THE BRIDGE

CYBER SECURITY

Esquema Nacional de Seguridad (ENS)

ENS

- El **Esquema Nacional de Seguridad** (**ENS**) es un marco normativo en España que establece principios, requisitos y medidas de seguridad para proteger la información y los servicios electrónicos gestionados por el sector público y sus proveedores
- Su objetivo es asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los datos y servicios
- El ENS se aplica a toda la Administración Electrónica y se actualiza periódicamente para adaptarse a los cambios en el entorno normativo y tecnológico
- . La última actualización importante fue en 2022 con el Real Decreto 311/20222.

Principios Básicos

Los **Principios Básicos** que desarrolla el ENS son los siguientes:

- Seguridad como proceso integral
- Gestión de la seguridad basada en los riesgos
- Prevención, detección, respuesta y conservación
- Existencia de líneas de defensa
- Vigilancia continua
- Reevaluación periódica
- Diferenciación de responsabilidades

El artículo 5 del ENS señala que el objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información.

Gestión de la seguridad basada en Riesgo

La gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad **continua y permanentemente actualizada.**

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada **aplicación de medidas de seguridad, de manera equilibrada** y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que éstos estén expuestos.

Aplicabilidad

Medidas de Seguridad

- Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario."

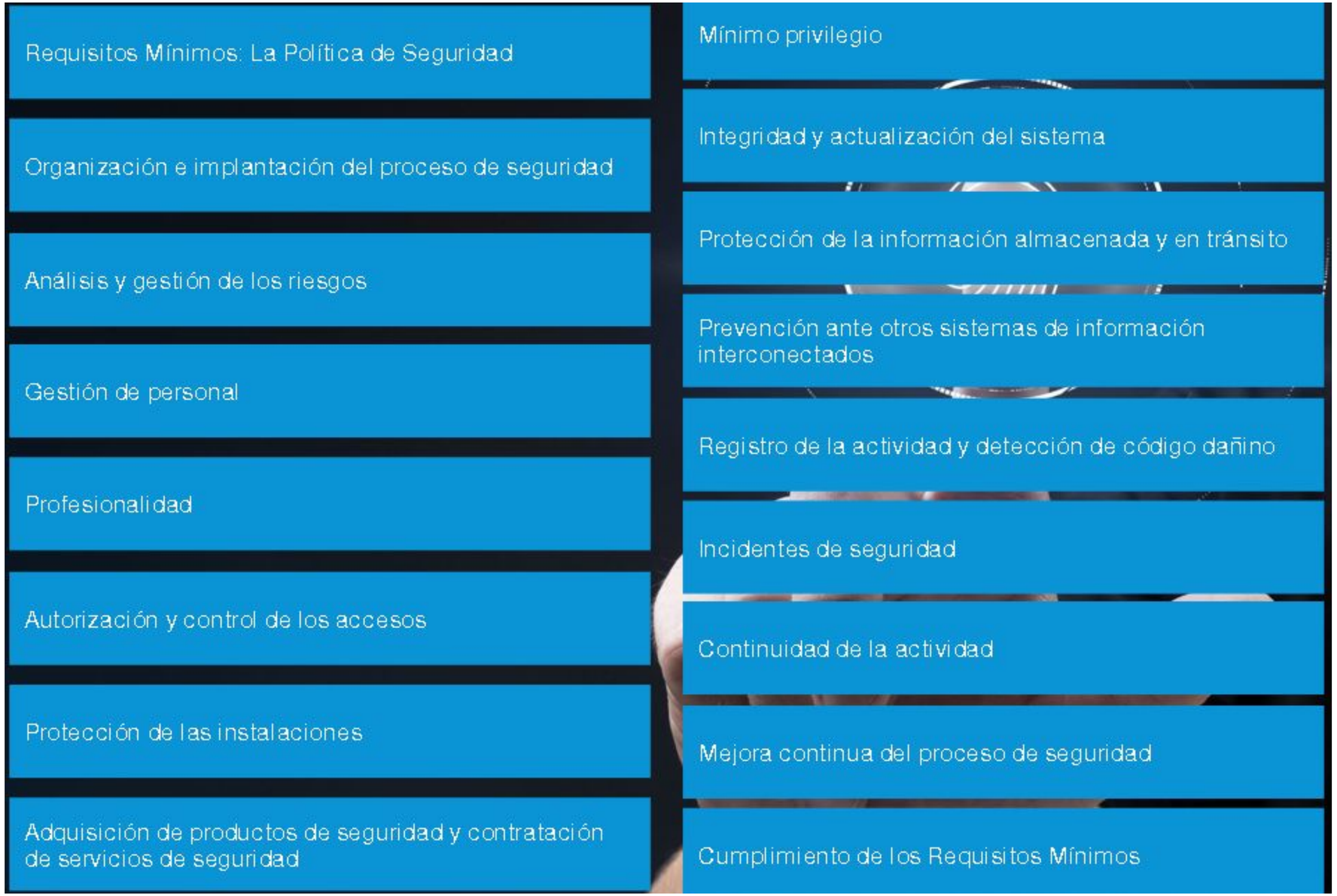
- Esto significa que las medidas de seguridad no son estáticas; deben adaptarse continuamente para abordar nuevas amenazas y mejorar la protección.

- Las Medidas de Seguridad en el ENS son:
  - **PREVENCIÓN**: Implementar medidas para evitar que ocurran incidentes de seguridad.
  - **DETECCIÓN**: Capacidad de identificar incidentes de seguridad cuando ocurren.
  - **RESPUESTA**: Acciones que se deben tomar cuando se detecta un incidente.
  - **CONSERVACIÓN**: Mantener evidencias y registros para futuras investigaciones y cumplimiento.

Organización de la Seguridad

- La gestión de la seguridad de los sistemas de información en las organizaciones exige establecer una Organización de la Seguridad.
- Tal organización debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.
- Distinguiremos entre comités y roles, así como estos últimos los estructuraremos en tres niveles:
  - **Gobierno**
  - **Supervisión**
  - **Operativo**.

Requisitos mínimos de la seguridad de la información.



Categorías de los sistemas

- Como se ha dicho, la determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectará a la seguridad de la información o de los servicios con perjuicio para las dimensiones de seguridad
  - **Disponibilidad**
  - **Autenticidad**
  - **Integridad**
  - **Confidencialidad**
  - **Trazabilidad**

Categorización de los Activos

- Se categoriza cada activo (servicios, información, etc.) según el impacto que tendría un incidente en cada una de las dimensiones de seguridad
- El nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio
- La categoría del sistema viene dada por el Valor máximo en cada parámetro

ACTIVOS	D	A	I	C	T	
Servicios						
Portal web	M	B	M	B	A	
Gestión de Usuarios	A	M	A	B	A	
Gestión de Nóminas	A	M	B	B	A	
Control de presencia	M	M	A	B	A	
…						
Información						
Datos de Nóminas	A	B	A	B	A	
Datos de Personas	A	M	A	B	A	
…	↓	↓	↓	↓	↓	
SISTEMA	**A**	**M**	**A**	**B**	**A**	**Categoría ALTA**

Disponibilidad
Autenticidad
Integridad
Confidencialidad
Trazabilidad

Dimensiones de Seguridad

Alto
Medio
Bajo

Impacto

Medidas del ENS

Marco organizativo ORG

El marco organizativo esta constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

4

Marco operacional OP

El marco operacional esta constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

31

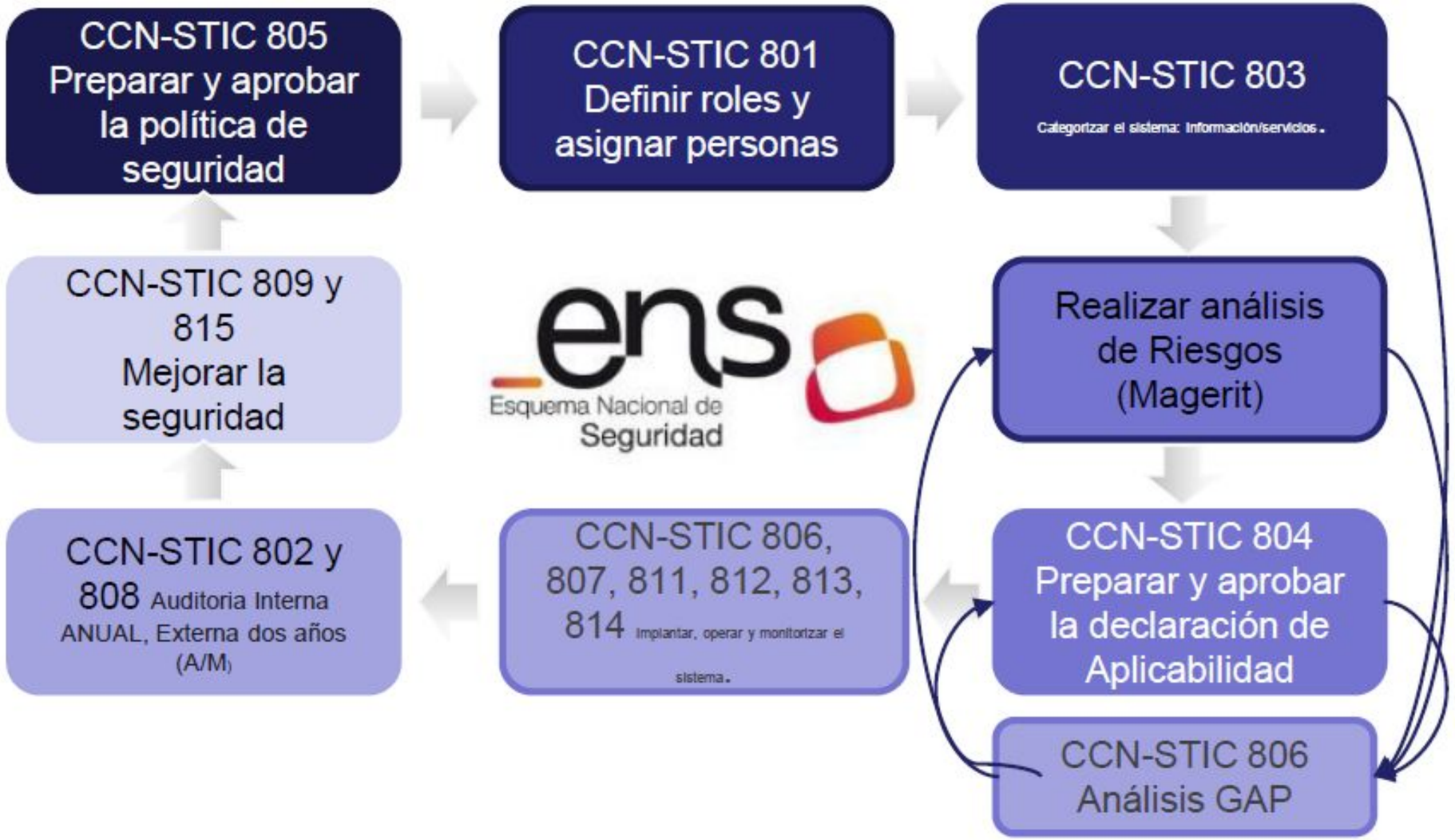
Medidas de Protección MP

Las medidas de protección, se centrarán en activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

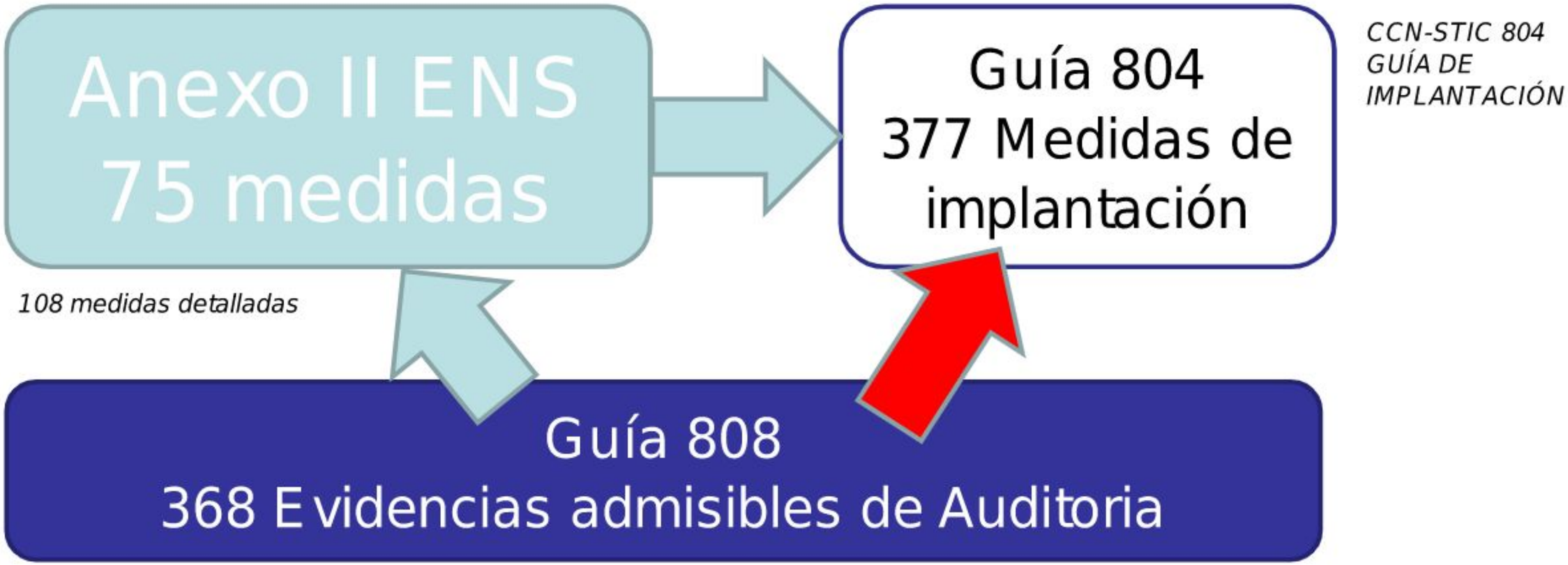
40

Marco de las Guías

https://www.ccn-cert.cni.es/ens.html



Verificación del cumplimiento



Guía CCN-STIC 808. Verificación del cumplimiento del ENS

Declaración de Aplicabilidad

La **Declaración de APLICABILIDAD** es un documento utilizado para mantener el registro y control de las medidas de seguridad que son aplicadas:

enumera y justifica los controles de seguridad establecidos en el ENS y aplicados a nuestra casuística.

Las referencias para la implementación de las medidas de protección son:

- Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS.
- ENS. Verificación del cumplimiento del ENS. Guía CCN-STIC 808. Junio 2017
- ENS. Guía de implantación. Guía CCN-STIC 804. Junio 2017

¡Firmada por el responsable de seguridad!

Lo relevante es:

- Las medidas/controles seleccionados y las razones por las cuales han sido seleccionados.
- Las medidas/controles descartados y la justificación
- Las que son innecesarias (por categoría) y la razón del porqué no son requeridas en una organización.
- Las medidas compensatorias si procede


THE
BRIDGE