Commented [AES1]: Para saber cómo completar este documento, y ver ejemplos reales de lo que necesita escribir, vea este tutorial en vídeo: "How to Write the ISO 27001 Risk Assessment Methodology".

Para acceder al tutorial: en su bandeja de entrada, busque el correo electrónico que recibió en el momento de la compra. Allí, verá un enlace y una contraseña que le permitirán acceder al tutorial en vídeo.

[logo de la organización]

Commented [AES2]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

[nombre de la organización]

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

Commented [AES3]: Para ver cómo redactar la metodología, lea estos artículos:

- Evaluación y Tratamiento del Riesgo en ISO 27001 – 6 pasos básicos https://advisera.com/27001academy/es/knowledgebase/evaluacion-y-tratamiento-del-riesgo-en-iso-27001-6-pasos-basicos/

- How to write ISO 27001 risk assessment methodology https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/#section3

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

Commented [AES4]: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización. En el caso que no exista ese sistema, se puede eliminar esta línea.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1	Advisera	Descripción básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en [nombre de la organización] y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

La evaluación y tratamiento de riesgos se aplican a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los activos que se utilizan dentro de la organización o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

Los usuarios de este documento son todos los empleados de [nombre de la organización] que participan en la evaluación y tratamiento de riesgos.

Commented [AES5]: Incluya el nombre de su organización.

Commented [AES6]: Escriba "ISO 22301" si está implementando solo ISO 22301 y no ISO 27001.

Commented [AES7]: O escribir "Sistema de Gestión de Continuidad de Negocio (SGCN)" si está solamente implementando la continuidad de negocio.

Commented [AES8]: Igual que el comentario anterior.

Commented [AES9]: O "SGCN".

Commented [AES10]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas 6.1.2, 6.1.3, 8.2, y 8.3
- Norma ISO 22301, cláusulas 8.1.2 y 8.2.3
- Política de seguridad de la información
- Lista de requisitos legales, normativos, contractuales y de otra índole
- Política de seguridad para proveedores
- Declaración de aplicabilidad

Commented [AES11]: Borrar esto si solo se implementa ISO 22301.

Commented [AES12]: Borrar esto si solo se implementa ISO 27001.

Commented [AES13]: Borrar esto si solo se implementa ISO 22301.

Commented [AES14]: Eliminar esto si no va a utilizar esta Política.

Commented [AES15]: Borrar esto si solo se implementa ISO 22301.

3. Metodología de evaluación y tratamiento de riesgos

Commented [AES16]: Se debe modificar esta Metodología si

3.1. Evaluación de riesgos

3.1.1. El proceso

La evaluación de riesgos se implementa a través del Cuadro de evaluación de riesgos. El proceso de evaluación de riesgos es coordinado por [cargo].

Commented [AES17]: Para simplificar el proceso, usted puede definir que el propietario del activo para cada riesgo también será el propietario del riesgo.

3.1.2. Activos, vulnerabilidades y amenazas

El primer paso en la evaluación de riesgos es la identificación de todos los activos dentro del alcance del SGSI por los representantes de cada área en el alcance del SGSI; es decir, identificar todos los activos que pueden interrumpir las operaciones.

Commented [AES18]: Agregar también otros tipos de activos

El siguiente paso es que los propietarios de los activos identifiquen todas las amenazas y vulnerabilidades relacionadas con cada activo. Las amenazas y vulnerabilidades se identifican utilizando los catálogos incluidos en el Cuadro de evaluación de riesgos.

3.1.3. Identificación de los propietarios de riesgos

Para cada riesgo es necesario identificar un propietario: la persona o unidad organizativa responsable de cada riesgo.

Commented [AES19]: Para simplificar el proceso, usted puede

3.1.4. Consecuencias y probabilidad

Una vez que se han identificado los riesgos, es necesario evaluar las consecuencias para cada combinación de amenazas y vulnerabilidades de un activo específico en caso que ello se pueda producir:

Baja consecuencia	0	La pérdida de confidencialidad, disponibilidad o integridad no afecta las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.

Luego de la evaluación de consecuencias es necesario evaluar la probabilidad de que se materialice ese riesgo; es decir, la probabilidad de que una amenaza se aproveche de la vulnerabilidad del activo en cuestión.

Probabilidad moderada	1	Los controles de seguridad existentes son moderados y en general han suministrado un adecuado nivel de protección. Es posible la ocurrencia de nuevos incidentes, pero no muy probable.

Ingresando los valores de consecuencia y probabilidad en el Cuadro de evaluación de riesgos, el nivel de riesgo se calcula automáticamente sumando los dos valores.

3.2. Criterios para la aceptación de riesgos

Los riesgos con niveles 0, 1 y 2 son riesgos aceptables, mientras que los riesgos con niveles 3 y 4 son riesgos no aceptables. [illegible]

3.3. Tratamiento del riesgo

El tratamiento de riesgos se implementa mediante el Cuadro de tratamiento de riesgos, copiando desde el Cuadro de evaluación de riesgos todos los riesgos identificados como no aceptables. [illegible]

Para los riesgos con niveles calificados en 3 y 4 se deben seleccionar una o más opciones de tratamiento.

1. Elección de control o controles de seguridad de [defina aquí la fuente de controles a emplear].
2. Transferencia de los riesgos a terceros; por ejemplo, suscribiendo una póliza de seguros o un contrato con proveedores o socios.
3. [illegible]
4. [illegible]

La elección de opciones se implementa a través del Cuadro de tratamiento de riesgos. Generalmente, se escoge la opción 1: elección de uno o más controles de seguridad. Cuando se escogen varios controles de seguridad para un riesgo, se insertan filas adicionales en la tabla, inmediatamente debajo de la fila en que se especifica el riesgo.

[illegible]

En el caso de la opción 1 (elección de controles de seguridad), es necesario evaluar el nuevo valor de consecuencia y probabilidad en el Cuadro de tratamiento de riesgos, para evaluar la efectividad de los controles planificados.

3.4. Revisiones periódicas de la evaluación y el tratamiento de riesgos

Los propietarios de riesgos deben revisar los riesgos vigentes y deben actualizar el Cuadro de evaluación de riesgos y el Cuadro de tratamiento de riesgos de acuerdo con los nuevos riesgos identificados. [illegible]

3.5. Declaración de aplicabilidad y Plan de tratamiento del riesgo

Commented [AES20]: Por ejemplo: gerente de continuidad del [illegible]

Commented [AES21]: Por ejemplo: controles estándar ISO 27001 del Anexo A, publicaciones especiales del NIST, etc.

Commented [AES22]: La selección de controles de seguridad debe considerar las opciones que:
[illegible]

Commented [AES23]: Borrar si no utilizará esta Política.

Commented [AES24]: Este nuevo valor se llama [illegible]

Commented [AES25]: Borrar esto si solo se implementa [illegible]

El [cargo] debe documentar los siguiente en la Declaración de aplicabilidad: qué controles de seguridad del Anexo A de la norma ISO/IEC 27001 son aplicables y cuáles no, la justificación de esa decisión y si están implementados o no.

En nombre de los propietarios de riesgos, la [alta dirección] aceptará todos los riesgos residuales a través de la Declaración de aplicabilidad.

El [cargo] preparará el Plan de tratamiento de riesgos en el que se planificará la implementación de los controles. En nombre de los propietarios de riesgos, [alta dirección] aprobará el Plan de tratamiento de riesgos.

3.6. Informes

El [cargo] documentará los resultados de la evaluación y del tratamiento de riesgos, y de todas las revisiones subsiguientes, en el Informe de evaluación y tratamiento de riesgos.

El [cargo] supervisará el progreso de la implementación del Plan de tratamiento de riesgos e informará los resultados al [cargo] mensualmente.

4. Gestión de registros guardados en base a este documento

[Nombre del registro]	[Ubicación de archivo]	[Persona responsable del archivo]	[Controles para la protección del registro]	[Tiempo de retención]
Cuadro de evaluación de riesgos (formulario electrónico, documento en Excel)	Ordenador del [cargo]	[cargo del propietario del Cuadro de evaluación de riesgos]	Solamente el [cargo] tiene derecho a crear entradas y a realizar modificaciones en el Cuadro de evaluación de riesgos.	Los datos son archivados de forma permanente.
[Cuadro de tratamiento de riesgos (formulario electrónico, documento en Excel)]	[Ordenador del [cargo]]	[Cargo del propietario del Cuadro de tratamiento de riesgos]	[Solamente el [cargo] tiene derecho a crear entradas y a realizar modificaciones en el Cuadro de tratamiento de riesgos.]	[Los datos son archivados de forma permanente.]
[Informe sobre evaluación y tratamiento de riesgos (formulario electrónico, en formato PDF)]	[Ordenador del [cargo]]	[Cargo del propietario del informe]	[El informe se prepara en formato PDF de solo lectura.]	[El informe se almacenará por el plazo de 5 años.]

Commented [AES26]: Si, por algún motivo, esta aceptación de

Commented [AES27]: Puede encontrar una plantilla para este

Commented [AES28]: Por ejemplo: gerente de continuidad del

Commented [AES29]: Por ejemplo: gerente de continuidad del

Commented [AES30]: Por ejemplo: CEO, responsable de la

Commented [AES31]: Esta es solo nuestra recomendación.

Commented [AES32]: En esta columna ingrese datos que

Commented [AES33]: Por ejemplo: gerente de continuidad del

Commented [AES34]: Por ejemplo: gerente de continuidad del

Plan de tratamiento de riesgos (formulario electrónico, documento de Word)	Ordenador del [cargo]	[cargo de la persona responsable del Plan de tratamiento de riesgos]	Solamente el [cargo] tiene derecho a crear entradas y a realizar modificaciones en el Plan de tratamiento de riesgos.	Las versiones no vigentes del Plan de tratamiento de riesgos son almacenadas por un plazo de 3 años.

Commented [AES35]: Borrar esto si solo se implementa

Commented [AES36]: Por ejemplo: gerente de continuidad del

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

Commented [AES37]: Por ejemplo: gerente de continuidad del

Commented [AES38]: Esto es sólo una recomendación; ajustar

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- La cantidad de incidentes que se produjeron pero que no fueron incluidos en la evaluación de riesgos.

6. Apéndices

- Apéndice 1 – Cuadro de evaluación de riesgos

[cargo]
[nombre]

[firma]

Commented [AES39]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.