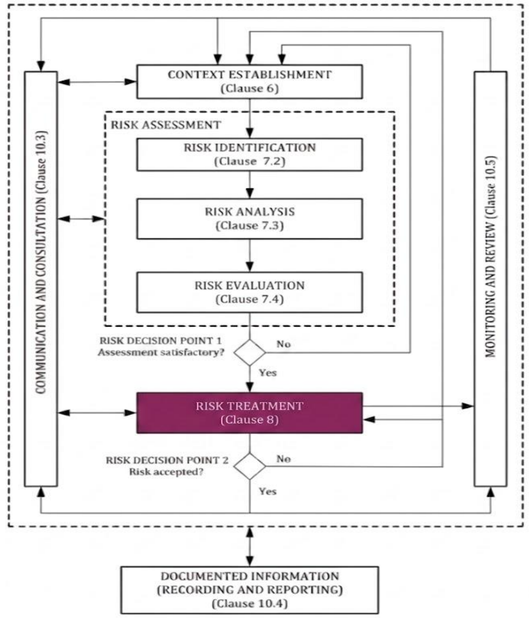


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

8.5 Producción de una Declaración de Aplicabilidad

Entradas (Inputs):

-El Plan de Tratamiento de Riesgos (PTR) finalizado (de la Cláusula 8.4), que detalla los controles específicos seleccionados para mitigar los riesgos inaceptables.

-La lista completa de los 93 controles del Anexo A de la ISO/IEC 27001:2022.

- Los requisitos legales, regulatorios, estatutarios y contractuales identificados en el contexto de la organización (Cláusula 6).

Acciones (Actions):

-Mapeo y Comparación: Contrastar uno a uno los controles seleccionados en el plan de tratamiento contra los 93 controles del Anexo A de la ISO/IEC 27001:2022.

-Declaración de Inclusión/Exclusión: Determinar explícitamente para cada control del Anexo A si es Aplicable o No Aplicable para la organización.

-Redacción de Justificaciones: Para los controles incluidos: Justificar por qué son necesarios (ej. "Requisito para mitigar el riesgo R01" o "Obligatorio por ley de protección de datos").

-Para los controles excluidos: Justificar detalladamente por qué no se aplican (ej. "No aplicable porque la organización no realiza desarrollo de software propio").

-Verificación del Estado actual: Indicar el estado real de cada control dentro de la empresa (ej. Implementado, Parcialmente implementado o Planificado).

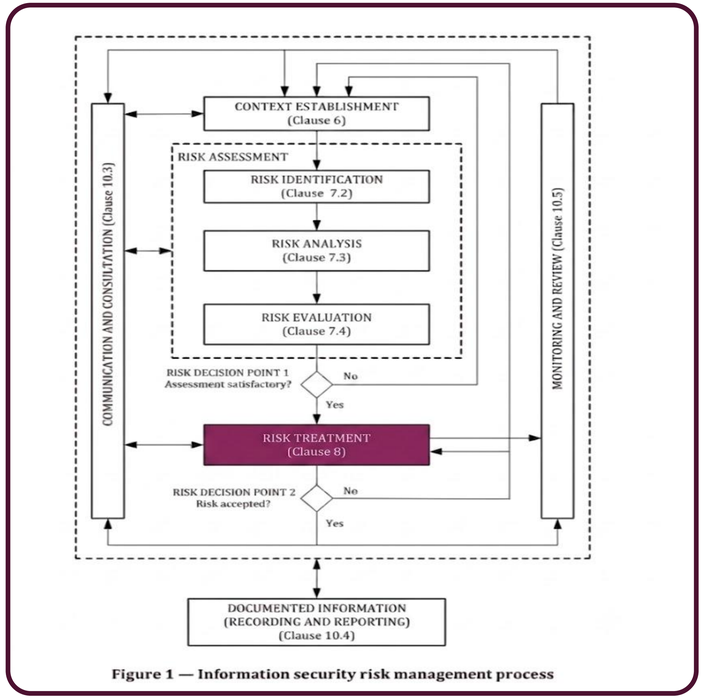


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

8.5 Producción de una Declaración de Aplicabilidad

Desencadenadores (Triggers):

-La culminación del diseño del Plan de Tratamiento de Riesgos (8.4), lo que significa que ya se sabe exactamente qué controles se van a implementar, mejorar o mantener.

-Cambios en el Anexo A del estándar o actualizaciones en el inventario de riesgos que obliguen a revisar qué controles aplican y cuáles no.

Salida (Output):

El documento **final** de la Declaración de Aplicabilidad (SoA) **aprobado**. Este entregable resume la postura de control de la organización y es el puente mandatorio para la auditoría de certificación bajo la ISO/IEC 27001.

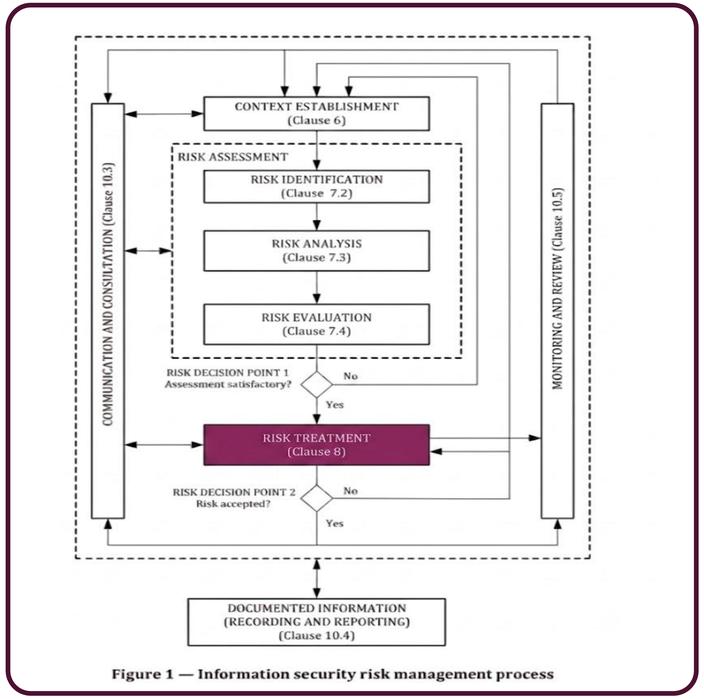


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

8.6 Plan de tratamiento del riesgo de seguridad de la información

Entradas (Inputs):

-El SoA (Declaración de Aplicabilidad) estructurado y validado (de la Cláusula 8.5).

-Las estimaciones de los Niveles de Riesgo Residual asociados a cada escenario.

-La disponibilidad presupuestaria, recursos tecnológicos y asignación de personal de la organización.

Acciones (Actions):

-Asignación Operativa de Responsabilidades: Designar formalmente a los ejecutores técnicos (líderes de proyecto, administradores de sistemas, etc.) que implementarán o mantendrán cada control específico del plan.

-Establecimiento de Calendarios y Hitos (8.6.2): Fijar fechas límite (deadlines) concretas y realistas para el despliegue de cada salvaguarda.

-Asignación de Recursos Financieros y Humanos: Documentar el presupuesto aprobado y las horas-hombre requeridas para cada iniciativa de seguridad.

-Gobernanza y Aceptación Formal del Riesgo Residual (8.6.3): Presentar el panorama de riesgos remanentes ante los Propietarios del Riesgo (Risk Owner) y la Alta Dirección. La acción crítica aquí es obtener su firma formal de aprobación. Al firmar este plan (8.6), los Risk Owners asumen oficialmente la responsabilidad corporativa sobre los riesgos residuales que persistirán en la empresa.

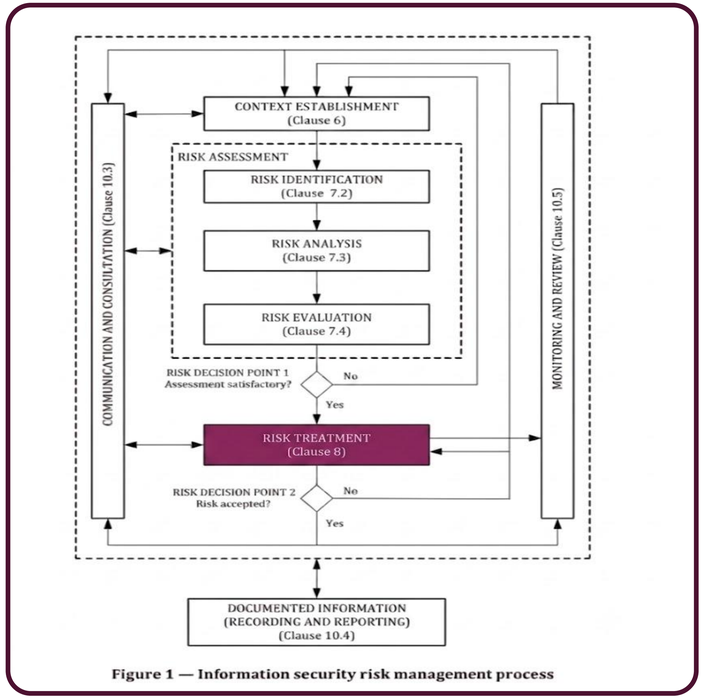


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

8.6 Plan de tratamiento del riesgo de seguridad de la información

Desencadenadores (Triggers):

-La finalización y estructuración completa de la Declaración de Aplicabilidad (8.5).

-La necesidad de iniciar formalmente las inversiones financieras y la ejecución de los proyectos de ciberseguridad.

-Revisiones del comité de dirección ante desviaciones de tiempos o recursos en controles previamente planificados.

Salida (Output):

El Plan de Tratamiento de Riesgos (PTR) Oficial, Firmado y Aprobado. Este documento es la evidencia reina solicitada por los auditores de certificación de la ISO 27001 para validar que la dirección lidera activamente la gestión del riesgo y que el presupuesto de seguridad está justificado metodológicamente.

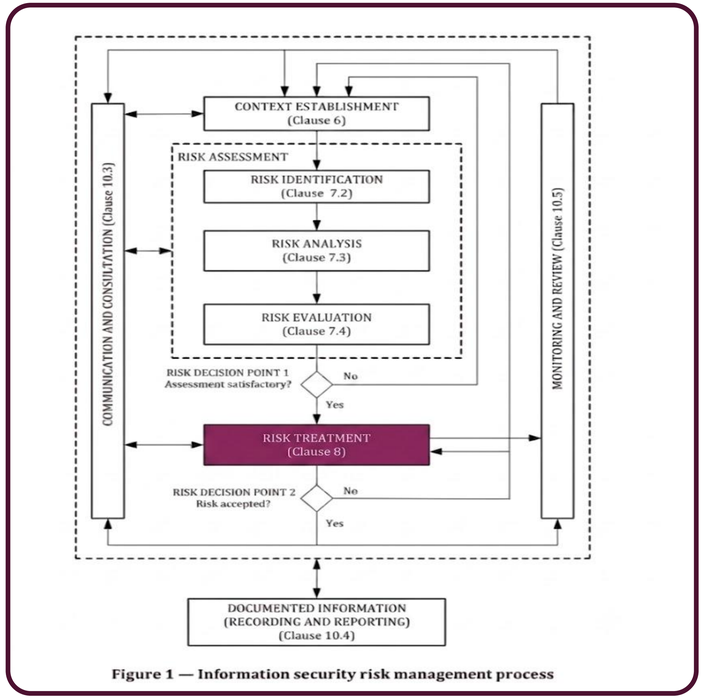
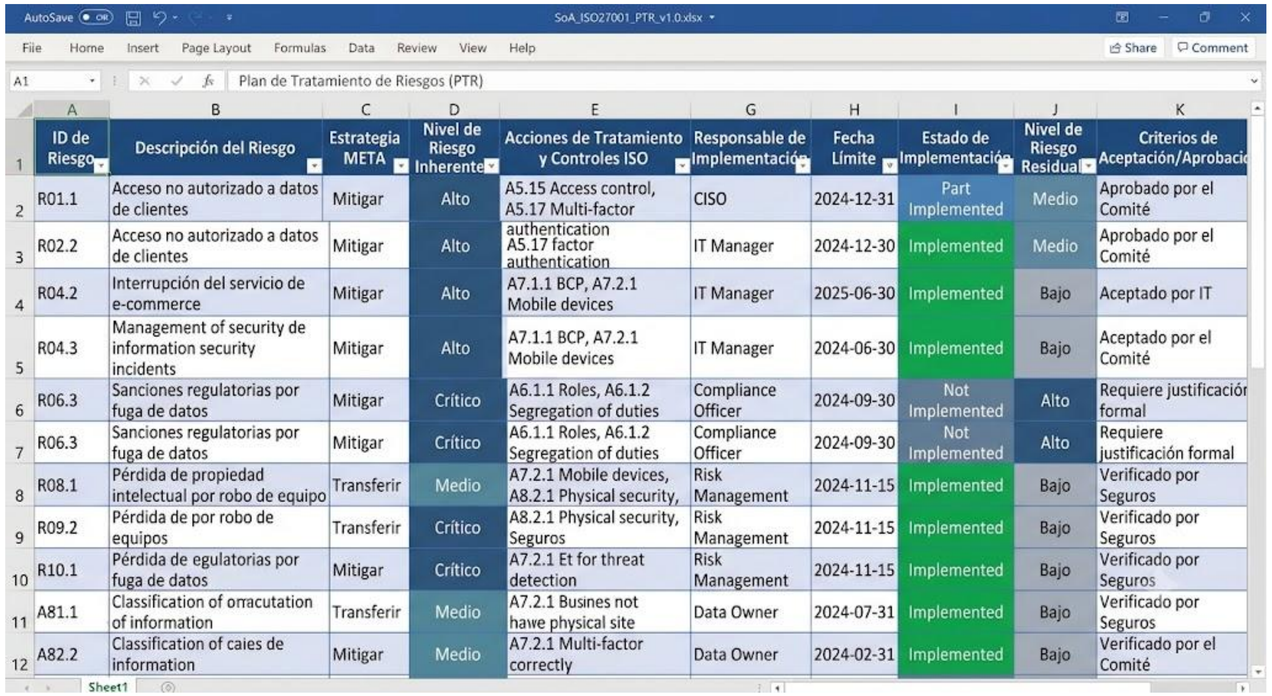


Figure 1 — Information security risk management process

8. Proceso de tratamiento del riesgo de S.I.

8.6 Plan de tratamiento del riesgo de seguridad de la información



AutoSave | SoA_ISO27001_PTR_v1.0.xlsx

File Home Insert Page Layout Formulas Data Review View Help | Share | Comment

A1 | Plan de Tratamiento de Riesgos (PTR)

ID de Riesgo	Descripción del Riesgo	Estrategia META	Nivel de Riesgo Inherente	Acciones de Tratamiento y Controles ISO	Responsable de Implementación	Fecha Límite	Estado de Implementación	Nivel de Riesgo Residual	Criterios de Aceptación/Aprobaci
R01.1	Acceso no autorizado a datos de clientes	Mitigar	Alto	A5.15 Access control, A5.17 Multi-factor	CISO	2024-12-31	Part Implemented	Medio	Aprobado por el Comité
R02.2	Acceso no autorizado a datos de clientes	Mitigar	Alto	authentication A5.17 factor authentication	IT Manager	2024-12-30	Implemented	Medio	Aprobado por el Comité
R04.2	Interrupción del servicio de e-commerce	Mitigar	Alto	A7.1.1 BCP, A7.2.1 Mobile devices	IT Manager	2025-06-30	Implemented	Bajo	Aceptado por IT
R04.3	Management of security de information security incidents	Mitigar	Alto	A7.1.1 BCP, A7.2.1 Mobile devices	IT Manager	2024-06-30	Implemented	Bajo	Aceptado por el Comité
R06.3	Sanciones regulatorias por fuga de datos	Mitigar	Crítico	A6.1.1 Roles, A6.1.2 Segregation of duties	Compliance Officer	2024-09-30	Not Implemented	Alto	Requiere justificación formal
R06.3	Sanciones regulatorias por fuga de datos	Mitigar	Crítico	A6.1.1 Roles, A6.1.2 Segregation of duties	Compliance Officer	2024-09-30	Not Implemented	Alto	Requiere justificación formal
R08.1	Pérdida de propiedad intelectual por robo de equipo	Transferir	Medio	A7.2.1 Mobile devices, A8.2.1 Physical security,	Risk Management	2024-11-15	Implemented	Bajo	Verificado por Seguros
R09.2	Pérdida de por robo de equipos	Transferir	Crítico	A8.2.1 Physical security, Seguros	Risk Management	2024-11-15	Implemented	Bajo	Verificado por Seguros
R10.1	Pérdida de egulatorias por fuga de datos	Mitigar	Crítico	A7.2.1 Et for threat detection	Risk Management	2024-11-15	Implemented	Bajo	Verificado por Seguros
A81.1	Classification of orracutation of information	Transferir	Medio	A7.2.1 Busines not have physical site	Data Owner	2024-07-31	Implemented	Bajo	Verificado por Seguros
A82.2	Classification of caies de information	Mitigar	Medio	A7.2.1 Multi-factor correctly	Data Owner	2024-02-31	Implemented	Bajo	Verificado por el Comité

Sheet1

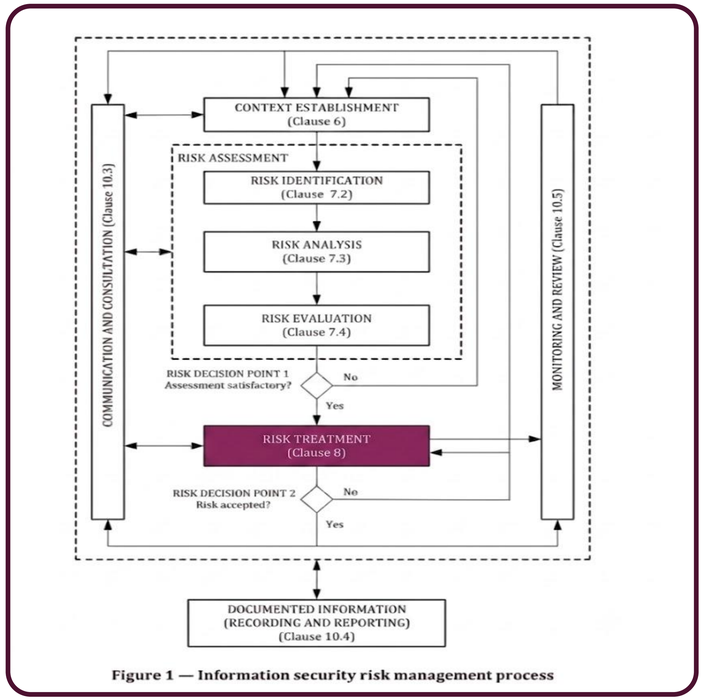


Figure 1 — Information security risk management process

9. Operación

9.1 Ejecución del proceso de valoración del riesgo de seguridad de la información

NOTA: Esta subcláusula se relaciona directamente con el requisito **8.2 de la ISO/IEC 27001:2022.**

Este es el punto donde la teoría del contexto y los criterios definidos previamente se ponen en marcha. Es la ejecución operativa para identificar, analizar y evaluar los riesgos reales sobre los activos de información de la empresa.

- **Entradas (Inputs):**
  - -Documentos sobre el proceso de valoración del riesgo (la metodología definida en las cláusulas previas).
  - -El inventario de activos de información, los dueños de los procesos (Risk Owner) y el alcance del SGSI.
  - -Información sobre el entorno de amenazas actualizado y las vulnerabilidades tecnológicas u organizacionales conocidas.

- **Acciones (Actions):**
  - -Identificación del Riesgo: Descubrir, reconocer y describir los riesgos que podrían causar la pérdida de confidencialidad, integridad o disponibilidad de la información.
  - -Análisis del Riesgo: Estimar las consecuencias potenciales (Impacto) y la posibilidad real de ocurrencia (Probabilidad) de los escenarios identificados, utilizando los criterios establecidos.
  - -Evaluación del Riesgo: Comparar los resultados del análisis numérico o cualitativo contra los criterios de aceptación del riesgo (por ejemplo, tu tabla de cruce 0-2, 3-5, 6-9) para determinar qué riesgos requieren tratamiento prioritario y cuáles pueden ser aceptados.

9. Operación

9.1 Ejecución del proceso de valoración del riesgo de seguridad de la información

- **Desencadenadores (Triggers):**

  -La planificación del ciclo anual de gestión de riesgos dentro del SGSI.

  -Cambios significativos en la infraestructura, procesos de negocio o regulaciones de la organización que obliguen a realizar una valoración de impacto.

  -La solicitud formal del comité de seguridad tras la aparición de nuevas amenazas críticas globales.

- Salida (Output):

El Listado/Matriz de Riesgos Valorados y Priorizados. Este entregable contiene la foto real del estado de los riesgos de la empresa (Riesgo Inherente) y es el insumo operativo mandatorio que se transferirá a la siguiente fase del bloque de Operación (el proceso de tratamiento de riesgos ligado a la 8.3 de la ISO 27001).

9. Operación

9.2 Ejecución del proceso de tratamiento del riesgo de seguridad de la información

Entradas (Inputs):

-El Listado/Matriz de Riesgos Valorados y Priorizados generado en la fase anterior (Cláusula 9.1).

-La metodología institucional y los criterios de tratamiento definidos en la Cláusula 8 (las opciones META).

-El catálogo de controles del Anexo A de la ISO/IEC 27001:2022 y las guías de la ISO/IEC 27002.

Acciones (Actions):

-Seleccionar las Opciones de Tratamiento (META): Determinar formalmente qué camino se tomará para cada riesgo inaceptable (Mitigar, Evitar, Transferir o Aceptar bajo justificación).

-Determinar y Comparar Controles (Alineación 8.3 y 8.4): Seleccionar las salvaguardas técnicas u organizacionales necesarias y cruzarlas minuciosamente contra los 93 controles del Anexo A de la ISO 27001 para asegurar una cobertura normativa total.

-Estructurar y Formalizar el SoA y el PTR (Alineación 8.5 y 8.6): Documentar las justificaciones de inclusión/exclusión en la Declaración de Aplicabilidad y vaciar el plan en un cronograma de proyectos real, asignando presupuestos, responsables técnicos y fechas límite.

-Validación del Riesgo Residual: Asegurar que, tras simular la aplicación de las acciones planificadas, el riesgo remanente baje a los niveles tolerables por la organización (ej. llevarlo a la zona 0-2 de aceptación).

Salida (Output):

El conjunto de Artefactos de Tratamiento Operativos Aprobados (SoA finalizado y el Plan de Tratamiento de Riesgos firmado por los Risk Owners). Esta salida es la evidencia reina que demuestra que la organización no solo sabe qué le duele (9.1), sino que ha puesto en marcha la maquinaria operativa (9.2) para proteger sus activos críticamente.

10. Aprovechamiento de los procesos relacionados del SGSI

10.1 Contexto de la organización

El propósito de la Cláusula 10.1 es actuar como un lazo de retroalimentación interna. Explica cómo la información viva que se obtiene al operar y tratar los riesgos (en el Capítulo 9) debe regresar al Contexto de la Organización (vinculado a la Cláusula 4 de la ISO/IEC 27001) para actualizar la visión estratégica de la empresa. El contexto no es estático; muta con cada riesgo analizado.

Entradas (Inputs):

-Los resultados actualizados de la valoración y tratamiento de riesgos (Cláusula 9).

-El inventario de nuevas amenazas del entorno, cambios tecnológicos o nuevas regulaciones de cumplimiento aplicables al sector.

-La definición previa del alcance del SGSI y los objetivos de negocio de la empresa.

Acciones (Actions):

-Retroalimentación del Contexto Interno/Externo: Utilizar los hallazgos operativos de los riesgos para modificar o enriquecer el análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas) o PESTEL de la organización.

-Ajuste del Alcance del SGSI: Evaluar si los riesgos identificados en la operación demuestran que el alcance actual de la certificación es insuficiente y requiere ser ampliado (ej. descubrir riesgos críticos en un proveedor en la nube que originalmente se dejó fuera del alcance).

-Alineación con las Partes Interesadas: Utilizar la información de los riesgos para actualizar las expectativas y necesidades de seguridad de los clientes, socios de negocio y entes reguladores (Cláusula 4.2 de la ISO 27001).

10. Aprovechamiento de los procesos relacionados del SGSI

10.1 Contexto de la organización

Desencadenadores (Triggers):

-La detección de riesgos críticos repetitivos o sistemáticos en la Cláusula 9 que evidencian que el contexto externo o interno de la empresa ha cambiado profundamente.

-Fusiones, adquisiciones, lanzamiento de nuevas líneas de negocio o migración masiva a nuevas tecnologías (como la adopción de IA corporativa).

-La revisión anual del alcance del Sistema de Gestión de Seguridad de la Información.

Salida (Output):

Actualización documentada del Contexto y Alcance del SGSI. Esta salida es el insumo que regresa a la Alta Dirección para demostrar que el sistema es dinámico, asegurando que las bases estratégicas de la empresa (Cláusula 4 de la ISO 27001) estén perfectamente alineadas con la realidad de los riesgos que se viven en el día a día operativo.

10. Aprovechamiento de los procesos relacionados del SGSI

10.2 Liderazgo y compromiso

El propósito de la Cláusula 10.2 es potenciar el rol de la Alta Dirección. La norma explica que el proceso de riesgos es la herramienta principal que tiene la dirección para demostrar su liderazgo real. No se trata solo de que firmen políticas por cumplir, sino de que utilicen la información de los riesgos para tomar decisiones estratégicas, asignar recursos de forma eficiente (tal como planteaste al inicio con tu tabla de criterios 0-2, 3-5, 6-9) y asegurar que el SGSI logre los resultados previstos.

Entradas (Inputs):

-Los informes ejecutivos del estado actual de los riesgos y el Plan de Tratamiento de Riesgos (PTR) consolidado (Cláusula 9.2).

-La política de seguridad de la información de la organización.

-Las métricas sobre el desempeño y la eficacia del SGSI (Cláusula 10 de la 27001).

Acciones (Actions):

-Integración del Riesgo en la Estrategia: Asegurar que los objetivos de gestión de riesgos de seguridad de la información estén alineados con los objetivos estratégicos globales del negocio.

-Aseguramiento de Recursos: Utilizar la matriz de criterios de riesgo para autorizar y proveer los recursos financieros, humanos y tecnológicos necesarios para ejecutar el Plan de Tratamiento.

-Promoción de la Mejora Continua: Dirigir y apoyar a las personas para que contribuyan a la eficacia del proceso de riesgos, promoviendo una cultura organizacional consciente de las amenazas.

-Asignación de Roles y Autoridades: Apoyar a otros roles gerenciales pertinentes (como los Risk Owner) para demostrar su propio liderazgo aplicado a sus áreas de responsabilidad.

10. Aprovechamiento de los procesos relacionados del SGSI

10.2 Liderazgo y compromiso

Desencadenadores (Triggers):

-La planeación del presupuesto anual de la organización donde la dirección debe asignar los recursos financieros a seguridad.

-La escalación de un riesgo crítico que no puede ser mitigado por los equipos técnicos y requiere una decisión de negocio al más alto nivel.

-La revisión formal del SGSI por la dirección (Management Review).

Salida (Output):

Evidencias de Dirección Estratégica basada en Riesgos (actas de asignación presupuestaria firmadas, minutas de aprobación del PTR por la junta directiva y directrices organizacionales explícitas sobre el apetito de riesgo). Esta salida es la prueba contundente ante un auditor de que la Alta Dirección ejerce un liderazgo activo y no es un actor pasivo en el sistema.

10. Aprovechamiento de los procesos relacionados del SGSI

10.3 Comunicación y consulta

Su propósito en esta sección específica es servir de puente operativo con las actividades de Comunicación (Cláusula 7.4 de la ISO/IEC 27001:2022), garantizando que el flujo de información sobre los riesgos y los controles no se quede estancado y se comparta de manera adecuada con las partes interesadas internas y externas.

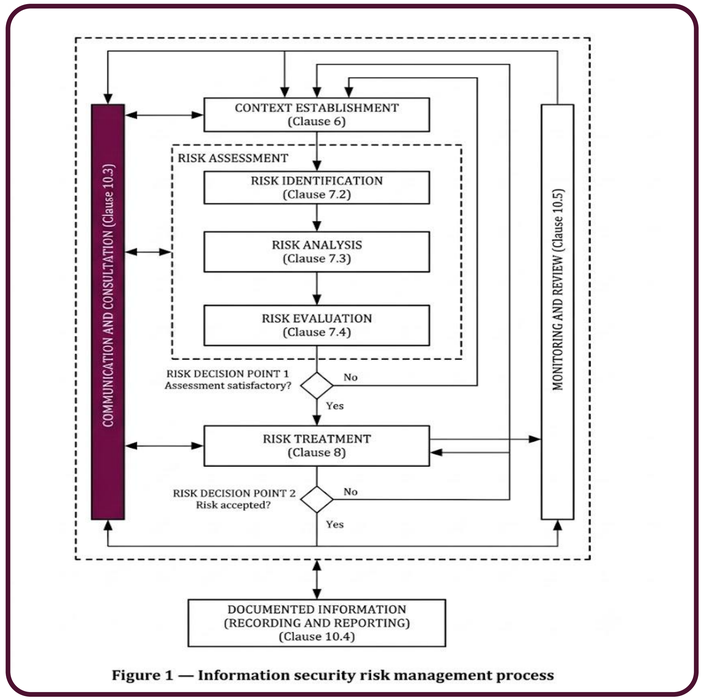


Figure 1 — Information security risk management process

Entradas (Inputs):

-Los resultados de la valoración de riesgos (9.1) y el Plan de Tratamiento (9.2) aprobados.

-El inventario de partes interesadas (internas como empleados y directivos; externas como clientes, proveedores y entes reguladores).

-Los canales oficiales de comunicación de la organización (comités, correos).

Acciones (Actions):

-Establecer el Flujo Informativo del Riesgo: Definir con claridad qué información sobre los riesgos se va a compartir, cuándo es oportuno hacerlo, a quién va dirigida y a través de qué medios, asegurando la confidencialidad de los datos sensibles del análisis.

-Consultas e Involucramiento Bidireccional: Realizar mesas de trabajo con los dueños de los procesos (Risk Owner) para acordar la viabilidad operativa de los controles antes de su despliegue, evitando imponer medidas de seguridad de forma aislada.

-Reporte a la Alta Dirección: Traducir las métricas técnicas de riesgo a un lenguaje financiero y de negocio para presentar el estado del SGSI de forma clara ante el comité de dirección, facilitando la toma de decisiones estratégicas.

10. Aprovechamiento de los procesos relacionados del SGSI

10.3 Comunicación y consulta

Desencadenadores (Triggers):

-La aprobación o actualización formal de la Declaración de Aplicabilidad (SoA) o el Plan de Tratamiento de Riesgos (PTR).

-La necesidad de coordinar acciones técnicas de mitigación con un proveedor crítico debido a un riesgo compartido en la cadena de suministro.

-La ocurrencia de un incidente de seguridad de la información que obligue a activar canales de consulta o notificación externa de emergencia.

Salida (Output):

Evidencias del Proceso de Comunicación y Consulta de Riesgos (minutas de comités de seguridad, registros de notificaciones a proveedores, reportes ejecutivos de riesgos distribuidos a la dirección). Este entregable cubre de forma directa los requisitos de comunicación exigidos en la auditoría de la ISO 27001.

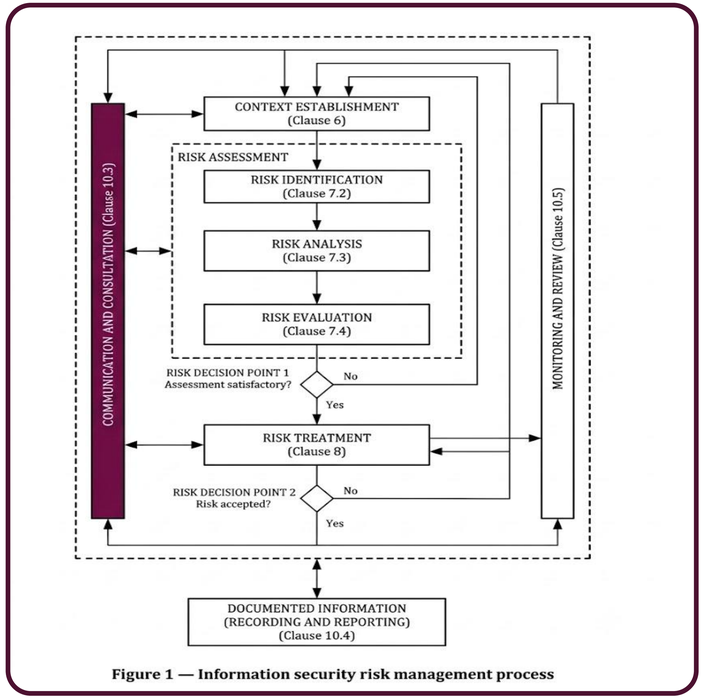


Figure 1 — Information security risk management process

10. Aprovechamiento de los procesos relacionados del SGSI

10.4 Información documentada

El propósito de la Cláusula 10.4 es establecer el control de calidad y la trazabilidad de los artefactos de riesgo. La norma señala que no basta con hacer análisis de riesgos en pizarrones o archivos temporales; todo el proceso (criterios, valoraciones, planes de tratamiento, SoA) debe estar debidamente controlado, protegido contra modificaciones no autorizadas, versionado y disponible para cuando el sistema de gestión lo requiera (como en las auditorías).

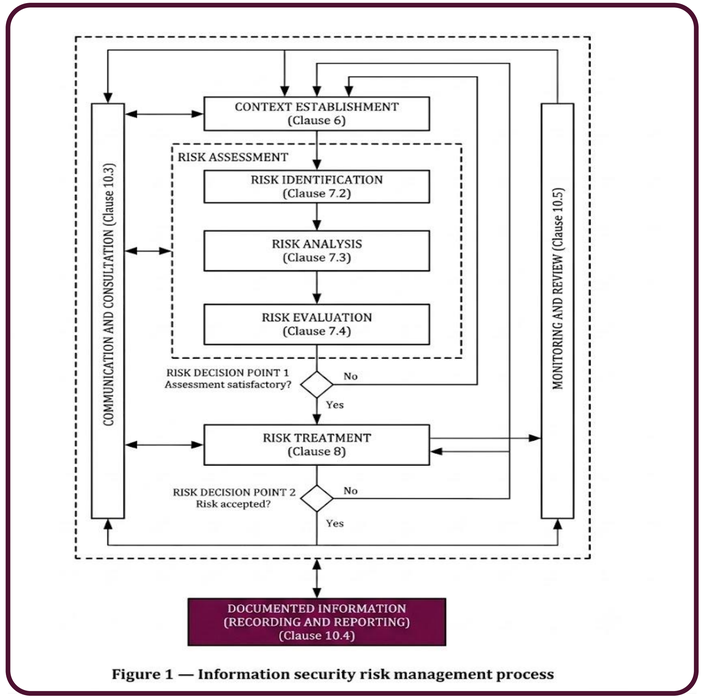


Figure 1 — Information security risk management process

- **10.4.1 Generalidades (General)**

  NOTA: Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 7.5.

  ISO/IEC 27001 especifica los requisitos para que las organizaciones conserven información documentada relativa a:

  -El proceso de valoración del riesgo (ver ISO/IEC 27001:2022, 6.1.2) y sus resultados (ver ISO/IEC 27001:2022, 8.2);

  El proceso de tratamiento del riesgo (ISO/IEC 27001:2022, 6.1.3) y sus resultados (ISO/IEC 27001:2022, 8.3).

- **10.4.2 Información documentada sobre los procesos:**Esta subcláusula se enfoca en la metodología. La norma exige que las reglas del juego de cómo se gestionan los riesgos en la empresa estén por escrito. No se documentan los riesgos aquí, sino el procedimiento formal que deben seguir los analistas para que la valoración sea repetible, consistente y válida a lo largo del tiempo.

10. Aprovechamiento de los procesos relacionados del SGSI

10.4 Información documentada

Entradas (Inputs):

-Los criterios de riesgo de la organización (definidos en la Cláusula 6), que incluyen los umbrales de impacto, escalas de probabilidad y niveles de riesgo aceptable (como tu tabla 0-2, 3-5, 6-9).

-El enfoque o modelo metodológico seleccionado (cualitativo, cuantitativo o semicuantitativo).

-Roles y responsabilidades asignados dentro del proceso de gestión de riesgos.

Acciones (Actions):

-Redacción del Manual/Procedimiento de Gestión de Riesgos: Documentar formalmente los pasos secuenciales para identificar amenazas, estimar consecuencias y tratar los riesgos.

-Formalizar las Escalas y Formulas: Dejar asentada por escrito la matriz de cálculo (ej. Impacto x Probabilidad) y los criterios exactos para declarar cuándo un riesgo residual requiere tratamiento obligatorio.

-Aprobación del Proceso: Someter el procedimiento metodológico a la revisión y firma del CISO y el comité de seguridad para otorgarle validez institucional.

Desencadenadores (Triggers):

-El diseño inicial o la reestructuración del SGSI.

-Cambios en la estrategia del negocio o en las normativas del sector que obliguen a modificar cómo la empresa define qué es un impacto "Bajo", "Medio" o "Alto".

-Hallazgos en auditorías.

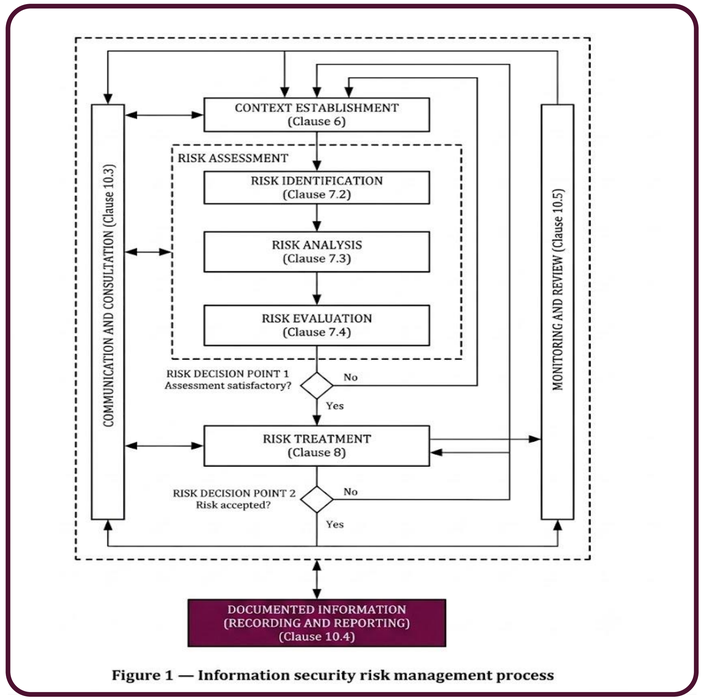


Figure 1 — Information security risk management process

10. Aprovechamiento de los procesos relacionados del SGSI

10.4 Información documentada

Salida (Output):

Metodología / Procedimiento de Gestión de Riesgos de Seguridad de la Información Aprobado. Este es el documento maestro que el auditor revisará para comprobar que la empresa tiene un proceso estructurado bajo la Cláusula 7.5.1 a) de la ISO 27001.

- **10.4.3 Información documentada sobre los resultados (Documented information about results)**

A diferencia de la anterior, esta subcláusula se enfoca en la evidencia viva. Aquí es donde se resguarda el resultado de haber ejecutado la metodología: qué riesgos se encontraron en la vida real, cómo se trataron y qué firmas de responsabilidad se obtuvieron. Es el registro histórico de la postura de seguridad de la empresa.

- **Entradas (Inputs):**
  - -Los datos crudos y conclusiones de la valoración operativa de riesgos (9.1).
  - -Los planes de acción técnicos, cronogramas y asignaciones presupuestarias (9.2 / 8.6).
  - -Las decisiones y firmas de aceptación formal de riesgo residual emitidas por los Risk Owners.

- **Acciones (Actions):**
  - -Consolidar el Registro de Riesgos (Matriz): Documentar los escenarios específicos detectados, sus niveles de riesgo inherente, los controles aplicados y el nivel de riesgo residual calculado.

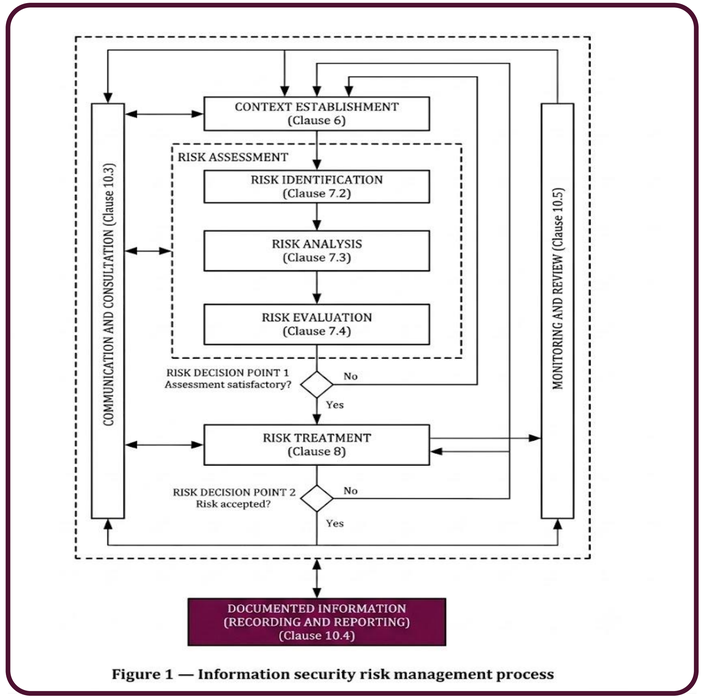


Figure 1 — Information security risk management process

10. Aprovechamiento de los procesos relacionados del SGSI

10.4 Información documentada

-Mantener la Trazabilidad Histórica: Versionar los archivos de resultados para poder demostrar la evolución del riesgo a lo largo de los meses o años.

-Resguardar las Evidencias de Gobernanza: Archivar de forma segura el SoA oficial y el Plan de Tratamiento (PTR) debidamente firmados por la Alta Dirección y los dueños de los procesos.

Salida (Output):

Expediente de Evidencias de Riesgos (Matriz de Riesgos activa, SoA firmado y PTR autorizado). Estas son las salidas definitivas que demuestran la operación real del sistema ante una auditoría de certificación (Cláusula 7.5.1 b) de la ISO 27001).

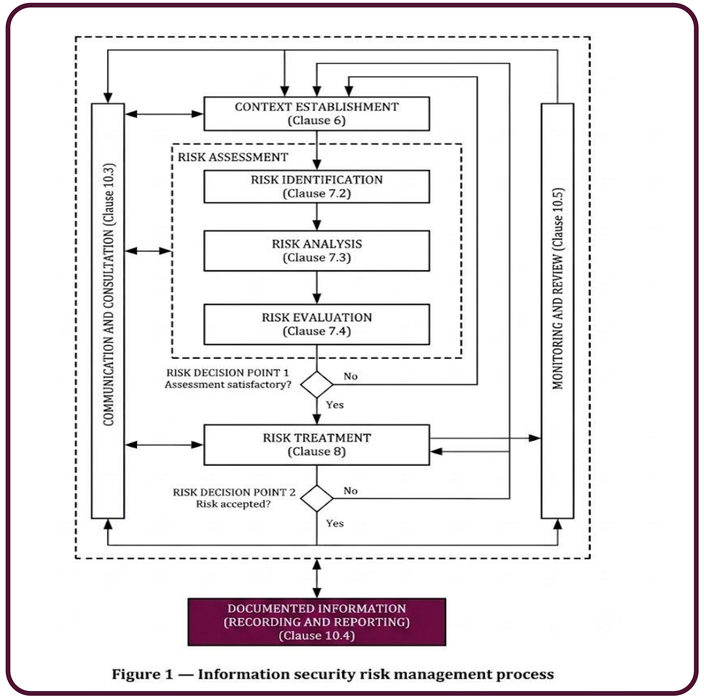


Figure 1 — Information security risk management process

10. Aprovechamiento de los procesos relacionados del SGSI

10.5 Monitoreo y revisión

El propósito de la Cláusula 10.5 es asegurar la vigilancia continua. El estándar establece que los riesgos no son estáticos; las amenazas evolucionan, las vulnerabilidades cambian y los controles pueden perder eficacia con el tiempo. Esta cláusula obliga a la organización a monitorear constantemente el entorno y a realizar revisiones periódicas para garantizar que el análisis de riesgos siga siendo válido y útil para la toma de decisiones de la Alta Dirección.

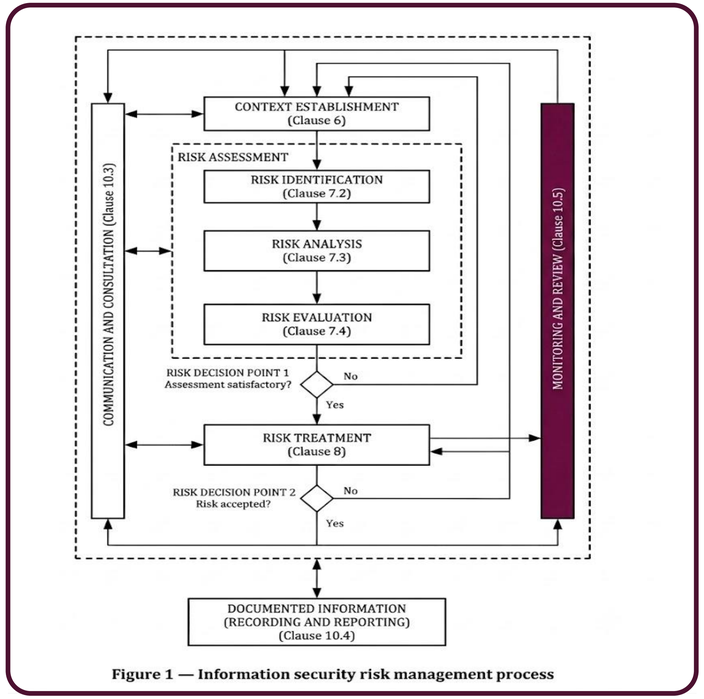


Figure 1 — Information security risk management process

- **Cláusula 10.5.1 General**

NOTA: Esta subcláusula se relaciona con la norma ISO/IEC 27001:2022, 9.1.

El proceso de monitoreo de la organización (ver ISO/IEC 27001:2022, 9.1) debe abarcar todos los aspectos de los procesos de valoración del riesgo y tratamiento del riesgo con el propósito de:

a) asegurar que los tratamientos del riesgo sean eficaces, eficientes y económicos tanto en su diseño como en su operación;

b) obtener información para mejorar las valoraciones de riesgo futuras;

c) analizar y aprender lecciones a partir de los incidentes (incluyendo los cuasi-incidentes o near misses), cambios, tendencias, éxitos y fracasos;

d) detectar cambios en el contexto interno y externo, incluyendo cambios en los criterios de riesgo y en los riesgos mismos, los cuales puedan requerir la revisión de los tratamientos del riesgo y de sus prioridades;

e) identificar riesgos emergentes.

Los escenarios de riesgo retenidos, provenientes de las actividades de gestión de riesgos, pueden ser transpuestos en escenarios de monitoreo con el fin de asegurar un proceso de monitoreo eficaz.

10. Aprovechamiento de los procesos relacionados del SGSI

10.5 Monitoreo y revisión

- **10.5.2 Monitoreo y revisión de los factores que influyen en los riesgos**

El propósito de la Cláusula 10.5.2 es vigilar el entorno. La norma reconoce que el valor de un riesgo cambia porque cambian sus componentes esenciales: las amenazas se vuelven más agresivas, aparecen nuevas vulnerabilidades técnicas, los activos adquieren mayor valor para el negocio o el impacto regulatorio se endurece. Si no se monitorean estos factores, la matriz de riesgos se vuelve obsoleta rápidamente.

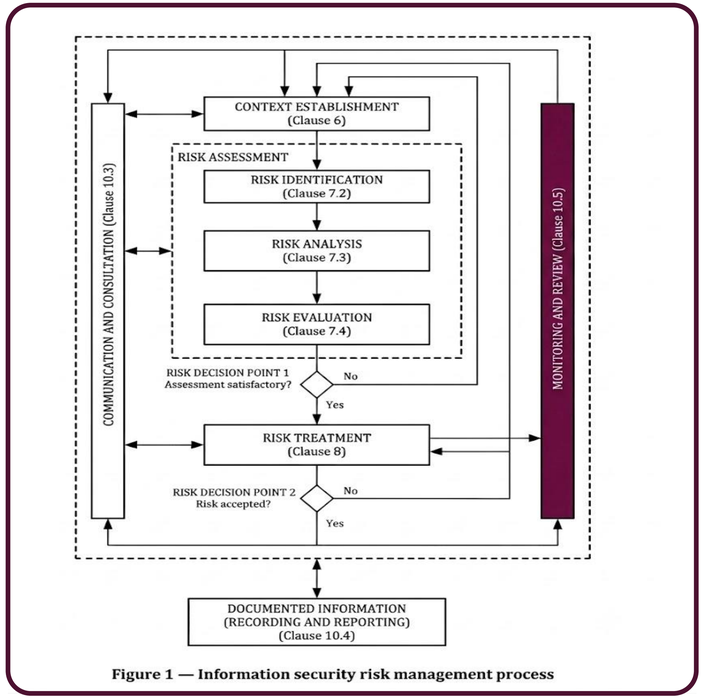


Figure 1 — Information security risk management process

Entradas (Inputs):

-La Matriz de Riesgos activa (9.1) con los factores de riesgo identificados (valores de activos, listado de amenazas y vulnerabilidades asociadas).

-Fuentes externas de inteligencia de amenazas (boletines de ciberseguridad, reportes de fabricantes, alertas de CERTs/CSIRTs nacionales).

-Informes internos de TI y desarrollo (nuevos parches de seguridad pendientes, cambios en la arquitectura, inventario de sistemas obsoletos o Legacy).

Acciones (Actions):

-Vigilancia de Amenazas y Vulnerabilidades: Monitorear de forma sistemática si los factores de exposición han cambiado (ej. comprobar si una amenaza que antes se consideraba "Baja" o poco probable ahora tiene herramientas automatizadas en internet que facilitan su ejecución).

-Revaluación del Valor de los Activos: Revisar si los datos o sistemas analizados previamente han adquirido mayor criticidad para la continuidad del negocio o el cumplimiento legal.

10. Aprovechamiento de los procesos relacionados del SGSI

10.5 Monitoreo y revisión

-Actualización del Perfil de Riesgo: Si se detecta que los factores han variado significativamente, activar una actualización inmediata en la puntuación de la matriz operativa (9.1) sin esperar al ciclo de revisión anual.

Desencadenadores (Triggers):

-La publicación global de una vulnerabilidad crítica de tipo Zero-Day que afecte directamente a los sistemas core de la organización.

-Cambios drásticos en el mercado o en las leyes locales (ej. nuevas multas severas por protección de datos que elevan el factor de Impacto).

-Modificaciones internas en los procesos del negocio que incrementen el valor o la criticidad de un activo de información.

Salida (Output):

Registro de Factores de Riesgo Actualizados (actualizaciones en la sección de amenazas/vulnerabilidades de la matriz de riesgos o bitácoras de inteligencia de amenazas integradas al proceso). Esta salida demuestra al auditor de la ISO 27001 que la organización realiza una gestión analítica y proactiva del entorno antes de que los riesgos se materialicen en incidentes.

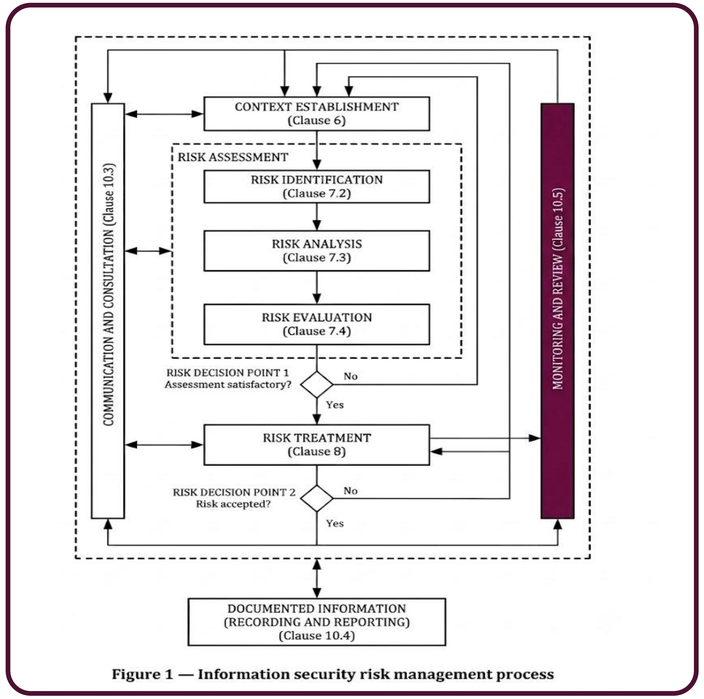


Figure 1 — Information security risk management process

10. Aprovechamiento de los procesos relacionados del SGSI

10.6 Revisión por la dirección

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

Entrada (Input): Resultados de la(s) valoración(es) del riesgo de seguridad de la información, estado del plan de tratamiento del riesgo de seguridad de la información.

Acción (Action): Los resultados de la valoración del riesgo de seguridad de la información y el estado del plan de tratamiento del riesgo de seguridad de la información deben revisarse para confirmar que los riesgos residuales cumplan con los criterios de aceptación del riesgo, y que el plan de tratamiento del riesgo aborde todos los riesgos relevantes y sus opciones de tratamiento del riesgo.

Desencadenador (Trigger): Una parte del calendario programado de las actividades de revisión.

Salida (Output): Cambios en los criterios de aceptación del riesgo y en los criterios para realizar las valoraciones del riesgo de seguridad de la información, plan de tratamiento del riesgo de seguridad de la información o SOA (Declaración de Aplicabilidad) actualizados.

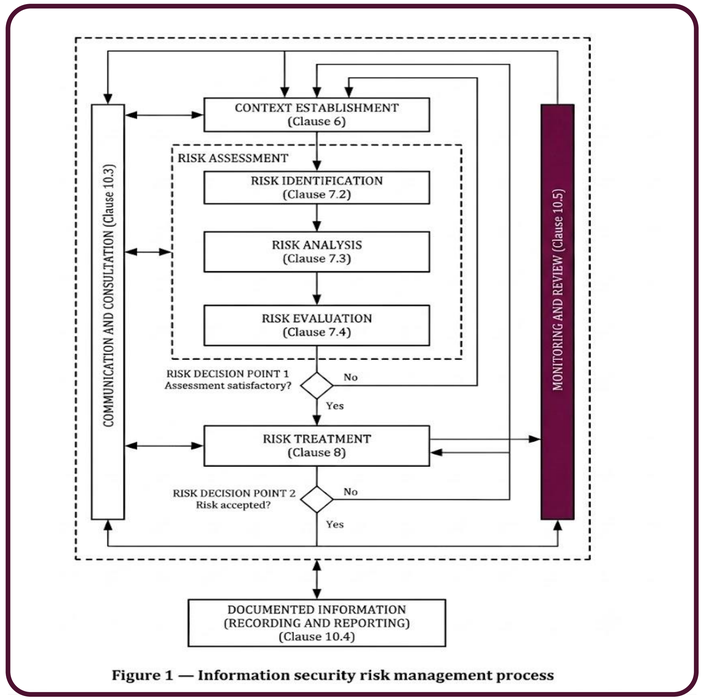


Figure 1 — Information security risk management process

10. Aprovechamiento de los procesos relacionados del SGSI

10.7 Acciones correctivas

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

El propósito de esta cláusula es cerrar el círculo del aprendizaje. Cuando un control falla, se identifica una no conformidad en una auditoría, o se materializa un incidente que no estaba previsto o cuyo impacto fue subestimado, la organización debe usar el proceso de riesgos para identificar la causa raíz y aplicar acciones correctivas que eviten que vuelva a suceder.

Entrada (Input): No conformidades identificadas (en auditorías o revisiones), incidentes de seguridad de la información materializados, fallas detectadas en la efectividad de los controles vigentes y análisis de causa raíz.

Acción (Action): Cuando ocurra una no conformidad o un incidente de seguridad, se debe evaluar la necesidad de actuar para eliminar la causa raíz mediante la revaluación de los riesgos asociados. El proceso de gestión de riesgos debe ejecutarse para asegurar que las acciones correctivas propuestas no introduzcan nuevos riesgos inaceptables y que los riesgos previamente identificados se mitiguen de manera definitiva.

Desencadenador (Trigger): La identificación formal de una no conformidad en el SGSI, el reporte de un hallazgo de auditoría o la ocurrencia de un incidente de seguridad de la información.

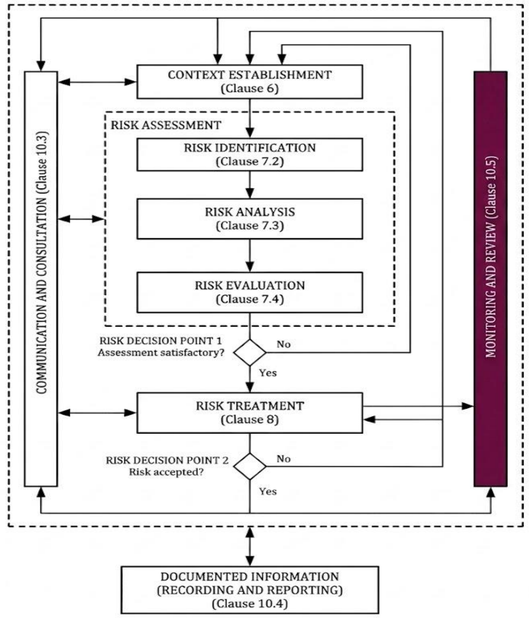


Figure 1 — Information security risk management process

10. Aprovechamiento de los procesos relacionados del SGSI

10.8 Mejora continua

Entrada (Inputs):

-Los resultados acumulados de las revisiones por la dirección (10.6) y las lecciones aprendidas en el cierre de las acciones correctivas (10.7).

-Evaluaciones sobre la madurez del proceso de riesgos y retroalimentación de los analistas de seguridad sobre la facilidad de uso de las escalas.

-Métricas del cumplimiento de los objetivos de seguridad y nuevas guías técnicas de la familia ISO u otros marcos (como NIST).

Acción (Action):

-La idoneidad, adecuación y eficacia del proceso de gestión de riesgos de seguridad de la información deben mejorarse continuamente. La organización debe analizar las tendencias de los riesgos y la precisión de sus estimaciones previas para simplificar el marco de trabajo, elevar la precisión de las valoraciones de impacto, y asegurar que el proceso se adapte ágilmente a la estrategia de crecimiento y a la transformación digital del negocio.

Desencadenadores (Triggers):

-La conclusión del ciclo anual de auditoría y revisión general del SGSI.

-La detección de ineficiencias o retrasos reiterados al momento de calificar riesgos mediante la metodología actual.

-Cambios en los objetivos comerciales a largo plazo de la empresa que requieran una postura de gestión de riesgos más sofisticada.

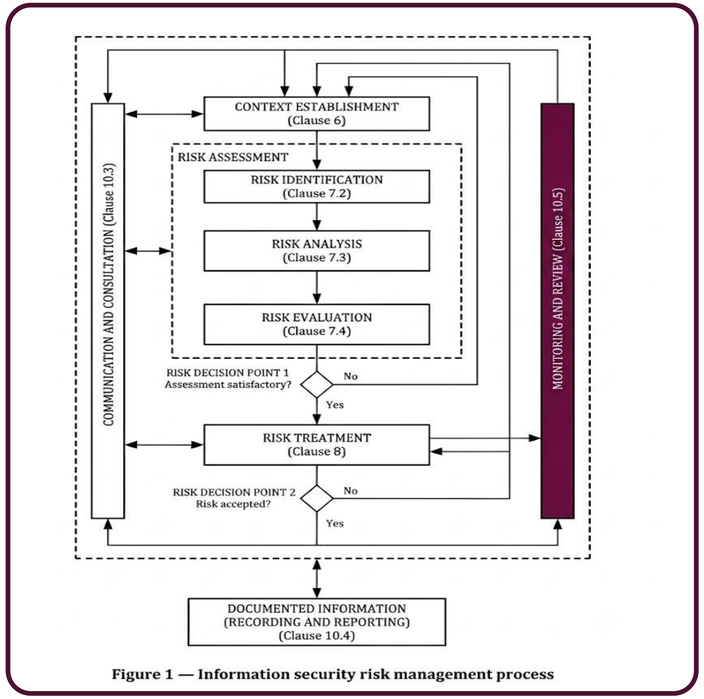


Figure 1 — Information security risk management process

10. Aprovechamiento de los procesos relacionados del SGSI

10.8 Mejora continua

Salida (Output):

Metodología de Gestión de Riesgos optimizada (criterios de impacto/probabilidad refinados para el siguiente ciclo), planes de capacitación avanzada para los Risk Owners, o la adopción de nuevas herramientas de automatización (como plataformas GRC) para incrementar la madurez del sistema.

💡 **Nota de implementación:**

Con esta cláusula demuestras ante el auditor que tu matriz de riesgos no es un documento fósil. Si hace tres años medías el riesgo de forma puramente cualitativa (Alto/Medio/Bajo) y hoy incorporas un enfoque basado en eventos más detallado o escalas numéricas más precisas, estás aplicando la Cláusula 10.8 de forma impecable.

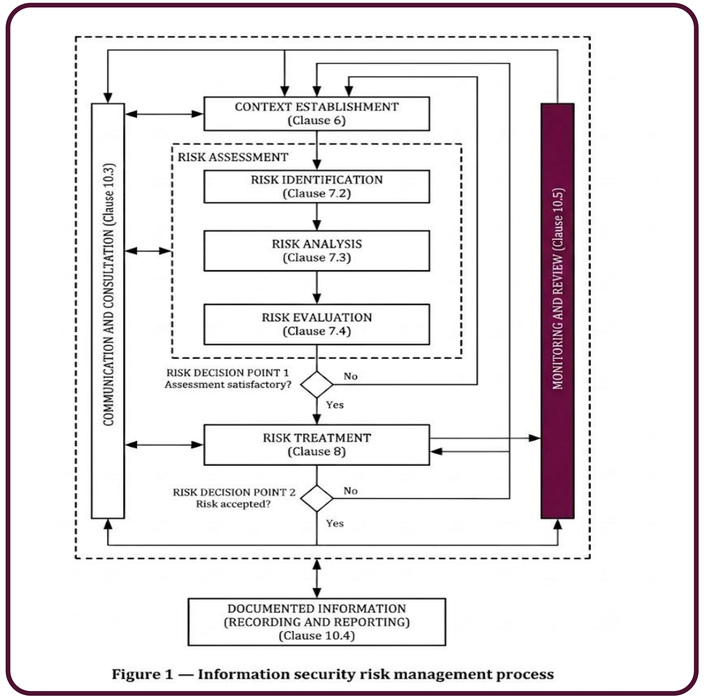


Figure 1 — Information security risk management process

Gracias por su atención

🌐 www.valfraitconsulting.com