[logo de la organización]

[nombre de la organización]

POLÍTICA DE CLAVES

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]: No es necesario escribir un documento separado para la Política de claves si las mismas reglas están establecidas en la Política de seguridad de TI y en la Política de control de acceso.

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 establecer reglas para garantizar la gestión y utilización seguras de las claves.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los puestos de trabajo y sistemas ubicados dentro del alcance del SGSI.

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.5.16, A.5.17 y A.5.18
- Política de seguridad de la información
- Declaración de aceptación de los documentos del SGSI

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".

3. Obligaciones de los usuarios

Commented [AES6]: Eliminar toda esta sección si las reglas ya

Los usuarios deben aplicar las siguientes buenas prácticas de seguridad en cuanto a la elección y uso de claves:

Commented [AES7]: Estos son solo ejemplos de mejores

- No se deben revelar las claves a otras personas, incluyendo la gerencia y los administradores del sistema.
- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por [cargo].
- Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.); las claves deben ser cambiadas a ambos indicios de que pueden estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).
- Se deben escoger claves seguras de la siguiente forma:
  - utilizando al menos 16 caracteres;
  - utilizando al menos un carácter numérico;
  - utilizando al menos un carácter alfabético en mayúscula y uno en minúscula;
  - utilizando al menos un carácter especial;
  - una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma, como tampoco ninguna de estas palabras escritas hacia atrás;
  - las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.);
  - no se deben usar nuevamente las últimas tres claves.
- Se deben cambiar las claves cada 3 meses.
- Se deben cambiar las claves en el primer ingreso al sistema.

- Las claves no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador).
- [illegible]

Cuando algunas de estas reglas escritas anteriormente no se pueden aplicar (por ejemplo, debido a las limitaciones de los sistemas), se deben usar las prácticas más sólidas disponibles.

4. Gestión de la clave del usuario

[illegible]

- Al firmar la Declaración de aceptación de los documentos del SGSI, los usuarios también aceptan la obligación de mantener sus claves en forma confidencial, como se establece en este documento.
- Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.
- Cada usuario debe tener la posibilidad de escoger su propia clave, en los casos corresponda.
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- Una clave no debe ser visible en la pantalla durante el inicio de sesión.
- Si un usuario ingresa una clave incorrecta tres veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión.
- [illegible]
- [illegible]

5. Validez y gestión de documentos

Commented [AES8]: Eliminar toda esta sección si las reglas ya [illegible]

Commented [AES9]: Adaptar estas reglas según los riesgos [illegible]

Commented [AES10]: Se pueden establecer reglas [illegible]

Commented [AES11]: Aquí se puede agregar más información.

Commented [AES12]: Por ejemplo, enviando un correo [illegible]

Commented [AES13]: Por ejemplo, ingresando al sistema [illegible]

Commented [AES14]: Por ejemplo, tres claves anteriores.

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.

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 el uso indebido de claves por personas no autorizadas.
- Cantidad de incidentes relacionados con el manejo inadecuado de claves.

[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.