

[logo de la organización]

[nombre de la organización]

PROCEDIMIENTOS PARA TRABAJO EN ÁREAS SEGURAS

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 estos artículos:

- Physical security in ISO 27001: How to protect the secure areas
<https://advisera.com/27001academy/blog/2015/03/23/physical-security-in-iso-27001-how-to-protect-the-secure-areas/>
- The most common physical and network controls when implementing ISO 27001 in a data center
<https://advisera.com/27001academy/blog/2019/02/26/the-most-common-physical-and-network-controls-when-implementing-iso-27001-in-a-data-center/>

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.....3

2. DOCUMENTOS DE REFERENCIA.....3

3. REGLAS PARA ÁREAS SEGURAS.....3

3.1. LISTA DE ÁREAS SEGURAS 3

3.2. DERECHO DE ACCESO A ÁREAS SEGURAS..... 3

3.3. CONTROLES DE INGRESO 3

3.4. MONITOREO CONTINUO 3

3.5. ACCESO DE VISITANTES 3

3.6. ACTIVIDADES PROHIBIDAS 4

3.7. VERIFICACIONES PERIÓDICAS..... 4

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

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS 5

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir las reglas básicas de comportamiento en las áreas seguras.

Este documento se aplica a todas las áreas seguras del Sistema de Gestión de Seguridad de la Información (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.7.4 y A.7.6
- Política de control de acceso
- Inventario de activos

Commented [AES5]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "09_Anexo_A_de_ISO_27001_Controles_de_seguridad".

Commented [AES6]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "09_Anexo_A_de_ISO_27001_Controles_de_seguridad".

3. Reglas para áreas seguras

3.1. Lista de áreas seguras

Este procedimiento es aplicable a las siguientes áreas seguras:

- *

Commented [AES7]: Detallar aquí todas las instalaciones; por ejemplo, planta de energía.

Las personas responsables para cada área segura se detallan en el Inventario de activos.

3.2. Derecho de acceso a áreas seguras

El acceso a las áreas seguras se autoriza de acuerdo con la Política de control de acceso.

3.3. Controles de ingreso

El acceso a las áreas seguras está protegido con los siguientes controles de ingreso:

- *

Commented [AES8]: Enumerar los controles; por ejemplo, control de acceso físico, control de acceso lógico.

3.4. Monitoreo continuo

El [cargo] es responsable del monitoreo continuo de las áreas seguras con el fin de detectar accesos no autorizados e incidentes de seguridad, a través de los siguientes medios:

Commented [AES9]: Elimine esta sección si el control A.7.4 no es aplicable.

Commented [AES10]: Por ejemplo, gerente de seguridad, CISO, administrador de sistemas.

- *

Commented [AES11]: Enumere todos los medios utilizados para el monitoreo; por ejemplo, cámaras de video, sensores de movimiento.

3.5. Acceso de visitantes

Las personas que no son empleados de [nombre de la organización] (en adelante, visitantes) deben obtener un permiso de acceso de acuerdo con la Política de control de acceso.

Commented [AES12]: Incluya el nombre de su organización.

Los visitantes pueden ingresar y permanecer en las áreas seguras solamente cuando esté presente un empleado designado; este empleado debe acompañar al visitante durante toda su estadía en el área segura.

Los temas permitidos de discusión o título de las reuniones en las áreas seguras serán registrados en [AES13] por el [cargos].

3.6. Actividades prohibidas

En las áreas seguras no está permitido:

- Realizar ningún tipo de grabación fotográfica, de audio o de video.
- Enchufar cualquier dispositivo eléctrico en una red eléctrica a menos que esté específicamente autorizado para hacerlo.

- Tener o manejar de cualquier forma cualquier dispositivo en áreas seguras a menos que esté específicamente autorizado para hacerlo.
- Conectar cualquier dispositivo a una red o sistema que esté específicamente autorizado para hacerlo.
- Almacenar una gran cantidad de papales.
- Usar dispositivos o equipos inalámbricos.
- Utilizar cualquier tipo de dispositivo de almacenamiento.
- Tener comida o beber.

3.7. Verificaciones periódicas

Si [nombre del área segura] no se ha utilizado durante [período de tiempo], el [cargo] debe verificar si cumple los requerimientos de seguridad y protección.

4. Gestión de registros guardados en base a este documento

Nombre del registro	Nombre del sistema	Personas responsables del registro	Acciones para la protección del registro	Período de retención
[Registros de lectura de tarjetas]	[nombre del sistema]	[cargo]	Solamente el [cargo] tiene acceso al sistema.	3 años
[Registros de la cámara de CCTV]	[nombre del sistema]	[cargo]	[acciones de registro] [acciones de acceso al sistema]	[años]
[Registros de nombre del sistema]	[nombre del sistema] [nombre de la aplicación]	[cargo]	[acciones de registro] [acciones de acceso al sistema]	[años]

Commented [AES13]: Escriba aquí el nombre de la aplicación

[acciones de registro] [acciones de acceso al sistema]

Commented [AES14]: Por ejemplo, más de seis meses

Commented [AES15]: Modifique estos registros para que

Commented [AES16]: Adaptar este período en función de sus

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el [cargos], que debe verificar y/o reemplazar actualizado el documento por lo menos **una vez al año**.

Commented [AES17]: 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 que surgen por el no cumplimiento de este documento.

[cargos]

[nombre]

[firma]

Commented [AES18]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.