AC04

Ingeniería Tecnologías de la Información 9°A

INTEGRANTES:

- **Mendieta Chimal Sony Luis MCSO220598**
- **Nava Sanchez Axel NSAO220388**

Docente: Enrique Solano García

Materia: Seguridad

14/05/2025

TABLA DE CONTENIDO

INTRODUCCIÓN.

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) son las entidades responsables de la creación y gestión de una amplia gama de normas internacionales, incluyendo aquellas dedicadas a la seguridad de la información. En el panorama digital actual, donde las organizaciones dependen cada vez más de la tecnología para sus operaciones y gestionan grandes volúmenes de datos sensibles, la protección de la información se ha convertido en una prioridad crítica. La creciente sofisticación de las amenazas cibernéticas y el aumento de las filtraciones de datos subrayan la necesidad de enfoques estandarizados y efectivos para salvaguardar los activos informacionales.

1. ISO 17799

- **Nombre completo:** *Oficialmente conocida como ISO/IEC 17799. También se le ha denominado "Tecnología de la Información - Código de Práctica para la Gestión de la Seguridad de la Información".*

- **Objetivo:** Proporcionar un marco de referencia y las mejores prácticas para el establecimiento, implementación, mantenimiento y mejora de la gestión de la seguridad de la información dentro de una organización.

- **Descripción:** Describe controles de seguridad en diversos dominios, incluyendo la política de seguridad, la seguridad organizacional, la clasificación y control de activos, la seguridad del personal, la seguridad física y ambiental, la gestión de comunicaciones y operaciones, el control de acceso, el desarrollo y mantenimiento de sistemas, la gestión de la continuidad del negocio y el cumplimiento.

---

2. ISO 27000

- **Nombre completo:** *Oficialmente conocida como la familia de normas ISO/IEC 27000. También se le denomina familia de normas SGSI o ISO27K.*

- **Objetivo:** Su objetivo es proporcionar los fundamentos y el lenguaje común para el resto de las normas de la serie ISO 27000. Recomienda las mejores prácticas para la gestión de los riesgos de la información mediante la implementación de controles de seguridad dentro del marco de un Sistema de Gestión de Seguridad de la Información (SGSI)

- **Descripción:** Enfatiza la importancia de gestionar los riesgos de la información a través de controles de seguridad dentro de un marco SGSI, de manera similar a los sistemas de gestión de calidad y protección ambiental.

---

3. ISO/IEC 27002

- **Nombre completo:** *Oficialmente conocida como ISO/IEC 27002:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información". Existieron versiones anteriores, como la ISO/IEC 27002:2013.*

- **Objetivo:** Su objetivo es proporcionar un conjunto de referencia de controles de seguridad de la información genéricos, incluyendo orientación para su implementación, basados en las mejores prácticas reconocidas internacionalmente. Está diseñada para ser utilizada dentro del contexto de un SGSI basado en la ISO/IEC 27001, para implementar controles de seguridad de la información y para desarrollar directrices de gestión de seguridad de la información específicas para la organización. La norma busca ayudar a las organizaciones a mitigar los riesgos inaceptables para la confidencialidad, integridad y disponibilidad de la información.

- **Descripción:** Proporciona una lista exhaustiva de controles de seguridad de la información que las organizaciones pueden adoptar para reducir los riesgos, cubriendo políticas, procesos, sistemas tecnológicos y otras medidas. La amplitud de estos controles asegura que se consideren diversos aspectos de la seguridad.

---

4. ISO 27003

- **Nombre completo:** *Oficialmente conocida como ISO 27003:2017 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Guía.*

- **Objetivo:** Su objetivo es proporcionar orientación para la implementación exitosa de un Sistema de Gestión de Seguridad de la Información (SGSI) tal como se especifica en la ISO/IEC 27001. Ayuda a las organizaciones a traducir los requisitos de la ISO 27001 en pasos prácticos.

- **Descripción:** Es un documento de apoyo a la ISO 27001, que ofrece una guía básica pero completa para implementar sus requisitos. Clarifica y facilita la comprensión de los requisitos de la ISO 27001.

---

5. ISO 27004

- **Nombre completo:** *Oficialmente conocida como ISO/IEC 27004:2016 Tecnología de la información – Técnicas de seguridad – Gestión de seguridad de la información – Monitoreo, medición, análisis y evaluación. Existieron versiones anteriores, como la*

ISO 27004:2009.

- **Objetivo:** Su objetivo es proporcionar orientación sobre la medición, evaluación y gestión del desempeño de la seguridad de la información y la eficacia de un Sistema de Gestión de Seguridad de la Información (SGSI) para cumplir con los requisitos de la ISO/IEC 27001 y los propios objetivos de seguridad de una organización.

- **Descripción:** Se centra en determinar qué medir en un programa de seguridad y cómo analizar el rendimiento de los sistemas de seguridad. Su enfoque práctico ayuda a las organizaciones a obtener información valiosa sobre su postura de seguridad.

---

6. ISO 27005

- **Nombre completo:** *Oficialmente conocida como ISO/IEC 27005 "Tecnología de la información — Técnicas de seguridad — Gestión de riesgos de seguridad de la información".*

- **Objetivo:** Su objetivo es proporcionar directrices para la gestión de riesgos de seguridad de la información, apoyando los conceptos generales especificados en la ISO/IEC 27001 y ayudando a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Busca asegurar que las organizaciones diseñen, implementen, administren, monitoreen y gestionen sus controles de seguridad de la información de manera apropiada y basada en el riesgo.

- **Descripción:** Es una norma dedicada exclusivamente a la gestión de riesgos de seguridad de la información, que describe los procedimientos para identificar, evaluar, tratar y monitorear los riesgos de seguridad de la información. Su enfoque específico la convierte en una guía esencial en este ámbito.

---

7. ISO 27006

- **Nombre completo:** *Oficialmente conocida como ISO/IEC 27006 "Técnicas de seguridad de la información - Requisitos para los organismos que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información". La versión más reciente es ISO/IEC 27006-1:2024. Las versiones anteriores incluyen ISO/IEC 27006:2015.*

- **Objetivo:** Su objetivo es especificar los requisitos para los organismos que proporcionan auditoría y certificación de Sistemas de Gestión de Seguridad de la Información (SGSI) basados en la ISO/IEC 27001. Su objetivo principal es garantizar

la credibilidad de los certificados ISO 27001 y ayudar en la acreditación de los organismos de certificación.

- **Descripción:** Es una norma que define los procedimientos formales que los organismos de certificación deben implementar al auditar los SGSI para garantizar la validez y credibilidad de las certificaciones ISO 27001. Establece un marco para asegurar la calidad del proceso de certificación.

---

8. ISO 27007

- **Nombre completo:** *Oficialmente conocida como ISO/IEC 27007 "Seguridad de la información, ciberseguridad y protección de la privacidad — Directrices para la auditoría de sistemas de gestión de la seguridad de la información". Las versiones anteriores incluyen ISO/IEC 27007:2017.*

- **Objetivo:** Su objetivo es proporcionar orientación reconocida internacionalmente para la auditoría de Sistemas de Gestión de Seguridad de la Información (SGSI) para garantizar el cumplimiento de la ISO 27001 y mejorar la gobernanza de la seguridad. Busca ayudar a las organizaciones a planificar, realizar y gestionar auditorías internas y externas, y a mejorar la competencia de los auditores de SGSI.

- **Descripción:** Es una norma que se basa en la guía de auditoría contenida en la ISO 19011, proporcionando sugerencias adicionales específicas para las auditorías de SGSI. Complementa la norma general de auditoría con directrices específicas para la seguridad de la información.

---

9. ISO/IEC 27011

- **Nombre completo:** *ISO/IEC 27011:2016 – Código de prácticas para la gestión de la seguridad de la información en telecomunicaciones basado en ISO/IEC 27002*

- **Objetivo:** Proporcionar directrices específicas para el sector de telecomunicaciones en cuanto a la gestión de la seguridad de la información.

- **Descripción:** Esta norma adapta la ISO/IEC 27002 al contexto de los operadores de telecomunicaciones, estableciendo controles de seguridad y medidas específicas para proteger los activos de información en redes y servicios de telecomunicaciones.

---

10. ISO/IEC 27031

- **Nombre completo:** *ISO/IEC 27031:2011 – Directrices para la preparación de la continuidad del negocio de las tecnologías de la información y comunicación (TIC)*

- **Objetivo:** Garantizar la preparación para la continuidad del negocio en entornos TIC.

- **Descripción:** Proporciona un marco para planificar, establecer, implementar, operar, monitorear, revisar y mantener la preparación de las TIC ante interrupciones que puedan afectar la continuidad del negocio.

---

11. ISO/IEC 27032

- **Nombre completo:** *ISO/IEC 27032:2012 – Directrices para la ciberseguridad*
- **Objetivo:** Establecer un enfoque general para abordar la ciberseguridad, complementando otras normas como la ISO/IEC 27001.
- **Descripción:** Define la ciberseguridad como la protección de la información en el ciberespacio y proporciona directrices sobre colaboración, intercambio de información, gestión de incidentes y protección contra amenazas como ciberataques, hacktivismo o malware.

---

12. ISO/IEC 27033

- **Nombre completo:** *ISO/IEC 27033 (serie) – Seguridad de la red*
- **Objetivo:** Garantizar la seguridad en las redes y en la transmisión de datos.
- **Descripción:** Es una serie de normas (con varios apartados) que proveen directrices para implementar controles de seguridad en redes, incluyendo planificación, diseño, implementación y monitoreo. Complementa la ISO/IEC 27002 con medidas específicas de seguridad de red.

---

13. ISO/IEC 27034

- **Nombre completo:** *ISO/IEC 27034 – Seguridad de las aplicaciones*
- **Objetivo:** Proporcionar un marco para integrar la seguridad en los procesos de desarrollo y operación de aplicaciones.
- **Descripción:** Establece principios y prácticas para la gestión de la seguridad en aplicaciones a lo largo de su ciclo de vida, considerando riesgos, requisitos de seguridad, validación y verificación de controles.

---

14. ISO 27799

- **Nombre completo:** *ISO 27799:2016 – Gestión de seguridad de la información en salud usando ISO/IEC 27002*

- **Objetivo:** Proteger la información personal de salud en entornos médicos y sanitarios.

- **Descripción:** Aplica los principios de seguridad de la ISO/IEC 27002 a organizaciones de salud. Establece controles y buenas prácticas para garantizar la confidencialidad, integridad y disponibilidad de los datos de salud.

---

15. NTC-ISO/IEC 27001:2013 (Colombia)

- **Nombre completo:** *Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 – Sistemas de gestión de seguridad de la información*

- **Objetivo:** Establecer los requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).

- **Descripción:** Es la adopción nacional colombiana de la norma ISO/IEC 27001. Define un enfoque basado en riesgos para proteger la información y gestionar su seguridad dentro de las organizaciones, aplicable a cualquier tipo de entidad pública o privada.

Conclusión

La familia de normas ISO 27000 representa un pilar fundamental en la estandarización de la seguridad de la información a nivel global. Desde la pionera ISO 17799, que estableció las bases para las mejores prácticas, hasta la ISO 27001, el estándar de referencia para la certificación de Sistemas de Gestión de Seguridad de la Información (SGSI), y las normas complementarias que ofrecen guías detalladas para la implementación, la gestión de riesgos, la medición del desempeño y la auditoría, esta serie proporciona un marco integral para proteger los activos de información de las organizaciones. La evolución de estas normas, como se evidencia en las actualizaciones de la ISO/IEC 27002 e ISO/IEC 27006, demuestra su compromiso continuo con la adaptación a los desafíos emergentes en el panorama de la ciberseguridad y la protección de la privacidad. En última instancia, la adopción y aplicación de las normas ISO 27000 no solo fortalece la postura de seguridad de una organización, sino que también fomenta la confianza de los clientes, socios y otras partes interesadas en su capacidad para salvaguardar la información en un mundo cada vez más digitalizado y amenazado.

Referencias

- Perez, P. (2023, 6 octubre). ¿Qué es la ISO 27011 y por qué es crucial para la seguridad de la información? PMG SSI - ISO 27001. https://www.pmg-ssi.com/2023/08/que-es-la-iso-27011-y-por-que-es-crucial-para-la-seguridad-de-la-informacion/

- ISO/IEC 27031:2011. (s. f.). ISO. https://www.iso.org/standard/44374.htm

- SL, I. S. A. (s. f.). Implementación de un marco de ciberseguridad ISO 27032. Internet Security Auditors. https://www.isecauditors.com/consultoria-csf-iso-27032

- Admin. (2014, 25 abril). ISO 27034 Seguridad de aplicaciones. PMG SSI - ISO 27001. https://www.pmg-ssi.com/2014/04/iso-27034-seguridad-de-aplicaciones/

- Wikipedia. (s.f.). ISO/IEC 27007. Wikipedia. https://en.wikipedia.org/wiki/ISO/IEC_27007

- ITeh Standards. (2022). SIST EN ISO 27007:2022 - Information security, cybersecurity and privacy protection. https://standards.iteh.ai

- Amnafzar. (s.f.). INTERNATIONAL STANDARD ISO/IEC 27007. https://amnafzar.net

- ITeh Standards. (s.f.). INTERNATIONAL STANDARD ISO/IEC 27007. https://cdn.standards.iteh.ai

- Sprinto. (s.f.). ISO 27003: The Blueprint for Effective ISMS Implementation. https://sprinto.com

- Neumetric. (s.f.). ISO 27001 vs 27003: Understanding the Guidelines and Implementation Frameworks. https://neumetric.com

- DataGuard. (s.f.). ISO 27003: Information Security Techniques for ISMS. https://dataguard.com

- ISMS.online. (s.f.). ISO 27003: Guidance for ISO 27001 Implementation. https://isms.online