UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Seguridad de la información en las organizaciones. Claves para entender y aplicar la norma ISO/IEC 27001

Apellidos, nombre	Galán Cubillo, Javier[1] (jagacu@doctor.upv.es) García Ortega, Beatriz[2] (beagaror@doctor.upv.es)
Departamento	Departamento de Organización de Empresas
Centro	[1]Escuela Técnica Superior de Ingeniería de Caminos, Canales y Puertos [2]Escuela Técnica Superior de Ingeniería Informática Universitat Politècnica de València

1 Resumen de las ideas clave

La seguridad de la información es un componente esencial para el funcionamiento sostenible y confiable de las organizaciones en la era digital. Este artículo docente tiene como propósito ayudar al estudiante a comprender la importancia de gestionar la seguridad de la información de manera integral, introduciendo los principios básicos de la norma ISO/IEC 27001:2022. A través de un enfoque didáctico y aplicado, se pretende que el estudiante identifique los elementos esenciales de un Sistema de Gestión de Seguridad de la Información (SGSI) y reflexione sobre su implementación práctica en distintos contextos organizativos.

2 Objetivos

Los objetivos de aprendizaje son:

- **Reconocer** la relevancia de la seguridad de la información en el contexto organizativo actual.
- **Identificar** los componentes esenciales de un Sistema de Gestión de Seguridad de la Información (SGSI) según ISO/IEC 27001.
- **Analizar** casos reales de aplicación y los beneficios derivados de su implementación.
- **Reflexionar** sobre cómo la cultura organizacional influye en la eficacia de la seguridad de la información.

3 Introducción

Actividad 1: *Antes de entrar en materia, tomemos unos minutos para reflexionar individualmente sobre las siguientes cuestiones:*

¿Qué consecuencias podría tener para una empresa perder la información de sus clientes?

¿Por qué las organizaciones logran mantener la confianza digital y otras no?

¿Qué diferencia hay entre tener medidas de seguridad y gestionar la seguridad

La información constituye hoy uno de los activos más valiosos de cualquier organización. En un entorno interconectado y digitalizado, las amenazas a la seguridad, desde ataques cibernéticos hasta errores humanos, pueden comprometer no solo los datos, sino también la reputación e incluso la continuidad operativa. Resulta por tanto esencial ser conscientes de ello y actuar en consecuencia.

La norma ISO/IEC 27001 surge como un marco que permite establecer, implementar y mejorar de forma continua un sistema de gestión de la seguridad de la información. Más que una

colección de controles representa un enfoque estratégico que integra la seguridad en la cultura organizativa, fomentando la confianza y la mejora constante.

4 Desarrollo

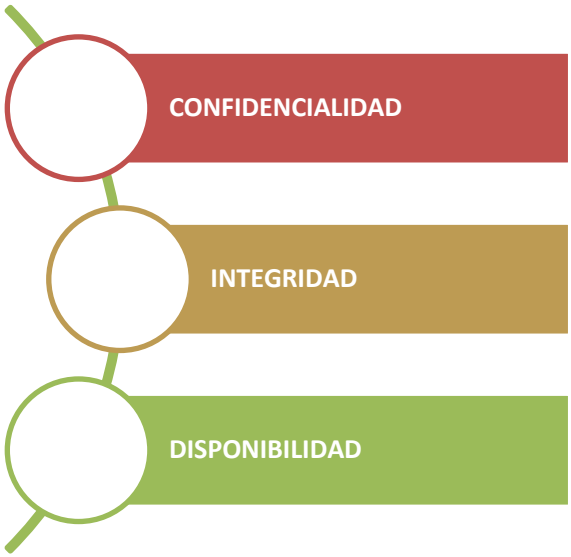
4.1 El valor de la información en la era digital

La digitalización ha convertido la información en el corazón de los procesos empresariales. Desde datos financieros hasta registros médicos, su pérdida o manipulación indebida puede tener consecuencias graves. Por ejemplo, una brecha en una plataforma de comercio electrónico puede comprometer miles de cuentas de clientes, afectando la confianza y la viabilidad de la empresa.

4.2 De la reacción al sistema: por qué necesitamos una gestión estructurada

La ISO/IEC 27001 propone un enfoque sistemático frente a la seguridad. En lugar de reaccionar ante incidentes, busca prevenirlos mediante un proceso de gestión de riesgos continuo. Sus tres pilares: confidencialidad, integridad y disponibilidad garantizan que la información esté protegida, sea fiable y accesible solo para quienes corresponda.

Figura 1. Pilares de la norma ISO/IEC 27001



Fuente: Elaboración propia

4.3 Estructura general de la ISO/EIC 27001

La norma se estructura en torno a un ciclo de mejora continua que abarca desde la comprensión del contexto organizativo hasta la evaluación del desempeño y la implementación de acciones

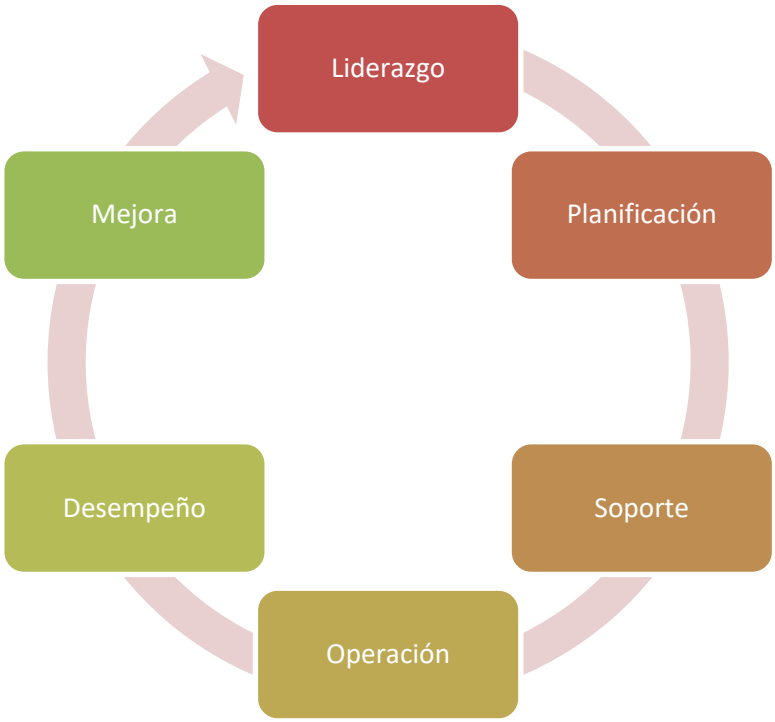
de mejora. Los requisitos incluyen liderazgo, planificación, soporte, operación, evaluación y mejora. Destacan especialmente el compromiso de la alta dirección, la evaluación de riesgos y la integración de la seguridad en todos los procesos de la organización. Este enfoque facilita que la seguridad de la información se gestione de manera dinámica y adaptativa dentro de la organización.

En términos de requisitos, la norma se articula en seis bloques principales:

1. **Liderazgo:** La norma enfatiza que la alta dirección debe demostrar un compromiso activo con la seguridad de la información, estableciendo políticas claras, objetivos estratégicos y asignando responsabilidades concretas. Este liderazgo es clave para integrar la seguridad en la cultura organizativa y asegurar que los recursos necesarios estén disponibles.
2. **Planificación:** Incluye la identificación de riesgos y oportunidades relacionados con la seguridad de la información, así como la definición de objetivos medibles y planes de acción para mitigarlos. La evaluación de riesgos es uno de los pilares fundamentales, ya que permite priorizar los controles necesarios y adaptar las medidas a las amenazas específicas de la organización.
3. **Soporte:** Se centra en los recursos, competencias, concienciación, comunicación y documentación necesarios para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo. Esto asegura que todos los miembros de la organización comprendan sus responsabilidades y contribuyan al mantenimiento de la seguridad.
4. **Operación:** Comprende la implementación de los procesos y controles definidos en la planificación, garantizando que la seguridad de la información se integre en todas las actividades organizativas. Aquí se incluyen procedimientos para el manejo de incidentes, gestión de cambios y control de accesos, entre otros.
5. **Evaluación del desempeño**: Implica la monitorización, medición, análisis y evaluación del SGSI. La norma exige auditorías internas y revisiones periódicas por la dirección para verificar la eficacia de los controles y la alineación con los objetivos estratégicos.
6. **Mejora:** Basándose en los resultados de la evaluación, la organización debe identificar oportunidades de mejora continua, implementar acciones correctivas y prevenir incidentes futuros. Esto asegura que el SGSI evolucione y se adapte a nuevos riesgos, tecnologías y cambios en el entorno empresarial.

En conjunto, estos elementos hacen que la ISO/IEC 27001 no solo se enfoque en establecer controles de seguridad, sino también en crear una cultura de seguridad integradora y proactiva, donde la gestión de la información crítica esté alineada con los objetivos estratégicos de la organización y en constante evolución frente a nuevas amenazas.

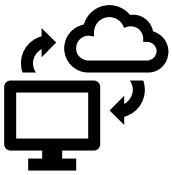
Figura 1. Requisitos de la norma ISO/IEC 27001



Fuente: Elaboración propia

4.4 Cómo se aplica en la práctica: casos de uso

CASO 1. Empresa tecnológica: proteger la confianza digital



Imagina una empresa de desarrollo de software que ofrece servicios en la nube para cientos de clientes empresariales. Su negocio depende totalmente de la confianza que los usuarios depositan en la protección de sus datos. Un incidente de seguridad —por ejemplo, la filtración de credenciales o la exposición de una base de datos mal configurada— podría provocar la pérdida de clientes, sanciones legales y un daño reputacional difícil de revertir.

La dirección decide implantar un Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo la norma ISO/IEC 27001 para pasar de una gestión reactiva a una gestión sistemática.

El proceso comienza con la identificación de activos críticos (datos de clientes, código fuente, infraestructura cloud) y la evaluación de riesgos, que revela debilidades en el control de accesos y en la configuración del entorno de desarrollo. Entre los controles priorizados destacan:

- Gestión de identidades y accesos con autenticación multifactor.
- Cifrado de datos en tránsito y en reposo.
- Gestión de incidentes y copias de seguridad verificadas.
- Formación continua para desarrolladores en buenas prácticas de seguridad.

Al cabo de unos meses, la empresa no solo reduce incidentes, sino que gana credibilidad ante nuevos clientes que exigen certificaciones o auditorías externas.

De este modo, la norma se convierte en un lenguaje común entre dirección, técnicos y clientes, alineando la seguridad con la estrategia de negocio.

CASO 2. Hospital: proteger la información que salva vidas

Un hospital gestiona miles de historiales clínicos electrónicos, resultados de laboratorio e imágenes diagnósticas. Cada día, decenas de profesionales acceden a estos sistemas para tomar decisiones médicas. La disponibilidad y confidencialidad de la información no son solo un requisito legal, sino una cuestión de salud pública.

La amenaza más temida: un ataque de ransomware que cifre los historiales y paralice los sistemas durante horas o días.

Para anticiparse, el hospital implementa un SGSI basado en ISO/IEC 27001 con un enfoque integral. El proyecto incluye:

- Evaluar riesgos clínicos y tecnológicos.
- Clasificar la información según su sensibilidad.
- Establecer controles técnicos: autenticación por roles, cifrado de comunicaciones, copias de seguridad inmutables.
- Controles organizativos: formación del personal sanitario y simulacros de respuesta a incidentes.

Durante una auditoría interna, se descubre que algunos dispositivos médicos conectados no estaban incluidos en el inventario del sistema. Esa lección lleva a ampliar el alcance del SGSI y a reforzar la colaboración entre el personal clínico y técnico.

En este contexto, la seguridad no solo protege los datos, sino la continuidad de la atención y la confianza de los pacientes.

CASO 3. PYME industrial: seguridad a escala humana

Una pequeña empresa industrial diseña y fabrica componentes mecánicos. Sus recursos tecnológicos son limitados, pero sus diseños son el núcleo de su ventaja competitiva. Tras sufrir la pérdida accidental de archivos de diseño por un ataque de malware, la gerencia decide implantar medidas básicas inspiradas en la ISO/IEC 27001.

El enfoque es proporcional a su tamaño, priorizando lo esencial:

- Copias de seguridad automáticas y pruebas de restauración mensuales.

- Bloqueo de puertos USB en estaciones críticas.
- Concienciación del personal sobre phishing y buenas prácticas.
- Política simple de contraseñas y acceso.

A medida que madura, la empresa amplía su sistema con controles más avanzados: segmentación de red entre oficina y planta, acuerdos con proveedores y una revisión anual de riesgos.

Incluso con recursos limitados, la gestión de la seguridad puede integrarse gradualmente, reforzando la sostenibilidad y la confianza en la organización.

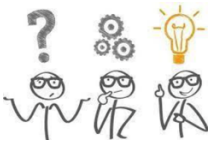
Estos tres ejemplos muestran que la ISO/IEC 27001 no es exclusiva del sector tecnológico o de grandes corporaciones, sino una guía flexible que puede adaptarse a distintos contextos organizacionales, donde lo fundamental es adoptar una mentalidad de mejora continua y gestión del riesgo.

5 Cultura organizacional y personas

Un SGSI efectivo depende tanto de la tecnología como de las personas. La ISO/IEC 27001 subraya la importancia de la formación, la concienciación y la responsabilidad compartida. La cultura organizacional debe fomentar comportamientos seguros, ya que de poco sirven los controles si los empleados comparten contraseñas o ignoran los protocolos establecidos. Uno de los aspectos clave es, por tanto, la formación y concienciación tanto del personal propio como de los actores que interactúan con la organización.

Actividad 2

Análisis de caso: Elige una organización (real o simulada) y describe tres riesgos críticos de seguridad de la información. Propón medidas de mitigación alineadas con la filosofía de la ISO 27001.



Actividad 3

Reflexión individual: identifica una práctica cotidiana en tu entorno académico o laboral que ponga en riesgo la información. ¿Cómo podrías mejorarla?

6 Conclusión

La gestión de la seguridad de la información constituye una necesidad estratégica en cualquier tipo de organización. La ISO/IEC 27001 ofrece un marco sólido y adaptable que permite establecer procesos, roles y controles para proteger los activos de información, impulsando una cultura de seguridad sostenida por la mejora continua.

En definitiva, más allá de los riesgos que implica el manejo de información en el contexto de una organización, su seguridad, gestionada mediante un enfoque estratégico, pasa a convertirse en fuente de ventajas competitivas, al tiempo que refuerza una adecuada gobernanza, protegiendo tanto a la organización como a sus grupos de interés.

Para más detalle se recomienda consultar la bibliografía propuesta.

7 Bibliografía

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 33(7), 76-105.

Garcia-Ortega, B. (2021). Auditorias de sistemas de gestión para empresas. Riunet Repositorio Institucional UPV. https://riunet.upv.es/handle/10251/165991

Garcia-Ortega, B. (2022). Planteamiento de un sistema de información estratégico en la empresa. Riunet Repositorio Institucional UPV. https://riunet.upv.es/handle/10251/184670

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

Malatji, M. (2023, January). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In 2023 *International conference on cyber management and engineering (CyMaEn)* (pp. 117-122). IEEE.

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, 142, 103744.