[logo de la organización]

[nombre de la organización]

POLÍTICA DEL USO DEL ENCRIPTADO

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

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

Commented [AES2]: Para obtener más información sobre este tema, lea este artículo:

How to use cryptography according to ISO 27001 control A.8.24
https://advisera.com/27001academy/how-to-use-the-cryptography-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.

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 definir reglas para el uso de los controles y claves criptográficas para proteger la confidencialidad, integridad, autenticidad e inviolabilidad de la información.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los sistemas e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son los [enumere los cargos de las personas que deben cumplir con esta Política].

Commented [AES4]: Por ejemplo: alta dirección, personal de TI, usuarios remotos, etc.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.5.31 y A.8.24
- Política de seguridad de la información
- [Política de clasificación de la información]
- [Lista de requisitos legales, normativos, contractuales y de otra índole]

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]: Si no tiene esta Lista, entonces detalle toda la legislación y contratos relacionados con el uso de criptografía.

3. Uso de criptografía

3.1. Controles criptográficos

De acuerdo con la Política de clasificación de la información, como también con obligaciones legales y contractuales, la organización debe proteger a los sistemas individuales o a la información a través de los siguientes controles criptográficos:

[illegible]	[illegible]	[illegible]	[illegible]
Sistema de pago electrónico	*Token de seguridad*	*Algoritmo AES*	*256 bits*
[illegible]	[illegible]	[illegible]	[illegible]

Commented [AES7]: También incluye canales de comunicación, [illegible]

Commented [AES8]: Enumere todo lo que está regulado por la [illegible]

El [cargo] es el responsable de redactar instrucciones detalladas sobre el uso de las mencionadas herramientas criptográficas. [illegible]

3.2. Claves criptográficas

Commented [AES9]: En la mayoría de los casos, la organización [illegible]

[Cargo] es el responsable de establecer las siguientes reglas sobre la gestión de claves:

- Generación de claves criptográficas privadas y públicas.
- Activación y distribución de claves criptográficas.
- Definición del plazo para el uso de las claves y de su actualización periódica (de acuerdo con la evaluación de riesgos).
- Almacenar claves, identificando quién tiene autorización para acceder a ellas.
- Manejo de claves comprometidas.
- Archivo de claves inactivas que son necesarias para archivos electrónicos encriptados.
- Destrucción de claves.

Las claves son administradas por sus propietarios, en conformidad con las reglas mencionadas precedentemente.

Las claves criptográficas serán protegidas [proporcionar una descripción de cómo se protegerán las claves ante pérdidas, modificación o destrucción]. En el caso de pérdida, corrupción o destrucción, las claves serán recuperadas [describir el método de recuperación].

Commented [AES10]: De acuerdo a las necesidades, es posible ampliar las responsabilidades.

Commented [AES11]: Por ejemplo: almacenándolos en un lugar

Commented [AES12]: Por ejemplo.: mediante copia de

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
[Registros de gestión de claves]	Ordenador del [cargo]	[cargo responsable de la gestión de claves]	Solamente el [cargo] tiene derecho de acceso a estos registros.	Los registros son almacenados por el plazo de 10 años.
[Instrucciones detalladas sobre el uso de herramientas criptográficas]	[Intranet de la organización]	[Cargo]	Solamente el [cargo] puede editar y publicar las instrucciones.	Las instrucciones no vigentes son almacenadas por el plazo de 5 años.
[Reglas para administración de claves]	[Intranet de la organización]	[Cargo]	Solamente el [Cargo] puede editar y publicar las reglas.	Las reglas no vigentes son almacenadas por el plazo de 5 años.

Commented [AES13]: Modifique estos registros para que

Commented [AES14]: Adaptar según sea necesario.

Solamente el [cargo] puede permitir a otros empleados el acceso a cualquiera de los registros mencionados precedentemente.

5. 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 cada año [fecha].

Commented [AES15]: 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 la pérdida, compromiso o destrucción de claves criptográficas.
- Cantidad de sistemas sobre los cuales se aplican controles criptográficos contrarios a esta Política.

[cargo]
[nombre]

[firma]

Commented [AES16]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.