# SGSI (Sistema de Gestión de la Seguridad de la Información)

Alejandro Corletti Estrada (*acorletti@darFe.es*)

Según:

- **ISO 27000 (SGSI)** (International Standards Organization)
- **Controles críticos CIS** (Center for Internet Security)
- **NIST SP 800-53** (National Institute of Standards and Technology)
- **CMMI** (Capability Maturity Model Integration)
- **ENS** (Esquema Nacional de Seguridad – España)
- **ISO/IEC 27701** (**SGPI:** Sistema de Gestión de la Privacidad de la Información)

Este documento, y la serie de videos que lo acompañan, es un desafío ÚNICO, cuyo objetivo es concentrar en un solo artículo, los diferentes referentes internacionales que nos indican las mejores prácticas para implementar un robusto **SGSI**.

El objetivo de esta artículo, es ofrecerte todos los puntos de vista actuales, para poder, de forma práctica y concreta, diseñar e implantar un **SGSI** en tu organización, para lo cual lo hemos dividido en una serie de charlas, ejercicios y prácticas para ir abordando el tema de forma metódica y avanzando "paso a paso" (como todo nuestro ciclo de Ciberseguridad).

**Contenido de este artículo**


- **Charla 1 - Presentación del ciclo**
- **Charla 2 – Conceptos del SGSI**
- **Charla 3 – El enfoque a Riesgos**
- **Charla 4 – La dirección de la organización**
- **Charla 5 – Organización del SGSI**
- **Charla 6 – Los Controles**
- **Charla 7 – Métricas e indicadores**
- **Charla 8 – El ciclo de vida de la Seguridad**
- **Charla 9 – Debate sobre cada una de estas referencias**

# Charla 1 - Presentación del ciclo

**Objetivo:** Definir los contenidos y desarrollo del ciclo.


Este ciclo que comenzamos, abordará el tema del SGSI. Para diferenciarnos de todo lo que encontrarás en Internet sobre el mismo, desde www.darFe.es lo haremos desde un enfoque totalmente diferente y, sobre todo, completo. Para ello abordaremos el tema desde todos los ángulos posibles para que tengas la totalidad de los referentes y buenas prácticas internacionales sobre el tema.

Si bien tomaremos como referencia la familia **ISO 27000**, debemos tener presente que existen varias referencias más que pueden sernos de utilidad, que es bueno conocerlas para poder rescatar los aspectos positivos que nos ofrecen cada una de ellas. Por esta razón, en este artículo iremos poniendo de manifiesto las que presentamos a continuación:

- **ISO 27000 (SGSI)** (International Standards Organization)
- **Controles críticos CIS** (Center for Internet Security)
- **NIST SP 800-53** (National Institute of Standards and Technology)
- **CMMI** (Capability Maturity Model Integration)
- **ENS** (Esquema Nacional de Seguridad – España)
- **ISO/IEC 27701** (**SGPI:** Sistema de Gestión de la Privacidad de la Información)

La familia de estándares ISO son de pago y si deseas adquirirlos, puedes hacerlo en:

https://www.iso.org/store.html

https://webstore.ansi.org

https://tienda.aenor.com (versiones en español)

Los **Controles críticos CIS** (Center for Internet Security) puedes descargarlos en:

https://www.cisecurity.org/controls

Las publicaciones **NIST** (National Institute of Standards and Technology) puedes descargarlos en:

https://www.nist.gov/publications

Las publicaciones sobre **CMMI** (Capability Maturity Model Integration) también son de pago, pero tienes bastante información en:

https://cmmiinstitute.com/learning/appraisals/levels

https://cmmiinstitute.com/getattachment/8d1133ac-4050-4ad0-9273-e4c43d356f06/attachment.aspx

https://cmmiinstitute.com/getattachment/738104c0-a6f0-4e1c-8bbe-35076b75f36e/attachment.aspx

**ENS** (Esquema Nacional de Seguridad – España) puedes descargarlos a través de la serie 800 en

https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad?format=html

## Cuadro Comparativo de las normas de este documento

| Criterio | ISO 27000 (SGSI) | Controles Críticos CIS | NIST SP 800-53 | CMMI | ENS (España) | ISO/IEC 27701 |
|---|---|---|---|---|---|---|
| **Objetivo** | Proteger la información mediante un sistema de gestión de seguridad (SGSI). | Definir buenas prácticas y controles esenciales para reducir riesgos. | Proveer un catálogo de controles de seguridad para sistemas federales y privados. | Mejorar la madurez y calidad de los procesos en una organización. | Garantizar la seguridad de la información en entidades públicas. | Extensión de ISO 27001 para gestionar la privacidad de los datos. |
| **Alcance** | Organizaciones de cualquier tamaño o sector. | Empresas y organismos que buscan seguridad práctica. | Principalmente para entidades gubernamentales de EEUU, pero adaptable. | Aplicable a cualquier sector, incluyendo ciberseguridad. | Organismos públicos y empresas que trabajan con el gobierno español. | Organizaciones que manejan datos personales. |
| **Estructura** | Basada en un ciclo de mejora continua (PDCA). | 18 Controles Críticos, agrupados en tres categorías, que suman 153 controles. | Agrupación de controles en familias de seguridad. | Modelo de niveles de madurez. | Basado en principios de seguridad y requisitos mínimos. | Añade requisitos específicos de privacidad a ISO 27001. |
| **Enfoque** | Gestión de riesgos y controles de seguridad. | Enfoque técnico basado en amenazas reales. | Basado en la gestión de riesgos y cumplimiento regulatorio. | Optimización de procesos y mejora continua. | Gestión riesgos de seguridad y cumplimiento normativo. | Protección de datos personales y cumplimiento con GDPR. |
| **Niveles o Controles** | 114 controles en el Anexo A (ISO 27001:2022). | 18 Controles Críticos agrupados en tres categorías que suman 153 controles. | Controlado por niveles de impacto (bajo, medio, alto). | 5 niveles de madurez. | Categorías de sistemas (bajo, medio, alto) y medidas de seguridad asociadas. | Basado en controles adicionales a ISO 27001. |
| **Certificación** | Certificación disponible a través de organismos acreditados. | No tiene certificación oficial, pero se usa ampliamente. | No certificable, pero se usa para auditorías de cumplimiento. | Certificación disponible para organizaciones. | Requiere certificación para cumplimiento normativo. | Certificación disponible para sistemas de gestión de privacidad. |
| **Relación con otras normativas** | Compatible con NIST, ENS y CIS Controls. | Se alinea con NIST y ISO 27001 en controles específicos. | Alineado con CIS, ISO 27001 y ENS. | Puede integrarse con ISO 27001 y NIST en seguridad. | Relacionado con ISO 27001 y NIST en requisitos de seguridad. | Relacionado con ISO 27001, GDPR y otras leyes de privacidad. |

# Charla 2 – Conceptos del SGSI


**Objetivo:** Comprender qué es un SGSI, su importancia y qué normativas lo sustentan.

Un **SGSI** (Sistema de Gestión de Seguridad de la Información) es un conjunto de políticas, procesos y controles diseñados para gestionar la seguridad de la información dentro de una organización.

**Líneas principales de un SGSI**

- **Basado en riesgos**: Identifica y gestiona amenazas a la información.
- **Ciclo de mejora continua (PDCA)**: Planificar, Hacer, Verificar, Actuar.
- **Normativas y estándares**: Se basa en marcos, referencias o buenas prácticas, que se desarrollarán a lo largo de esta artículo.
- **Documentación y monitoreo**: Registro de incidentes, auditorías y revisiones.
- **Auditorías y seguimiento** (acciones correctivas y preventivas).
- **IMPORTANTE**: Involucramiento de la dirección y, secundariamente, el resto de la organización.

Implementar un **SGSI** ayuda a las organizaciones a cumplir regulaciones, reducir riesgos y generar confianza en clientes y socios comerciales.

El objetivo de pensar la Ciberseguridad de una organización basada en un **SGSI**, no tiene por qué ser obtener una certificación del mismo (aunque puede serlo también), sino el diseño, planificación, producción y seguimiento detallado de todo el "**ciclo de vida de la Ciberseguridad**", tal cual lo iremos desarrollando en este artículo.

Sin duda, el mayor referente internación son la familia **ISO 27000**, compuesta por varias normas. Nos centraremos particularmente en las normas ISO 27001 (que es la que se certifica) y la ISO 27002 (que define los controles).

Como hemos mencionado, en este artículo consideraremos las siguientes referencias:

- **ISO 27001 (SGSI)** (International Standards Organization)
- **Controles críticos CIS** (Center for Internet Security)
- **NIST SP 800-53** (National Institute of Standards and Technology)
- **CMMI** (Capability Maturity Model Integration)

- **ENS** (Esquema Nacional de Seguridad – España)
- **ISO/IEC 27701** (**SGPI:** Sistema de Gestión de la Privacidad de la Información)

Adicionalmente, si se desea profundizar aún más sobre el tema, pueden ser tenidos en cuenta otros más qué se refieren a **SGSI**. Algunos de los más importantes son:

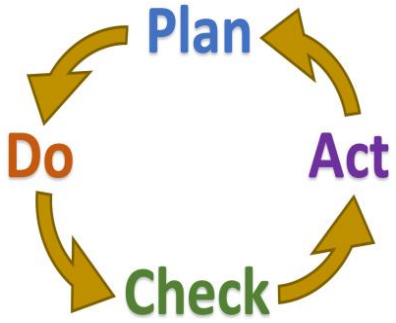
1) **COBIT** (Control Objectives for Information and Related Technologies)
   - Marco de gestión de TI que incluye seguridad de la información.
   - Enfatiza el **gobierno y control de la seguridad** dentro de una organización.
2) **ITIL** (Information Technology Infrastructure Library)
   - Incluye procesos de gestión de seguridad dentro del ciclo de vida de TI.
   - Aporta buenas prácticas para la operación segura de los servicios de TI.

Normas y regulaciones específicas

3) **PCI DSS** (Payment Card Industry Data Security Standard)
   - Obligatorio para empresas que procesan, almacenan o transmiten datos de tarjetas de pago.
4) **RGPD** (Reglamento General de Protección de Datos - Europa)
   - Establece requisitos para la protección de datos personales.
   - Puede formar parte de un SGSI que maneje información personal.
5) **HIPAA** (Health Insurance Portability and Accountability Act - EE.UU.)
   - Protege datos de salud electrónica (ePHI).
6) **ISO/IEC 22301** (Gestión de Continuidad del Negocio)
   - Complementa un SGSI asegurando la continuidad ante incidentes de seguridad.

Si iniciamos el tema, sobre la base de implementar un SGSI considerando la norma ISO 27001, los pasos básicos serían:

- **Requisitos de ISO 27001** y su estructura (Anexos A y cláusulas).
- Cuerpo de la norma (organización del SGSI)
- El **ciclo PDCA** (Planificar, Hacer, Verificar, Actuar).
- Identificación de **activos y evaluación de riesgos**.
- **Estructura documental**.
- **Controles de seguridad**.
- **Desafíos y buenas prácticas** en la implementación.



Más detalle de la norma:

- Contexto de la organización.
- Liderazgo y compromiso de la dirección.
- Planificación del SGSI.
- Evaluación de riesgos y oportunidades.
- Operación y monitoreo.
- Mejora continua.
- Controles del Anexo A.

Origen y posicionamiento del estándar ISO/IEC 27001:

**ISO** (Organización Internacional de Estándares) e **IEC** (Comisión Internacional de Electrotécnia) conforman un sistema especializado para la definición de estándares mundiales. Organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo.

En el campo de tecnologías de la información (**TI**), ISO e IEC han establecido unir un comité técnico, ISO/IEC **JTC 1** (Join Technical Committee Nº1). Los borradores de estas normas internacionales adoptadas por este comité técnico son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una norma internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

El Estándar Internacional **ISO/IEC 17799** fue preparado inicialmente por el Instituto de Normas Británico (como **BS 7799**: Britsh Standard) y fue adoptado, bajo la supervisión del grupo de trabajo "Tecnologías de la Información", del Comité Técnico de esta unión entre ISO/IEC JTC 1, en paralelo con su aprobación por los organismos nacionales de ISO e IEC.

El estándar ISO/IEC 27001 pasó a ser el nuevo estándar oficial, su título completo en ese momento fue: **BS 7799-2:2005 (ISO/IEC 27001:2005)**. También fue preparado por este JTC 1 y en el subcomité **SC 27**, IT "Security Techniques". Esta fue la primera edición, de fecha 15 de octubre de 2005. En la actualidad, la última versión es la del año 2022:

> **ISO/IEC 27001 (Third edition) 2022-10: "***Information security, cybersecurity and privacy protection — Information security management systems — Requirements"*

Este estándar internacional adopta también el modelo "Plan-Do-Check-Act" (**PDCA**), el cual es aplicado a toda la estructura de procesos de ISMS, y significa lo siguiente:


- **Plan** (Establecer el SGSI): Implica, establecer la política SGSI, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la

seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.

- **Do** (Implementar y operar el SGSI): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.
- **Check** (Monitorizar y revisar el SGSI): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.
- **Act** (Mantener y mejorar el SGSI): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del SGSI o cualquier otra información relevante para permitir la continua mejora del SGSI.

Durante los años 2006 y 2007, cuando esta norma comenzó a aplicarse realmente en España, hemos publicado toda una serie de artículos, en una revista que existía por esos años que se llamaba "**Auditoría y Seguridad**".

Si bien se refieren a la primera versión de la norma, pueden serte de mucha utilidad para profundizar en la misma. Todos ellos puedes descargarlos en nuestra Web: www.darFe.es

en el menú "**DESCARGAS**" → "**Normas y estándares**"

Los artículos son:

- **ISO 27001 - Análisis del estándar**:

  analisis_de_iso-27001.pdf
- **ISO 27001 - Los controles (Parte 1):**

  iso-27001_los-controles_parteii.pdf
- **ISO 27001 - Los controles (Parte 2):**

  iso-27001_los-controles.pdf
- **ISO 27001 y las PyMes**:

  ays_nro13_sep-2007_iso-27001_y_las_pymes.pdf
- **Metodología de implantación y certificación en ISO 27001**:

  ays_nro17_metodologia_de_implantacion_certificacion_en_las_pymes.pdf
- **Auditoría Interna en ISO 27001**:

  ays_nro22_2008_auditoria_interna_en_iso-27001.pdf
- **métricas de seguridad y cuadros de mando (según ISO 27004):**

  ays_nro21_2008_metricas_indicadores_y_cuadros_de_mando.pdf
- **ISO 20000 e ISP 27000**:

  ays_nro16_nov_2007-nro_especial_iso_20000_o_iso_27000.pdf
- **ISO 27001 e ISO 27004**:

  iso-27001_e_iso-27004.pdf

- **ISO 27001 y la LOPD (Parte 1):**

  ays_nro19_2008_isoiec_27001-2005__lopd_1.pdf

- **ISO 27001 y la LOPD (Parte 2):**

  ays_nro20_2008_isoiec_27001-2005__lopd_2.pdf

- **ISO 27001 y las AAPP**:

  ays_nro18_2008_iso27001_y_las_aapp.pdf

También tienes un video de presentación de esta norma en la **UPM** (Universidad Politécnica de Madrid):

- **UPM TASSI 2009 Conferencia 2: Perspectiva española en seguridad: estándar ISO/IEC 27000**

https://www.youtube.com/watch?v=rC56SKnAns0&list=PL0QSAEWH0x_hBjTjob2z9sdaXeWP_oMTP&index=50&t=1s

# Charla 3 – El enfoque a Riesgos


**Objetivo:** Desarrollar el concepto de Gestión riesgos de seguridad y cumplimiento normativo.

Si buscamos en Internet el significado, veremos que:

- riesgo: Contingencia o proximidad de un daño.
- arriesgar: Poner a riesgo. Exponer a una persona o cosa a un riesgo o ponerlos en peligro.

Si volvemos a nuestro **Cuadro Comparativo de las normas de este documento** de la Charla 1, podemos ver que el enfoque a riesgos es común en ISO 27001, NIST SP 800-53 y en el ENS.

| Criterio | ISO 27000 (SGSI) | NIST SP 800-53 | ENS (España) |
|---|---|---|---|
| **Enfoque** | Gestión de riesgos y controles de seguridad. | Basado en la gestión de riesgos y cumplimiento regulatorio. | Gestión riesgos de seguridad y cumplimiento normativo. |

---

### 3.1. Enfoque de Riesgos en ISO 27000 (SGSI)

#### 3.1.1. Principios de Gestión de Riesgos en ISO 27000

ISO 27000 establece que **la gestión de riesgos es el pilar fundamental** de un SGSI. Su propósito es identificar, analizar y mitigar los riesgos para garantizar la confidencialidad, integridad y disponibilidad (CID) de la información.

**3.1.2. Proceso de Gestión de Riesgos en ISO/IEC 27005:2022** "*Gestión de riesgos de la Seguridad la Información*". Es una de las normas de la familia ISO 27k y se emplea como soporte.

ISO 27005 proporciona una guía detallada para la gestión de riesgos dentro de un SGSI, utilizando los siguientes pasos:

1) **Establecer el contexto** → Identificar activos, amenazas y vulnerabilidades.
2) **Evaluación del riesgo** →
   - Identificar riesgos (activos + amenazas + vulnerabilidades).
   - Analizar el impacto y la probabilidad.
   - Evaluar el nivel de riesgo.
3) **Tratamiento del riesgo** → Se decide:
   - Mitigarlo (implementando controles).
   - Transferirlo (seguros, outsourcing).
   - Evitarlo (cambiar procesos).
   - Aceptarlo (si el costo de mitigación es mayor que el daño potencial).
4) **Monitoreo y revisión** → Reevaluar riesgos continuamente.

#### 3. 1.3. Controles para la Mitigación de Riesgos en ISO 27001

- Basados en el **Anexo A de ISO 27001:2022**, que tiene 114 controles en 4 categorías:
  - Controles organizacionales.
  - Controles humanos.
  - Controles físicos.
  - Controles tecnológicos.

**Ejemplo Práctico (ISO 27000)**

Una empresa de comercio electrónico identifica un **riesgo de filtración de datos de clientes**. Aplica la metodología:

✅ **Riesgo identificado:** Ataques de phishing contra empleados con acceso a bases de datos.

✅ **Análisis:** Alta probabilidad y alto impacto.

✅ **Tratamiento:**

- Implementación de autenticación multifactor.
- Formación en seguridad para empleados.
- Monitoreo continuo de accesos sospechosos.

---

### 3.2. Enfoque de Riesgos en NIST SP 800-53

National Institute of Standards and Technology
U.S. Department of Commerce

#### 3.2.1. Principios de Gestión de Riesgos en NIST

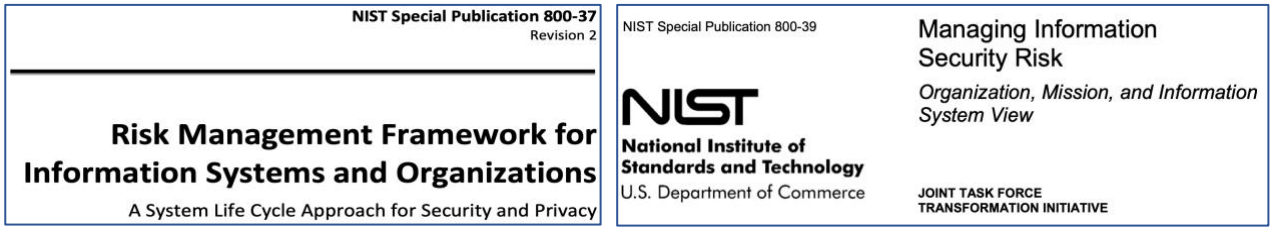
El **NIST Risk Management Framework (RMF)** ofrece un proceso estructurado para la **identificación, análisis y mitigación de riesgos**, integrándolo en el ciclo de vida de los sistemas de información.

El **NIST SP 800-53**, en el punto 1.3 ORGANIZATIONAL RESPONSIBILITIES, para desarrollar en detalle este tema, nos deriva hacia otras dos publicaciones: **SP 800-37** y **SP 800-39**

> To address the organization's concerns about assessment and determination of risk, security and privacy requirements are satisfied with the knowledge and understanding of the organizational risk management strategy.[17] The risk management strategy considers the cost, schedule, performance, and supply chain issues associated with the design, development, acquisition, deployment, operation, sustainment, and disposal of organizational systems. A risk management process is then applied to manage risk on an ongoing basis.[18]
>
> [17] [SP 800-39] provides guidance on risk management processes and strategies.
> [18] [SP 800-37] provides a comprehensive risk management process.

17 Organizational risk management strategy: Estrategia de gestión de riesgos de la organización.

18 Risk management process: Proceso de gestión de riesgos




La propuesta de ambas publicaciones son similares y se basan en que la gestión de riesgos debe ser gestionada en tres niveles, tal cual se puede ver a la derecha (*figura 1 de **SP 800-37***)

- Nivel 1: organización
- Nivel 2: Misión/Procesos de negocio
- Nivel 3: Sistema de Información

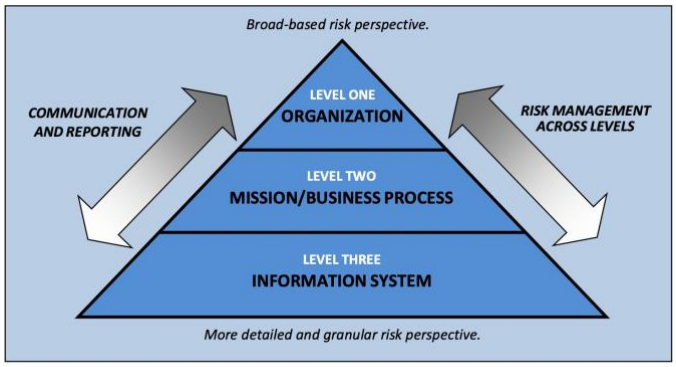



FIGURE 1: ORGANIZATION-WIDE RISK MANAGEMENT APPROACH

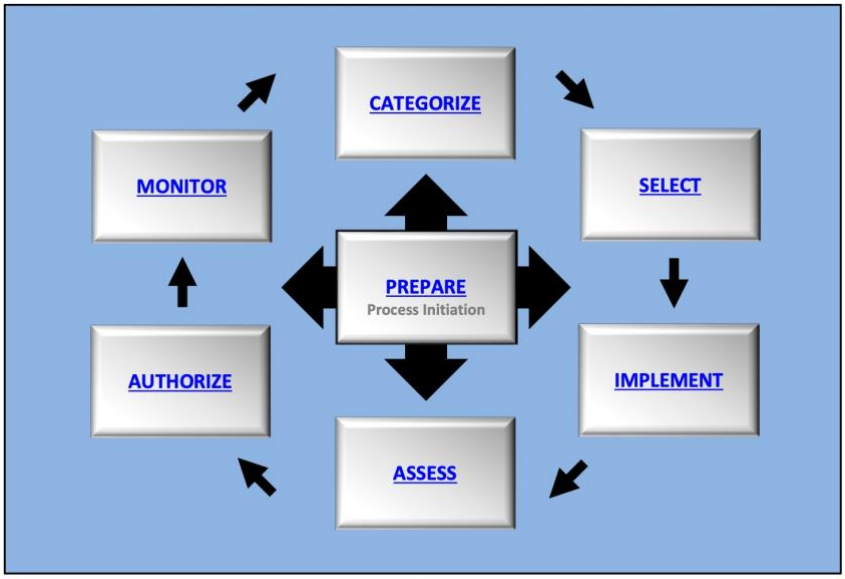



FIGURE 2: RISK MANAGEMENT FRAMEWORK

Y luego definen un marco de gestión de riesgos, tal cual podemos ver a la izquierda (*figura 2 de **SP 800-37***), donde una vez más se pone de manifiesto un ciclo de mejora continua que se prepara a través de:

- Categorización
- Selección
- Implementación
- Evaluación
- Autorización
- Monitorización

Si deseas profundizar en cada una de ellas, sus enlaces son:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

### 3.2.2. Pasos del Marco de Gestión de Riesgos NIST

1) **Categorización del sistema** → Determinar la sensibilidad de la información (bajo, medio, alto).
2) **Selección de controles de seguridad** → Basado en la categorización.
3) **Implementación de controles** → Aplicar medidas de seguridad.
4) **Evaluación de seguridad** → Verificar que los controles funcionan correctamente.
5) **Autorización de operación** → Aprobación para su uso en producción.
6) **Monitorización continua** → Revisión y ajuste de controles.

### 3.2.3. Controles Clave para Mitigar Riesgos (Ejemplos de NIST SP 800-53)

A su vez, también define una serie de controles que podemos tener en cuenta:

- **AC-2:** Gestión de accesos y cuentas de usuario.
- **SI-7:** Protección contra malware avanzado.
- **RA-3:** Realización de evaluaciones de riesgo de manera periódica.

**Ejemplo Práctico (NIST SP 800-53)**

Un banco implementa NIST SP 800-53 y detecta un **riesgo de ataques de ransomware**.

✅ **Riesgo identificado:** Un malware podría cifrar los datos críticos del banco.

✅ **Análisis:** Probabilidad media, impacto crítico.

✅ **Controles aplicados:**

- Implementar segmentación de red (SC-7).
- Copias de seguridad diarias (CP-9).
- Análisis de comportamiento de usuarios (AU-6).

---

## 3.3. Enfoque de Riesgos en ENS (España)

### 3.3.1. Principios del ENS en Gestión de Riesgos

El **Esquema Nacional de Seguridad (ENS)** exige que **todas las entidades públicas y empresas que trabajan con la Administración adopten una estrategia de gestión de riesgos** basada en principios como:

✅ **Seguridad integral**: Considerar seguridad desde el diseño.

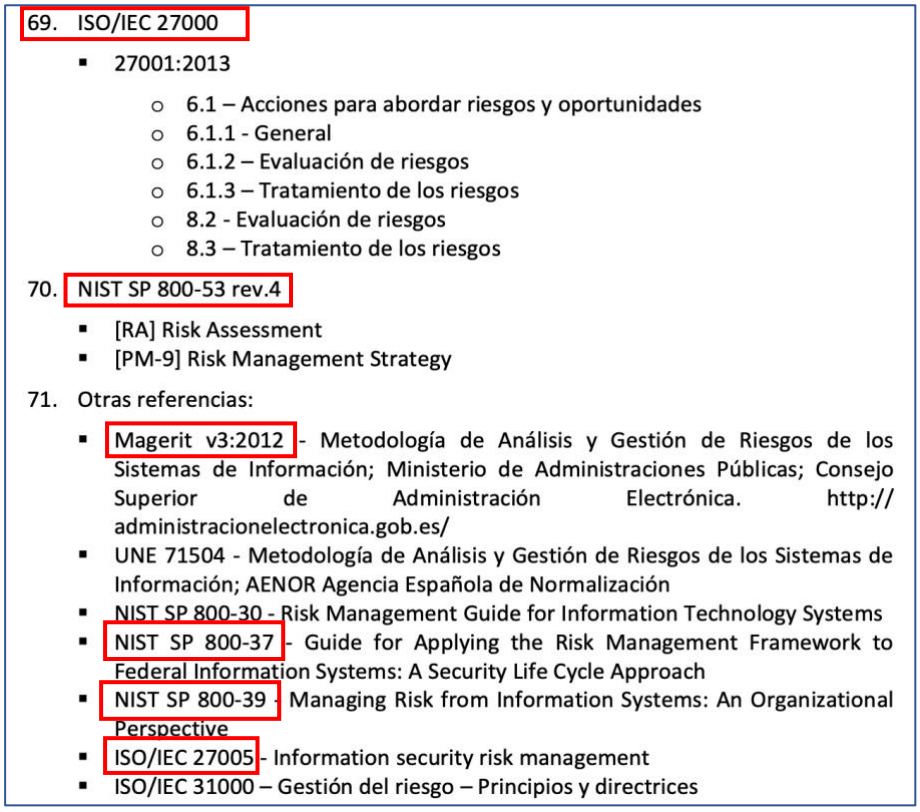
✅ **Gestión de riesgos continua**: Identificación, análisis y evaluación de amenazas.

✅ **Clasificación de sistemas**: Bajo, Medio, Alto, según impacto.

En general cuando necesitemos tratar el tema del ENS, nos referiremos a los documentos que tiene publicado el **CCN** (Centro Criptológico Nacional de España) a través de su serie 800.


Algo muy interesante respecto al ENS, es que si analizamos el documento **CCN-STIC 804** "ENS. Guía de implantación" (cuya imagen podemos ver a la derecha), al referirse a este tema, en su punto: 4.1.1 [OP.PL.1] "ANÁLISIS DE RIESGOS" nos propone como referencias, justamente los dos puntos que hemos desarrollado anteriormente, es decir lo que nos indican las normas ISO 27000, como así también los documentos de NIST que acabamos de presentar en el punto anterior. También pone como referencia la metodología "MAGERIT" que es la que se aplica en las administraciones públicas españolas y que la trataremos a continuación. Todo esto podemos verlo en la imagen que se

presenta aquí abajo, que es una captura de pantalla del punto: 4.1.1 [OP.PL.1] "ANÁLISIS DE RIESGOS" de esta guía 804.



69. ISO/IEC 27000
    - 27001:2013
        - 6.1 – Acciones para abordar riesgos y oportunidades
        - 6.1.1 - General
        - 6.1.2 – Evaluación de riesgos
        - 6.1.3 – Tratamiento de los riesgos
        - 8.2 - Evaluación de riesgos
        - 8.3 – Tratamiento de los riesgos
70. NIST SP 800-53 rev.4
    - [RA] Risk Assessment
    - [PM-9] Risk Management Strategy
71. Otras referencias:
    - Magerit v3:2012 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información; Ministerio de Administraciones Públicas; Consejo Superior de Administración Electrónica. http:// administracionelectronica.gob.es/
    - UNE 71504 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información; AENOR Agencia Española de Normalización
    - NIST SP 800-30 - Risk Management Guide for Information Technology Systems
    - NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
    - NIST SP 800-39 - Managing Risk from Information Systems: An Organizational Perspective
    - ISO/IEC 27005 - Information security risk management
    - ISO/IEC 31000 – Gestión del riesgo – Principios y directrices

### 3.3.2. Fases del Proceso de Gestión de Riesgos en ENS

1) **Identificación de activos críticos** → Infraestructura, datos, aplicaciones.
2) **Evaluación de riesgos** → Basada en impacto y probabilidad.
3) **Aplicación de medidas de seguridad ENS** →
    - Mínimas para nivel Bajo.
    - Reforzadas para nivel Medio.
    - Máximas para nivel Alto.
4) **Monitorización y auditoría** → Control periódico de riesgos.

**Ejemplo Práctico (ENS)**

Un Ayuntamiento con datos de ciudadanos aplica el ENS:

- ✅ **Riesgo identificado:** Ataques de inyección SQL en su portal de trámites.
- ✅ **Análisis:** Alto impacto en disponibilidad y confidencialidad.
- ✅ **Tratamiento:**
    - Implementar validación de entradas (Medida ENS específica).
    - Monitoreo activo de logs.
    - Auditorías de seguridad periódicas.

**Conclusión**

- **ISO 27000** gestiona riesgos dentro de un **SGSI estructurado** con enfoque PDCA.
- **NIST SP 800-53** ofrece **controles detallados** para sistemas de información.
- **ENS** es obligatorio en España y usa **clasificación de impacto** para aplicar medidas de seguridad, apoyándose en los dos anteriores.

---

### 3.4. Metodología MAGERIT para análisis de Riesgo

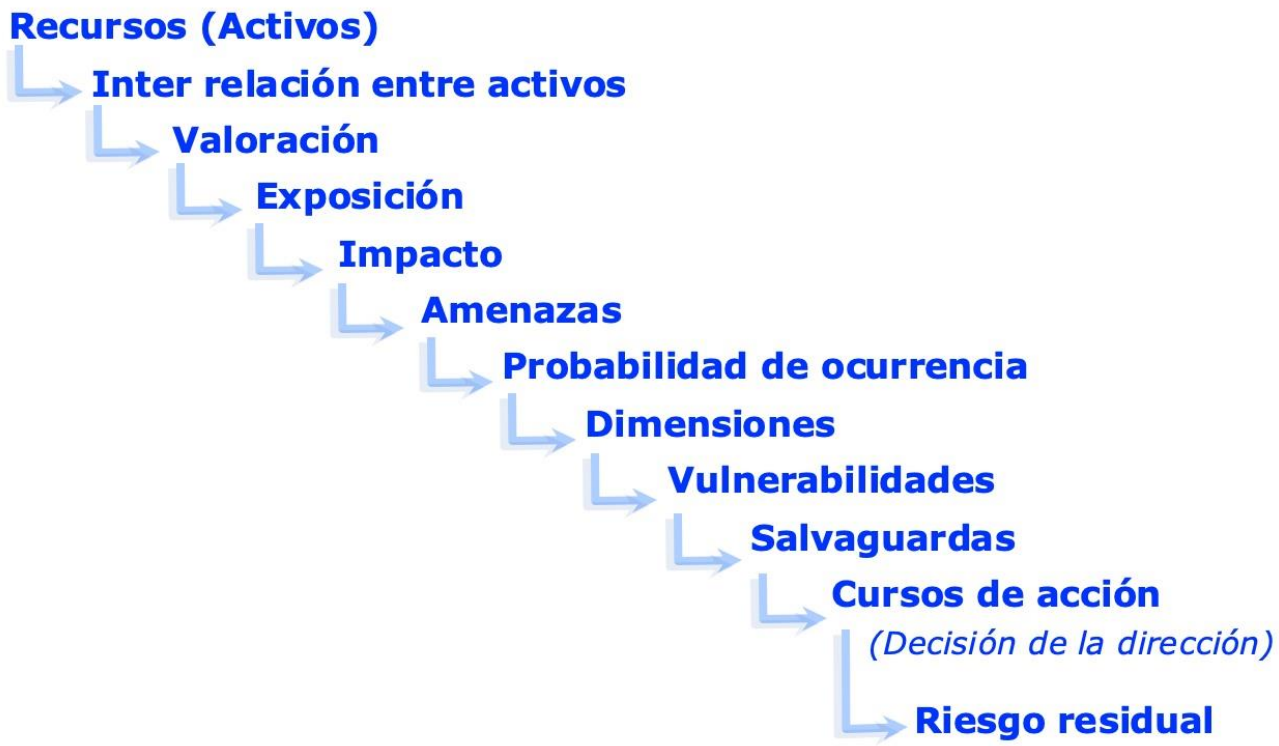
MAGERIT: Metodología española para la gestión y análisis de riesgos de los sistemas de la información que en sus tres libros "Método", "Catalogo de elementos" y "Guía de técnicas".

Pueden descargarse los tres libros en:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html


En el punto 6.2. Metodologías de análisis de Riesgo, del libro: "Manual de la Resiliencia (Una guía práctica de Ciberresiliencia en Redes y Sistemas de TI)" que podéis descargar gratuitamente de: www.darFe.es, encontraréis desarrollado con todo detalle esta metodología, por lo tanto, para no ser redundantes, os invitamos a que directamente os dirijáis a este libro.

Con independencia de MAGERIT, la Secuencia natural de una Análisis de Riesgo, en general para cualquier metodología, es algo similar a:



A título informativo, y con la única intención que podáis ver el grado de detalle de esta metodología, se presentan a continuación algunos ejemplos de las **Tablas del catálogo de MAGERIT.**

| | |
|---|---|
| [SW] Aplicaciones (software) | |
| | [prp] desarrollo propio (in house) |
| | [sub] desarrollo a medida (subcontratado) |
| | [std] estándar (off the shelf) |
| | [browser] navegador web |
| | [www] servidor de presentación |
| | [app] servidor de aplicaciones |
| | [email_client] cliente de correo electrónico |
| | [file] servidor de ficheros |
| | [dbms] sistema de gestión de bases de datos |
| | [tm] monitor transaccional |
| | [office] ofimática |
| | [av] anti virus |
| | [os] sistema operativo |
| | [ts] servidor de terminales |
| | [backup] sistema de backup |
| [HW] Equipos informáticos (hardware) | |
| | [host] grandes equipos |
| | [mid] equipos medios |
| | [pc] informática personal |
| | [mobile] informática móvil |
| | [pda] agendas electrónicas |
| | [easy] fácilmente reemplazable |
| | [data] que almacena datos |
| | [peripheral] periféricos |
| | [print] medios de impresión |
| | [scan] escáneres |
| | [crypto] dispositivos criptográficos |
| | [network] soporte de la red |
| | [modem] módems |
| | [hub] concentradores |
| | [switch] conmutadores |
| | [router] encaminadores |
| | [bridge] pasarelas |
| | [firewall] cortafuegos |
| | [wap] punto de acceso wireless |
| | [pabx] centralita telefónica |

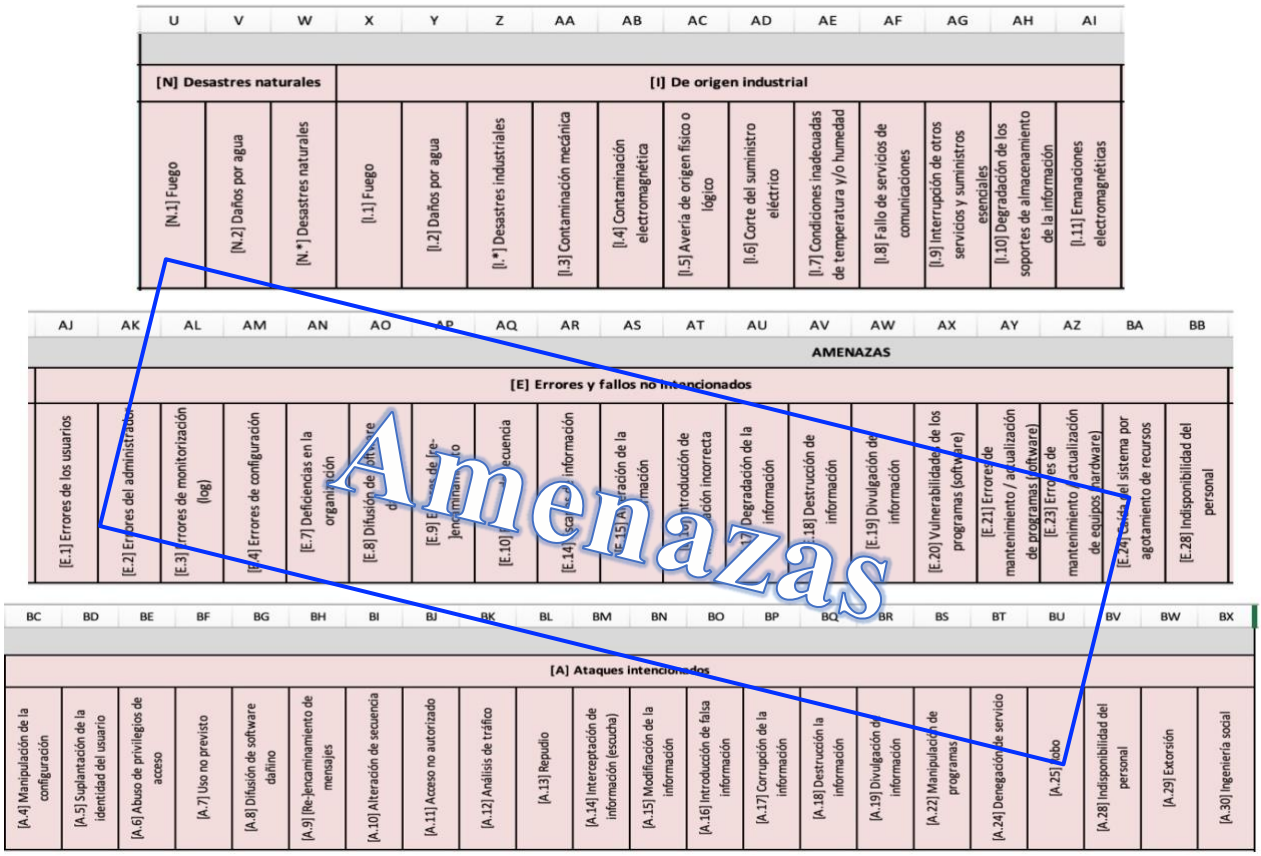
| TIPOS DE ACTIVOS | |
|---|---|
| [S] Servicios | |
| | [anon] anónimo (sin requerir identificación del usuario) |
| | [pub] al público en general (sin relación contractual) |
| | [ext] a usuarios externos (bajo una relación contractual) |
| | [int] interno (usuarios y medios de la propia organización) |
| | [cont] contratado a terceros (se presta con medios ajenos) |
| | [www] world wide web |
| | [telnet] acceso remoto a cuenta local |
| | [email] correo electrónico |
| | [file] almacenamiento de ficheros |
| | [ftp] transferencia de ficheros |
| | [edi] intercambio electrónico de datos |
| | [dir] servicio de directorio |
| | [idm] gestión de identidades |
| | [ipm] gestión de privilegios |
| | [pki] PKI - infraestructura de clave pública |
| [D] Datos / Información | |
| | [files] ficheros |
| | [password] credenciales (e.g. contraseñas) |
| | [auth] datos de validación de credenciales |
| | [acl] datos de control de acceso |
| | [vr] datos vitales (vital records) |
| | [com] datos de interés comercial |
| | [adm] datos de interés para la administración pública |
| | [int] datos de gestión interna |
| | [source] código fuente |
| | [exe] código ejecutable |
| | [conf] datos de configuración |
| | [log] registro de actividad (log) |
| | [test] datos de prueba |
| | [per] datos de carácter personal |
| | [A] de nivel alto |
| | [M] de nivel medio |
| | [B] de nivel básico |
| | [label] datos clasificados |
| | [S] secreto |
| | [R] reservado |
| | [C] confidencial |
| | [DL] difusión limitada |
| | [SC] sin clasificar |

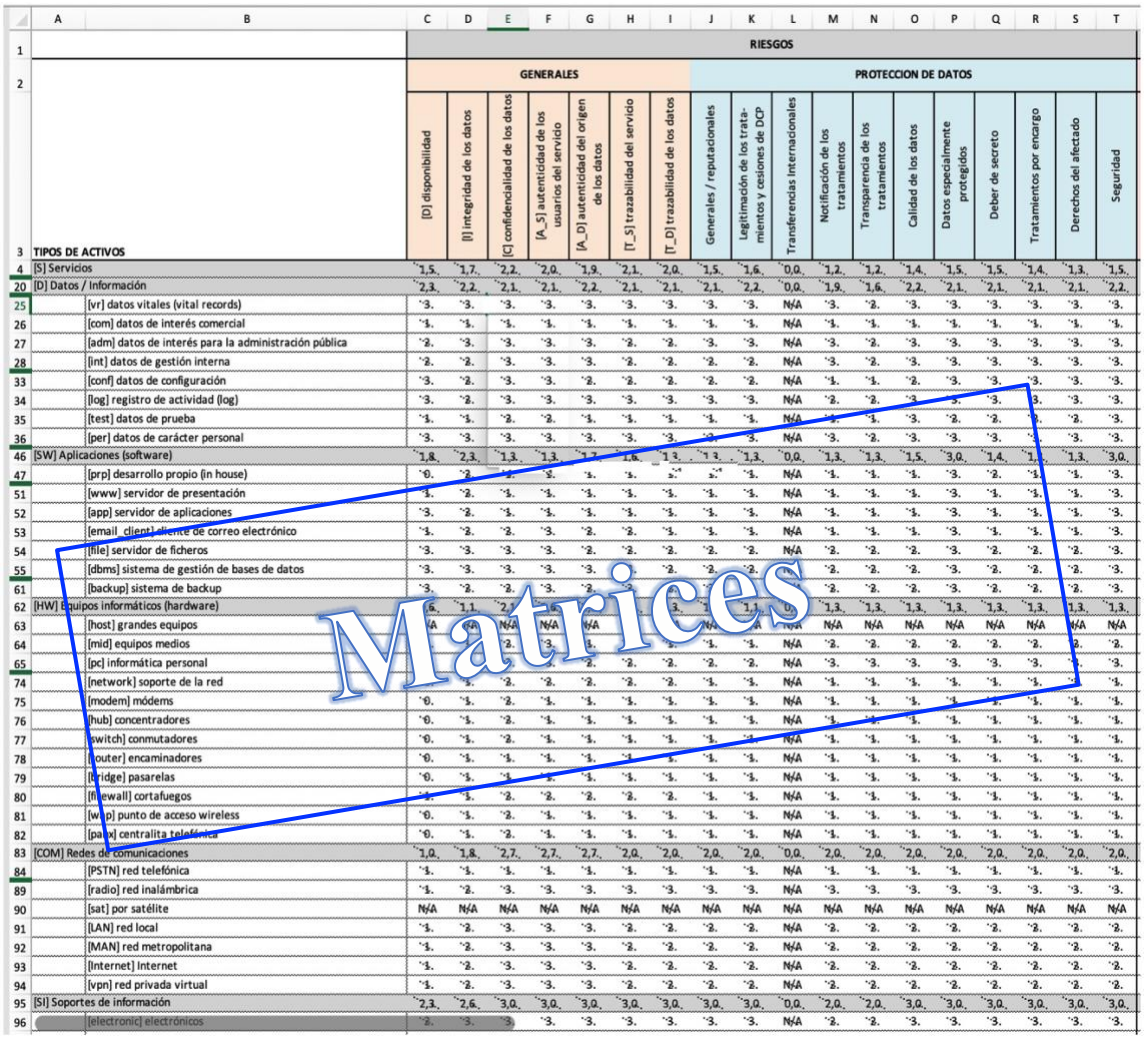
| | |
|---|---|
| [COM] Redes de comunicaciones | |
| | [PSTN] red telefónica |
| | [ISDN] rdsi (red digital) |
| | [X25] X25 (red de datos) |
| | [ADSL] ADSL |
| | [pp] punto a punto |
| | [radio] red inalámbrica |
| | [sat] por satélite |
| | [LAN] red local |
| | [MAN] red metropolitana |
| | [Internet] Internet |
| | [vpn] red privada virtual |
| [SI] Soportes de información | |
| | [electronic] electrónicos |
| | [disk] discos |
| | [san] almacenamiento en red |
| | [cd] cederrón (CD-ROM) |
| | [usb] dispositivos USB |
| | [dvd] DVD |
| | [tape] cinta magnética |
| | [non_electronic] no electrónicos |
| | [printed] material impreso |
| | [tape] cinta de papel |
| | [film] microfilm |
| [AUX] Equipamiento auxiliar | |
| | [power] fuentes de alimentación |
| | [ups] sistemas de alimentación ininterrumpida |
| | [gen] generadores eléctricos |
| | [ac] equipos de climatización |
| | [cabling] cableado |
| | [robot] robots |
| | [tape] ... de cintas |
| | [disk] ... de discos |
| | [supply] suministros esenciales |
| | [destroy] equipos de destrucción de soportes de información |
| | [furniture] mobiliario: armarios, etc |
| | [safe] cajas fuertes |
| | [car] vehículo terrestre: coche, camión, etc. |
| | [plane] vehículo aéreo: avión, etc. |
| | [ship] vehículo marítimo: buque, lancha, etc. |
| | [shelter] contenedores |
| | [channel] canalización |
| [P] Personal | |
| | [ue] usuarios externos |
| | [ui] usuarios internos |
| | [op] operadores |
| | [adm] administradores de sistemas |
| | [com] administradores de comunicaciones |
| | [dba] administradores de BBDD |
| | [des] desarrolladores |
| | [sub] subcontratas |
| | [prov] proveedores |

Activos

| Nº | Activo | Valoración |
|---|---|---|
| 1 | [files] ficheros | 50.000 € |
| 2 | [vr] datos vitales (vital records) | 80.000 € |
| 3 | [com] datos de interés comercial | 10.000 € |
| 4 | [source] código fuente | 5000 € |
| 5 | [prp] desarrollo propio (in house) | 35.000 € |
| 6 | [sub] desarrollo a medida (subcontratado) | 5000 € |
| 7 | [www] servidor de presentación | 5000 € |
| 8 | [app] servidor de aplicaciones | 10.000 € |
| 9 | [file] servidor de ficheros | 10.000 € |
| 10 | [dbms] sistema de gestión de bases de datos | 40.000 € |
| 11 | [office] ofimática | 10.000 € |
| 12 | [av] anti virus | 2000 € |
| 13 | [os] sistema operativo | 2000 € |
| 14 | [ts] servidor de terminales | 1000 € |
| 15 | [backup] sistema de backup | 40.000 € |
| 16 | [host] grandes equipos | 40.000 € |
| 17 | [mid] equipos medios | 10.000 € |
| 18 | [pc] informática personal | 5000 € |

Valoración


[N] Desastres naturales
[I] De origen industrial
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura y/o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios y suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas
AMENAZAS
[E] Errores y fallos no intencionados
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Escape de información
[E.15] Alteración de la información
[E.16] Introducción de información incorrecta
[E.17] Degradación de la información
[E.18] Destrucción de información
[E.19] Divulgación de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.28] Indisponibilidad del personal
[A] Ataques intencionados
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de la información
[A.16] Introducción de falsa información
[A.17] Corrupción de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social
Amenazas


RIESGOS
GENERALES
PROTECCION DE DATOS
TIPOS DE ACTIVOS
[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A_S] autenticidad de los usuarios del servicio
[A_D] autenticidad del origen de los datos
[T_S] trazabilidad del servicio
[T_D] trazabilidad de los datos
Generales / reputacionales
Legitimación de los tratamientos y cesiones de DCP
Transferencias Internacionales
Notificación de los tratamientos
Transparencia de los tratamientos
Calidad de los datos
Datos especialmente protegidos
Deber de secreto
Tratamientos por encargo
Derechos del afectado
Seguridad
[S] Servicios
[D] Datos / información
[vr] datos vitales (vital records)
[com] datos de interés comercial
[adm] datos de interés para la administración pública
[int] datos de gestión interna
[conf] datos de configuración
[log] registro de actividad (log)
[test] datos de prueba
[per] datos de carácter personal
[SW] Aplicaciones (software)
[prp] desarrollo propio (in house)
[www] servidor de presentación
[app] servidor de aplicaciones
[email_client] cliente de correo electrónico
[file] servidor de ficheros
[dbms] sistema de gestión de bases de datos
[backup] sistema de backup
[HW] Equipos informáticos (hardware)
[host] grandes equipos
[mid] equipos medios
[pc] informática personal
[network] soporte de la red
[modem] módems
[hub] concentradores
[switch] conmutadores
[router] encaminadores
[bridge] pasarelas
[firewall] cortafuegos
[wap] punto de acceso wireless
[pabx] centralita telefónica
[COM] Redes de comunicaciones
[PSTN] red telefónica
[radio] red inalámbrica
[sat] por satélite
[LAN] red local
[MAN] red metropolitana
[Internet] Internet
[vpn] red privada virtual
[SI] Soportes de información
[electronic] electrónicos
Matrices

**Ejercicios y Prácticas**

---

**Ejercicio 1: Evaluación de Riesgos en Diferentes Marcos**

1) Se presenta un caso donde una empresa sufre intentos de acceso no autorizado.
2) Se propone analizar el riesgo y proponer medidas según:
    - ISO 27000
    - NIST SP 800-53
    - ENS

---

**Ejercicio 2: Simulación de Análisis de Riesgos**

1) Se asigna un escenario (por ejemplo, ataque de ransomware en una universidad).
2) Se propone:
    - Aplicar la metodología de gestión de riesgos.
    - Proponer controles adecuados.
    - Evaluar impacto y probabilidad.

---

**Ejercicio 3: Propuesta de MAGERIT**

1) Sobre une empresa real que conozcas, o ficticia si lo prefieres.
2) Se propone analizar el catálogo de MAGERIT y:
    - Definir algunos activos.
    - Valorarlos.
    - Asociar las amenazas a las que estarían expuestos.
    - Evaluar sus riesgos.

# Charla 4 – La dirección de la organización


**Objetivo:** Despertar consciencia sobre la importancia que tiene el involucramiento y participación activa de la dirección de la empresa en un SGSI.

La **alta dirección** juega un papel fundamental en la seguridad de la información. Su liderazgo y compromiso determinan el éxito de la implementación, mantenimiento y mejora del SGSI y los controles de seguridad dentro de una organización.

A continuación, se comparan los requisitos de **ISO 27000, Controles Críticos CIS, NIST SP 800-53, CMMI, ENS (España) e ISO/IEC 27701** en relación con **las responsabilidades de la dirección**.

---

**Comparación de las Responsabilidades de la Dirección en Normas y Marcos de Referencia**

### 4.1. Compromiso de la Alta Dirección

**ISO 27000** ISO 27001 **(SGSI)**

La norma exige que la dirección **demuestre liderazgo y compromiso** en la gestión de la seguridad de la información. Esto se evidencia a través de:

- El establecimiento de una **política de seguridad** alineada con los objetivos del negocio.
- La participación activa en auditorías y revisiones del SGSI.
- La asignación de recursos adecuados para la seguridad de la información.
- El apoyo a la cultura de seguridad dentro de la organización.

**Controles Críticos** CIS Center for Internet Security **CIS**

Los Controles CIS **no establecen explícitamente un compromiso de la alta dirección**, pero sugieren que la gerencia debe:

- **Apoyar la implementación de controles clave** (ej. control de accesos, inventario de activos).
- Proporcionar recursos para la adopción de medidas de seguridad esenciales.
- Supervisar el cumplimiento de los controles mediante reportes internos.

**NIST SP 800-53** NIST National Institute of Standards and Technology U.S. Department of Commerce

El NIST requiere que la alta dirección:

- **Apruebe** políticas y procedimientos de seguridad.
- Asigne roles y responsabilidades para la gestión de la seguridad.
- **Supervise y lidere la evaluación de riesgos** en la organización.
- **Asigne recursos** y garantice la implementación de controles efectivos.

📌 **CMMI**

CMMI **incorpora la seguridad en los procesos de mejora continua** y establece que la dirección debe:

- Involucrarse en la **madurez de los procesos de seguridad**.
- Asegurar que la seguridad de la información esté alineada con los objetivos estratégicos.
- Proporcionar liderazgo en la implementación de mejoras en seguridad.

📌 **ENS** **(España)**

El ENS **exige un compromiso explícito de la alta dirección** en organismos públicos y privados que lo adopten. Las responsabilidades incluyen:

- Liderar la **implantación del ENS** en la organización.
- Aprobar la **política de seguridad**.
- Designar responsables de seguridad y supervisar su cumplimiento.

📌 **ISO/IEC** **27701**

Como norma específica para la **gestión de la privacidad**, ISO 27701 exige que la dirección:

- **Demuestre compromiso** con la protección de datos personales.
- Integre la privacidad en la estrategia organizacional.
- Asigne recursos suficientes para garantizar el cumplimiento de regulaciones como el **GDPR**.

---

### 4.2. Definición de Roles y Responsabilidades

📌 **ISO 27000** **(SGSI)**

- La dirección debe designar un **Responsable de Seguridad de la Información (CISO o equivalente)**.
- Se deben definir claramente los roles en la seguridad de la información.
- Se requiere documentar y comunicar las responsabilidades a todo el personal.

**Controles Críticos**  **CIS**

- No define un **marco de roles específico**, pero recomienda que cada control tenga un responsable asignado.

**NIST SP 800-**  **53**

- Define roles clave como el **Oficial de Seguridad de la Información (ISO)**.
- Asigna responsabilidades específicas a equipos técnicos y administrativos.

**CMMI** 

- Cada nivel de madurez en seguridad tiene responsables asignados.
- La dirección debe garantizar la existencia de equipos responsables de la mejora de procesos.

**ENS**  **(España)**

- Establece la figura del **Responsable de Seguridad** y del **Responsable del Sistema**.
- Define una estructura organizativa clara para la gestión de la seguridad.

**ISO/IEC**  **27701**

- Designa un **Responsable de Privacidad de la Información** dentro de la organización.
- Define roles para la gestión y supervisión de los datos personales.

---

### 4.3. Supervisión y Toma de Decisiones

**ISO 27000**  **(SGSI)**

- La dirección debe **aprobar y revisar** periódicamente la política de seguridad.
- Debe liderar la evaluación de **riesgos y oportunidades** en seguridad de la información.

📌 **Controles Críticos**  **CIS**

- Propone la supervisión de la **implementación de controles**, pero sin una estructura formal de toma de decisiones.

📌 **NIST SP 800-**  **53**

- Exige que la dirección **apruebe políticas y estrategias de seguridad**.
- Debe supervisar auditorías, evaluaciones de riesgos y gestión de incidentes.

📌  **CMMI**

- La toma de decisiones está ligada a la **madurez de los procesos de seguridad**.
- La dirección debe evaluar métricas y resultados antes de implementar mejoras.

📌 **ENS**  **(España)**

- La dirección debe aprobar el **Informe de Estado de Seguridad** de la organización.

📌 **ISO/IEC**  **27701**

- Supervisa la aplicación de los **principios de privacidad y protección de datos** en toda la organización.

---

### 4.4. Gestión de Recursos y Presupuesto

📌 **ISO 27000 (SGSI)** 

- La dirección debe asignar **recursos adecuados** (humanos, tecnológicos y financieros) para el SGSI.

📌 **Controles Críticos CIS** 

- No menciona explícitamente la **gestión de presupuesto**, pero recomienda priorizar medidas de seguridad críticas.

📌 **NIST SP 800-53** NIST National Institute of Standards and Technology U.S. Department of Commerce

- Debe garantizar que **los controles de seguridad estén debidamente financiados**.

📌 CMMI Capability Maturity Model Integration **CMMI**

- Requiere inversión en **tecnología y capacitación** para mejorar la madurez de la seguridad.

📌 **ENS** ens Esquema Nacional de Seguridad **(España)**

- La dirección debe garantizar **recursos adecuados** para cumplir con los controles exigidos por ENS.

📌 **ISO/IEC** ISO 27701 **27701**

- Se debe invertir en **protección de datos personales y auditorías de privacidad**.

---

### 4.5. Seguimiento y Evaluación del SGSI

📌 **ISO 27000** ISO 27001 **(SGSI)**

- Exige auditorías internas y revisiones periódicas para garantizar la mejora continua.

📌 **Controles Críticos** CIS Center for Internet Security **CIS**

- Recomienda evaluaciones periódicas de la efectividad de los controles, sin requerir auditorías formales.

📌 **NIST SP 800-53** NIST National Institute of Standards and Technology U.S. Department of Commerce

- Exige un **monitoreo continuo** y revisiones de seguridad periódicas.

📌 CMMI Capability Maturity Model Integration **CMMI**

- Incluye evaluaciones de madurez para medir la efectividad de los procesos de seguridad.

📌 **ENS** ens Esquema Nacional de Seguridad **(España)**

- Requiere auditorías periódicas y la presentación de informes de seguridad.

📌 **ISO/IEC** ISO ISO 27701 **27701**

- Exige auditorías internas y externas para garantizar el cumplimiento de privacidad.

---

A continuación presentamos un cuadro comparativo de estos puntos.

| Criterio | ISO 27000 (SGSI) | Controles Críticos CIS | NIST SP 800-53 | CMMI | ENS (España) | ISO/IEC 27701 |
|---|---|---|---|---|---|---|
| **Compromiso de la Alta Dirección** | Requiere que la dirección demuestre liderazgo y compromiso con la seguridad de la información. | No establece requisitos explícitos para la dirección, pero sugiere el compromiso de la gerencia. | Requiere que la dirección apruebe políticas y procedimientos de seguridad. | Requiere liderazgo activo en la mejora de procesos y calidad en seguridad de la información. | Exige que la alta dirección lidere la implantación del ENS en organismos públicos. | Requiere que la dirección demuestre compromiso con la privacidad de la información. |
| **Definición de Roles y Responsabilidades** | Debe asignar responsables claros para la seguridad de la información y delegar autoridad. | Asigna responsabilidades en los primeros controles, como gestión de activos y accesos. | Define roles específicos como el Oficial de Seguridad de la Información (ISO). | Asigna roles y responsabilidades dentro de los niveles de madurez del modelo. | Define la figura del Responsable de Seguridad y el Responsable del Sistema. | Debe asignar un Responsable de Privacidad y establecer procesos claros. |
| **Supervisión y Toma de Decisiones** | Debe aprobar la política de seguridad, tomar decisiones sobre riesgos y liderar revisiones periódicas. | Propone la supervisión de implementación de controles, pero sin una estructura formal. | Supervisa la evaluación de riesgos, la implementación de controles y la respuesta a incidentes. | Propone que la dirección esté involucrada en la supervisión de la mejora de procesos. | La dirección debe aprobar el informe de estado de la seguridad y las políticas de seguridad. | Debe supervisar la implementación de controles de privacidad y la gestión de riesgos. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Gestión de Recursos y Presupuesto** | Debe garantizar que existan recursos adecuados (humanos, tecnológicos y financieros) para el SGSI. | No menciona explícitamente la gestión de presupuesto, pero recomien-da priorizar medidas críticas. | Debe asignar los recursos adecuados para implementar controles de seguridad. | Debe garantizar inversiones en tecnología y capacitación para la madurez de seguridad. | Requiere garantizar recursos adecuados para cumplir con las medidas de seguridad exigidas. | Debe asignar recursos suficientes para garantizar la protección de datos personales. |
| **Seguimiento y Evaluación del SGSI** | Debe supervisar auditorías internas y revisiones del SGSI para su mejora continua. | Sugiere evaluaciones periódicas de efectividad de controles, sin requerir auditorías formales. | Exige monitoreo continuo y revisiones de seguridad periódicas. | Incluye evaluaciones de madurez para medir la efectividad de los procesos de seguridad. | Requiere auditorías periódicas de cumplimiento y mejora continua. | Requiere auditorías internas y externas para garantizar el cumplimiento de privacidad. |

---

## Conclusiones

- **ISO 27000, NIST SP 800-53, ENS e ISO 27701** son los marcos más detallados en la definición de responsabilidades de la dirección.
- **CMMI** se enfoca en la madurez de los procesos de seguridad.
- **Los Controles Críticos CIS** son más flexibles y dependen del compromiso interno.

---

Como **ejercicio**, te proponemos que le des una mirada a los capítulos:

6. Análisis de Riesgo de Resiliencia
7. Análisis de Resiliencia en Redes y Sistemas
8. Matriz de Resiliencia
9. Estrategias Resilientes en Redes y Sistemas


Del libro: "**Manual de la Resiliencia** (Una guía práctica de Ciberresiliencia en Redes y Sistemas de TI)" que podéis descargar gratuitamente de: www.darFe.es.

La idea es que analices en la página 124 el "**Compromiso de la dirección**" cuando se decide y al adopta un curso de acción, sobre las diferentes opciones que se le presentan como "**Plan Director de Seguridad**".

Estos capítulos son importantes, pues te servirán para profundizar más en los pasos a seguir en un "**Análisis de Riesgo**" y en la implementación práctica de la metodología MAGERIT, ambos temas que acabamos de ver en el capítulo anterior.

# Charla 5 – Organización del SGSI


## 5.1. Organización del SGSI según las Normas y Referencias

Cada marco normativo aporta una estructura para la gestión de la seguridad de la información. Aunque ISO 27001 es la norma específica para un SGSI, otras referencias complementan su aplicación.

### 5.1.1. ISO 27001: Organización del SGSI

ISO 27001 define un **Sistema de Gestión de Seguridad de la Información (SGSI)** como un conjunto de **políticas, procedimientos, procesos y recursos** para gestionar los riesgos de seguridad de la información.

**Principales aspectos organizativos del SGSI en ISO 27001:**

- Definir el **Alcance del SGSI**.
- Asignar **responsabilidades** y un **líder de seguridad (CISO o equivalente)**.
- Establecer un **Comité de Seguridad de la Información**.
- Desarrollar un **Enfoque basado en Riesgos**.
- Definir un **Ciclo de Mejora Continua (PDCA - Plan, Do, Check, Act)**.

**Estructura documental en ISO 27001:**

- **Política de seguridad** (obligatoria).
- **Evaluación de riesgos** y **tratamiento de riesgos** (obligatorios).
- **Declaración de Aplicabilidad (SoA, Statement of Applicability)**.
- **Procedimientos de control de acceso, continuidad, gestión de incidentes, etc.**
- **Registros de auditorías y revisiones por la dirección**.

**ISO 27001 establece jerarquía documental:**

1. **Política de Seguridad de la Información** (documento principal).
2. **Procedimientos y normas** (respaldan la política).
3. **Registros y evidencias** (demuestran conformidad con los controles).

---

### 5.1.2. NIST SP 800-53: Enfoque organizativo del SGSI

El **NIST SP 800-53** define un marco para implementar controles de seguridad en organizaciones gubernamentales y privadas. No define explícitamente un SGSI como ISO 27001, pero sus controles organizacionales ayudan a estructurar la seguridad.

**Principales aspectos organizativos:**

- Definir un **programa de seguridad de la información**.
- Establecer **roles y responsabilidades** dentro de la organización.
- Implementar **controles de gestión, operacionales y técnicos**.
- Integrar la seguridad con la gestión de riesgos empresariales.

🔷 **Documentos clave según NIST SP 800-53:**

- **Política de seguridad y normas**.
- **Plan de seguridad del sistema (SSP, System Security Plan)**.
- **Evaluaciones de impacto de riesgos y privacidad**.
- **Plan de respuesta a incidentes**.
- **Auditorías y registros de cumplimiento**.

📌 **Jerarquía documental en NIST SP 800-53:**

1. **Plan de Seguridad del Sistema (SSP)**.
2. **Procedimientos operacionales de seguridad**.
3. **Registros de evaluación y auditorías**.

---

### 5.1.3. CIS Controls: Organización práctica de la seguridad

Los **Controles Críticos CIS** ofrecen una estructura operativa basada en buenas prácticas. No definen un SGSI completo, pero sí recomiendan roles y procesos clave.

🔷 **Aspectos organizativos en CIS Controls:**

- **Asignación de roles de seguridad** (CISO, administradores, auditores).
- **Priorización de controles en tres niveles:**
  - Controles básicos (esenciales).
  - Controles fundamentales (seguridad avanzada).
  - Controles organizacionales (estrategia de seguridad).

🔷 **Documentación recomendada:**

- Inventario de activos y software.
- Procedimientos de control de acceso.
- Políticas de respuesta a incidentes.

📌 **No establece una jerarquía documental estricta, pero se enfoca en documentos operativos esenciales.**

---

### 5.1.4. CMMI: Organización basada en madurez

El modelo **CMMI (Capability Maturity Model Integration)** mide la madurez de los procesos de seguridad en una empresa. No prescribe controles específicos, pero sí una estructura organizativa basada en niveles de madurez.

🔷 **Estructura organizativa en CMMI:**

- **Definir roles y responsabilidades** según niveles de madurez.
- **Medición de desempeño y mejora continua**.
- **Estandarización de procesos de seguridad**.

📌 **No impone documentos obligatorios, pero recomienda evidencia documental del nivel de madurez alcanzado.**

---

### 5.1.5. ENS (Esquema Nacional de Seguridad – España)

El **ENS** define una estructura de seguridad para organismos públicos en España. Su enfoque es jerárquico y basado en tres niveles de seguridad.

🔷 **Aspectos organizativos en el ENS:**

- **Responsable de Seguridad**: Coordina la implementación.
- **Responsable del SGSI**: Mantiene el sistema de gestión.
- **Responsable del Sistema**: Supervisa la infraestructura.

🔷 **Documentos mandatorios en el ENS:**

- **Política de seguridad**.
- **Análisis y gestión de riesgos**.
- **Plan de continuidad y recuperación**.
- **Declaración de conformidad**.

📌 **ENS establece una jerarquía documental alineada con ISO 27001.**

---

### 5.1.6. ISO/IEC 27701: Organización para la privacidad

Esta norma extiende **ISO 27001** para gestionar privacidad y datos personales.

🔷 **Organización del sistema de privacidad:**

- **Definir un Responsable de Privacidad**.
- **Gestionar tratamiento de datos personales**.
- **Alinear seguridad con regulaciones como GDPR.**

🔷 **Documentación obligatoria en ISO 27701:**

- **Política de privacidad**.
- **Registro de actividades de tratamiento**.
- **Evaluaciones de impacto en privacidad**.

📌 **Estructura jerárquica similar a ISO 27001, con foco en privacidad.**

### 5.2. Comparativa de Documentación Obligatoria

| Norma | Documentos Obligatorios | Jerarquía Documental |
|---|---|---|
| **ISO 27001** | Política de Seguridad, Evaluación de Riesgos, SoA, Procedimientos | Sí, basada en niveles de documentación |
| **NIST SP 800-53** | Plan de Seguridad del Sistema (SSP), Evaluación de Riesgos, Plan de Respuesta a Incidentes | Sí, pero flexible |
| **CIS Controls** | Inventario de activos, Políticas de acceso y respuesta a incidentes | No formalmente definida |
| **CMMI** | Evidencia documental de madurez | No establece documentos obligatorios |
| **ENS (España)** | Política de seguridad, Declaración de conformidad, Plan de continuidad | Sí, basada en ISO 27001 |
| **ISO/IEC 27701** | Política de Privacidad, Evaluación de Impacto en Privacidad | Sí, similar a ISO 27001 |

**Conclusiones**

- ✓ ISO 27001 y ENS tienen la organización más formal para un SGSI.
- ✓ NIST SP 800-53 enfatiza la documentación técnica y la gestión de riesgos.
- ✓ CIS Controls prioriza controles prácticos sin una jerarquía estricta.
- ✓ CMMI mide la madurez de la seguridad sin exigir documentación específica.
- ✓ ISO 27701 amplía ISO 27001 para la gestión de privacidad.

# Charla 6 – Los Controles


**Objetivo:** Desarrollar con todo detalle el concepto y misión de los controles y compararlos entre todas las referencias de este artículo.

**Análisis detallado de los controles de cada norma:**

6.1. ISO 27001 (Anexo A de ISO 27002).

6.2. Controles Críticos CIS (CIS Controls v8).

6.3. NIST SP 800-53 (familias de controles).

6.4. CMMI (procesos y niveles de madurez en seguridad).

6.5. ENS (Categorías y principios de seguridad en España).

6.6. ISO/IEC 27701 (Extensión de privacidad para ISO 27001).

Se desea incidir especialmente sobre el "DESCONCEPTO" de **Control**, pues al escuchar la palabra "Control", automáticamente viene a la mente la idea de alarma, hito, evento, medición, monitorización, etc…., se piensa en algo muy técnico o acción. En el caso de estos estándares, el concepto de "Control", es mucho (pero mucho) más que eso, pues abarca todo el conjunto de acciones, documentos, medidas a adoptar, procedimientos, medidas técnicas, etc.

---

## 6.1. Controles de ISO 27001 (ISO 27002)

Antes de entrar en el tema, es importante conocer la lógica que aplica la norma **ISO 27001** es presentar el SGSI en dos partes importantes. La primera de ella es lo que se conoce como "**Cuerpo de la orden**". En el caso de su versión 2022, está compuesto por los siguientes puntos:

4 Contexto de la organización

5 Liderazgo

6 Planificación

7 Apoyo

8 Operación

9 Evaluación del funcionamiento

10 Mejora

En este cuerpo de la orden, como se puede apreciar en sus puntos, es donde se desarrolla todo el contenido organizativo, responsabilidades y obligaciones de la dirección, planeamiento, operación y gestión del SGSI para definir el ciclo de mejora continua.

La segunda parte de ISO 27001 es el "Anexo A", y es aquí donde se definen los controles. En 27001 solo se definen con una breva explicación, y luego en **ISO 27002:2022** es donde se ofrece todo el detalle de cada uno de los mismos.

Para entrar de lleno en los controles, vamos a hacer un poco de historia, volviendo a la primera publicación de este estándar en el año 2005, que nos presentaba los siguientes:

A.5 Política de seguridad

A.6 Organización de la información de seguridad

A.7 Administración de recursos

A.8 Seguridad de los recursos humanos

A.9 Seguridad física y del entorno

A.10 Administración de las comunicaciones y operaciones

A.11 Control de accesos

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.13 Administración de los incidentes de seguridad

A.14 Administración de la continuidad de negocio

A.15 Cumplimiento (legales, de estándares, técnicas y auditorías)

Es decir **11** grupos de controles que en total sumaban **133** controles en su versión del año 2005.

Lo presentamos así porque si tienes que trabajar con ellos, probablemente puedas encontrar en la red mucho más detalle, e inclusive, hasta el mismo estándar dando vueltas por allí (pues recordemos que son de pago).

A su vez, también puedes profundizar en dos de nuestros artículos que hemos puesto de manifiesto al principio:

- **ISO 27001 - Los controles (Parte 1):**

  iso-27001_los-controles_parteii.pdf

- **ISO 27001 - Los controles (Parte 2):**

  iso-27001_los-controles.pdf

Que recuerda, los puedes descargar en nuestra Web: www.darFe.es

en el menú "**DESCARGAS**" → "**Normas y estándares**"

A lo largo de los años, las diferentes versiones de esta norma se fueron ajustando a los cambios de ciberseguridad, llegando ahora a la nueva versión de **ISO 27001:2022** (y su detalle en **ISO 27002:2022**) que define un total de **93 controles** de seguridad, organizados en **4 dominios**. Que son los siguientes:

Punto 5. Controles organizacionales (5.1 - 5.37 = 37)

Punto 6. Controles de personas (6.1 - 6.8 = 8)

Punto 7 .Controles físicos (7.1 - 7.14 = 14)

Punto 8. Controles Tecnológicos (8.1 - 8.34 = 34)

**TOTAL = 93 controles**

◈ **Ejemplo práctico:** Implementar una política de control de acceso basada en roles (RBAC) y validar su efectividad mediante auditorías.

## 6.2. Controles Críticos CIS (CIS Controls v8)

Los **Controles CIS** están organizados en **tres categorías** según su prioridad:

1. **Controles básicos (Fundamentales, Prioridad 1 - P1):**
   - Inventario de activos y software.
   - Protección de datos y configuración segura.
   - Gestión de accesos y autenticación.
2. **Controles avanzados (Defensivos, Prioridad 2 - P2):**
   - Seguridad en redes y monitoreo de actividad.
   - Configuración segura de hardware y software.
   - Evaluación continua de vulnerabilidades.
3. **Controles organizacionales (Estrategia, Prioridad 3 - P3):**
   - Respuesta a incidentes y continuidad del negocio.
   - Protección contra amenazas internas.
   - Seguridad en la gestión de proveedores.

◈ **Ejemplo práctico:** Implementar un control de acceso mediante MFA (Multi-Factor Authentication) y medir su efectividad reduciendo accesos no autorizados.

### 6.3. Controles de NIST SP 800-53

El NIST define más de **1,000 controles**, organizados en **20 familias**:

1. Control de acceso (AC).
2. Conciencia y capacitación en seguridad (AT).
3. Auditoría y rendición de cuentas (AU).
4. Gestión de configuración (CM).
5. Continuidad del negocio (CP).
6. Seguridad de los datos (SC).
7. Gestión de riesgos (RA).
8. Seguridad en sistemas y comunicaciones (SC).

◈ **Ejemplo práctico:** Aplicar controles de auditoría y monitoreo en un sistema de gestión de identidad.

### 6.4. Controles de CMMI (Madurez en Seguridad de la Información)

CMMI no tiene **controles específicos**, pero clasifica la seguridad en **cinco niveles de madurez:**

1. **Inicial:** Procesos caóticos y sin gestión formal de seguridad.
2. **Gestionado:** Se establecen políticas de seguridad básicas.
3. **Definido:** Seguridad integrada en los procesos.
4. **Cuantitativamente Gestionado:** Uso de métricas para evaluar la seguridad.
5. **Optimizado:** Mejora continua con aprendizaje organizacional.

🔷 **Ejemplo práctico:** Evaluar el nivel de madurez de seguridad en una organización mediante encuestas y auditorías internas.

### 6.5. Controles del ENS (Esquema Nacional de Seguridad – España)

El ENS clasifica los controles en **tres niveles:**

1. **Básico:** Seguridad mínima exigida para cualquier entidad.
2. **Medio:** Controles adicionales para organizaciones críticas.
3. **Alto:** Seguridad reforzada en sistemas esenciales.

🔷 **Ejemplo práctico:** Clasificar un sistema gubernamental y definir qué nivel ENS aplica.

### 6.6. Controles de ISO/IEC 27701 (Privacidad y Protección de Datos)

Esta norma extiende ISO 27001 para incluir protección de privacidad:

- Gestión de datos personales.
- Consentimiento y derechos de los usuarios.
- Transferencia segura de datos.

🔷 **Ejemplo práctico:** Implementar una política de retención de datos basada en ISO 27701.

Cuadro resumen de controles en cada norma

| Norma/Referencia | Categorías de Controles | Ejemplo de Control Clave | Aplicación Práctica |
|---|---|---|---|
| **ISO 27001** | 4 dominios de seguridad y 93 controles | Gestión de accesos y autenticación | Implementar MFA y revisar logs. de acceso |
| **CIS Controls v8** | 3 categorías: Básico, Defensivo, Organizacional | Inventario de activos y software | Monitorear software autorizado y no autorizado |
| **NIST SP 800-53** | 20 familias de controles | Gestión de configuración (CM-2) | Configurar seguridad en cambios de infraestructura |
| **CMMI** | 5 niveles de madurez | Evaluación de ma-durez en procesos de seguridad | Evaluar la madurez en un SGSI |
| **ENS (España)** | 3 niveles: Básico, Medio, Alto | Control de acceso y autenticación | Definir clasificación ENS en una entidad pública |

| | | | |
|---|---|---|---|
| **ISO/IEC 27701** | Extensión de ISO 27001 para privacidad | Gestión del consentimiento del usuario | Gestionar transferencias seguras de datos personales |

# Charla 7 – Métricas e indicadores

**Objetivo:** Desarrollar una metodología para la monitorización y supervisión del SGSI que permita obtener valores concretos de medición por medio de métricas e indicadores.


**Métricas e Indicadores de un SGSI**

Las **métricas e indicadores** en un Sistema de Gestión de Seguridad de la Información **(SGSI)**, permiten medir la eficacia de los controles de seguridad, evaluar el cumplimiento normativo y mejorar continuamente la protección de la información.

---

### 7.1. Definiciones clave

- **Métrica**: Valor cuantificable que mide el desempeño de un control o proceso de seguridad.
- **Indicador (KPI - Key Performance Indicator)**: Métrica que permite evaluar el éxito de una acción en seguridad.
- **Indicador Clave de Riesgo (KRI - Key Risk Indicator)**: Mide la probabilidad de que ocurra un riesgo de seguridad.

---

### 7.2. ISO 27004

Dentro de la familia ISO 27000, la norma que trata este tema es **ISO/IEC-27004**: "*Mediciones para la Gestión de la Seguridad de la Información*". A continuación haremos una breve presentación de la misma.

Esta norma comienza con una Introducción, de la que se debe destacar:

> "*El empleo de este estándar permitirá a las organizaciones dar respuesta a los interrogantes de cuán efectivo y eficiente es el SGSI y qué niveles de implementación y madurez han sido alcanzados. Estas mediciones permitirán comparar los logros obtenidos en seguridad de la información sobre períodos de tiempo en áreas de negocio similares de la organización y como parte de continuas mejoras*".

El segundo apartado define el ámbito, como una guía sobre la especificación y uso de técnicas de medición, para proveer precisión en la observación del SGSI en cualquier tipo de organizaciones y con el propósito de crear una base para recolectar, analizar y comunicar datos relacionados a este SGSI, los cuales serán empleados para tomar decisiones que permitan mejorar el mismo.

Hace referencia a que es indispensable para la aplicación de este documento, el conocimiento del estándar ISO 27001.

Una organización debe describir como se interrelacionan e interactúan el SGSI y las mediciones, desarrollando guías que aseguren, aclaren y documenten esta relación, con todo el detalle posible.

Los objetivos de estos procesos de mediciones son:

- Evaluar la efectividad de la implementación de los controles de seguridad.
- Evaluar la eficiencia del SGSI, incluyendo continuas mejoras.
- Proveer estados de seguridad que guíen las revisiones del SGSI, facilitando mejoras a la seguridad y nuevas entradas para auditar.
- Comunicar valores de seguridad a la organización.
- Servir como entradas al plan de análisis y tratamiento de riesgos.

El **método** define cómo los atributos deben ser medidos.

Existen dos tipos de métodos para cuantificar los atributos:

- **Subjetivos**: Implica el criterio humano.
- **Objetivos**: Se basan en una regla numérica, que puede ser aplicada por personas o recursos automatizados.

Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicar a múltiples atributos. Algunos ejemplos de métodos son:

- Encuestas/indagaciones.
- Observación.
- Cuestionarios.
- Valoración de conocimientos.
- Inspecciones.
- Re-ejecuciones.
- Consulta a sistemas.
- Monitorización (“Testing”)
- Muestreo.

Un tema a considerar es la asociación de mediciones con determinadas escalas, de las cuales se proponen los siguiente tipos:

- Nominal: Los valores son categóricos.
- Ordinal: Los valores son ordenados.
- Intervalos: Se poseen máximos y mínimos con distancias entre ellos.
- Ratio: Tienen escalas de distancias, relacionadas a mediciones.

Para avanzar con máximo detalle sobre este tema, os recomendamos que recurráis a nuestro artículo:

- **ISO 27001 e ISO 27004**:

  iso-27001_e_iso-27004.pdf

Que recuerda, los puedes descargar en nuestra Web: www.darFe.es

en el menú “**DESCARGAS**” → “**Normas y estándares**”

De este artículo, dedícale buen tiempo al **ANEXO A**: “Formato de las métricas de seguridad de la información”, cuando necesites definir tus propias métricas del SGSI.

### 7.3. Tipos de Métricas en un SGSI

| Tipo de Métrica | Descripción | Ejemplo |
|---|---|---|
| **Eficacia de Controles** | Mide si los controles de seguridad cumplen su propósito. | % de ataques bloqueados por el firewall. |
| **Cumplimiento Normativo** | Evalúa el nivel de alineación con normas de seguridad. | Nivel de cumplimiento ISO 27001 (%) |
| **Gestión de Incidentes** | Mide la respuesta y resolución de incidentes. | Tiempo medio de detección de incidentes (MTTD). |
| **Madurez del SGSI** | Evalúa la evolución del sistema de gestión. | Nivel CMMI alcanzado. |
| **Sensibilización y Formación** | Mide el impacto de la capacitación en seguridad. | % de empleados que superan simulacros de phishing. |
| **Disponibilidad y Continuidad** | Evalúa la resiliencia del sistema ante fallos. | Tiempo medio de recuperación (MTTR). |

### 7.4 Comparativa de Métricas según Normas y Referencias

| Norma/ Referencia | Enfoque en Métricas | Ejemplos de Métricas Utilizadas | Ventajas | Desventajas |
|---|---|---|---|---|
| **ISO 27001** | Basado en cumplimiento normativo y gestión de riesgos. | % de controles aplicados, tiempo de resolución de incidentes. | Orientado a la gestión de riesgos y mejora continua. | No define métricas específicas, depende de la empresa. |
| **NIST SP 800-53** | Medición detallada de controles técnicos. | Tasa de fallos de autenticación, % de sistemas parcheados. | Muy técnico y adaptable a entornos de TI. | Puede ser complejo y requiere herramientas avanzadas. |
| **CIS Controls** | Métricas de seguridad operativa. | Número de vulnerabilidades corregidas, % de dispositivos protegidos. | Práctico y fácil de implementar. | Enfoque técnico, menos alineado con gobernanza. |
| **CMMI** | Medición de madurez y procesos. | Nivel de madurez alcanzado, % de procesos documentados. | Permite evaluar la evolución de la seguridad. | No define métricas técnicas específicas. |
| **ENS (España)** | Medición de cumplimiento regulatorio y controles. | % de cumplimiento por categoría de ENS. | Alineado con regulaciones y obligatorio en España. | Requiere auditorías constantes. |
| **ISO/IEC 27701** | Enfoque en privacidad y protección de datos. | % de cumplimiento GDPR, número de quejas de privacidad. | Protege datos personales y fortalece SGSI. | Limitado a privacidad, no cubre seguridad general. |

# Charla 8 – El ciclo de vida de la Seguridad

**Objetivo:** Concienciar acerca de la importancia de mantener un ciclo de vida continuo en Ciberseguridad.


El **Ciclo de Vida de la Seguridad** en un **Sistema de Gestión de Seguridad de la Información (SGSI)** es un proceso continuo para **planificar, implementar, monitorear, mejorar y auditar** las medidas de seguridad en una organización. Su objetivo es **garantizar la protección de la información** frente a amenazas y riesgos cambiantes.

**Cómo Implementar el Ciclo de Vida de la Seguridad en una Organización**

Para llevar a la práctica el **ciclo de vida de la seguridad en una organización**, es necesario aplicar metodologías estructuradas, herramientas de monitorización y planes de acción bien definidos.

A continuación, veremos **cómo ejecutar cada fase en la vida real** con ejemplos detallados, herramientas recomendadas y casos prácticos.

---

## 8.1. Fases del Ciclo de Vida de la Seguridad

El ciclo de vida sigue la metodología **PDCA (Plan-Do-Check-Act)** o **ciclo de mejora continua**, utilizada en marcos como **ISO 27001, NIST, CIS Controls, ENS y CMMI**.

### 8.1.1. Fase 1: Planificación (Plan)

**Objetivo:** Definir la estrategia de seguridad alineada con los riesgos del negocio.

En esta fase se **establecen objetivos de seguridad, se identifican activos y riesgos, y se definen controles** para mitigar amenazas.

**Pasos clave:**

1) **Definir la política de seguridad:**

   Redactar un documento con principios de seguridad alineados con ISO 27001 y ENS.

2) **Identificar activos críticos:**

   Crear un inventario con servidores, bases de datos, aplicaciones y redes.
   **Herramientas recomendadas:** CMDB, nmap, Open-Audit.

3) **Realizar análisis de riesgos:**

   Aplicar metodologías como **MAGERIT, OCTAVE o NIST RMF**.

   **Ejemplo práctico:**

   - Identificar amenazas (ransomware, phishing, ataques DDoS).
   - Evaluar impacto y probabilidad.
   - Asignar niveles de riesgo (Alto, Medio, Bajo).

4) **Definir controles de seguridad:**

   Seleccionar controles de ISO 27001, NIST SP 800-53 o CIS Controls.

**Ejemplo práctico:**

- Si el riesgo es "Fuga de datos en correos electrónicos", implementar **DLP (Data Loss Prevention)**.
- Si el riesgo es "Ataques a servidores web", implementar **WAF** (Web Application Firewall)**.**

5) **Establecer indicadores y métricas:**

📌 Medir el porcentaje de incidentes detectados, tiempo de resolución, cumplimiento de auditorías.

📌 **Ejemplo práctico:**

Una empresa de comercio electrónico identifica que sus bases de datos con datos de clientes son activos críticos. Evalúa el riesgo de ataques SQL Injection y decide implementar controles de seguridad en su firewall y base de datos.

---

### 8.1.2. Fase 2: Implementación (Do)

**Objetivo:** Ejecutar las medidas de seguridad planificadas.

En esta fase se **ejecutan los controles y medidas de seguridad** definidas en la planificación.

🔷 **Acciones clave:**

1) **Configurar herramientas de seguridad:**

📌 Implementar firewalls, IDS/IPS, SIEM, antivirus, segmentación de red.
**Ejemplo práctico:**

- Configurar un **SIEM** como **Splunk o AlienVault** para monitorear eventos en tiempo real.
- Aplicar reglas en **nftables o iptables** para restringir tráfico no autorizado.

2) **Implementar políticas de acceso y autenticación:**

📌 Aplicar **MFA** (Multi-Factor Authentication) en sistemas críticos.
**Ejemplo práctico:**

- Configurar MFA en Microsoft 365, VPN y servidores internos.

3) **Capacitar a empleados en ciberseguridad:**

📌 Realizar simulaciones de ataques de phishing y concienciación.

**Ejemplo práctico:**

- Usar herramientas como **KnowBe4 o PhishMe** para entrenar a empleados en detección de phishing.

4) **Probar la efectividad de los controles:**

📌 Realizar **pruebas de penetración y escaneos de vulnerabilidades**.

**Ejemplo práctico:**

- Usar **Nessus o OpenVAS** para detectar fallos en la infraestructura.

- Realizar tareas de **Red Team** para evaluar la resistencia ante ataques.

📌 **Ejemplo práctico:**

Un banco implementa autenticación multifactor para los accesos de sus empleados y monitorización continua con un SIEM para detectar actividades sospechosas.

---

**8.1.3. Fase 3: Seguimiento y Medición (Check).** Evaluar efectividad de controles

**Objetivo:** Monitorizar continuamente la seguridad y evaluar la eficacia de los controles implementados.

En esta fase se **evalúa la efectividad de los controles implementados** mediante métricas e indicadores.

🔷 **Acciones clave:**

1) **Monitorizar eventos de seguridad:**

📌 Revisar los logs de sistemas, firewalls, SIEM, endpoints.
**Herramientas recomendadas:**

- **SIEM:** Splunk, Graylog, Wazuh.
- **EDR:** CrowdStrike, SentinelOne.

2) **Evaluar métricas e indicadores de seguridad:**

📌 Medir el número de incidentes detectados, tiempo de resolución, cumplimiento de políticas.

**Ejemplo práctico:**

- Si el tiempo de respuesta ante incidentes es **superior a 8 horas**, se necesita mejorar la detección.

3) **Realizar auditorías internas:**

📌 Revisar cumplimiento de políticas, accesos y registros.

**Ejemplo práctico:**

- Auditoría de accesos a bases de datos para detectar accesos indebidos.

4) **Simular ataques y pruebas de seguridad:**

📌 Ejecutar trabajos de **Red Team / Blue Team** y simulaciones de ataques APT.

**Ejemplo práctico:**

- Simular un ataque de ransomware en un entorno controlado para probar la respuesta del equipo de seguridad.

📌 **Ejemplo práctico:**

Una empresa realiza auditorías internas cada 6 meses para verificar si se han aplicado los controles de ISO 27001 y NIST SP 800-53 correctamente.

---

**8.1.4. Fase 4: Mejora Continua (Act)**. Optimizar la seguridad.

**Objetivo:** Corregir fallos, mejorar controles y fortalecer el SGSI.

Se revisan los resultados de auditorías y métricas para **corregir desviaciones, optimizar controles y fortalecer la seguridad**.

🔷 **Acciones clave:**

1) **Análisis de desviaciones:**

   📌 Identificar fallos en controles detectados en auditorías.

   **Ejemplo práctico:**

   - Si un firewall tiene **puertos abiertos innecesarios**, cerrarlos y reforzar reglas de acceso.

2) **Acciones correctivas y preventivas:**

   📌 Implementar mejoras y evitar futuros problemas.

   **Ejemplo práctico:**

   - Si se detecta phishing recurrente, reforzar la capacitación y configurar **bloqueo de dominios sospechosos en correo electrónico**.

3) **Actualización de normativas y controles:**

   📌 Revisar cambios en marcos como **ISO 27001, NIST, ENS**.

   **Ejemplo práctico:**

   - Si NIST SP 800-53 actualiza un control, implementarlo en la organización.

4) **Revisión periódica del SGSI:**

   📌 Evaluar si el sistema sigue siendo eficaz y cumple con normativas.

   **Ejemplo práctico:**

   - Si una nueva ley de privacidad entra en vigor, revisar si se cumplen los requisitos.

📌 **Ejemplo práctico:**

Una empresa descubre que el 30% de sus empleados cayó en un simulacro de phishing. Refuerza la capacitación en concienciación de seguridad.

---

**8.2. Seguimiento y Mediciones**

El seguimiento del SGSI se realiza mediante:

🔷 **Indicadores clave (KPIs y KRIs)**:

- ✔ % de incidentes detectados y resueltos en tiempo definido.
- ✔ % de cumplimiento con ISO 27001, ENS, NIST.
- ✔ % de usuarios capacitados en ciberseguridad.

🔷 **Herramientas de Monitorización**:

- ✔ SIEM (Security Information and Event Management).
- ✔ IDS/IPS para detección de intrusiones.
- ✔ Auditorías internas y externas.

◈ **Auditorías de Seguridad**:

- ✔ Internas: revisión de políticas y controles.
- ✔ Externas: certificaciones y revisiones de terceros.

---

### 8.3. Comparativa: Cómo lo presentan las diferentes normas y marcos de referencia

| Norma/Referencia | Enfoque en el Ciclo de Vida de la Seguridad | Énfasis en Auditorías y Medición |
|---|---|---|
| **ISO 27001** | Basado en PDCA, identifica y gestiona riesgos, implementa controles. | Auditorías internas y externas obligatorias, métricas de SGSI. |
| **NIST SP 800-53** | Enfoque basado en gestión de riesgos, aplicable principalmente a sistemas gubernamentales. | Evaluaciones de control continuo, monitorización de incidentes. |
| **CIS Controls** | Modelo basado en controles prioritarios de seguridad. | Énfasis en monitorización continua y pruebas de seguridad. |
| **CMMI** | Evalúa la madurez en seguridad, mejora progresiva. | Autoevaluaciones y auditorías de procesos. |
| **ENS (España)** | Aplicación obligatoria en sector público, basado en niveles de seguridad. | Auditorías periódicas exigidas por la ley. |
| **ISO/IEC 27701** | Gestión de privacidad dentro de un SGSI. | Auditorías de privacidad y cumplimiento de GDPR. |

---

**Auditorías Periódicas en un SGSI**

Las auditorías periódicas son una parte fundamental del ciclo de vida de la seguridad. Permiten **evaluar la eficacia de los controles de seguridad, identificar vulnerabilidades y asegurar el cumplimiento con normativas como ISO 27001, NIST SP 800-53, CIS Controls, ENS e ISO 27701**.

---

### 8.4. Tipos de Auditorías en un SGSI

#### 8.4.1. Auditoría Interna

- ☑ Realizada por personal de la organización o consultores externos contratados.
- ☑ Verifica el cumplimiento de políticas y procedimientos de seguridad.
- ☑ Se realiza antes de una auditoría externa para identificar no conformidades.

📌 **Ejemplo práctico:**

- Un equipo de seguridad revisa los accesos a sistemas críticos y detecta que algunos empleados tienen privilegios excesivos.
- Se recomienda reducir permisos según el principio de **mínimos privilegios**.

🔧 **Herramientas útiles:**

- **SIEM** (Splunk, Wazuh, AlienVault) para revisar logs de eventos.

---

### 8.4.2. Auditoría Externa

✅ Realizada por un organismo de certificación o auditores externos.
✅ Es obligatoria para la certificación de ISO 27001, ENS e ISO 27701.
✅ Evalúa si el SGSI cumple con estándares y regulaciones.

📌 **Ejemplo práctico:**

- Una empresa quiere certificarse en ISO 27001, por lo que contrata a una entidad certificadora para auditar su sistema de gestión.
- Durante la auditoría, se detecta que **no hay un procedimiento formal para la gestión de incidentes**.
- Se documenta el proceso y se capacita al equipo de TI en respuesta a incidentes.

---

### 8.4.3. Auditoría de Cumplimiento

✅ Asegura que la organización cumple con regulaciones específicas como GDPR, ENS o HIPAA.

✅ Puede ser realizada por autoridades regulatorias.

✅ Se centra en la protección de datos y privacidad.

📌 **Ejemplo práctico:**

- Una empresa de telecomunicaciones en España debe cumplir con el **ENS**.
- Se revisa que los sistemas tengan **cifrado de datos y registros de accesos** adecuados.
- Se genera un informe con medidas correctivas.

🔧 **Herramientas útiles:**

- **Nessus o Qualys** para detectar vulnerabilidades técnicas.
- **Checklists de ENS o ISO 27001** para evaluar requisitos de cumplimiento.

---

### 8.4.4. Auditoría Técnica de Seguridad

✅ Evalúa la seguridad de infraestructura, aplicaciones y redes.
✅ Puede incluir **pruebas de penetración, análisis de código y revisión de configuraciones**.

📌 **Ejemplo práctico:**

- Un banco contrata un equipo de **Red Team** para evaluar la seguridad de sus sistemas.
- Se realiza una prueba de phishing a empleados y se detecta que el 30% cae en la trampa.
- Se refuerza la capacitación y se implementa **bloqueo automático de enlaces sospechosos** en correos electrónicos.

🔧 **Herramientas útiles:**

- **Burp Suite, Metasploit, Wireshark** para auditorías técnicas.
- **OWASP ZAP** para pruebas de seguridad web.

---

### 8.5. Proceso de Auditoría Paso a Paso

1) **Planificación**

- 📌 Definir los objetivos de la auditoría (cumplimiento, certificación, seguridad técnica).
- 📌 Seleccionar auditores internos o externos.
- 📌 Preparar listas de verificación (ISO 27001, NIST SP 800-53, ENS, CIS).

2) **Ejecución**

- 📌 Revisar documentación (políticas, procedimientos, registros de eventos).
- 📌 Entrevistar a empleados y revisar procesos en la organización.
- 📌 Realizar pruebas técnicas (escaneos de vulnerabilidades, simulaciones de ataques).

3) **Análisis de Resultados**

- 📌 Identificar **no conformidades** y clasificar su impacto (bajo, medio, alto).
- 📌 Comparar resultados con auditorías anteriores para medir mejoras.
- 📌 Redactar un informe con hallazgos y recomendaciones.

4) **Acciones Correctivas y Preventivas**

- 📌 Implementar cambios en configuraciones, procesos o formación del personal.
- 📌 Realizar una auditoría de seguimiento para verificar mejoras.

---

### 8.6. Comparativa: Cómo presentan las Auditorías las Normas de Referencia

| Norma/ Referencia | Requiere Audito-rías Internas | Requiere Audito-rías Externas | Evalúa Seguridad Técnica | Frecuencia Recomendada |
|---|---|---|---|---|
| **ISO 27001** | Sí (Obligatoria) | Sí (Para certificación) | No directamente, pero se recomienda | Anual |
| **NIST SP 800-53** | Sí (Parte de monito-reo continuo) | No obligatoria, p/recomendada | Sí (En controles de seguridad técnica) | Periódica según el riesgo |
| **CIS Controls** | Sí (Autoevaluación recomendada) | No obligatoria | Sí (Pruebas de seguridad técnica) | Según necesidades de la empresa |
| **CMMI** | Sí (Para evaluar madurez de procesos) | No obligatoria | No, se centra en procesos | Según nivel de madurez |
| **ENS (España)** | Sí (Para organismos públicos) | Sí (Obligatoria en ciertos casos) | Sí (Incluye controles de seguridad) | Variable, según nivel de seguridad |
| **ISO/IEC 27701** | Sí (Para privacidad y protección de datos) | Sí (Para certificación) | No directamente | Anual |

---

### 8.7. Cómo Implementar Auditorías en una Organización

✅ **Ejemplo de Plan de Auditoría para una Empresa**

📌 **Objetivo:** Evaluar la seguridad de la infraestructura y el cumplimiento de ISO 27001.

📌 **Pasos:**

1) **Revisar documentación** (Política de seguridad, procedimientos de gestión de incidentes).
2) **Entrevistar a empleados clave** (CISO, equipo de TI, responsables de datos).
3) **Revisar logs y eventos de seguridad** (SIEM, firewalls, endpoints).
4) **Realizar pruebas técnicas** (Escaneo de vulnerabilidades, auditoría de accesos).
5) **Redactar informe con hallazgos y recomendaciones**.
6) **Implementar medidas correctivas y volver a auditar**.

📌 **Herramientas:**

- **Para auditorías de cumplimiento:** GRC Tools.
- **Para auditorías técnicas:** Nessus, Wireshark, Splunk, OpenVAS.
- **Para evaluación de madurez:** CMMI Appraisal, ISO 27001 Gap Analysis.

---

**Conclusión y Recomendaciones sobre auditorías**

✔ **Las auditorías son esenciales** para detectar vulnerabilidades y evaluar el cumplimiento normativo.

✔ **Cada estándar tiene un enfoque diferente:**

- ISO 27001 y ENS requieren auditorías formales.
- NIST y CIS recomiendan auditorías técnicas y autoevaluaciones.
- CMMI se enfoca en la mejora de procesos.

✔ **El éxito de una auditoría depende de un buen plan de acción y herramientas adecuadas.**

---

**Conclusiones y Recomendaciones finales**

✅ Un SGSI requiere un **ciclo de vida estructurado** basado en **planificación, implementación, medición y mejora continua**.

✅ Cada norma tiene un enfoque particular en la **gestión de seguridad**, pero todas coinciden en la necesidad de **auditorías, seguimiento de métricas y corrección de desviaciones**.

✅ La **automatización de la monitorización** y el uso de herramientas como **SIEM, IDS y auditorías regulares** son clave para una seguridad efectiva.

# Charla 9 – Debate sobre cada una de estas referencias

**Objetivo:** Cerrar este ciclo, presentando y analizando las ventajas y desventajas de cada referencia.


En este análisis, exploramos **ISO 27000, Controles Críticos CIS, NIST SP 800-53, CMMI, ENS (España) e ISO/IEC 27701**, considerando su evolución histórica, ventajas y desventajas, aplicación por sector, costes y esfuerzo de implementación, entre otros aspectos clave.

### 9.1. Historia y evolución de cada marco de referencia

| Norma/ Referencia | Año de Creación | Historia y Evolución |
|---|---|---|
| **ISO 27000** | 1995 (BS 7799) → 2005 (ISO 27001) | Basada en BS 7799 del Reino Unido. Se convirtió en ISO 27001 en 2005 y ha evolucionado con nuevas revisiones (2013, 2017 y 2022). Es el estándar global para SGSI. |
| **CIS Controls** | 2008 | Desarrollado por el Center for Internet Security, enfocado en controles prioritarios para mejorar la ciberseguridad. Evoluciona con nuevas amenazas. |
| **NIST SP 800-53** | 1990s | Creado por el Instituto Nacional de Estándares y Tecnología de EE.UU. como guía para agencias gubernamentales y empresas críticas. Actualizado constantemente. |
| **CMMI** | 1990s | Desarrollado por SEI (Software Engineering Institute) de Carnegie Mellon. Nació para mejorar la gestión y madurez de procesos en IT, luego expandiéndose a otros sectores. |
| **ENS (España)** | 2010 | Normativa española para el sector público y empresas tecnológicas. Se actualizó en 2022 con requisitos más estrictos de seguridad. |
| **ISO/IEC 27701** | 2019 | Extensión de ISO 27001 para gestionar privacidad de datos personales. Responde a regulaciones como GDPR y otras normativas de protección de datos. |

### 9.2. Análisis comparativo: ventajas y desventajas

| Norma/ Referencia | Ventajas | Desventajas |
|---|---|---|
| **ISO 27000** | Enfoque estructurado para SGSI, reconocido globalmente, facilita certificación. | Costoso y complejo de implementar. No detalla controles técnicos específicos. |
| **CIS Controls** | Controles concretos y priorizados, fácil de aplicar, útil para cualquier empresa. Ofrece también sus guías de bastionado. | No es certificable, menos formal que ISO o NIST. Puede necesitar complementos. |

| | | |
|---|---|---|
| **NIST SP 800-53** | Marco detallado, usado en entornos críticos, buen enfoque de gestión de riesgos. | Extenso y difícil de implementar sin experiencia. Más centrado en EE.UU. |
| **CMMI** | Evalúa madurez de procesos, mejora continua, adaptable a múltiples industrias. | No es un estándar de seguridad, sino de gestión. Difícil integración con SGSI. |
| **ENS (España)** | Aplicación obligatoria en el sector público español, alineado con ISO 27001. | Aplicabilidad limitada a España, burocracia compleja para su implementación. |
| **ISO/IEC 27701** | Gestión específica de privacidad, compatible con GDPR, útil para organizaciones con datos sensibles. | Requiere certificación previa en ISO 27001, lo que incrementa costos. |

### 9.3. Aplicabilidad según tipo de empresa

| Norma/ Referencia | Mejor Aplicación |
|---|---|
| **ISO 27000** | Empresas grandes y medianas que buscan certificación y gestión formal de SGSI. |
| **CIS Controls** | PYMEs, startups y empresas que necesitan controles rápidos y efectivos. |
| **NIST SP 800-53** | Gobierno, infraestructura crítica y grandes corporaciones con requisitos de seguridad avanzada. |
| **CMMI** | Empresas tecnológicas y de software que buscan madurez en sus procesos. |
| **ENS (España)** | Entidades públicas y proveedores tecnológicos en España. |
| **ISO/IEC 27701** | Empresas que manejan datos personales sensibles y deben cumplir con GDPR u otras regulaciones. |

### 9.4. Coste y tiempo de implementación

| Norma/Referencia | Costo Aproximado | Tiempo Estimado | Recursos Necesarios |
|---|---|---|---|
| **ISO 27000** | $$$$ | 6-18 meses | Equipo SGSI, consultoría externa, auditorías. |
| **CIS Controls** | $$ | 2-6 meses | Implementación técnica de controles, formación. |
| **NIST SP 800-53** | $$$ | 6-24 meses | Análisis de riesgos, seguridad avanzada. |
| **CMMI** | $$$$ | 12-24 meses | Consultoría, evaluación de madurez, cambio organizacional. |
| **ENS (España)** | $$$ | 6-12 meses | Auditoría ENS, adaptación a regulaciones españolas. |
| **ISO/IEC 27701** | $$$$ | 6-12 meses | Extensión de ISO 27001, gestión de privacidad. |

**Nota:** El tiempo de implementación depende del tamaño de la organización y su madurez en seguridad.

### 9.5. Comparación de esfuerzo requerido

| Norma/Referencia | Esfuerzo de Implementación | Mantenimiento Requerido |
|---|---|---|
| **ISO 27000** | Alto (requiere documentación, auditorías) | Alto (auditorías anuales, mejora continua). |
| **CIS Controls** | Medio (controles técnicos rápidos) | Bajo-Medio (actualización de controles). |
| **NIST SP 800-53** | Alto (modelo complejo, enfoque gubernamental) | Alto (gestión continua de seguridad). |
| **CMMI** | Muy Alto (cambio organizacional) | Medio (evaluaciones periódicas). |
| **ENS (España)** | Medio-Alto (cumplimiento regulatorio) | Medio (auditorías periódicas, mantenimiento de certificación). |
| **ISO/IEC 27701** | Alto (expansión de SGSI existente) | Alto (auditorías y actualizaciones constantes). |

### 9.6. Comentarios finales y preguntas para el debate

1) **¿Es mejor ISO 27001 o NIST SP 800-53 para empresas privadas?**
2) **¿CIS Controls puede reemplazar otros marcos en PYMEs?**
3) **¿El ENS debería expandirse a otros países o solo aplica a España?**
4) **¿ISO/IEC 27701 es realmente útil o solo una extensión costosa de ISO 27001?**
5) **¿CMMI tiene** relevancia en seguridad o es más útil para procesos de negocio?

**Conclusión: ¿Qué marco es mejor?**

Depende de las necesidades de cada empresa.

- **Para certificación internacional:** ISO 27001 o ISO/IEC 27701.
- **Para cumplimiento gubernamental:** NIST SP 800-53 o ENS.
- **Para protección rápida:** CIS Controls.
- **Para mejora de procesos:** CMMI.

## Enlaces de interés:


1) **ISO 27001**

https://www.normaiso27001.es

https://www.iso27000.es

2) **CIS**

https://www.cisecurity.org/controls/cis-controls-navigator

https://learn.cisecurity.org/CIS-Controls-v8-Spanish-PDF

https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

3) **NIST**

familia 800 del NIST: https://csrc.nist.gov/publications/sp800

4) **CMMI**

https://cmmiinstitute.com

https://es.wikipedia.org/wiki/Capability_Maturity_Model_Integration#:~:text=El%20CMMI%20o%20Capability%20Maturity,operación%20de%20sistemas%20de%20software.

5) **ENS**

https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/543-ccn-stic-825-ens-iso27001/file.html

ens_e_iso-27001.pdf: https://misdocumentos.net/wiki/doku.php/a2/plantilla/ens

ens.pdf: Esquema Nacional de Seguridad, se lanzó la "cuenta atrás"

6) **ISO 27701**

https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0067527

https://www.incibe.es/empresas/blog/conoces-nueva-norma-gestion-privacidad