[logo de la organización]

[nombre de la organización]

Commented [AES1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Commented [AES2]: Para conocer cómo clasificar la información, lea el siguiente artículo:

Information classification according to ISO 27001
https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso-27001/

Commented [AES3]: 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.

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

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 garantizar que se proteja la información en un nivel adecuado.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los tipos de información, independientemente del formato, ya sean documentos en papel o electrónicos, aplicaciones y bases de datos, conocimiento de las personas, etc.

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

Commented [AES4]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.5.9, A.5.10, A.5.12, A.5.13, A.5.14, A.7.10, A.8.3, A.8.5, A.8.11 y A.8.12
- Política de seguridad de la información
- Informe sobre la evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Inventario de activos
- Lista de requisitos legales, normativos, contractuales y de otra índole
- Procedimiento para gestión de incidentes
- [Procedimientos de seguridad para el departamento de TI] / [Política de eliminación y destrucción]
- Política de seguridad de TI

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 "06_Evaluacion_y_tratamiento_de_riesgos".

Commented [AES7]: 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 [AES8]: Si no tiene esta Lista, entonces aquí detalle toda la legislación y obligaciones contractuales relacionadas con clasificación de la información.

Commented [AES9]: Escoger el documento que establece el borrado seguro de datos.

3. Información clasificada

3.1. Pasos y responsabilidades

Los pasos y responsabilidades para la gestión de la información son los siguientes:

[illegible]	[illegible]
1. Ingreso del activo de información en el Inventario de activos	[cargo]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

Si la información clasificada proviene de afuera de la organización, el [cargo] es el responsable de su clasificación según las reglas establecidas en esta Política, y esta persona se convierte en el propietario de ese activo de información.

3.2. Clasificación de la información

3.2.1. Criterios de clasificación

El nivel de confidencialidad se determina de acuerdo a los siguientes criterios:

- Valor de la información: según los impactos evaluados durante la evaluación de riesgos.
- [illegible]
- [illegible]

Commented [AES10]: Esto también incluye las normas de privacidad.

3.2.2. Niveles de confidencialidad

Toda la información debe ser clasificada en niveles de confidencialidad.

[illegible]	[illegible]	[illegible]	[illegible]
Pública	(sin etiquetar)	Hacer pública la información no puede dañar a la organización de ninguna forma	La información está disponible para todo el público
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

Commented [AES11]: Los niveles de confidencialidad y el [illegible]

La regla básica es utilizar el nivel de confidencialidad más bajo garantizando un adecuado nivel de protección para evitar gastos de protección innecesarios.

3.2.3. Lista de personas autorizadas

La información clasificada como "Restringido" y "Confidencial" debe estar acompañada de una Lista de personas autorizadas en la que el propietario de la información específica los nombres o los cargos de las personas que tienen derechos de acceso para esa información.

La misma regla aplica para el nivel de confidencialidad "Uso interno" a las personas externas a la organización tendrán acceso a este documentos.

3.2.4. Reclasificación

Los propietarios de activos deben revisar el nivel confidencialidad de sus activos de información cada [dos años] y deben evaluar si se puede cambiar dicho nivel. Si es posible, deberían bajarlo.

Commented [AES12]: Esto es sólo una recomendación; ajustar

3.3. Etiquetado de la información

Los niveles de confidencialidad son etiquetados de la siguiente forma:

- **Documentos en papel:** se indica el nivel de confidencialidad en la esquina superior derecha de cada página del documento; también se indica en la portada o en el sobre que contiene dicho documento, como también en la carpeta de archivo en la que se guarda el documento.
- **Documentos electrónicos:** se indica el nivel de confidencialidad en la esquina superior derecha de cada página del documento.
- **Sistemas de información:** el nivel de confidencialidad en aplicaciones y bases de datos debe ser indicado en la pantalla de acceso al sistema, como también en la esquina superior derecha de cada pantalla consecutiva que muestra información confidencial.
- **Correo electrónico:** se indica el nivel de confidencialidad en la primera línea del cuerpo del correo electrónico.
- **Medios de almacenamiento electrónicos** (discos, tarjetas de memoria, etc.): se debe indicar el nivel de confidencialidad sobre la superficie de cada medio.
- **Información transmitida oralmente:** el nivel de confidencialidad de la información confidencial que se transmite a través de una comunicación cara a cara, por teléfono o por alguna otra vía de comunicación debe ser comunicado antes que la información propiamente dicha.

3.4. Manejo de información clasificada

Commented [AES13]: Todas las reglas mencionadas aquí deben

Todas las personas que tienen acceso a información clasificada deben seguir las reglas enumeradas en el siguiente cuadro. El [cargo] debe activar acciones disciplinarias cada vez que se no se cumplan las reglas o si la información se transmite a personas no autorizadas. Cada incidente relacionado con el manejo de información clasificada debe ser reportado de acuerdo con el Procedimiento para gestión de incidentes.

Los activos de información pueden ser llevados fuera de las instalaciones solamente con autorización, de acuerdo a lo establecido en la Política de seguridad de TI.

Commented [AES14]: Eliminar este párrafo si el control A.7.10

El método para borrado y destrucción seguro de medios está establecido en el documento [Procedimientos de seguridad para el departamento de TI / Política de eliminación y destrucción].

Commented [AES15]: Escoger el documento que establece el

	"Uso interno"	"Restringido"	"Confidencial"

Documentos en papel	• Si es enviado fuera de la organización, el documento debe ser enviado por correo certificado. • Los documentos solo pueden ser guardados en salas sin acceso público. • Los documentos deben ser retirados inmediatamente de impresoras y máquinas de fax.	• El documento debe ser almacenado en un gabinete con llave. • Los documentos pueden ser transferidos dentro y fuera de la organización solamente en un sobre cerrado. • Si es enviado fuera de la organización, el documento debe ser enviado con acuse de recibo. • Los documentos deben ser retirados inmediatamente de impresoras y máquinas de fax. • Solamente el propietario del documento puede copiarlo. • Solamente el propietario del documento puede destruirlo.	• El documento debe ser almacenado en una caja fuerte. • El documento puede ser transferido dentro y fuera de la organización solamente por una persona confiable y en un sobre cerrado y sellado. • No está permitido enviar el documento por fax. • Es posible imprimir el documento solo si la persona autorizada está al lado de la impresora. • Solamente el propietario del documento puede copiarlo. • Solamente el propietario del documento puede destruirlo.
Documentos electrónicos	• El acceso a los sistemas de información en los que están almacenados los documentos debe estar protegido por una clave segura. • La pantalla en la que se muestra el documento debe bloquearse automáticamente luego de [cantidad] minutos de inactividad.	• El acceso al sistema de información donde se almacena el documento debe estar protegido por una autenticación de 2 factores. • Cuando se intercambian archivos a través de servicios como FTP, mensajería instantánea, etc., deben tener la clave protegida.	• El documento debe ser almacenado en un formato encriptado. • El acceso al sistema de información donde se almacena el documento debe estar protegido por autenticación de 2 factores utilizando tarjetas inteligentes, tokens o lectores biométricos. • El documento

		• Solamente el propietario del documento puede borrarlo.	• Solamente puede ser archivado en servidores controlados por la organización. • Cuando los archivos se intercambian a través de servicios como FTP, mensajería instantánea, etc., deben estar encriptados. • Solamente el propietario del documento puede borrar el documento.
Sistemas de información	• El acceso al sistema de información debe estar protegido por una clave segura. • La pantalla debe bloquearse automáticamente luego de [cantidad] minutos de inactividad. • El sistema de información puede estar ubicado solamente en salas con acceso físico controlado.	• El acceso al sistema de información debe ser controlado a través de una autenticación de 2 factores. • Los usuarios deben finalizar la sesión en el sistema de información o abandonar temporal o permanentemente su lugar de trabajo. • Los datos deben ser borrados solamente con un algoritmo que garantice un borrado seguro. • El sistema de información solamente puede estar ubicado en salas con acceso físico controlado.	• El acceso al sistema de información debe estar controlado mediante una autenticación de 2 factores que utilice tarjetas inteligentes, tokens o lectores biométricos. • El sistema de información solamente puede ser instalado en servidores controlados por la organización. • El sistema de información solamente puede estar ubicado en salas con acceso físico controlado y con control de identidad de las personas.
Correo	• El remitente debe	• El correo	• Todos los correos

electrónico	verificar cuidadosamente el destinatario. • [illegible]	electrónico debe estar encriptado si se envía fuera de la organización. • [illegible]	electrónicos deben ser encriptados. • [illegible]
Medios de almacenamiento electrónico	• Los medios o archivos deben estar protegidos con clave. • [illegible]	• Los medios y archivos deben estar encriptados. • [illegible]	• Los medios y archivos deben estar encriptados • [illegible]
Información transmitida oralmente	• Las personas no autorizadas no deben estar presentes en la sala cuando se comunica la información.	• La sala debe estar insonorizada. • [illegible]	• La sala debe estar insonorizada. • [illegible]

*Los controles se implementan acumulativamente; es decir, los controles para cualquier nivel de confidencialidad conllevan los controles definidos para los niveles inferiores: si se establecen controles más estrictos para un nivel de confidencialidad mayor, sólo se implementan esos controles.

3.5. Enmascaramiento de datos

Commented [AES16]: Eliminar esta sección si se encontró que

Si el propietario del activo decide que la exposición de los datos es una preocupación (por ejemplo, información de identificación personal, secretos comerciales, etc.), la clasificación de la información debe ser al menos "RESTRINGIDO" y se deben aplicar las siguientes reglas adicionales para evitar que los datos sean presentados:

- [illegible]
- [illegible]

4. Gestión de registros guardados en base a este documento

Nombre del registro	*Ubicación de archivo*	[illegible]	[illegible]	[illegible]
[Lista de personas autorizadas con acceso a los documentos]	Junto con la información en la que se indica el nivel de confidencialidad	[illegible]	[illegible]	[illegible]

Commented [AES17]: Modifique este registro para que

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

[illegible]

Commented [AES18]: 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 incidentes relacionados con el acceso no autorizado a la información.
- [illegible]

[cargo]
[nombre]

[firma]

Commented [AES19]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.