\*\* VERSIÓN DE MUESTRA GRATIS \*\*

[logo de la organización]

[nombre de la organización]

**PROCEDIMIENTOS DE SEGURIDAD DEL DEPARTAMENTO DE TI**

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

**Historial de modificaciones**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha** | **Versión** | **Creado por** | **Descripción del cambio** |
| dd.mm.aaaa | 0.1 | EUGDPRAcademy | Descripción básica del documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Tabla de contenido**

[1. Objetivo, alcance y usuarios 3](#_Toc503865492)

[2. Documentos de referencia 3](#_Toc503865493)

[3. Procedimientos de seguridad 3](#_Toc503865494)

[3.1. Gestión de cambios 3](#_Toc503865495)

[3.2. Copias de seguridad 3](#_Toc503865496)

[3.2.1. Procedimiento para copias de seguridad 3](#_Toc503865497)

[3.2.2. Prueba de las copias de seguridad 4](#_Toc503865498)

[3.3. Gestión de seguridad de red 4](#_Toc503865499)

[3.4. Servicios de red 4](#_Toc503865500)

[3.5. Supervisión del sistema 5](#_Toc503865501)

[4. Gestión de registros guardados en base a este documento 5](#_Toc503865502)

[5. Validez y gestión de documentos 6](#_Toc503865503)

# 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.

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
* Política de Seguridad de TI
* [Política sobre Dispositivos Móviles y Tele-trabajo]
* [Política de Clasificación de la Información]

# Procedimientos de seguridad

## 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]

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

Para descargar la versión completa de este documento haga clic aquí:  
<https://advisera.com/eugdpracademy/es/documentation/procedimientos-de-seguridad-del-departamento-de-ti/>