**UNIVERSIDAD NACIONAL DE SAN**

**AGUSTÍN DE AREQUIPA**

**FACULTAD DE PRODUCCIÓN Y SERVICIOS**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**



**SEGURIDAD INFORMATICA**

**INVESTIGACION FORMATIVA 1.3**

**INTEGRANTES:**

* Cozco Mauri Yoset
* 2
* 3

# **DOCENTE:** LUCY ANGELA DELGADO BARRA

**AREQUIPA – PERÚ**

**2023**

Resumen ISO27000/SGSI

Las normas internacionales que explican cómo gestionar la seguridad de la información dentro de una organización forman parte de la serie ISO/IEC 27000. La serie ISO/IEC 27000 se compone de varias normas que se centran en diferentes aspectos de la seguridad de la información. La norma principal que establece los requisitos previos para un Sistema de Gestión de Seguridad de la Información (SGSI) es ISO/IEC 27001. La norma ISO/IEC 27002 proporciona un conjunto de controles para implementar un SGSI. La norma ISO/IEC 27003 brinda orientación sobre cómo implementar un SGSI. La norma ISO/IEC 27004 proporciona orientación sobre cómo medir y evaluar la efectividad del SGSI. La norma ISO/IEC 27005 proporciona orientación sobre cómo realizar una evaluación de riesgos para el SGSI.

La norma ISO/IEC 27001 especifica los requisitos para un SGSI y es la certificación que deben obtener las organizaciones. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.

La norma ISO/IEC 27002 define un conjunto de buenas prácticas para la implantación del SGSI, a través de 114 controles, estructurados en 14 dominios y 35 objetivos de controles.

La norma ISO/IEC 27003 son directrices para la implementación de un SGSI.

La norma ISO/IEC 27004 son métricas para la gestión de seguridad de la información.

La norma ISO/IEC 27005 trata la gestión de riesgos en seguridad de la información y proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001.

**Ejemplo de implementación**

La empresa Cisco tiene una política de seguridad informática que incluye la protección de los datos confidenciales y la privacidad del cliente, la prevención de amenazas internas y externas, y la implementación de medidas de seguridad física y lógica.

Enlace: <https://www.cisco.com/c/es_mx/support/security/security-policy.html>

Puntos importantes sobre política global de privacidad y protección de datos personales:

* Implementación de un programa global de privacidad para establecer y mantener elevados estándares en la creación, la recolección, el uso, la divulgación, el almacenamiento, la seguridad, el acceso, la trasferencia o algún otro tipo de procesamiento de datos personales.
* Protección de los datos personales mediante medidas técnicas y organizativas adecuadas.
* Cumplimiento con las leyes y regulaciones aplicables en materia de privacidad y protección de datos personales.
* Proporcionar a los usuarios información clara y transparente sobre cómo se utilizan sus datos personales.

Puntos importantes de los estándares mínimos de seguridad:

* Protección contra amenazas internas y externas.
* Protección contra ataques conocidos y desconocidos.
* Protección contra vulnerabilidades conocidas y desconocidas.
* Protección contra el acceso no autorizado a los sistemas y datos.

Puntos importantes de la política de seguridad de red

* Revisión del proceso para crear y mantener una política de seguridad.
* Revisión de la política, postura y práctica de seguridad.
* Creación de una política dinámica que se adapte a un entorno evolutivo.

**Bibliografia**

[1] Cisco. “Política global de privacidad y protección de datos personales”. [En línea]. Disponible en: https://www.cisco.com/c/es\_mx/about/trust-center/global-privacy-policy.html. [Accedido en: 08-May-2023].

[2] Cisco. “Estándares mínimos de seguridad”. [En línea]. Disponible en: https://www.cisco.com/c/dam/global/es\_es/products/security/pdfs/estandares\_minimos\_de\_seguridad.pdf. [Accedido en: 08-May-2023].

[3] Cisco. “Política de seguridad de la red: Informe oficial de Mejores Prácticas”. [En línea]. Disponible en: https://www.cisco.com/c/es\_mx/support/docs/availability/high-availability/13601-secpol.html. [Accedido en: 08-May-2023].