

Fundamentos de las TICs y la Ciberseguridad



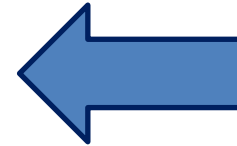
Eduardo Díaz-Mayordomo

Francisco de Santos

Facultad de CC. Jurídicas y Empresariales

Principios de la Seguridad de la Información





1. Introducción.
2. Integridad, confidencialidad y disponibilidad.
3. Identificación, Autenticación, Accountability y Autorización.
4. Introducción a los Sistemas de Gestión de la Seguridad de la Información.

Introducción

Seguridad de la Información

- Eliminar o mitigar riesgos
- No es un producto → Es un PROCESO



La información es el recurso más valioso

Confidencialidad, Integridad y Disponibilidad.

¿Qué implica?

- ¿Qué hay que proteger?
- ¿Por qué hay que proteger?
- ¿De qué y de quién protegerlo?
- ¿Cómo protegerlo?

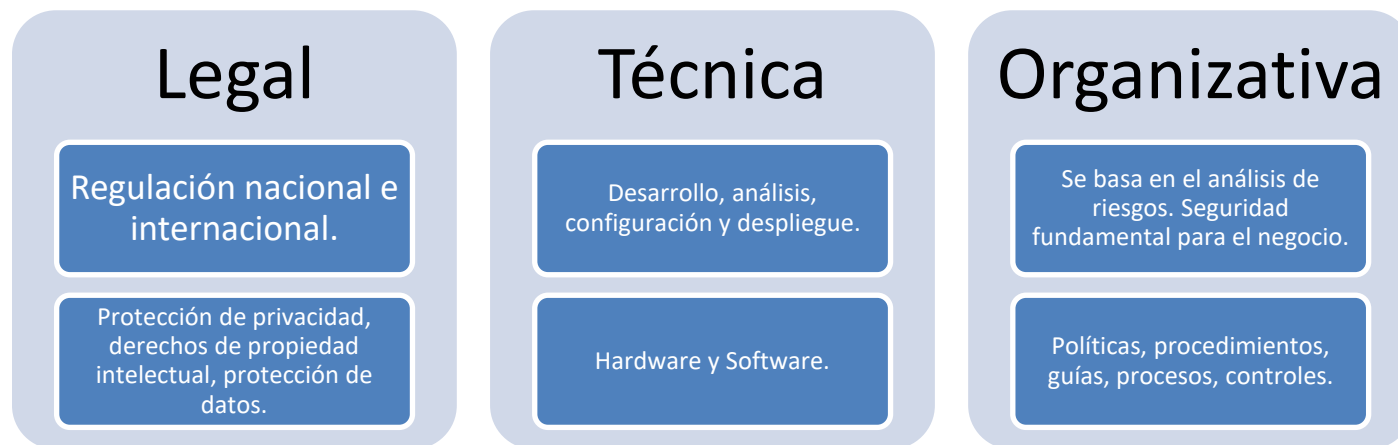


Información. Activo principal

Seguridad de la Información → Implementación de estrategias que cubran los procesos de negocio de una organización.

Seguridad informática → Seguridad técnica de los sistemas informáticos. → Concepto más restrictivo.

Seguridad → Perspectivas



Relación Implicaciones → Perspectivas

¿Qué hay que proteger?

Perspectivas:
Legal y Organizativa

Lo establecido en la ley y los recursos importantes de la organización.

¿Por qué y de qué proteger?

Perspectivas:
Legal y organizativa

Proteger derecho de las personas frente a violaciones de privacidad.
Amenazas y atacantes.

Comprometer recursos afecta al negocio
(robo de información, espionaje industrial, intrusión...)

¿Cómo proteger?


Perspectivas:
Técnica

Salvaguardas en base a las amenazas.
Controles, Auditoría y Revisión.




- **Proceso continuo de mejora.**
- **No existe seguridad 100%.**
- **Evaluar Coste Vs Beneficio.**
- **Decisión Básica de Gestión**



1. Introducción.
2. Integridad, confidencialidad y disponibilidad. 
3. Identificación, Autenticación, Accountability y Autorización.
4. Introducción a los Sistemas de Gestión de la Seguridad de la Información.

Principios de la Seguridad



1. Introducción.
2. Integridad, confidencialidad y disponibilidad.
3. Identificación, Autenticación, Accountability y Autorización. 
4. Introducción a los Sistemas de Gestión de la Seguridad de la Información.

Principios de la Seguridad



Identificación

Procesos que permiten que los usuarios demuestren su identidad.

Soy quien digo ser. Usuarios y claves, Técnicas Biométricas, Tarjetas de Autenticación.



Autenticación

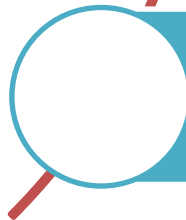
Comprobación por parte del responsable que el usuario que se identifica es quien dice ser.

Comprobación de técnicas de identificación.



Contabilidad (Accountability)

Trazabilidad. Capacidad de los sistemas de hacer seguimiento de las acciones y procesos de los sistemas y los usuarios. Logs, Bitácoras, etc...

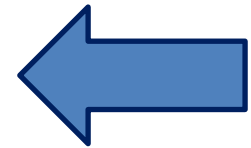


Autorización

Los derechos y permisos asignados a cada individuo para acceder a los recursos del sistema.

Derechos de acceso de lectura y escritura. Roles.

1. **Introducción.**
2. **Integridad, confidencialidad y disponibilidad.**
3. **Identificación, Autenticación, Accountability y Autorización.**
4. **Introducción a los Sistemas de Gestión de la Seguridad de la Información.**



Clasificación de la información

Tipo	Definición
Sin Clasificar	Información no clasificada como sensible o clasificada. Por definición, la difusión de esta información no afecta a la confidencialidad.
Sensible pero no clasificada	Información que tiene un impacto menor si se difunde.
Confidencial	La información que de ser difundida puede causar daño a la seguridad nacional.
Secreta	Su difusión causaría un daño importante.
Alto secreto	Su difusión causaría un daño extremadamente grave.

Tipo	Definición
Uso público	Puede difundirse públicamente.
Uso interno	Información que se puede difundir internamente pero no externamente. Por ejemplo, información sobre los proveedores y su eficiencia.
Confidencial	La información más sensible. Por ejemplo, información sobre diseños industriales, fusiones empresariales, lanzamiento de nuevos productos.

Seguridad física y lógica

Perdidas Físicas → Temperatura, gases, líquidos, organismos, proyectiles, movimientos, anomalías eléctricas, etc...

Controles Administrativos

- Planificación de los requisitos de las instalaciones.
- Gestión de la seguridad de las instalaciones.
- Controles administrativos al personal.



Controles del Entorno

- Suministro eléctrico.
- Detección de incendios.
- Calefacción y refrigeración.



Controles técnicos y físicos

- Inventario de equipamiento.
- Control de acceso.
- Detección de intrusos.



La seguridad implica a las personas

Ingeniería Social → Arte de engañar y manipular a las personas para que **revelen información confidencial**. Phising.

Claves:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza.
- No nos gusta decir **NO**.
- A todos nos gusta que nos alaben.



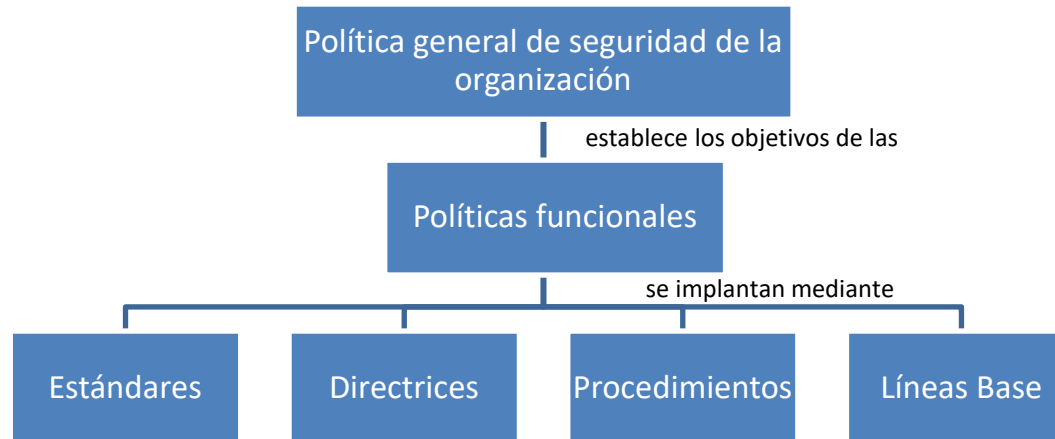
El eslabón más débil de la cadena → **USUARIO**

Controles:

- Formación continua.
- Labores de concienciación.
- Responsabilidades.
- Medidas técnicas



Medidas Organizativas. Políticas, estándares, procedimientos.



Política General → Alto Nivel. Fundamental obtener el compromiso de la dirección.

Políticas Funcionales → ¿Qué debe hacerse? → **NO** ¿Cómo debe hacerse?

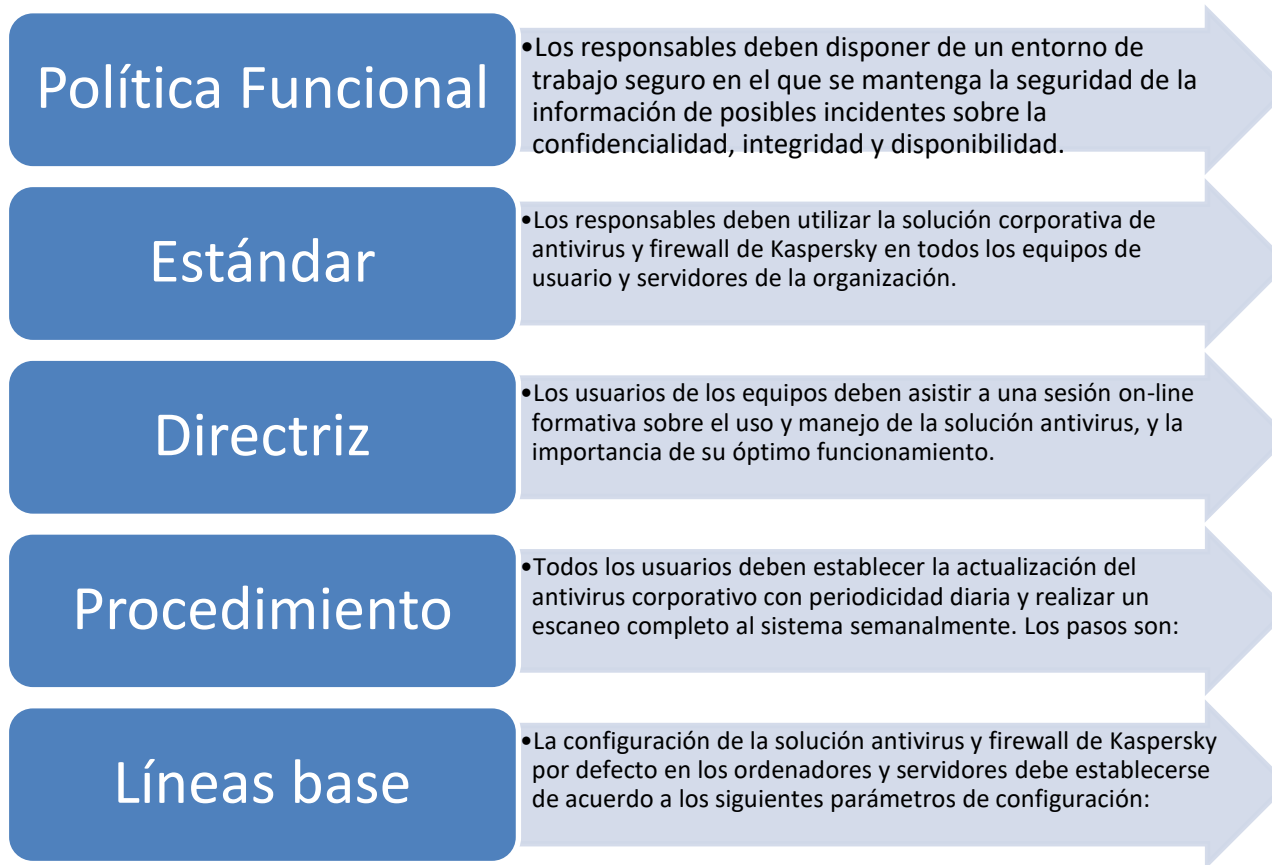
Estándares → **Obligatorios**. Especifican el uso de tecnologías y métodos (buenas prácticas).

Directrices → **No son Obligatorios**. Son recomendaciones.

Procedimientos → Describe los pasos o procesos para la realización de una tarea.

Líneas base → Descripciones de configuración de elementos de seguridad.

Ejemplo de política.



Sistema de Gestión de la Seguridad de la Información. SGSI.

Un SGSI es un marco de trabajo compuesto de:

- Normativa.
- Procedimientos y Guías.
- Documentación, Personas y Controles.
- Recursos y Actividades asociadas.

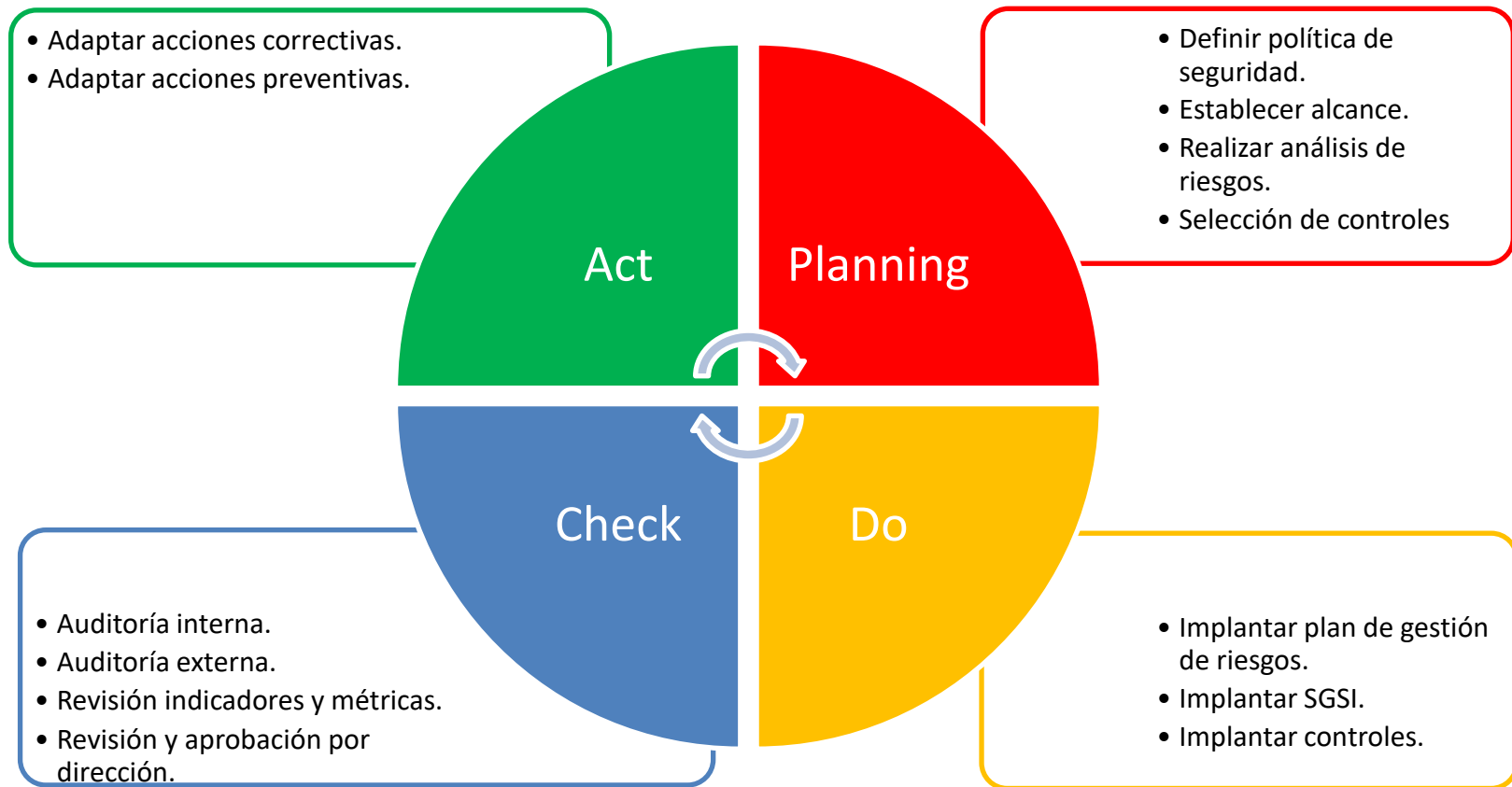


Es un proceso de mejora continua cuyo objetivo es la preservación de la confidencialidad, integridad y disponibilidad de la información mediante la implantación, seguimiento, auditoría y mejora de controles.

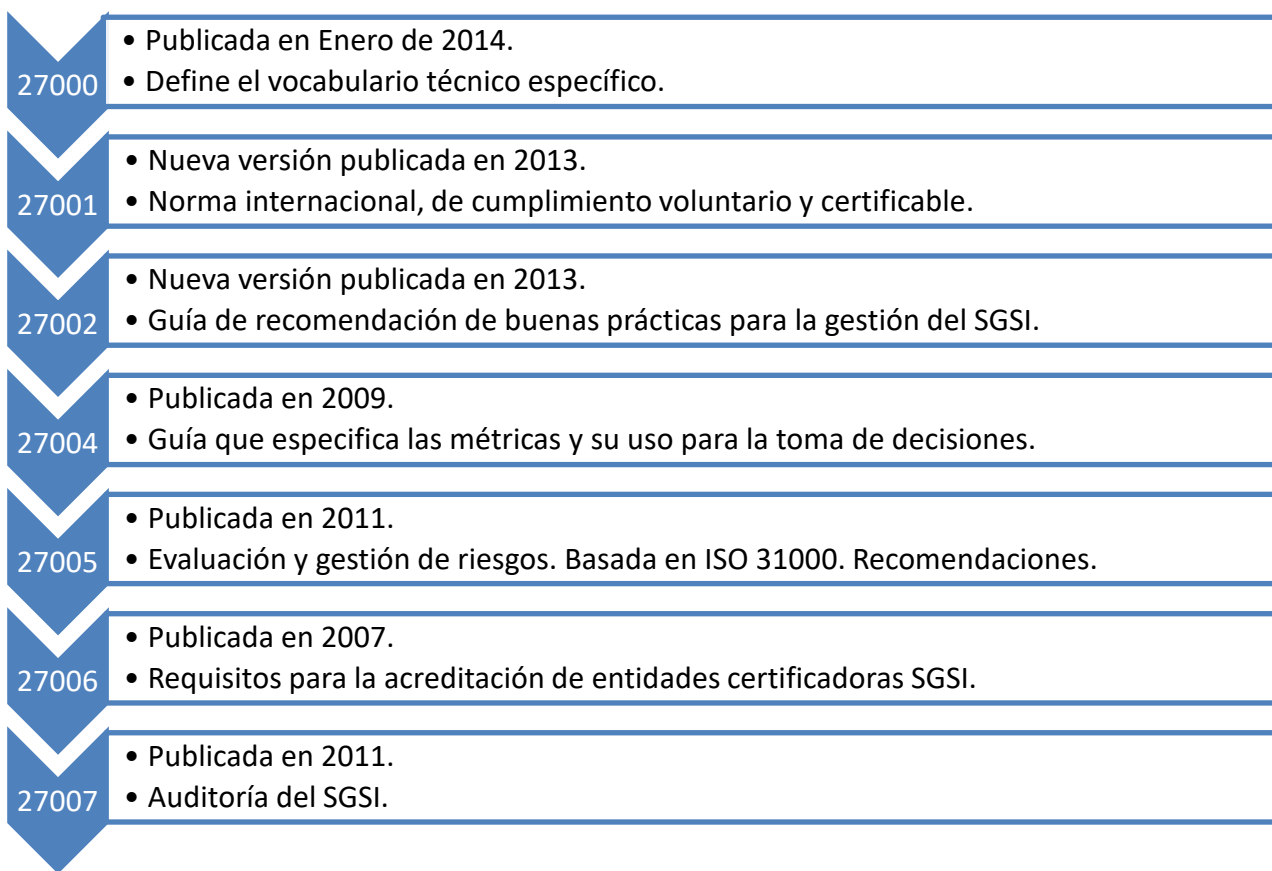
Un SGSI es una aproximación sistemática para establecer, implantar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información de una organización a fin de alcanzar sus objetivos de negocio.

Se basa en el análisis de riesgos y en la asunción controlada de cierto nivel de riesgo con el objetivo de tratar y gestionar de manera eficiente y eficaz los mismos.

Sistema de Gestión de la Seguridad de la Información. SGSI. Modelo PDCA



La Familia 27000.



Esquema Nacional de Seguridad.

Real Decreto 3/2010 8 Enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

- Generar confianza en la ciudadanía en el uso de medios electrónicos en el ámbito de las administraciones públicas.
- Ley 11/2007 de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos mediante la creación del Esquema Nacional de Seguridad.
- Medidas para garantizar la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos para el ejercicio de derechos y deberes por parte de los ciudadanos en las Administraciones Públicas.
- Establece los principios básicos y requisitos mínimos que permiten una protección adecuada de la información y los servicios.
- Se determinan las dimensiones de seguridad y sus niveles, se categorizan los sistemas, las medidas de seguridad adecuadas y la auditoría periódica de la seguridad.
- Seguridad como actividad o proceso integral.

Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias

Fundamentos de las TICs y la Ciberseguridad

¡Muchas gracias!

