

[Línea horizontal para el código de la declaración]

**Commented [AES1]:** Para saber cómo completar este documento, y ver ejemplos reales de lo que necesita escribir, vea este tutorial en vídeo: "How to Write ISO 27001 Statement of Applicability".

Para acceder al tutorial: en su bandeja de entrada, busque el correo electrónico que recibió en el momento de la compra. Allí, verá un enlace y una contraseña que le permitirán acceder al tutorial en vídeo.

[logo de la organización]

**Commented [AES2]:** Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

[nombre de la organización]

### DECLARACIÓN DE APLICABILIDAD

**Commented [AES3]:** Para aprender a escribir la Declaración de aplicabilidad, lea este artículo:

La importancia de la Declaración de aplicabilidad para la norma ISO 27001 <https://advisera.com/27001academy/es/knowledgebase/la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001/>

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

**Commented [AES4]:** El sistema de codificación de documentos debe estar en línea con el sistema existente de la organización para la codificación de documentos; en caso de que no exista tal sistema, esta línea puede eliminarse.

### Historial de cambios

Fecha	Versión	Creado por	Descripción del cambio
	0.1	Advisera	Esquema básico del documento

### Tabla de contenido

- 1. OBJETIVO, ALCANCE Y USUARIOS.....3
- 2. DOCUMENTOS DE REFERENCIA.....3
- 3. APLICABILIDAD DE LOS CONTROLES .....3
- 4. ACEPTACIÓN DE RIESGOS RESIDUALES ..... 19
- 5. VALIDEZ Y GESTIÓN DE DOCUMENTOS ..... 19

### 1. Objetivo, alcance y usuarios

El propósito de este documento es definir qué controles son apropiados para implementar en [nombre de la organización], los objetivos de estos controles y cómo se implementan, así como aprobar los riesgos residuales y aprobar formalmente la implementación de dichos controles.

Este documento incluye todos los controles enumerados en el Anexo A de la norma ISO 27001. Los controles son aplicables a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

Los usuarios de este documento son todos los empleados de [nombre de la organización] que tienen un rol en el SGSI.

Commented [AES5]: Incluya el nombre de su organización.

### 2. Documentos de referencia

- Norma ISO/IEC 27001, cláusula 6.1.3 d)
- Política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Informe sobre la evaluación y tratamiento de riesgos

Commented [AES6]: Incluya el nombre de su organización.

Commented [AES7]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "05\_Políticas\_generales".

Commented [AES8]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "06\_Evaluacion\_y\_tratamiento\_de\_riesgos".

Commented [AES9]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "06\_Evaluacion\_y\_tratamiento\_de\_riesgos".

Commented [AES10]: Para obtener más información sobre los controles del Anexo A de ISO 27001, eche un vistazo a este libro:

### 3. Aplicabilidad de los controles

Los siguientes controles del Anexo A de ISO 27001 son aplicables:

Identificación	Descripción	Aplicabilidad	Residual	Tratamiento	Residual	Tratamiento
A.5.1	Políticas para seguridad de la información					Todas las políticas a las que se hace referencia a continuación en esta columna; cada póliza tiene un propietario designado que tiene que revisar el documento a intervalos planificados.

Commented [AES15]: Indique el estado de implementación, [ ] para no aplicable, [ ] para aplicable.

Commented [AES14]: Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

Commented [AES13]: Para obtener más información sobre los objetivos de control, lea este artículo: [ ]

Commented [AES11]: Con base en los resultados de la [ ]

Commented [AES12]: Deben definirse para cada uno de sus [ ]

Commented [AES13]: Para obtener más información sobre los objetivos de control, lea este artículo: [ ]

ID	Descripción del control	Categoría	Estado	Evidencia	Observaciones
A.5.2	Roles y responsabilidades sobre seguridad de la información				Los roles y responsabilidades para la seguridad de la información se enumeran en varios documentos del SGSI. Si es necesario, el [cargo] define roles y responsabilidades adicionales
A.5.2	[Faint text]				[Faint text]
A.5.2	[Faint text]				[Faint text]
A.5.2	[Faint text]				[Faint text]

**Commented [AES15]:** Indique el estado de implementación, [Faint text]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable. [Faint text]

**Commented [AES11]:** Con base en los resultados de la [Faint text]

**Commented [AES12]:** Deben definirse para cada uno de sus [Faint text]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [Faint text]

Control	Objetivo del control	Descripción del control	Indicador de riesgo	Indicador de control	Indicador de cumplimiento
A.5.6	Contacto con grupos de interés especial			El [cargo] es responsable de monitorear [enumere los nombres de los grupos de interés y los foros de seguridad]	

**Commented [AES15]:** Indique el estado de implementación, [AES15]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable. [AES14]

**Commented [AES11]:** Con base en los resultados de la [AES11]

**Commented [AES12]:** Deben definirse para cada uno de sus [AES12]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [AES13]

**Commented [AES16]:** Se pueden asignar diferentes grupos de [AES16]

ID	Objetivo de Control	Objetivo de Información	Objetivo de Seguridad	Objetivo de Disponibilidad	Objetivo de Integridad	Objetivo de Confidencialidad
A.5.10	Uso aceptable de la información y otros activos asociados					[Política de seguridad de TI], [Política de clasificación de la información]
A.5.10.1	Identificación de activos					[Política de seguridad de TI], [Política de clasificación de la información]
A.5.10.2	Clasificación de la información					[Política de clasificación de la información]
A.5.10.3	Respaldo de la información					[Política de clasificación de la información]
A.5.14	Transferencia de la información					[Procedimientos de seguridad para el departamento de TI] / [Política de transferencia de información], [Política Trae tu propio dispositivo (BYOD)], [Política de clasificación de la información], [Política de seguridad de TI]
A.5.14.1	Identificación de activos					[Política de seguridad de TI], [Política de clasificación de la información]
A.5.14.2	Identificación de identidad					[Política de seguridad de TI], [Política de clasificación de la información], [Política de transferencia de información]
A.5.14.3	Identificación de dispositivos					[Política de seguridad de TI], [Política de clasificación de la información], [Política de transferencia de información], [Política de seguridad de TI]
A.5.14.4	Identificación de activos					[Política de seguridad de TI], [Política de clasificación de la información]

**Commented [AES15]:** Indique el estado de implementación, [Política de seguridad de TI], [Política de clasificación de la información]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

[Política de seguridad de TI], [Política de clasificación de la información]

[Política de seguridad de TI], [Política de clasificación de la información]

[Política de seguridad de TI], [Política de clasificación de la información]

**Commented [AES11]:** Con base en los resultados de la [Política de seguridad de TI], [Política de clasificación de la información]

**Commented [AES12]:** Deben definirse para cada uno de sus [Política de seguridad de TI], [Política de clasificación de la información]

[Política de seguridad de TI], [Política de clasificación de la información]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [Política de seguridad de TI], [Política de clasificación de la información]

	Objetivo de control	Criterios de control	Evidencias de control	Evidencias de control	Evidencias de control
A.5.19	Seguridad de la información en las relaciones con los proveedores				[Política de seguridad para proveedores]
A.5.20	Abordar la seguridad de la información en los acuerdos con los proveedores				[Política de seguridad para proveedores], cláusulas de seguridad seleccionadas del documento [Cláusulas de seguridad para proveedores y socios]
A.5.21	Seguridad de la propiedad de la información en la cadena de custodia de la TI				Política de seguridad para proveedores
A.5.22	Seguridad de la propiedad de la información en la cadena de custodia de servicios de proveedores				Política de seguridad para proveedores
A.5.23	Seguridad de la información en el uso de servicios de proveedores				Política de seguridad para proveedores
A.5.24	Seguridad y privacidad en el uso de la propiedad de la información de proveedores de información				Procedimientos de gestión de proveedores
A.5.25	Seguridad y privacidad en el uso de la propiedad de la información de proveedores de información				Procedimientos de gestión de proveedores
A.5.26	Seguridad y privacidad de la propiedad de la información				Procedimientos de gestión de proveedores

**Commented [AES15]:** Indique el estado de implementación, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la auditoría.

**Commented [AES12]:** Deben definirse para cada uno de sus objetivos de control.

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo:

**Commented [AES17]:** Escriba esto solo si la gestión de la información.

ID	Descripción del control	Categoría	Estado	Evidencia	Referencias
A.5.27	Aprendizaje a partir de los incidentes en seguridad de la información				[Procedimiento para gestión de incidentes], [Procedimiento para la acción correctiva], [Formulario de revisión post-incidente]
A.5.28	Resolución de incidentes				[Procedimiento para gestión de incidentes], [Formulario de revisión post-incidente]
A.5.29	Seguridad de la información de los proveedores				[Procedimiento para gestión de incidentes], [Formulario de revisión post-incidente]

**Commented [AES15]:** Indique el estado de implementación, [Procedimiento para gestión de incidentes], [Formulario de revisión post-incidente]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la [Procedimiento para gestión de incidentes], [Formulario de revisión post-incidente]

**Commented [AES12]:** Deben definirse para cada uno de sus [Procedimiento para gestión de incidentes], [Formulario de revisión post-incidente]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [Procedimiento para gestión de incidentes], [Formulario de revisión post-incidente]



ID	Descripción del control	Categoría	Nivel de riesgo	Evidencia	Estado
A.5.30	Preparación de las TIC para la continuidad del negocio			Plan de recuperación ante desastres], [Procedimiento para auditoría interna]	
A.5.31	Requisitos legales, estatutarios, reglamentarios y contractuales			[Procedimiento para la identificación de requisitos], [Lista de requisitos legales, normativos, contractuales y de otra índole], [Política del uso del encriptado]	
A.5.32	[Descripción del control]			[Evidencia]	
A.5.33	[Descripción del control]			[Evidencia]	
A.5.34	[Descripción del control]			[Evidencia]	
A.5.35	[Descripción del control]			[Evidencia]	

**Commented [AES15]:** Indique el estado de implementación, [Evidencia]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la [Evidencia]

**Commented [AES12]:** Deben definirse para cada uno de sus [Evidencia]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [Evidencia]

ID	Descripción del control	Categoría	Estado	Evidencia	Implementación
A.5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información				Todos los propietarios de activos de información, así como la dirección, revisan periódicamente la implementación de controles de seguridad; el [cargo] es responsable de verificar el cumplimiento técnico de los sistemas de información con los requisitos de seguridad
A.5.37	Procedimientos operativos documentados				Procedimientos de seguridad de la información
A.5.38	Evaluación				Evaluación de la implementación de los controles de seguridad

**Commented [AES15]:** Indique el estado de implementación, [estado de implementación]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la [evaluación]

**Commented [AES12]:** Deben definirse para cada uno de sus [objetivos de control]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [enlace]

**Commented [AES18]:** Por ejemplo, verificar el CV, contactar a [persona]

ID	Objetivo de Control	Categoría de Control	Tipo de Control	Evidencia	Descripción del Control
A.6.2	Términos y condiciones de empleo				Todos los empleados firman la [Declaración de aceptación de los documentos del SGSI] y la [Declaración de confidencialidad]; [Política de seguridad para proveedores]
A.6.3	Confidencialidad, integridad y disponibilidad de la información				<ul style="list-style-type: none"> <li>Política de confidencialidad</li> <li>Política de integridad</li> <li>Política de disponibilidad</li> <li>Política de seguridad de la información</li> <li>Política de seguridad de los datos</li> <li>Política de seguridad de los sistemas de información</li> <li>Política de seguridad de los recursos humanos</li> <li>Política de seguridad de los recursos tecnológicos</li> <li>Política de seguridad de los recursos financieros</li> <li>Política de seguridad de los recursos legales</li> <li>Política de seguridad de los recursos físicos</li> <li>Política de seguridad de los recursos ambientales</li> <li>Política de seguridad de los recursos sociales</li> <li>Política de seguridad de los recursos culturales</li> <li>Política de seguridad de los recursos educativos</li> <li>Política de seguridad de los recursos científicos</li> <li>Política de seguridad de los recursos tecnológicos</li> <li>Política de seguridad de los recursos financieros</li> <li>Política de seguridad de los recursos legales</li> <li>Política de seguridad de los recursos físicos</li> <li>Política de seguridad de los recursos ambientales</li> <li>Política de seguridad de los recursos sociales</li> <li>Política de seguridad de los recursos culturales</li> <li>Política de seguridad de los recursos educativos</li> <li>Política de seguridad de los recursos científicos</li> </ul>
A.6.4	Proceso de gestión				<ul style="list-style-type: none"> <li>Política de gestión</li> <li>Política de gestión de la calidad</li> <li>Política de gestión de la innovación</li> <li>Política de gestión de la sostenibilidad</li> <li>Política de gestión de la reputación</li> <li>Política de gestión de la responsabilidad social</li> <li>Política de gestión de la ética</li> <li>Política de gestión de la transparencia</li> <li>Política de gestión de la comunicación</li> <li>Política de gestión de la cultura organizacional</li> <li>Política de gestión de la diversidad</li> <li>Política de gestión de la inclusión</li> <li>Política de gestión de la equidad</li> <li>Política de gestión de la justicia</li> <li>Política de gestión de la libertad</li> <li>Política de gestión de la paz</li> <li>Política de gestión de la seguridad</li> <li>Política de gestión de la salud</li> <li>Política de gestión de la educación</li> <li>Política de gestión de la ciencia</li> <li>Política de gestión de la tecnología</li> <li>Política de gestión de los recursos humanos</li> <li>Política de gestión de los recursos tecnológicos</li> <li>Política de gestión de los recursos financieros</li> <li>Política de gestión de los recursos legales</li> <li>Política de gestión de los recursos físicos</li> <li>Política de gestión de los recursos ambientales</li> <li>Política de gestión de los recursos sociales</li> <li>Política de gestión de los recursos culturales</li> <li>Política de gestión de los recursos educativos</li> <li>Política de gestión de los recursos científicos</li> </ul>
A.6.5	Seguridad de la información, integridad y disponibilidad de la información				<ul style="list-style-type: none"> <li>Política de seguridad de la información</li> <li>Política de integridad de la información</li> <li>Política de disponibilidad de la información</li> <li>Política de seguridad de los datos</li> <li>Política de seguridad de los sistemas de información</li> <li>Política de seguridad de los recursos humanos</li> <li>Política de seguridad de los recursos tecnológicos</li> <li>Política de seguridad de los recursos financieros</li> <li>Política de seguridad de los recursos legales</li> <li>Política de seguridad de los recursos físicos</li> <li>Política de seguridad de los recursos ambientales</li> <li>Política de seguridad de los recursos sociales</li> <li>Política de seguridad de los recursos culturales</li> <li>Política de seguridad de los recursos educativos</li> <li>Política de seguridad de los recursos científicos</li> </ul>

**Commented [AES15]:** Indique el estado de implementación, [Declaración de aceptación de los documentos del SGSI] y la [Declaración de confidencialidad]; [Política de seguridad para proveedores]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la [Declaración de aceptación de los documentos del SGSI] y la [Declaración de confidencialidad]; [Política de seguridad para proveedores]

**Commented [AES12]:** Deben definirse para cada uno de sus [Declaración de aceptación de los documentos del SGSI] y la [Declaración de confidencialidad]; [Política de seguridad para proveedores]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [Declaración de aceptación de los documentos del SGSI] y la [Declaración de confidencialidad]; [Política de seguridad para proveedores]

**Commented [AES19]:** Vea la lista de videos gratuitos de [Declaración de aceptación de los documentos del SGSI] y la [Declaración de confidencialidad]; [Política de seguridad para proveedores]

ID	Descripción del control	Categoría	Estado	Fecha de revisión	Implementación
A.6.6	Acuerdos de confidencialidad o no divulgación				El formulario [Declaración de confidencialidad] se utilizará para todos los empleados y terceros relevantes; el formulario debe ser revisado por [cargo] [una vez al año]
A.6.7	Trabajo remoto				Procedimientos de seguridad de la información
A.6.8	Almacenamiento de información				Procedimientos de seguridad de la información
A.6.9	Sistemas de seguridad física				Procedimientos de seguridad de la información
A.6.10	Seguridad física				Procedimientos de seguridad de la información

**Commented [AES15]:** Indique el estado de implementación, [estado de implementación]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la [evaluación]

**Commented [AES12]:** Deben definirse para cada uno de sus [objetivos de control]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [enlace]

**Commented [AES20]:** Por ejemplo, oficinas, archivos, almacenes, centros de datos, etc..

**Commented [AES21]:** Por ejemplo, con paredes, sistemas de [seguridad]

**Commented [AES22]:** Por ejemplo, tarjetas de acceso, guardias [de seguridad]

**Commented [AES23]:** Por ejemplo, tarjetas de acceso, guardias [de seguridad]

**Commented [AES24]:** Por ejemplo, la puerta trasera de su [edificio]

**Commented [AES25]:** Por ejemplo, con paredes, sistemas de [seguridad]

ID	Objetivo de control	Categoría	Estado	Evidencia	Implementación
A.7.3	Asegurar oficinas, salas e instalaciones				No se puede acceder a las instalaciones desde las áreas públicas y las áreas seguras no son perceptibles para las personas externas
A.7.3.1	Monitoreo de seguridad física			Procedimientos de monitoreo de seguridad física	
A.7.3.2	Procedimientos de seguridad física			Procedimientos de seguridad física	
A.7.3.3	Trabaja en áreas seguras			Procedimientos de seguridad física	
A.7.3.4	Seguridad controlada			Procedimientos de seguridad física	

**Commented [AES15]:** Indique el estado de implementación, el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la

**Commented [AES12]:** Deben definirse para cada uno de sus

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo:

**Commented [AES26]:** Por ejemplo, con monitoreo de video,

**Commented [AES27]:** Por ejemplo, central de monitoreo de

	Objetivo del control	Requisitos	Evidencia	Evaluación	Implementación	Evaluación
A.7.8	Ubicación y protección del equipo				<p>Todo el equipo está ubicado en un área protegida físicamente, y el equipo altamente sensible [especifique cuál] está ubicado en [nombre del área segura]</p>	
A.7.9	Seguridad de los centros de datos de las instalaciones				<p>Procedimientos de seguridad de IT Procedimientos de seguridad Alquileres Acceso de seguridad Acceso de seguridad de red Acceso de seguridad de red Acceso de seguridad de red</p>	
A.7.10	Seguridad de las instalaciones de IT				<p>Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT</p>	
A.7.11	Seguridad de las instalaciones de IT				<p>Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT Procedimientos de seguridad de IT</p>	

**Commented [AES15]:** Indique el estado de implementación,   
 [estado de implementación]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la   
 [evaluación de la implementación]

**Commented [AES12]:** Deben definirse para cada uno de sus   
 [objetivos de control]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo:   
 [enlace]

**Commented [AES28]:** Por ejemplo, sala de servidores.

**Commented [AES29]:** Por ejemplo, UPS, generador de energía, etc.

ID	Objetivo de Control	Categoría de Control	Código de Control	Tipo de Control	Descripción de Control
A.7.12	Seguridad del cableado				Los cables de energía y datos se instalan dentro del área segura de la organización, y donde esto no ha sido posible, se protegen [especifique cómo]
A.7.13	Seguridad de la información				Procedimientos de seguridad de la información
A.7.14	Seguridad de la información				Procedimientos de seguridad de la información
A.7.15	Seguridad de la información				Procedimientos de seguridad de la información
A.7.16	Seguridad de la información				Procedimientos de seguridad de la información

**Commented [AES15]:** Indique el estado de implementación, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la implementación del control, indique si el control es aplicable.

**Commented [AES12]:** Deben definirse para cada uno de sus objetivos de control, los procedimientos de implementación del control.

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [https://www.advisera.com/es/controls/controls-101/](#)

**Commented [AES30]:** Por ejemplo, protectores de cables, cerraduras de seguridad.

ID	Objetivo de Control	Control	Estado	Implementación	Referencia
A.8.3	Restricción al acceso a la información			[Política de control de acceso], [Política de clasificación de la información]	
A.8.4	Acceso al código fuente			[Procedimientos de seguridad para el departamento de TI], [Política de control de acceso]	
A.8.5	Identificación de riesgos			[Política de control de acceso], [Política de clasificación de la información]	
A.8.6	Control de seguridad			[Procedimientos de seguridad en el departamento de TI]	
A.8.7	Protección de datos críticos			[Procedimientos de seguridad en el departamento de TI], [Política de clasificación de TI]	
A.8.8	Control de confidencialidad de datos			[Procedimientos de seguridad en el departamento de TI]	
A.8.9	Control de configuración			[Procedimientos de seguridad en el departamento de TI]	
A.8.10	Eliminación de información			[Política de seguridad de TI], [Política de clasificación de la información], [Procedimientos de seguridad en el departamento de TI]	

**Commented [AES15]:** Indique el estado de implementación, [estado de implementación]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

[Procedimientos de seguridad en el departamento de TI], [Política de clasificación de la información]

[Procedimientos de seguridad en el departamento de TI], [Política de clasificación de la información]

[Procedimientos de seguridad en el departamento de TI], [Política de clasificación de la información]

**Commented [AES11]:** Con base en los resultados de la [evaluación de riesgos]

**Commented [AES12]:** Deben definirse para cada uno de sus [objetivos de control]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo:

[Enlace a artículo de referencia]



ID	Descripción del control	Objetivo	Referencia	Estado	Implementación	Comentarios
A.8.11	Enmascaramiento de datos				[Política de clasificación de la información], [Política de control de acceso], [Política de desarrollo seguro]	
A.8.12	Prevención de fuga de datos				[Política de clasificación de la información], [Política de seguridad de TI], [Procedimientos de seguridad para el departamento de TI]	
A.8.13	Clasificación de la información				Procedimientos de seguridad de TI, Políticas de seguridad de TI, Políticas de seguridad de TI	
A.8.14	Procedimientos de seguridad de TI				Políticas de seguridad de TI, Políticas de seguridad de TI, Políticas de seguridad de TI	
A.8.15	Seguros				Procedimientos de seguridad de TI, Políticas de seguridad de TI	
A.8.16	Actividades de mantenimiento				Procedimientos de seguridad de TI, Políticas de seguridad de TI	
A.8.17	Desarrollo seguro				Procedimientos de seguridad de TI, Políticas de seguridad de TI	

**Commented [AES15]:** Indique el estado de implementación, el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la

**Commented [AES12]:** Deben definirse para cada uno de sus

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo:

ID	Objetivo de Control	Objetivo de Control	Objetivo de Control	Objetivo de Control	Objetivo de Control	Objetivo de Control
A.8.18	Uso de programas de utilidad privilegiados				[Procedimientos de seguridad para el departamento de TI]	
A.8.19	Instalación de software en sistemas operativos				[Política de seguridad de TI]	
A.8.20	Disponibilidad de roles				Procedimientos de seguridad en el departamento de TI	
A.8.21	Disponibilidad de los servicios de red				Procedimientos de seguridad en el departamento de TI	
A.8.22	Disponibilidad de roles				Procedimientos de seguridad en el departamento de TI	
A.8.23	Uso de roles				Política de seguridad de TI Procedimientos de seguridad en el departamento de TI	
A.8.24	Uso de privilegios				Política de seguridad de TI	
A.8.25	Uso de roles de administrador de red				Política de seguridad de red	
A.8.26	Procedimientos de seguridad de los sistemas				Política de seguridad de red	
A.8.27	Procedimientos de configuración y registro de sistemas operativos				Política de seguridad de red	
A.8.28	Configuración de red				Política de seguridad de red	
A.8.29	Procedimientos de seguridad de dispositivos de red				Política de seguridad de red	
A.8.30	Disponibilidad de roles				Política de seguridad de red Procedimientos de seguridad en el departamento de TI Política de seguridad de red	

**Commented [AES15]:** Indique el estado de implementación, el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la

**Commented [AES12]:** Deben definirse para cada uno de sus

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo:

No.	Nombre del activo	Procedimiento de control	Estado	Responsable	Fecha de revisión	Fecha de implementación
A.8.31	Separación de los entornos de desarrollo, prueba y producción	[Procedimientos de seguridad para el departamento de TI], [Política de desarrollo seguro]				
A.8.32	Control de acceso	Procedimientos de seguridad en el departamento de TI, Política de gestión de cambios, Política de seguridad de desarrollo seguro				
A.8.33	Información de control	Política de desarrollo seguro				
A.8.34	Procedimientos de control de acceso	Procedimientos de seguridad en el departamento de TI, Política de gestión de cambios, Política de seguridad de desarrollo seguro				

**Commented [AES15]:** Indique el estado de implementación, [estado de implementación]

**Commented [AES14]:** Método de implementación: especifique el documento, el control técnico o describa el proceso. Déjelo en blanco si el control está marcado como no aplicable.

**Commented [AES11]:** Con base en los resultados de la [evaluación]

**Commented [AES12]:** Deben definirse para cada uno de sus [objetivos de control]

**Commented [AES13]:** Para obtener más información sobre los objetivos de control, lea este artículo: [enlace]

**Commented [AES31]:** La aceptación de riesgos residuales debe [definirse]

**Commented [AES32]:** Borrar este texto y el cuadro si no existen [datos]

#### 4. Aceptación de riesgos residuales

Dado que no todos los riesgos pueden reducirse en el proceso de gestión de riesgos, por la presente se aceptan todos los riesgos residuales:

1. todos los riesgos con el valor 0, 1 o 2

[Texto de comentario relacionado con la lista de riesgos]

[Completar el cuadro con datos de todos los riesgos específicos que no son aceptables; utilizar el Cuadro de tratamiento de riesgos para tomar los datos.]

No.	Nombre del activo	Procedimiento de control	Estado	Responsable	Fecha de revisión	Fecha de implementación

#### 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 al año e inmediatamente después de las revisiones de evaluación

**Commented [AES33]:** Esto es sólo una recomendación; ajustar [datos]

de riesgos y de las actualizaciones del Cuadro de evaluación de riesgos y del Cuadro de tratamiento de riesgos.

Al evaluar la efectividad y adecuación de este documento, se deben considerar los siguientes criterios:

- Cantidad de no conformidades debido métodos de implementación de controles específicos no definidos claramente.
- Cantidad de no conformidades debido a deficiencias del control no definidos claramente.
- Cantidad de controles para los cuales no se pueden hacer ningún tipo de ajustes.

[cargo]

[nombre]

**Commented [AES34]:** La Declaración de aplicabilidad debe ser [redacted]

[firma]

**Commented [AES35]:** Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.