[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

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 [illegible]

Las personas responsables para cada área segura se detallan [illegible]

3.2. Derecho de acceso a áreas seguras

El acceso a las áreas seguras se autoriza de acuerdo con [illegible]

3.3. Controles de ingreso

El acceso a las áreas seguras está protegido con [illegible]

- *

Commented [AES8]: Enumerar los controles; por ejemplo, [illegible]

3.4. Monitoreo continuo

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

El [cargo] es responsable del monitoreo continuo de las áreas seguras con el fin de detectar accesos [illegible]

Commented [AES10]: Por ejemplo, gerente de seguridad, CISO, [illegible]

- *

Commented [AES11]: Enumere todos los medios utilizados [illegible]

3.5. Acceso de visitantes

Las personas que no son empleados de [nombre de la organización] (en adelante, visitantes) [illegible]

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.

[redacted]

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

3.6. Actividades prohibidas

En las áreas seguras no está permitido:

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

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.

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

4. Gestión de registros guardados en base a este documento

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[Registros de lectura de tarjetas]	[nombre del sistema]	[cargo]	Solamente el [cargo] tiene acceso al sistema.	3 años
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Commented [AES15]: Modifique estos registros para que [redacted]

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

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

[illegible]

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

[cargo]
[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.