\*\* VERSIÓN DE MUESTRA GRATIS \*\*

Gracias por descargar la vista previa gratuita del Paquete de documentos de ISO 27001.

[logo de la organización]

[nombre de la organización]

**PROCEDIMIENTOS DE SEGURIDAD PARA EL DEPARTAMENTO DE TI**

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

**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 4](#_Toc129594825)

[2. Documentos de referencia 4](#_Toc129594826)

[3. Procedimientos de seguridad para el departamento de TI 4](#_Toc129594827)

[3.1. Gestión de cambios 4](#_Toc129594828)

[3.2. Gestión de configuración 5](#_Toc129594829)

[3.3. Gestión de capacidad 5](#_Toc129594830)

[3.4. Protección antivirus 5](#_Toc129594831)

[3.5. Copias de seguridad 5](#_Toc129594832)

[3.5.1. Procedimiento para copias de seguridad 5](#_Toc129594833)

[3.5.2. Prueba de las copias de seguridad 5](#_Toc129594834)

[3.6. Gestión de seguridad de red 6](#_Toc129594835)

[3.7. Servicios de red 6](#_Toc129594836)

[3.8. Eliminación de datos 6](#_Toc129594837)

[3.9. Eliminación y destrucción de equipos y medios 7](#_Toc129594838)

[3.9.1. Equipos 7](#_Toc129594839)

[3.9.2. Medios de almacenamiento móviles 7](#_Toc129594840)

[3.9.3. Medios en papel 7](#_Toc129594841)

[3.9.4. Borrado y destrucción de registros; comisión para la destrucción de datos 7](#_Toc129594842)

[3.10. Transferencia de información 7](#_Toc129594843)

[3.10.1. Canales de comunicación electrónica 7](#_Toc129594844)

[3.10.2. Relaciones con entidades externas 8](#_Toc129594845)

[3.11. Manejo del código fuente 8](#_Toc129594846)

[3.12. Uso de programas de utilidad 8](#_Toc129594847)

[3.13. Supervisión del sistema 8](#_Toc129594848)

[3.14. Monitoreo de amenazas externas 9](#_Toc129594849)

[4. Gestión de registros guardados en base a este documento 9](#_Toc129594850)

[5. Validez y gestión de documentos 10](#_Toc129594851)

# Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar el funcionamiento correcto y seguro de la tecnología de la información y de la comunicación.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a toda la tecnología de la información y de la comunicación, como también a la documentación relacionada dentro del alcance del SGSI.

Los usuarios de este documento son empleados de [unidad organizativa de tecnología de la información y de la comunicación].

# Documentos de referencia

* Norma ISO/IEC 27001, cláusulas A.5.7, A.5.14, A.5.37, A.7.10, A.7.14, A.8.4, A.8.6, A.8.7, A.8.8, A.8.9, A.8.10, A.8.12, A.8.13, A.8.15, A.8.16, A.8.17, A.8.18, A.8.20, A.8.21, A.8.22, A.8.23, A.8.31 y A.8.32
* Política de seguridad de la información
* [Plan de recuperación ante desastres]
* [Política sobre dispositivos móviles, tele-trabajo y trabajo desde casa]
* [Política de clasificación de la información]
* [Inventario de activos]
* [Política de seguridad para proveedores]
* [Política de desarrollo seguro]
* [Política de control de acceso]

# Procedimientos de seguridad para el departamento de TI

## Gestión de cambios

Cualquier cambio sobre sistemas operativos o de producción debe ser realizado de la siguiente forma:

1. Los cambios pueden ser propuestos por [indicar los cargos].
2. Los cambios deben ser autorizados por el [cargo], que debe evaluar su justificación para el negocio y las potenciales consecuencias negativas sobre la seguridad.
3. Los cambios deben ser implementados por [cargo].
4. El [cargo] es el responsable de verificar que los cambios se han implementado de acuerdo al requerimiento.
5. El [cargo] es el responsable de probar y verificar la estabilidad del sistema; el sistema no debe ser puesto en producción antes de haber realizado pruebas exhaustivas.
6. La implementación de los cambios debe ser reportada a las siguientes personas: [detallar todos los cargos necesarios].

El [cargo] es responsable de actualizar los documentos (políticas, procedimientos, planes, etc.) que se han visto afectados por el cambio. Los registros sobre los cambios son llevados en [indicar el nombre del formulario o informar un método diferente para registrar los cambios].

## Gestión de configuración

El [cargo] es responsable de documentar los ajustes de configuración de hardware, software, servicios y redes que se deben aplicar para garantizar el funcionamiento correcto y seguro, y para proporcionar una línea de base contra cambios incorrectos.

## Gestión de capacidad

El [cargo] es responsable de monitorear el uso de los activos de TIC y de planificar la capacidad requerida.

## Protección antivirus

El [nombre del software antivirus] debe instalarse en cada plataforma (p. ej., servidores físicos, virtuales o en la nube) que alojan sistemas de TI que son manejados por el departamento de TI, con actualizaciones automáticas activadas.

## Copias de seguridad

### Procedimiento para copias de seguridad

Se deben crear copias de seguridad para todos los sistemas identificados en la [Estrategia de continuidad de negocio] y con la frecuencia especificada en dicho documento.

El [cargo] es el responsable de crear copias de seguridad de información, software e imágenes del sistema y garantizar que las fallas en las copias de seguridad programadas se aborden adecuadamente. [Si fuera necesario, detallar qué tecnología se utiliza para crear las copias de seguridad, indicar las responsabilidades sobre las actividades individuales, las ubicaciones para almacenar las copias, la protección física que tienen, encriptado, claves, etc.]

…

\*\* FIN DE MUESTRA GRATIS \*\*

Si ha decidido que el Paquete de documentos de ISO 27001 es la mejor elección para su compañía, consulte la siguiente tabla para elegir el paquete de documentos con el nivel de soporte experto adecuado.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Paquete de documentos con apoyo de un experto** | **Paquete de documentos con ampliación de soporte** | **Paquete de documentos superior** |
|  | **US $897** | **US $1397** | **US $2397** |
| **45 plantillas de documentos que cumplen con ISO 27001** | **🗸** | **🗸** | **🗸** |
| **Acceso a tutoriales en video (en inglés)** | **🗸** | **🗸** | **🗸** |
| **Plantillas de documentos actualizadas a la versión ISO 27001:2022** | **🗸** | **🗸** | **🗸** |
| **Herramienta de Análisis de Brecha en ISO 27001** | **🗸** | **🗸** | **🗸** |
| **Soporte mediante correo electrónico** | 10 preguntas por mes | Ilimitado | Ilimitado |
| **Asistencia personalizada con un experto en ISO 27001** | 1 hora | 5 horas | 15 horas |
| **Revisión de expertos (documentos completos)** | 1 documento | 5 documentos | 15 documentos |
| **Formación en concienciación sobre seguridad (en inglés)** | **X** | 20 usuarios | 50 usuarios |
| **Revisión previa a la auditoría** | **X** | **🗸** | **🗸** |
|  | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718229&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-expert-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718230&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-extended-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718232&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-power-support&utm_content=lang-es) |
|  | (haga clic en el siguiente enlace presionando CTRL+clic) | | |