Desarrollo de procedimientos para cumplimiento de controles aplicables para sistemas de información categorizados como nivel medio según ENS y desarrollo de instrucciones para aplicación de esos procedimientos empleando las herramientas técnicas e instrucciones que proporciona el CCN.

Alumno: Raúl Rodrigo Fernández

Tutor: Iñaki Moreno Fernández

Universitat Oberta de Catalunya

Máster Universitario en Ciberseguridad y Privacidad

Índice

Apartado 1: Objeto del trabajo y metodología

- **Objeto del trabajo**
  - Implementar un Sistema de Seguridad de la Información dentro de un órgano de la Administración Pública a través del Esquema Nacional de Seguridad (nivel MEDIO).

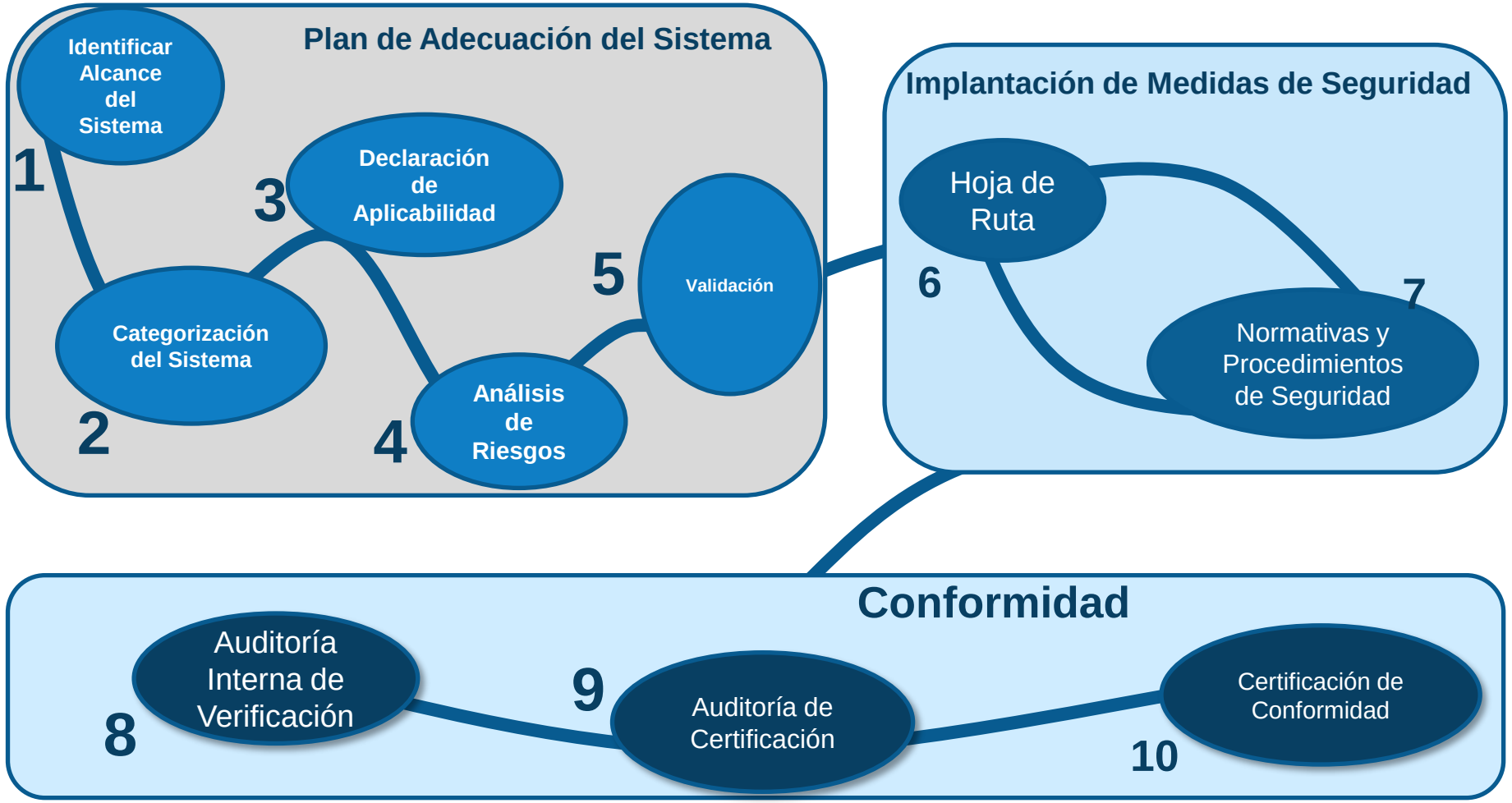
- **Metodología**
  - Consulta de las Guías CCN-STIC, normativa y referencias bibliográficas.
  - Análisis propio y creación de un organismo ejemplo.
  - Creación de un Plan de Adecuación.

Apartado 2: Normativa aplicable

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los **Servicios Públicos**.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad**.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad**.
- Guías CCN-STIC familia 800:
  - **CCN-STIC-804 ENS. Guía de implantación**
  - **CCN-STIC-806 Plan de Adecuación al ENS**
  - **CCN-STIC-822 Procedimientos de seguridad**

Estas guías se basan en el RD 3/2010

Apartado 3: Plan de Adecuación al ENS



Apartado 3: Plan de Adecuación al ENS

1. Plan de Adecuación del Sistema: Definir el alcance del sistema

Política de Seguridad de la Información

- Misión u objetivos del organismo
- Marco normativo
- Organización de Seguridad:
  - Definición del Comités
  - Funciones
  - Responsabilidades
  - Mecanismos de coordinación
  - Procedimientos de designación de personas
- Concienciación y formación
- Postura para la gestión de riesgos:
  - Plan de análisis
  - Criterios de evaluación de riesgos
  - Directrices de tratamiento
  - Proceso de aceptación del riesgo residual
- Proceso de revisión de la política de seguridad

Apartado 3: Plan de Adecuación al ENS

1. Plan de Adecuación del Sistema: Categorización del Sistema

- **Ficha de Servicios:** Datos esenciales de cada servicio prestado, incluyendo los tipos de información tratados y los sistemas de información sobre los que se prestan, así como una valoración inicial del nivel de seguridad de cada una de las dimensiones de seguridad aplicables al servicio/información de que se trate.

SISTEMA	Disponibilidad [D]	Integridad [I]	Confidencialidad [C]	Autenticidad [A]	Trazabilidad [T]
Servicio X	Bajo	Bajo	Bajo	Bajo	Bajo
	Medio	Medio	Medio	Medio	Medio
	Alto	Alto	Alto	Alto	Alto

Resultado categorización	
CATEGORÍA	MEDIA

Apartado 3: Plan de Adecuación al ENS

1. Plan de Adecuación del Sistema: Declaración de Aplicabilidad

Medidas del ENS que aplican a Categoría Media: 63

1. Plan de Adecuación del Sistema: Análisis de Riesgos

MAGERIT

Identificación de Activos
- Activos esenciales
- Activos de información

Valoración de los Activos
- 5 dimensiones: DICAT
- Niveles: Bajo, Medio, Alto.

Análisis de Salvaguardas
- Niveles de madurez de L0 a L5

Amenazas
- Catálogo de amenazas detectadas por Magerit

RIESGO
- Riesgo potencial
- Riesgo actual
- Riesgo objetivo ENS

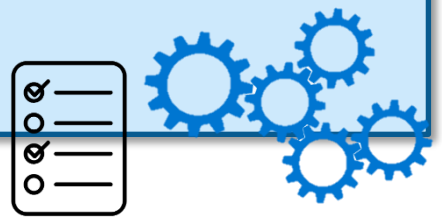
Apartado 3: Plan de Adecuación al ENS

2. Implantación de las medidas de seguridad: Hoja de Ruta

- Trazabilidad de las medidas del ENS con los documentos.
- Listado de documentos a desarrollar.

2. Implantación de las medidas de seguridad:
Normativas y procedimientos de seguridad

- Desarrollar listado de documentos: 39 documentos.
- Aterrizaje y adaptación de documentos al funcionamiento de la Organización.
- Implementación de medidas técnicas para solventar necesidades del ENS no cubiertas.
- Aprobación de la documentación.



▸ Apartado 3: Plan de Adecuación al ENS

3. Conformidad

Objetivo: Verificar el cumplimiento de los establecido en el ENS, tanto en sus principios básicos como en los requisitos de seguridad y emitir una opinión independiente, objetiva, íntegra, profesional y confidencial siempre basada en la evidencia del cumplimiento o no de las medidas de seguridad.

Resultados:

FAVORABLE: No presenta ningún tipo de disconformidad.

FAVORABLE CON NO CONFORMIDADES: Se evidencian 'No conformidades menores' o 'No conformidades mayores'

DESFAVORABLE: Se evidencian un número significativo de 'No conformidades mayores'.

▸ Apartado 4: Conclusiones

OBJETIVO → Crear un Plan de Adecuación al ENS

Se ha elaboración de una guía completa para que el 'Organismo X' pueda adecuarse al ENS siguiendo los Anexos del documento:

- **Ejemplo de Política de Seguridad de la Información**
- **Ficha de Servicio**
- **Categorización del Sistema**
- **Análisis de Riesgos**
- **Normativa interna de uso de medios**

▸ Apartado 4: Conclusiones

Se ha demostrado que las guías CCN-STIC-800 y el RD ENS definen un camino claro para conseguir crear un plan desde cero y certificar el ENS.

<u>Objetivos futuro:</u>

- ✓ **Identificar las desviaciones que se producen entre las nuevas guías CCN-STIC-800 del nuevo RD ENS y este trabajo.**
- ✓ **Analizar del grado de aplicación práctico que presenta este nuevo ENS.**

Muchas gracias por su atención

Universitat Oberta de Catalunya