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 ISO 27001 Procedure for Corrective and Preventive Action".

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]

PROCEDIMIENTO PARA LA ACCIÓN CORRECTIVA

Commented [AES3]: Para conocer más sobre este tema, lea el siguiente artículo:

Complete guide to corrective action vs. preventive action
https://advisera.com/blog/2021/07/19/complete-guide-to-corrective-action-vs-preventive-action/

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 de este Procedimiento es describir todas las actividades relacionadas con la iniciación, implementación y mantenimiento de registros de correcciones, como también de acciones correctivas.

Este Procedimiento se aplica a todas las actividades implementadas dentro del Sistema de Gestión de Seguridad de la Información (SGSI) [Sistema de Gestión de Continuidad de Negocio (SGCN)].

Los usuarios de este documento son todos los empleados de [nombre de la organización].

Commented [AES5]: Se debe insertar esta leyenda en lugar de SGSI en caso que el Procedimiento se refiera exclusivamente a la gestión de continuidad de negocio.

Commented [AES6]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas 10,1 y A.5.27
- Norma ISO 22301, cláusula 10.1
- Política de seguridad de la información
- Política de continuidad de negocio
- Procedimiento para auditoría interna
- Procedimiento para gestión de incidentes

Commented [AES7]: Borrar si el Procedimiento se refiere sólo a gestión de continuidad de negocio.

Commented [AES8]: Borrar esto si usted no implementa continuidad de negocio.

Commented [AES9]: Borrar si el Procedimiento se refiere sólo a gestión de continuidad de negocio.

Commented [AES10]: Borrar esto si usted no implementa continuidad de negocio.

Commented [AES11]: Si la documentación es escrita sólo para continuidad de negocio, reemplazar con Plan de respuesta a los incidentes.

3. Correcciones y acciones correctivas

3.1. No-conformidades y correcciones

Una no-conformidad es todo incumplimiento de los requerimientos de las normas, documentación interna, reglamentos, obligaciones contractuales y de otra clase dentro del SGSI.

Commented [AES12]: o SGCN

3.2. Acciones correctivas

La persona responsable debe evaluar la necesidad de eliminar el origen de la no-conformidad y evitar su recurrencia tomando acciones correctivas.

Una acción correctiva puede ser iniciada por cualquier empleado o, cuando sea pertinente, por cualquier cliente, proveedor o socio de la organización. [illegible]

Commented [AES13]: o SGCN

3.3. Implementación de acciones correctivas

Una acción correctiva se implementa de la siguiente forma:

Paso	Persona responsable de la implementación
1. Revisión de la no-conformidad	Cualquiera con un rol dentro del SGSI
2. Determinación de la causa de la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
3. Identificar si la no-conformidad ya existía	Persona responsable del área donde se ha identificado la no-conformidad
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	Persona a cargo de la implementación, designada por la persona responsable
[illegible]	[illegible]
[illegible]	Persona a cargo de la implementación, designada por la persona responsable
[illegible]	[illegible]

Commented [AES14]: o SGCN

Commented [AES15]: Se puede designar a una persona para [illegible]

Commented [AES16]: o SGCN

Commented [AES17]: Por ej., el jefe de seguridad o el [illegible]

Commented [AES18]: o SGCN

Commented [AES19]: También puede utilizar, por ejemplo, una [illegible]

Cada uno de los pasos anteriores debe quedar registrado en el Formulario de acción correctiva.

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	[illegible]	[illegible]	[illegible]
Formulario de acción correctiva	[nombre de la carpeta de archivo,	[illegible]	[illegible]	[illegible]

Commented [AES23]: La persona designada para manejar la [illegible]

	en qué gabinete] [nombre de carpeta en Intranet]			

Commented [AES20]: Si se guardan los registros en papel.

Commented [AES21]: Si utiliza una aplicación, especifique el

Commented [AES22]: Si se guardan los registros en formato electrónico.

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

Commented [AES24]: Ej.: gerente de continuidad del negocio,

Commented [AES25]: Esto es sólo una recomendación; ajustar

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

- Cantidad de acciones correctivas iniciadas

6. Apéndices

Commented [AES26]: Borrar esta sección si usted utiliza una aplicación.

- Apéndice 1 – Formulario de acción correctiva

[cargo]
[nombre]

[firma]

Commented [AES27]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.