[logo de la organización]

[nombre de la organización]

Commented [27A1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Commented [27A2]: 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/

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

Commented [27A3]: 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.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
DD-MM-AAAA	0.1	27001Academy	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS 3

2. DOCUMENTOS DE REFERENCIA 3

3. INFORMACIÓN CLASIFICADA 3

3.1. PASOS Y RESPONSABILIDADES 3
3.2. CLASIFICACIÓN DE LA INFORMACIÓN 4
3.2.1. Criterios de clasificación 4
3.2.2. Niveles de confidencialidad 4
3.2.3. Lista de personas autorizadas 4
3.2.4. Reclasificación 5
3.3. ETIQUETADO DE LA INFORMACIÓN 5
3.4. MANEJO DE INFORMACIÓN CLASIFICADA 5

4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO 8

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS 8

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

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].

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
- 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 operativos para el departamento de TI] / [Política de eliminación y destrucción]
- Política de seguridad de TI

Commented [27A4]: Si no tiene esta Lista, entonces aquí detalle toda la legislación y obligaciones contractuales relacionadas con clasificación de información.

Commented [27A5]: 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:

Nombre del paso	*Responsabilidad*
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

Si la información clasificada proviene de afuera de la organización, el [cargo] es el responsable de su [illegible]

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

3.2. Clasificación de la información

3.2.1. Criterios de clasificación

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

- [illegible]
- [illegible]
- Obligaciones legales y contractuales: según la [Lista de obligaciones legales, normativas y contractuales y de otra índole].

3.2.2. Niveles de confidencialidad

Toda la información debe ser clasificada en niveles de confidencialidad.

Nivel de confidencialidad	***Etiquetado***	[illegible]	***Restricción de acceso***
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

Commented [27A6]: 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

[illegible] cargos de las personas que tienen derechos de acceso para esa información.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

[redacted] organización tendrán acceso a esos documentos.

3.2.4. Reclasificación

Los propietarios de activos deben revisar el nivel confidencialidad de sus activos de información cada [redacted].

Commented [27A7]: Esto es sólo una recomendación; ajustar la frecuencia según sea necesario.

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 [redacted]
- **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 [redacted]
- **Soporte de almacenamiento electrónico** (discos, tarjetas de memoria, etc.): se debe indicar el nivel de confidencialidad sobre la superficie de cada soporte.
- **Información transmitida oralmente**: el nivel de confidencialidad de la información [redacted]

3.4. Manejo de información clasificada

Commented [27A8]: Todas las reglas mencionadas aquí deben ser adaptadas a las necesidades de la organización.

[redacted] 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 [redacted].

[redacted]

Commented [27A9]: Eliminar este párrafo si el control A.11.2.5 está excluido de la Declaración de aplicabilidad.

El método para borrado y destrucción segura de soportes está establecido en el documento [redacted]

Commented [27A10]: Escoger el documento que establece el borrado seguro de datos.

	Uso interno	*Restringida**	*Confidencial**
Documentos en papel	• Sólo las personas autorizadas pueden tener acceso.	• [redacted]	• El documento debe [redacted]

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

	• Si es enviado fuera de la organización, el documento debe ser [illegible] • [illegible] • [illegible]	llave. • Los documentos pueden ser [illegible] ser enviado con acuse de recibo. • Los documentos [illegible] copiarlo. • Solamente el [illegible]	• El documento puede ser transferido dentro y fuera de la organización [illegible] la persona autorizada está al [illegible]
Documentos electrónicos	• Sólo las personas [illegible] etc., deben estar protegidos con clave. • El acceso a los sistemas [illegible] • La pantalla en la que se muestra el documento debe bloquearse	• Sólo las personas con autorización [illegible] el documento. • Cuando se [illegible] instantánea, etc., deben estar [illegible]	• El documento debe [illegible] servidores controlados por la [illegible] • [illegible] instantánea, etc.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

	automáticamente luego de [cantidad] minutos de inactividad.	propietario del documento puede borrarlo.	
Controles de auditoría	• Sólo las personas [redacted] • [redacted] • [redacted] de [cantidad] minutos de inactividad. • [redacted]	• Los usuarios deben finalizar la sesión en [redacted] • [redacted]	• El acceso al sistema de información debe estar controlado mediante un proceso de [redacted] • [redacted] ser instalado en servidores controlados por la [redacted] • [redacted] control de identidad de las personas.
[redacted]	• Sólo las personas [redacted] • [redacted] • [redacted] "Sistemas de información".	• El correo [redacted]	• [redacted]
Soportes de [redacted]	• Sólo las personas [redacted] • [redacted] deben estar protegidos	• Los soportes y [redacted] • [redacted]	• El soporte debe ser [redacted] • [redacted] transferido dentro y

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

	con clave. • Si es enviado fuera de la organización, el soporte [redacted] • [redacted] físico controlado.	gabinete con llave. • Si es enviado fuera de la organización, [redacted] • [redacted] destruirlo.	fuera de la [redacted]
[redacted]	• Sólo las personas [redacted] • [redacted] comunica la información.	• La habitación debe [redacted] • [redacted]	• [redacted] • [redacted] conversación.

*Los controles se implementan acumulativamente; es decir, los controles para cualquier nivel de [redacted]

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
[Lista de personas autorizadas con acceso a los documentos]	Junto con la información en la que se indica el nivel de confidencialidad	Propietario del activo de información	El mismo que para la protección de información	Debe existir la lista siempre que exista la información propiamente dicha

Commented [27A11]: Modifique este registro para que coincida con lo que ya tiene en su empresa. Si no tiene un registro similar, puede crear uno nuevo en el formato que más le convenga.

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.

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.

Commented [27A12]: Esto es sólo una recomendación; ajustar la frecuencia según sea necesario.

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

- [illegible]
- [illegible]

[cargo]
[nombre]

_____
[firma]

Commented [27A13]: Sólo es necesario si el Procedimiento para control de documentos y registros establece que los documentos en papel deben ser firmados.

©2020 Esta plantilla puede ser utilizada por los clientes de Advisera Expert Solutions Ltd. www.advisera.com de acuerdo al contrato de licencia.