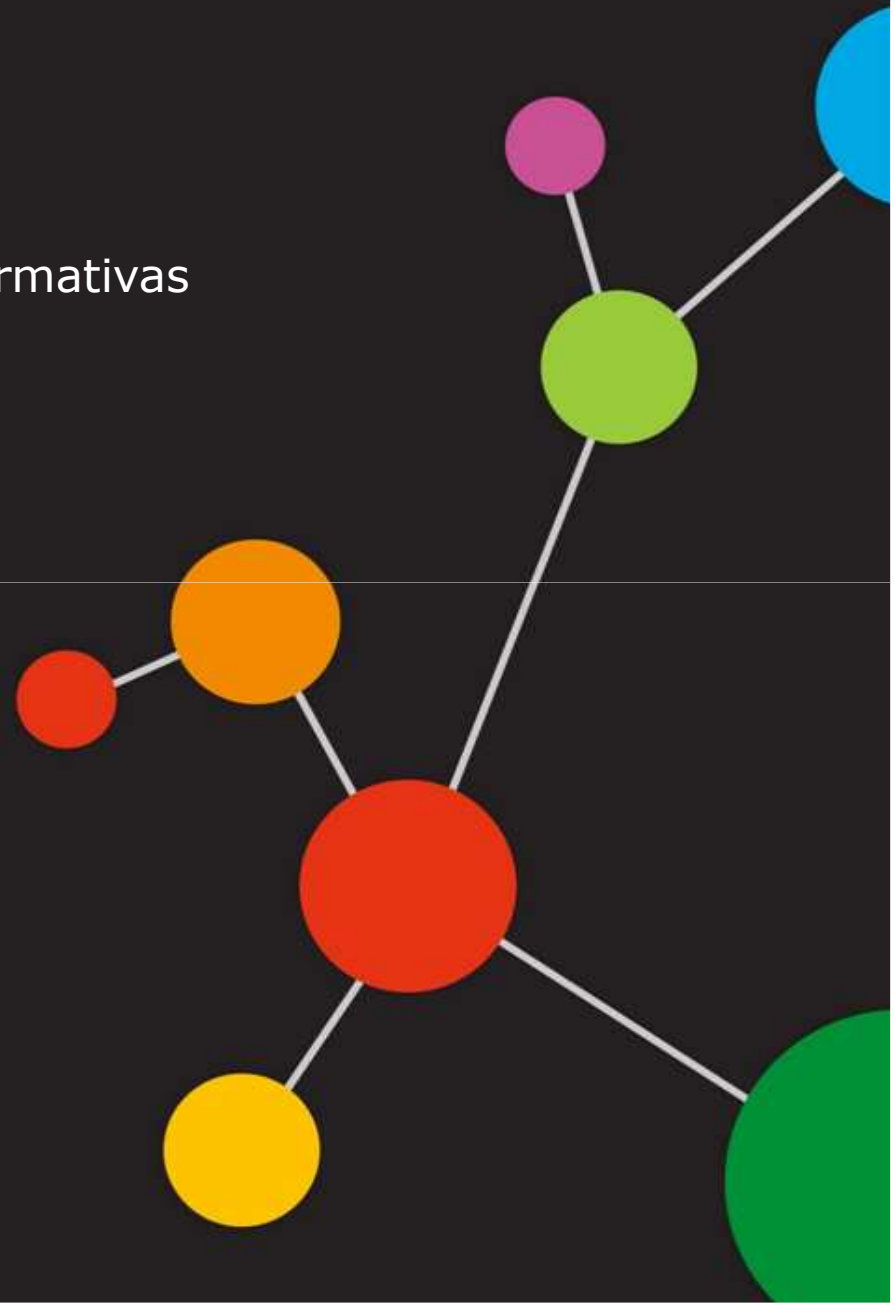
# Protección de Datos y Adecuación al Esquema Nacional

Puntos de encuentro y diferencias entre las normativas



# Acerca de Oesía

**TECNOLOGÍAS DE LA INFORMACIÓN**

**OUTSOURCING DE PROCESOS DE NEGOCIO**

**INGENIERÍA Y SERVICIOS AVANZADOS**

**CONSULTORÍA TECNOLÓGICA**

- Desarrollo de software
- Seguridad
- Movilidad
- Business Intelligence
- Infraestructura y Sistemas

- Outsourcing BPO
- Outsourcing TI
- Capital Humano

- Aviónica y Optrónica
- Mando y Control
- Simulación
- Homeland Security
- Espacio
- Radio Frecuencia

> “Somos una consultora multinacional especializada en tecnología e ingeniería avanzada”

# Servicios de Seguridad de la Información

## Oesía abarca todo el ciclo de vida de la Seguridad de la Información

### Consultoría

- Plan Director de Seguridad
- Análisis y Gestión de Riesgos
- Cumplimiento de Normativa
- Plan de Continuidad de Negocio
- Sistemas de Gestión de la Seguridad - SGSI
- Cuadro de Mando
- Oficina de Seguridad

### Arquitectura

- Definición e integración de soluciones de seguridad perimetral
- Gestión de identidades
- Prevención de fugas de información (DLP)
- Cifrado, certificación y firma digital
- Gestión de permisos de información (IRM)
- Detección de fraude

### Auditoría

- Auditoría de sistemas, redes y código (OSSTMM, OWASP)
- Penetration tests
- Hacking ético
- Servicios de Auditoría Continuada
- Servicios PCI DSS

### Seguridad Gestionada

- Servicios SOC
  - Análisis de seguridad
  - Gestión de eventos y alarmas
  - Gestión de incidencias
  - Monitorización del nivel de riesgo
  - Prevención y detección de intrusiones y vulnerabilidades
  - Gestión de infraestructuras de seguridad
  - Cuadro de mando y reporting

# Protección de Datos y Adecuación al Esquema Nacional

Un acercamiento a sus puntos de encuentro y diferencias

# INTRODUCCIÓN I

**Uno de los objetivos del ENS**

*Crear las condiciones necesarias para la confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.*

## ¿Que tienen en común el ENS, la LOPD y un SGSI?

- ✓ Establecen un sistema de gestión de información y los elementos relacionados con la misma
- ✓ Requiere la implantación de una serie de medidas técnicas, jurídicas y organizativas.
- ✓ Establece figuras de responsabilidad
- ✓ Necesitan un soporte documental
- ✓ Referidos a Sistemas de Información

# INTRODUCCION II

| RDLOPD | ENS |
| --- | --- |
| **Sistema de información:** conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal. | **Sistema de información:** conjunto Organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. |
| **Está orientado a los datos de carácter personal, a los elementos que le rodean y a las medidas de seguridad que se aplican a este tipo concreto de información.** | **Está orientado al sistema de Información en su conjunto y a la información que le sea inherente en el que los datos de carácter personal son uno mas de los tratados.** |

# CUADRO COMPARATIVO

| LOPD | ENS |
|---|---|
| Documento de Seguridad | Política y normas de seguridad<br>Declaración de aplicabilidad |
| Niveles de seguridad | Categorización de los sistemas |
| Responsable de Seguridad | Responsable de Seguridad<br>Responsable de los Servicios<br>Responsable de la Información |
| Ejercicio de derechos | Garantía de ejercitar derechos |
| Auditoría | Auditoría de la Seguridad |

| | |
|---|---|
| Funciones y obligaciones del personal | Deberes y obligaciones del personal |
| Identificación y autentificación | Identificación única de usuarios |
| Control de accesos | Autorización y control de accesos |
| Procedimiento de notificación, gestión y respuesta ante las incidencias | Gestión de incidencias Registro de incidencias |
| Control de acceso físico | Protección instalaciones e infraestructura |
| Gestión y distribución de soportes | Protección de los soportes de información<br>Gestión de soportes y documentos |
| Telecomunicaciones | Protección de las telecomunicaciones |

# EL DOCUMENTO DE SEGURIDAD

**¿Que relación existe entre el documento de seguridad y la política de seguridad?**

**¿Modifica el ENS el Documento de Seguridad LOPD?**

**¿La política de seguridad debe tener en cuenta el documento de seguridad LOPD?**

**¿Como se puede combinar ambos sin tener que duplicar y mantener dos documentos?**

- ✓ Son documentos independientes
- ✓ Son documentos relacionados

**CCN-STIC-805** La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda

# FICHEROS

## RDLOPD

**Datos de Carácter Personal Automatizados o no automatizados**

## ENS

**Ficheros soportados en medios electrónicos**

**Categorización en niveles ALTO, MEDIO Y BÁSICO**

En función de los datos tratados

Afectado por las dimensiones de seguridad
integridad, confidencialidad, trazabilidad, disponibilidad y autenticidad

Según el impacto que un incidente de seguridad podría tener en relación con la capacidad de la organización para determinados logros

- ✓ Alcanzar sus objetivos.
- ✓ Proteger los activos a su cargo.
- ✓ Cumplir sus obligaciones diarias de servicio.
- ✓ Respetar la legalidad vigente.
- ✓ Respetar los derechos de las personas

# El responsable de Seguridad

**¿El Responsable de Seguridad del ENS puede ser la misma persona que el Responsable de Seguridad de la LOPD?**

**¿Cuál es el perfil más idóneo para esta función?**

- ✓ Responsable de Seguridad ENS es un perfil orientado a entornos tecnológicos
- ✓ Responsable de Seguridad LOPD debe poseer conocimiento jurídico sobre este ámbito
- ✓ Responsable de Seguridad se situará en un nivel de dirección ejecutiva

**P.137 CCN-STIC-801** Las organizaciones harán bien en **hacer coincidir** estas responsabilidades en una **única figura**, recopilando todas las funciones en la Política de Seguridad

**P.137 CCN-STIC-801** El artículo 10 del ENS recoge el principio de **seguridad como función diferenciada**. Este principio exige que el Responsable de la Seguridad sea independiente del Responsable del Sistema.

# DERECHOS ARCO

El ámbito de aplicación del ENS se extiende a:

- ✓ Sedes electrónicas.
- ✓ Registros electrónicos.
- ✓ Sistemas de Información **accesibles electrónicamente por los ciudadanos**.
- ✓ Sistemas de Información **para el ejercicio de derechos**.
- ✓ Sistemas de Información para el cumplimiento de deberes.
- ✓ Sistemas de Información para **recabar información y estado del procedimiento administrativo.**

Las medidas de seguridad que serán de aplicación a cada sistema/servicio deben estar ponderadas respecto de los riesgos que la organización asume

- ✓ Informar adecuadamente
- ✓ Asegurar la disponibilidad de esta información
- ✓ Asegurar la integridad y la autenticidad de la información p.e. firmando electrónicamente un PDF de lectura
- ✓ Facilitar el ejercicio de los derechos por medios electrónicos
- ✓ Asegurar la integridad y la autenticidad de la recogida p.e. incorporándoles un Código Seguro de Verificación
- ✓ Asegurar la identidad del interesado (p.e. con el uso de DNI electrónico)

# AUDITORIA

**¿Son Auditorías diferentes las del ENS y la LOPD?**

**¿Pueden realizarse ambas en conjunto y simultáneamente?**

**¿Pueden ser auditadas ambas por el mismo equipo de auditoría?**

- ✓ El alcance de las auditorías es diferente en soporte, tipología y niveles de seguridad
- ✓ Pueden coincidir los ficheros a auditar y no así la clasificación de seguridad de ellos
- ✓ Las medidas de seguridad de LOPD son mínimos exigibles sin perjuicio de los requisitos de otras legislaciones o que se considere necesario para la protección de los datos

**CCN-STIC-802 Anexo C** Si el sistema de información auditado según el RD 3/2010, tratase datos de carácter personal, el equipo auditor podrá solicitar una copia de la auditoría preceptiva según el RD de protección de datos personales

**CCN-STIC-802 Anexo C** si durante la realización de la auditoría se identificase algún incumplimiento manifiesto del RD 1720/2007, es obligación del equipo auditor comunicarlo, e incluirlo en el informe de auditoría