[logo de la organización]

[nombre de la organización]

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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

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 ISMS Policy According to ISO 27001".

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.

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

Commented [AES3]: Este artículo le ayudará a entender el contenido de la Política de seguridad de la información:

What is the ISO 27001 Information Security Policy, and how can you write it yourself?
https://advisera.com/27001academy/blog/2016/05/30/what-should-you-write-in-your-information-security-policy-according-to-iso-27001/

Commented [AES4]: Si necesita un documento que proporcione reglas detalladas para la seguridad de la información, utilice la plantilla de Política de seguridad de TI incluida en el Paquete Premium de documentos sobre ISO 27001 e ISO 22301 en la carpeta "09_Anexo_A_de_ISO_27001_Controles_de_seguridad".

Commented [AES5]: Este artículo le ayudará a comprender el objetivo de la Política de seguridad de la información:

Política de Seguridad de la Información: ¿qué nivel de detalle debería tener?
https://advisera.com/27001academy/es/blog/2010/05/26/politica-de-seguridad-de-la-informacion-que-nivel-de-detalle-deberia-tener/

Commented [AES6]: 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 propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta Política se aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI), según se define en el Documento sobre el alcance del SGSI.

Los usuarios de este documento son todos los empleados de [nombre de la organización], como también terceros externos a la organización.

Commented [AES7]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas 5.2, 5.3, 6.2, 7.4 y A.6.3
- Documento sobre el alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de requisitos legales, normativos, contractuales y de otra índole
- [Otros documentos internos]
- [Política de continuidad de negocio]
- [Procedimiento para gestión de incidentes]

Commented [AES8]: 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 [AES9]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "06_Evaluacion_y_tratamiento_de_riesgos".

Commented [AES10]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "07_Aplicabilidad_de_los_controles".

Commented [AES11]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "03_Identificacion_de_requisitos".

Commented [AES12]: Enumerar otros documentos internos de la organización relacionados con esta Política; por ejemplo, plan de desarrollo estratégico, plan de negocios, documento sobre gestión de riesgos, etc.

Commented [AES13]: 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".

Commented [AES14]: Puede encontrar una plantilla para este documento en la carpeta del Paquete de Documentos sobre ISO 27001 "09_Anexo_A_Controles_de_seguridad".

3. Terminología básica sobre seguridad de la información

Confidencialidad: característica de la información por la cual solo está disponible para personas o sistemas autorizados.

Integridad: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.

[illegible]

4. Gestión de la seguridad de la información

4.1. Objetivos y medición

Los objetivos generales para el sistema de gestión de seguridad de la información son los siguientes:

[redacted] El [cargo] es el responsable de revisar estos objetivos generales del SGSI y de establecer nuevos.

[redacted]

Todos los objetivos deben ser revisados al menos una vez al año.

[redacted] El [cargo] es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos al menos una vez al año y el [cargo] analizará y evaluará los resultados y los reportará a [alta dirección] como material para la revisión por la dirección. [redacted]

4.2. Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales.

[redacted]

4.3. Controles de seguridad de la información

El proceso de escoger los controles (protección) está definido en la Metodología de evaluación y tratamiento de riesgos.

[redacted]

4.4. Continuidad de negocio

La gestión de la continuidad de negocio está reglamentada en la Política de continuidad de negocio.

4.5. Responsabilidades

Las responsabilidades para el SGSI son las siguientes:

- El [cargo] es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
- [redacted]

Commented [AES15]: Si es necesario, modificar y/o agregar otros objetivos como: cumplimiento de normas o leyes, cantidad de incidentes, satisfacción del usuario, etc.

[redacted]

Commented [AES16]: Para obtener más información sobre la alineación entre ISO 27001 y el negocio, vea este artículo:

[redacted]

Commented [AES17]: Para obtener información sobre la importancia de los objetivos de control, vea este artículo:

[redacted]

Commented [AES18]: Por ejemplo, los objetivos para los [redacted]

Commented [AES19]: Evaluar si la frecuencia es adecuada.

Commented [AES20]: Incluya el nombre de su organización.

Commented [AES21]: Puede encontrar una plantilla para este [redacted]

Commented [AES22]: Enumerar también otras áreas que estén [redacted]

Commented [AES23]: Eliminar esta sección si no se [redacted]

Commented [AES24]: Para obtener una mejor comprensión de las responsabilidades de la alta dirección, vea este artículo:

[redacted]

Commented [AES25]: Miembro de la alta dirección.

Commented [AES26]: Una o varias personas. Las [redacted]

- La [alta dirección] debe revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar actas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.
- El [cargo] implementará programas de formación y concienciación de empleados sobre seguridad de la información.
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad deben ser informados al [cargo].
- El [cargo] definirá qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.
- El [cargo] es el responsable de adoptar e implementar el Plan de Formación y concienciación, que corresponde a todas las personas que cumplen un rol en la gestión de la seguridad de la información.

4.6. Comunicación de la Política

El [cargo] debe asegurarse de que todos los empleados de [nombre de la organización], como también los participantes externos correspondientes, estén familiarizados con esta Política.

5. Apoyo para la implementación del SGSI

A través del presente, el [cargo u organismo directivo supremo dentro del alcance del SGSI] declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

6. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el [cargo], que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

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

- Cantidad de empleados y participantes externos que cumplen un rol en el SGSI pero que no están familiarizados con el presente documento.
- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del SGSI.
- Responsabilidades ambiguas para la implementación del SGSI.

Commented [AES27]: Este debe ser el organismo directivo

Commented [AES28]: Estos son obligatorios según ISO 27001;

Commented [AES29]: O hacer referencia al Procedimiento para

Commented [AES30]: Se pueden designar varias personas

Commented [AES31]: Esta formación le ayudará a capacitar a

Commented [AES32]: Estos son recomendados; puede

Commented [AES33]: Incluya el nombre de su organización.

Commented [AES34]: Para obtener una mejor comprensión de la provisión de recursos, vea este artículo:

Commented [AES35]: Esto es sólo una recomendación; ajustar

[cargo]
[nombre]

[firma]

Commented [AES36]: La Política de seguridad de la [redacted]

Commented [AES37]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.