

curso “Experto en Ciberseguridad de Redes y Sistemas”

TEMAS

1. Fingerprinting
2. Footprinting
3. IDSs - Snort
4. Nessus
5. Firewalls
6. **SGSI**
7. Antiphishing
8. MITRE
9. Red Team y Blue Team
10. Principales procesos de Seguridad



SGSI

6.1. SGSI - Presentación del Ciclo

SGSI, primer capítulo. Comenzamos con esta nueva serie temática dedicada de lleno al Sistema de Gestión de Seguridad de la Información (**SGSI**).

El día de hoy, presentamos la metodología, y un cuadro comparativo de los estándares y referencias con las que vamos a trabajar, que son 6 importantes buenas prácticas que no podemos dejar de tener en cuenta: ISO 27001, NIST 800-53, CIS Controls, ENS, CMMI e ISO 27701.

Todo el tema de estos nueve videos se sustenta en un artículo muy novedoso, que ya hemos subido a nuestra Web y lo puedes descargar en: www.darFe.es

→ "menú **DESCARGAS**", → "Artículos": [articulo_SGSI-darFe.pdf](#)



El objetivo de este capítulo, 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**



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 descargarlas 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>

Veamos el tema en detalle desde el video 141 (**Obligatorio**).

 **SGSI: Parte 1 - Presentación del ciclo - (Charla 141)** -
Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/FYCQ0wrbkUI>



6.2. SGSI – Conceptos del SGSI

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 este 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 estos capítulos 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)**



Para completar el tema te recomendamos nuevamente el artículo, que ya hemos subido a nuestra Web y lo puedes descargar en: www.darFe.es

→ "menú **DESCARGAS**", → "Artículos": [articulo_SGSI-darFe.pdf](#)



Veamos el tema en detalle desde el video 142 (**Obligatorio**).

 **SGSI: Parte 2 – Conceptos del SGSI - (Charla 142) - Aprendiendo Ciberseguridad paso a paso**

<https://youtu.be/ihSo5DvUf0U>



6.3. SGSI – El enfoque a Riesgos

NO ARRIESGUES... y atiende a este capítulo!

La gestión de riesgos, es la actividad MÁS IMPORTANTE de un SGSI (sin lugar a dudas). No puedo defenderme, si no sé qué es lo que tengo y cuáles son sus problemas, es saber en detalle "dónde me aprieta el zapato".

En este capítulo, nuevamente analizaremos el tema desde el enfoque de diferentes referencias internacionales, y abordaremos la metodología "MAGERIT" como punto de partida para esta actividad.

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.

Enfoque de Riesgos en ISO 27000 (SGSI)

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.



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.

Controles para la Mitigación de Riesgos en ISO 27001

Basados en el Anexo A de ISO 27001:2022, que tiene 93 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.

Veamos el tema en detalle desde el video 143 (**Obligatorio**).

 **SGSI: Parte 3 – El enfoque a Riesgos - (Charla 143) - Aprendiendo Ciberseguridad paso a paso**

<https://youtu.be/eioCjBChRNQ>



6.4. SGSI – La dirección de la organización

No puedes pensar en implementar un SGSI, si la dirección de tu organización pasa de ello.

El Liderazgo y compromiso de la dirección, es el pilar fundamental de un SGSI.

En este video, desarrollamos, los aspectos clave que debe considerar la dirección de una organización para sustentar y fomentar 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

Compromiso de la Alta Dirección



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.



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.



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 **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.



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**.

Veamos el tema en detalle desde el video 144 (**Obligatorio**).

 **SGSI: Parte 4 – La dirección de la organización - (Charla 144)**
- Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/1F4f6dAsXmk>



6.5. SGSI – Organización del SGSI

En este capítulo, se comparten "chuletas" que valen ORO!!!. Veremos cómo es la estructura documental de un SGSI, qué tipos de documentos son imprescindibles, y a su vez, cómo debemos relacionar cada uno de ellos con los puntos de la norma ISO 27001:2022 en cuanto al cuerpo de la misma.

La relación documental con los controles de la norma es mandatoria, con lo que no puedes dejar huecos o ausencias de desarrollo de cada uno de ellos. El enorme valor agregado de este capítulo, es que verás de forma práctica todos los documentos que hemos ido empleando de forma real y concreta de nuestras implantaciones y certificaciones de este estándar, y a su vez, cómo cada uno de ellos va cubriendo lo que la norma establece en sus "debe".

También como venimos haciendo en todo este ciclo del SGSI, comparamos las seis referencias del artículo que publicamos. En este quinto capítulo del curso sobre ISO 27001, exploramos cómo organizar correctamente un SGSI. Verás cómo estructurar la documentación del sistema, qué roles y responsabilidades deben definirse, y cómo asegurar la trazabilidad y efectividad del sistema.

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.

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).

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.

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.



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.

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.**

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.**

Veamos el tema en detalle desde el video 145 (**Obligatorio**).

🌐 **SGSI: Parte 5 – Organización del SGSI - (Charla 145) -**
Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/Pm5iuHHmXhk>



6.6. SGSI – Los Controles - (Charla 146)

Desarrollamos los controles que debe reunir un SGSI. Nos basamos eminentemente en la norma ISO 27002:2022 que es la que describe con todo detalle los **93 controles** que presenta esta última versión.

Analizaremos primero la comparativa entre nuestras seis normas o buenas prácticas de referencia, y luego pasaremos a ver de forma práctica los grupos y cada uno de sus controles, para que tengas una excelente referencia del camino a seguir al implantar los mismos en tu empresa.

En este sexto capítulo sobre SGSI, exploramos los controles de seguridad esenciales según la norma ISO 27001. Aprenderás a identificar, implementar y gestionar controles efectivos para proteger la información de tu organización.

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.

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 breve explicación, y luego en ISO 27002:2022 es donde se ofrece todo el detalle de cada uno de los mismos.

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**

El resto de las normas, te invitamos a que las veas directamente en el artículo, que ya hemos subido a nuestra Web y lo puedes descargar en: www.darFe.es

→ "menú **DESCARGAS**", → "Artículos": **articulo_SGSI-darFe.pdf**

Veamos el tema en detalle desde el video 146 (**Obligatorio**).

 **SGSI: Parte 6 – Los Controles - (Charla 146) - Aprendiendo Ciberseguridad paso a paso**

<https://youtu.be/bUWnQJ6-Q7Y>



6.7. SGSI– Métricas e indicadores

¿Cuándo conduces tu coche, vas bien y seguro?

Puedes saberlo, porque en el instrumental te indica, la velocidad, el combustible, los intermitentes, los kilómetros recorridos, etc. Todo esto se debe a las "Métricas e Indicadores", a medida que avanzamos cambian, nos dice que excedemos los límites o que debemos parar a repostar combustible. Imaginaros cómo podríamos conducir por una autovía sin esta información.

A su vez, cada año surgen nuevos parámetros (mejoras) que nos detectan distancia de frenado, si dejamos las líneas blancas de la ruta, si soltamos el volante, si llueve, etc. Es decir, es un ciclo de mejora continua.

En un SGSI es similar, las **Métricas e Indicadores** nos van manteniendo informado del estado del mismo y sus desvíos, para que en este "Ciclo de vida" de la Seguridad (ciclo PDCA), podamos ir obrando en consecuencia, y mejorándolos ciclo a ciclo.

En este capítulo, desarrollamos en detalle el estándar **ISO 27004**, que es justamente el mejor referente sobre este tema, y por supuesto, manteniendo la línea de nuestro artículo, comparamos también el resto de las referencias que venimos presentando desde del principio. En esta séptima charla, profundizamos en la importancia de las métricas e indicadores para evaluar la eficacia del SGSI. Descubre cómo establecer **KPIs** relevantes y utilizar datos para la mejora continua.

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.

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.

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.

Veamos el tema en detalle desde el video 147 (**Obligatorio**).

 **SGSI: Parte 7 – Métricas e indicadores - (Charla 147) -**
Aprendiendo Ciberseguridad paso a paso
<https://youtu.be/zuupRxIMV64>



6.8. SGSI – El ciclo de vida de la Seguridad

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.

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**.

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.

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.

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.

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**.

El resto del detalle, te invitamos a que lo veas directamente en el artículo, que ya hemos subido a nuestra Web y lo puedes descargar en: www.darFe.es

→ "menú **DESCARGAS**", → "Artículos": [articulo_SGSI-darFe.pdf](#)

Veamos el tema en detalle desde el video 148 (**Obligatorio**).



 **SGSI: Parte 8 – El ciclo de vida de la Seguridad - (Charla 148) - Aprendiendo Ciberseguridad paso a paso**
<https://youtu.be/1IOYfWIVlWw>



6.9. SGSI – Debate sobre cada una de estas referencias

En este capítulo, 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.

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.

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.

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.

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.

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).

Veamos el tema en detalle desde el video 149.

NOTA: Este video es solo un repaso de lo anterior, por lo que no será obligatorio verlo al completo, solo recomendamos que lo veas para reforzar todo lo anterior.

 **SGSI: Parte 9 – Debate sobre cada una de estas referencias - (Charla 149) - Aprendiendo Ciberseguridad paso a paso**
<https://youtu.be/AFHrpjvRcmI>

