

# Adecuación al ENS: Impacto en el 4<sup>o</sup> ejercicio

Normativa  
Plazos  
Conceptos  
Plan de adecuación  
Impacto en el 4<sup>o</sup> ejercicio

# Normativa

- Ley 11/2007. Art. 42
- RD 3/2010. Art 29
- Guías de implantación CCN



# Plazos

1. "(..) Los **nuevos** sistemas aplicarán lo establecido en el presente Real Decreto desde su **concepción**."
2. "Si a los **doce meses** de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un **plan de adecuación** que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a **48 meses** desde la entrada en vigor."



# Plazos

- 29 de enero de 2010: publicación en BOE
- 29 de enero de 2011: plan de adecuación
- 29 de enero de 2014: cumplimiento ENS

# Conceptos ENS

- Desarrollo normativo
- Información, Servicio, Sistema
- Responsables

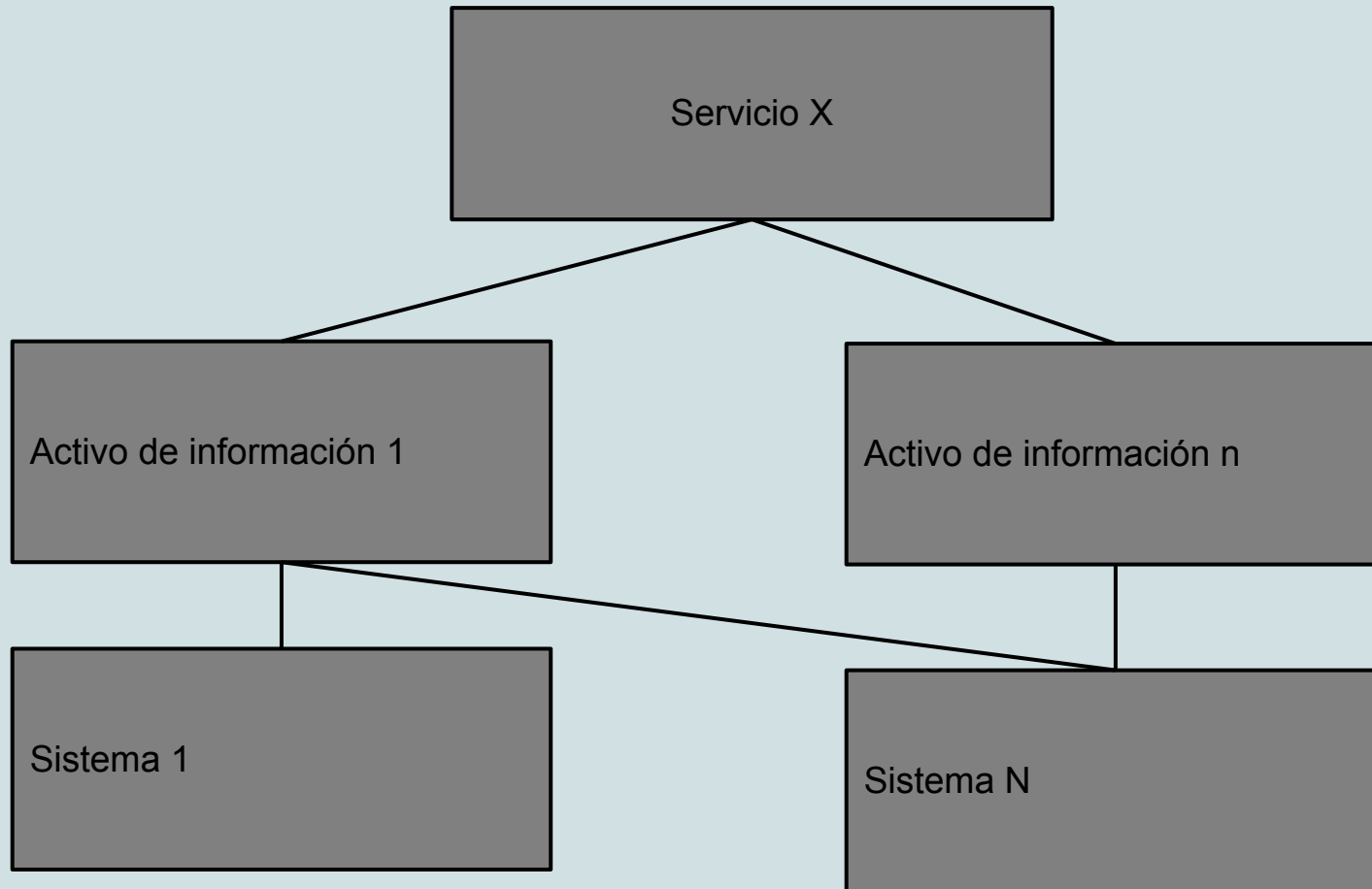


# Desarrollo Normativo

- Política de Seguridad de la Información
  - Principios generales
  - Ejemplo: Política MITyC (Orden ITC/657/2011)
- Normativa de Seguridad (el qué)
  - Norma de uso de internet
  - Norma de uso del correo electrónico
  - Soportes extraíbles
  - ...
- Procedimientos, guías, etc (cómo)



# Información - Servicio - Sistema



# Responsables en el ENS

- . Responsable(s) de la información
- . Responsable(s) de servicio(s)
- . Responsable de seguridad
- . Responsable(s) del sistema



# Responsables en el ENS

- Los responsables de información/servicios **valoran** su importancia
- El responsable de seguridad indica las **medidas de seguridad** a aplicar
- El responsable del sistema asegura su **implantación**



# ¿Quien debe tener política de seguridad?

Artículo 11. Requisitos mínimos de seguridad.

1. Todos los **órganos superiores** de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. (...)

Órganos superior según LOFAGE: **Ministro y Sº de Estado**



# ¿Y los organismos "autónomos"?

- En algunos casos, se han establecido **comités de seguridad**
- Ejemplo: MPTAP
- Un **vocal** por cada organismo autónomo
  - MUFACE
  - INAP
  - AEVAL



# Plan de Adecuación

- . Recursos propios vs externos
- . Pocos recursos internos
- . Área muy específica

# Estructura Plan de Adecuación

- . Política de Seguridad
- . Información que se maneja, con su valoración
- . Servicios que se prestan, con su valoración
- . Datos de carácter personal
- . Categoría de los Sistemas



# Estructura Plan de Adecuación

- . Análisis de Riesgos
- . Declaración de aplicabilidad de las medidas del Anexo II
- . Insuficiencias del sistema
- . Plan de mejora de la seguridad



# Plan de mejora de la seguridad

- **Proyectos** para asegurar el cumplimiento al 100% del ENS
- Los proyectos incorporan las medidas de seguridad del **Anexo II**
- A corto **plazo**, medio y largo

# Ejemplo proyectos a corto plazo

- . Desarrollo del **Marco Normativo** de Seguridad de la Información
- . Plan de **formación** y concienciación en Seguridad de la Información
- . Gestión de **incidencias**
- . Gestión de **Usuarios e identidades**
- . Desarrollo **Seguro** de Aplicaciones
- . Adecuación al **marco normativo** en materia de protecc. de datos de carácter personal
- . Protección de las **instalaciones** y gestión de suministros esenciales



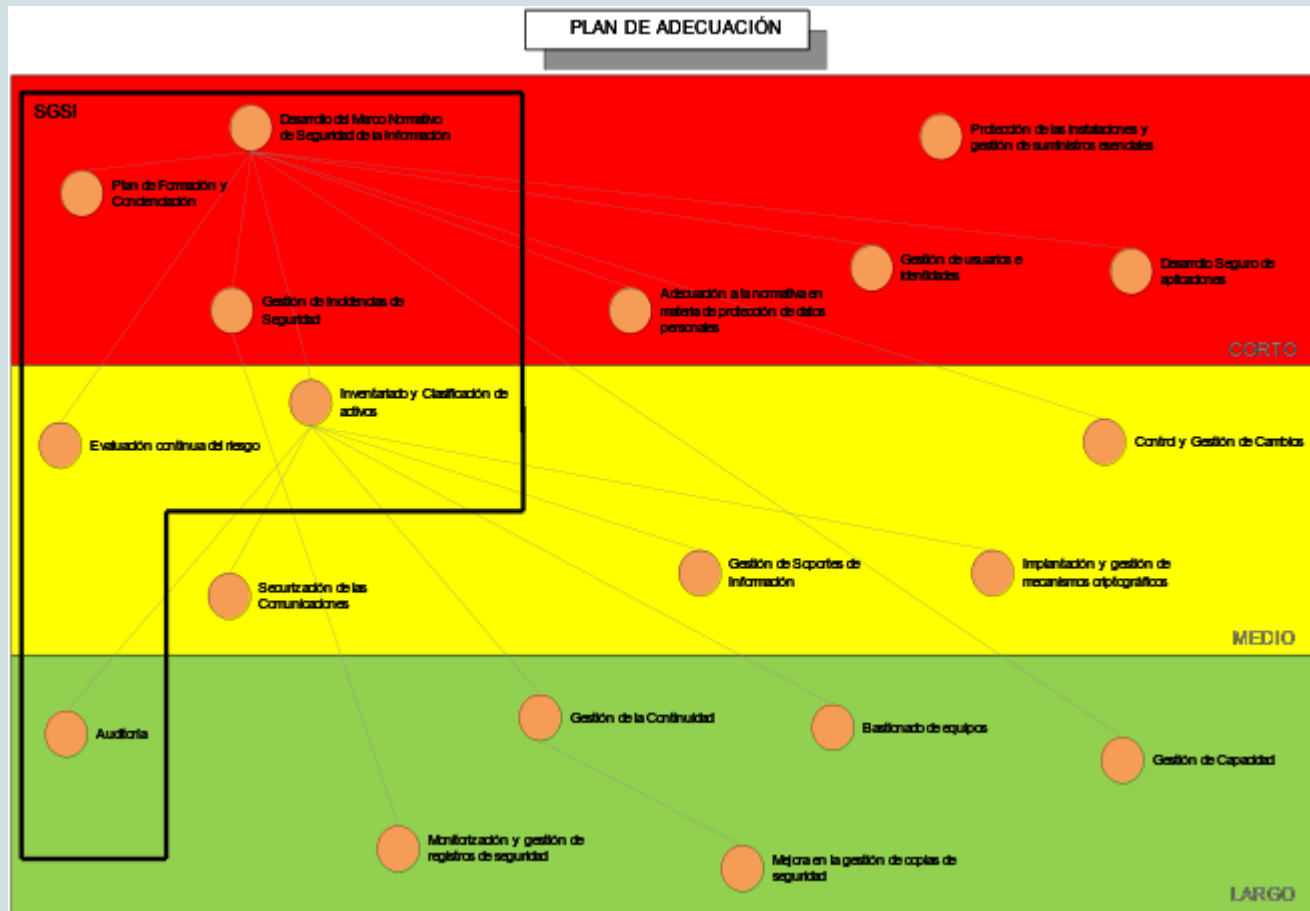
# Ejemplo proyectos a medio plazo

- . **Inventariado** y Clasificación de activos
- . Control y Gestión de **cambios**
- . **Evaluación** Continua del Riesgo
- . **Securización** de las Comunicaciones
- . Implantación y gestión de **mecanismos criptográficos**
- . Gestión de **Soportes** de Información

# Ejemplo proyectos a largo plazo

- . Gestión de la **Continuidad**
- . Monitorización y gestión de **registros** de seguridad
- . Gestión de **Capacidad**
- . Organización de **Auditorías**
- . **Bastionado** de Equipos
- . Mejora en la gestión de **copias** de **seguridad**

# Ejemplo proyectos

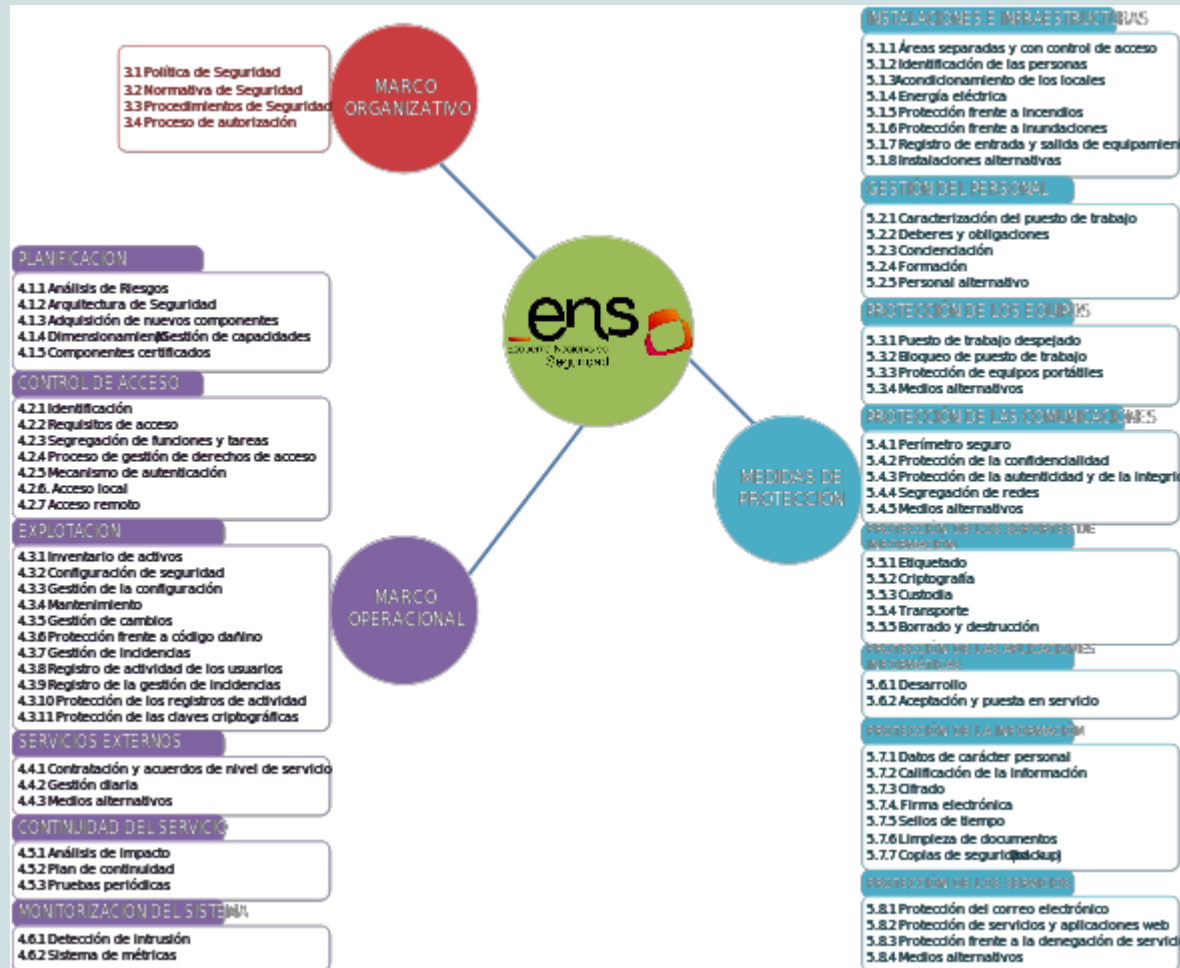


# Medidas de Seguridad ENS

- Marco Organizativo
- **Marco Operacional**
- **Medidas de Protección**



# Medidas de Seguridad ENS



# ¿Cómo puede caer en el 4º ejercicio?

1. Plan de Sistemas / Plan de adecuación
2. Ejecución de alguno de los proyectos
3. Desarrollo de un nuevo sistema => Debe cumplir el ENS

# 1. Plan de Adecuación

Tened claro el contenido mínimo del plan de adecuación



## 2. Ejecución de algunos proyectos

- ¿Gestión de identidades?
- ¿Plan de formación?
- ¿Gestión de la continuidad?



# 3.Desarrollo nuevo sistema

- El ENS enfoca la seguridad a partir de la **categoría** del sistema.
- Una vez determinada, marca las **medidas** a aplicar



# 3.Desarrollo nuevo sistema

- El sistema es importante en la medida que lo es la **información** que soporta y el **servicio** que presta
- La información y el servicio serán **categorizados** por los responsables de la información y servicio



# 3.Desarrollo nuevo sistema

- . En base a esa categorización, se determina la categoría del **sistema**
- . El responsable de seguridad **determina** qué medidas se aplican
- . El responsable del sistema se asegura que se **implementan**

# ¿Cómo valorar?

- . Habría que valorar activos de **información y servicios** que dependen del nuevo sistema
- . Siendo la valoración del sistema el **máximo**
- . En el cuarto ejercicio, mejor valorar el **servicio** y trasladar esa valoración al **sistema**



# ¿Cómo valorar?

- Valorar el **servicio** en cinco **dimensiones**
  - Autenticidad
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - Trazabilidad
- La categoría del sistema es el **máximo** de las cinco



# ¿Cómo valorar?

- ¡Cuidado! Valorar un sistema implica considerar varios **criterios** en cinco **dimensiones**
- Tal vez no tengáis **tiempo**
- Idea: Decir que **cumple** el ENS, que será **categorizado** pero...
- Preparar la categoría concreta para la **lectura**
- No olvidar la **LOPD**



# Posible enfoque

- . “De acuerdo a la normativa X, el responsable de la información/servicio **categorizarán** el servicio y sus activos”
- "Obteniéndose la categoría del sistema"
- "El responsable de seguridad **indicará** las medidas convenientes"
- . "En todo caso, se **considerarán** al menos las siguientes cuestiones..."

# Cuestiones a tratar

- Autenticación (cliente, servidor)
- Autorización
- Securitización de comunicaciones
- Integridad
- Disponibilidad
- Trazabilidad
- Seguridad física CPD
- Datos personales

# Posible enfoque

- Muchas de las medidas de seguridad son **horizontales**
- Las que tengan sentido, **suponerlas implantadas**
- **Ejemplo**
  - Protección de las instalaciones e infraestructuras
  - Medidas anti incendios, inundaciones..



# Referencias

- Ley 6/1999 LOFAGE
- Ley 11/2007 LAESCP
- RD 3/2010 ENS
- Guías CCN STIC
- Orden ITC/657/2011
- Orden TAP/3148/2011, de 7 de octubre

# Dudas, comentarios

Correo: [alvaroreig@gmail.com](mailto:alvaroreig@gmail.com)

Twitter: [@gonreg](https://twitter.com/gonreg)

**¡MUCHA SUERTE!**