[logo de la organización]

[nombre de la organización]

POLÍTICA DE CONTROL DE ACCESO

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 handle access control according to ISO 27001 https://advisera.com/27001academy/blog/2015/07/27/how-to-handle-access-control-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 de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados 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.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3, A.8.4, A.8.5 y A.8.11
- Política de seguridad de la información
- Declaración de aplicabilidad
- [Política de clasificación de la información]
- [Declaración de aceptación de los documentos del SGSI]
- [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]: 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 [AES7]: Si no tiene esta Lista, entonces aquí detalle toda la legislación y contratos que contengan requerimientos de control de acceso.

3. Control de acceso

3.1. Introducción

El principio básico del control de acceso es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios.

[redacted]

[redacted]

Commented [AES8]: Eliminar si la Política de clasificación de la [redacted]

3.2. Perfil de usuario A

Commented [AES9]: Adaptar al sistema de identificación [redacted]

El perfil de usuario A tiene los siguientes derechos de acceso:

Nombre del sistema / red / servicio	[redacted]

Commented [AES10]: Pueden ser especificados a nivel de todo [redacted]

Commented [AES11]: Especificar si incluyen derechos de [redacted]

Los siguientes cargos tienen derechos de acceso de acuerdo al Perfil de usuario A:

- [cargo 1]
- [cargo 2]

Commented [AES12]: Enumerar todos los cargos. También se

3.3. Perfil de usuario B

Commented [AES13]: Es posible enumerar perfiles de usuario

El perfil de usuario B tiene los siguientes derechos de acceso:

Nombre del sistema / red / servicio	[Derechos de usuario]

Commented [AES14]: Pueden ser especificados a nivel de todo

Commented [AES15]: Especificar si incluyen derechos de

Los siguientes cargos tienen derechos de acceso de acuerdo al Perfil de usuario B:

- [cargo 1]
- [cargo 2]

3.4. Gestión de privilegios

Commented [AES16]: Eliminar este punto si el control A.8.2

Los privilegios respecto de los perfiles de usuario mencionados anteriormente (concesión o eliminación de derechos de acceso) son asignados de la siguiente forma:

Commented [AES17]: Es posible reemplazar este cuadro con

Nombre del sistema / red / servicio / sector físico	[Quién está autorizado a conceder o eliminar derechos de acceso]	[Forma del proceso de autorización]

Commented [AES18]: Por correo electrónico, decisión escrita,

Al asignar privilegios, la persona responsable debe tener en cuenta los requerimientos de negocio y de seguridad para el acceso (definidos en la evaluación de riesgos), como también la clasificación de la información a la que se accede con esos derechos de acceso, de acuerdo con la Política de clasificación de la información.

3.5. Revisiones periódicas de los derechos de acceso

Los propietarios de cada sistema y de las instalaciones para los cuales se requieren derechos de acceso especiales deben, según los siguientes intervalos, revisar si los derechos de acceso concedidos se mantienen de acuerdo a los requerimientos de negocios y de seguridad:

Nombre del sistema / red / servicio / sector físico	Intervalos para revisiones periódicas

Cada revisión debe ser registrada [especificar cómo se llevan los registros].

3.6. Cambio de estado o finalización de un contrato

Cuando se produce un cambio o finalización de empleo, el [cargo] debe informar inmediatamente a la persona que autorizó los privilegios del empleado en cuestión.

Cuando se modifican las relaciones contractuales con entidades externas que tienen acceso a sistemas, servicios o instalaciones, o cuando finaliza el contrato, el propietario del contrato debe informar inmediatamente a las personas que administran los privilegios de las entidades externas en cuestión.

Los derechos de acceso para todas las personas que han modificado su condición de empleo o relación contractual deben ser eliminados o modificados inmediatamente por las personas responsables de acuerdo a lo que se define en la siguiente sección.

Commented [AES19]: Eliminar este punto si el control A.5.18 [illegible] no aplicable en la declaración de aplicabilidad.

Commented [AES20]: Adaptar en caso que sea necesario.

Commented [AES21]: La frecuencia debe ser definida, tomando en cuenta el nivel de riesgo relacionado con el sistema, según los resultados de la evaluación de riesgos.

Commented [AES22]: Se puede utilizar un formulario, un [illegible]

Commented [AES23]: Eliminar este punto si el control A.5.18 [illegible] no aplicable en la declaración de aplicabilidad.

3.7. Implementación técnica

La implementación técnica de la asignación o eliminación de derechos de acceso la realizan las siguientes personas:

Nombre del sistema / red / servicio / sector físico	[illegible]

Las personas detalladas en este cuadro no pueden asignar ni eliminar libremente los derechos de acceso, [illegible]

3.8. Autenticación segura

El [cargo] debe asegurarse de que se implemente un procedimiento de inicio de sesión seguro para todos los dispositivos, sistemas y servicios.

3.9. 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]

Commented [AES24]: Eliminar esta sección si el control A.8.5

Commented [AES25]: Eliminar este punto si la Política de claves

Commented [AES26]: Adaptar estas reglas según los riesgos

Commented [AES27]: Se pueden establecer reglas

Commented [AES28]: Aquí se puede agregar más información.

Commented [AES29]: Esta es solo una recomendación; puede

- Si el usuario solicita una nueva clave, el sistema de gestión de claves debe determinar la identidad del usuario [indicar cómo].
- El sistema de gestión de claves debe evitar la reutilización de las [especifique cuántas] últimas claves anteriores.
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Commented [AES30]: Por ejemplo, enviando un correo [illegible]

Commented [AES31]: Por ejemplo, tres claves anteriores.

Commented [AES32]: Por ejemplo, ingresando al sistema [illegible]

4. Gestión de registros guardados en base a este documento

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[Registro de asignación de privilegios (en formato electrónico, mensaje de correo electrónico)]	[carpeta de Intranet]	[cargo responsable de la implementación técnica]	Los registros no pueden ser editados, solamente el [cargo] puede guardar estos registros	Los registros son almacenados por el plazo de 3 años.
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Commented [AES33]: Modifique estos registros para que [illegible]

Commented [AES34]: Modificar según sea necesario.

Commented [AES35]: Modificar según sea necesario.

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

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

[illegible]

Commented [AES36]: Esto es sólo una recomendación; ajustar [illegible]

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.
- Cambio de derechos de acceso demorados en caso de cambio o finalización de empleo o contratos.
- [illegible]
- [illegible]

[cargo]
[nombre]

[firma]

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