Apéndice 3 – Informe sobre la evaluación y tratamiento de riesgos

Commented [27A1]: Para saber cómo completar este documento, y ver ejemplos reales de lo que necesita escribir, vea este tutorial en vídeo: "How to Write ISO 27001 Risk Assessment Report".

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.

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 presentar un resumen detallado del proceso y de los documentos utilizados durante la evaluación y el tratamiento de los riesgos de la información en [nombre de la organización] en el período [especificar el período].

La evaluación de riesgos se aplicó a todo el Sistema de Gestión de Seguridad de la Información (SGSI).

El presente documento está dirigido a la alta dirección de [nombre de la organización], al [cargo responsable de seguridad de la información], a los propietarios de activos de información y a todas las personas involucradas en la planificación, implementación, supervisión y mejora del SGSI.

Commented [AES2]: Incluya el nombre de su organización.

Commented [AES3]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas 8.2 y 8.3
- Norma ISO 22301, cláusula 8.2.3
- Documento sobre el alcance del SGSI
- Política de seguridad de la información
- Política de continuidad de negocio
- Metodología de evaluación y tratamiento de riesgos

Commented [AES4]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "04_Alcance_del_SGSI".

Commented [AES5]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "05_Politicas_generales".

Commented [AES6]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "10_Documentos_basicos_de_continuidad_del_negocio_ISO_22301".

3. Proceso de evaluación y tratamiento de riesgos de la información

Todo el proceso de evaluación y tratamiento de riesgos ha sido realizado en conformidad con el documento Metodología de evaluación y tratamiento de riesgos.

3.1. Objetivo de la gestión de riesgos

El objetivo de la evaluación de riesgos es identificar todos los activos, sus vulnerabilidades y las amenazas que se pueden aprovechar de dichas vulnerabilidades, como también evaluar esos parámetros para establecer el grado crítico de riesgos individuales.

El objetivo del tratamiento de riesgos es definir medios adecuados para disminuir o controlar esos riesgos.

3.2. Alcance de la evaluación y tratamiento de riesgos

La evaluación y tratamiento de riesgos fue realizado en [nombre de las unidades organizativas], en conformidad con el Documento sobre el alcance del SGSI.

Commented [AES7]: Incluya aquí solo las unidades organizativas donde se realizará la evaluación de riesgos y el tratamiento de riesgos.

3.3. Período de tiempo

La evaluación de riesgos fue implementada en el período comprendido entre el [día/ mes/ año] y el [día/ mes/ año]. El tratamiento de riesgos fue implementado en el período comprendido entre el

[día/ mes/ año] y el [día/ mes/ año]. Los informes finales fueron elaborados durante [especificar período].

3.4. Participantes en el proceso y recolección de información

Los procesos de evaluación y tratamiento de riesgos fueron dirigidos por [nombre y cargo], con la colaboración experimentada de [si se utilizó asistencia, indicar nombre y empresa].

Durante la evaluación de riesgos, se obtuvo información a través de cuestionarios y entrevistas con personas responsables, es decir, propietarios de activos de todas las unidades organizativas.

3.5. Breve resumen de la metodología aplicada

Resumidamente, el proceso se realizó de la siguiente manera:

- Se identificaron todos los activos y sus propietarios.
- Se identificaron las amenazas para cada activo y las correspondientes vulnerabilidades para cada amenaza.
- Se identificaron los propietarios de cada riesgo.
- Se evaluaron, con valores de 0 a 2, las consecuencias por la pérdida de confidencialidad, integridad y disponibilidad.
- Se evaluó, con valores de 0 a 2, la probabilidad de que se materialice un riesgo, es decir, que la amenaza se aproveche de la vulnerabilidad.
- Se calculó el nivel de riesgo sumando las consecuencias y la probabilidad.
- Se determinó que los riesgos valorados en 3 y 4 son riesgos no aceptables.
- Para cada riesgo no aceptable se tuvo en cuenta un tratamiento de riesgo y, del Anexo A de la norma ISO/IEC 27001, se escogieron controles que pueden disminuir el riesgo a un nivel aceptable, así como de otras fuentes de control de seguridad consideradas relevantes.
- Una vez que se aplicaron los controles, se evaluaron los riesgos residuales.

3.6. Resumen de los documentos utilizados durante el proceso de evaluación y tratamiento de riesgos

Durante la implementación de la evaluación y tratamiento de riesgos se utilizaron o redactaron los siguientes documentos:

- Cuadro de evaluación de riesgos (Apéndice 1): para cada combinación de activos, vulnerabilidades y amenazas, este cuadro muestra los valores de consecuencia y probabilidad y calcula el riesgo.
- Cuadro de tratamiento de riesgos (Apéndice 2): muestra las opciones para tratamiento de riesgos, la elección de controles para cada riesgo no aceptable y el nivel de riesgo residual.

4. Validez y gestión de documentos

Este documento es válido hasta el [fecha]. El propietario de este documento es el [cargo].

Commented [AES8]: Por ejemplo: gerente de continuidad del negocio, gerente de seguridad, gerente de seguridad de la información, etc.

Commented [AES9]: Puede eliminar esta parte si no se utilizó la entrevista de evaluación.

Commented [AES10]: O detallar si se utilizó algún otro método.

Commented [AES11]: Elimine este texto si solo se aplicaron los controles del Anexo A de la ISO 27001.

Commented [AES12]: Por ejemplo: gerente de continuidad del negocio, gerente de seguridad, gerente de seguridad de la información, etc.

5. Apéndices

- Apéndice 1 – Cuadro de evaluación de riesgos
- [illegible]

[cargo]
[nombre]

_____
[firma]

Commented [AES13]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.