
ens
Esquema Nacional de
Seguridad

# Conformidad legal y Seguridad

**SEGURIDAD DE LA INFORMACIÓN**

RD 3/2010  Esquema Nacional de Seguridad
Instrucciones Técnicas de Seguridad

**PROTECCIÓN DE DATOS**

Ley Orgánica 15/1999, LOPD
RD 1720/2007, RDLOPD
Reglamento (UE) 2016/679 General de Protección de Datos

# Sujetos obligados


¿Y los pequeños ayuntamientos?

# Sujetos obligados

**PERO ...**

**POR DÓNDE EMPIEZO...**

**NO SE LO  QUE ES EL ENS..**

**ANÁLISIS DE RIESGO...**

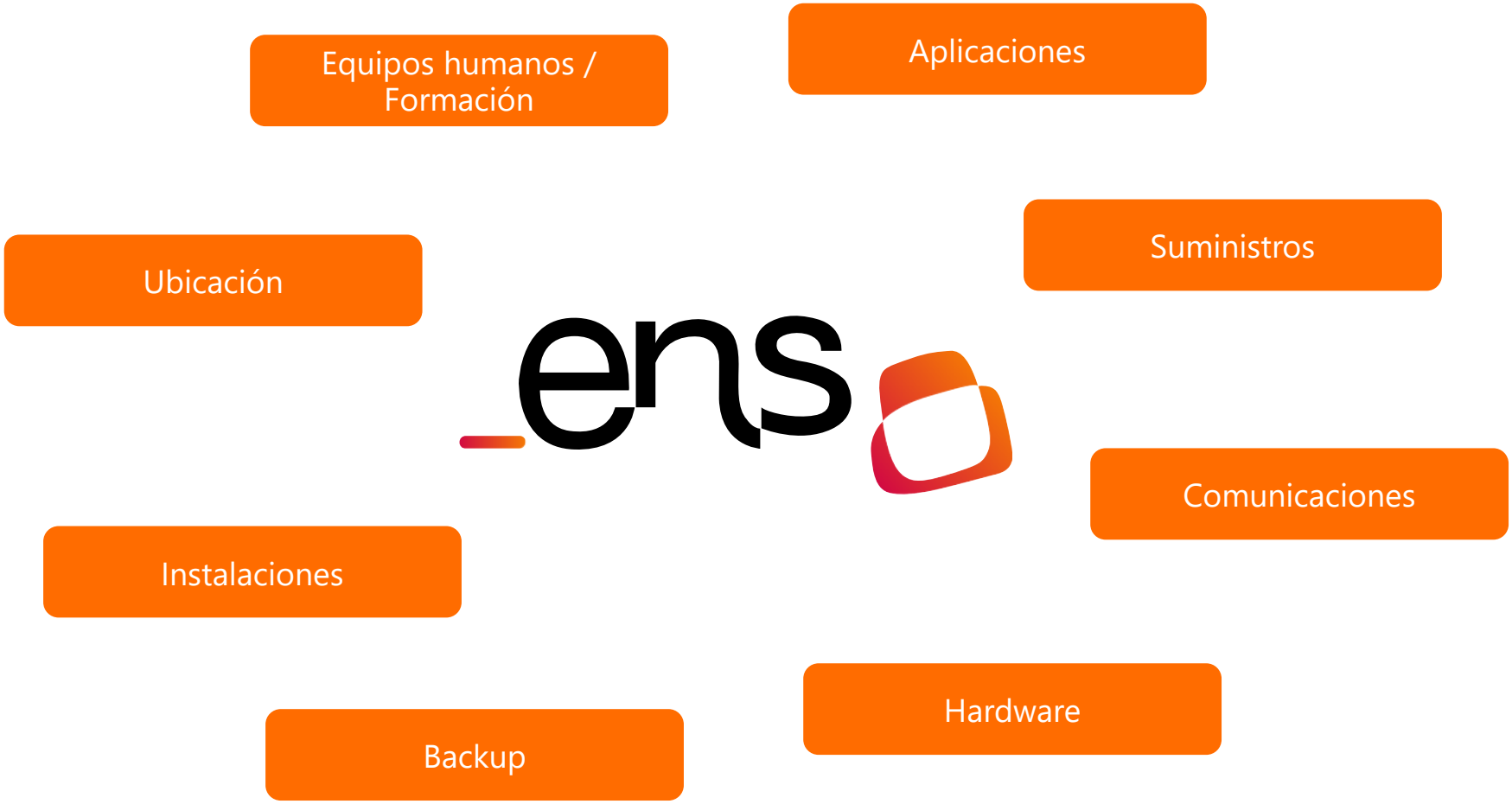
**INVENTARIO DE ACTIVOS...**

**PILAR, INÉS...**

**MI ORGANIZACIÓN ES PEQUEÑA...**

**NO TENGO PERSONAL ESPECIALIZADO...**

**TODO ESTO ME SOBREPASA...**




Si vamos a tener u incidente en nuestros sistemas de información, que inevitablemente va a ocurrir, ¿qué capacidad de resistencia tenemos?

Objetivo: reducir el riesgo al máximo sin hipotecarnos

Por el mero hecho de disponer de un móvil o un ordenador aceptamos un riesgo.

# Primeros pasos

**Política de seguridad**

**Asignación de roles y responsabilidades**

**Normativa de Seguridad**

**Categorización Información y Servicios**

**Análisis de riesgos (pilar)**

**Plan de adecuación (priorización / riesgo vs inversión)**

**Plan de formación / concienciación**

# Primeros pasos

**Política de seguridad**

Inicialmente un documento de política de seguridad mínimo, a desarrollar transversalmente.

**Asignación de roles y responsabilidades**

Adecuados al tamaño de nuestra organización

¿Segregación de responsabilidades?

Responsable del Sistema (servicios terceros)

Funciones se delegan, no la responsabilidad.

**Normativa de Seguridad**

Buenas prácticas en el uso del PC y SO, las aplicaciones, correo electrónico, navegación web,  etc.

# Primeros pasos

**Inventario de activos / Categorización Información y Servicios**

¿Nivel alto? ¿Categorización en otras EELL similares?

Sin embargo debemos asignar el nivel y categoría que corresponda.

En casa: nivel básico / Externalizado: nivel medio

**Análisis de riesgos (Pilar/uPilar)**

ENS es gestión de riesgos / RGPD es gestión de riesgos

EELL más pequeñas: Nivel de madurez L1 - L2 (Buenas prácticas - procedimientos definidos)

¿Qué prima? Servicios vs Seguridad

**Plan de adecuación (priorización / riesgo vs inversión)**


## Gestión Propia

- Nominas.
- Personal.
- Cementerios.
- Gestión animales.
- Asociaciones
- Fiestas

Red local
PCs /SO
Ofimática / Docs comp.
Antivirus

## Gestión Terceros

- Empresa Privada.
  - Contabilidad
  - Padrón.
  - Web.
  - E-mail.
- Otras Administraciones
  - FACE
  - ORVE

## Gestión Diputaciones

- Padrón
- Contabilidad
- Recaudación
- eAdministración
- Central compras
- Inventarios bienes
- Servicios sociales
- Etc

# ¿Servicios prestados por terceros?

VII. *Soluciones y servicios prestados por el sector privado*

VII.1 Cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas.

VIII.2 Es responsabilidad de las entidades públicas contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en la presente Instrucción Técnica de Seguridad.

También exigible a los convenios de prestación de servicios por parte de otras administraciones públicas.

No nos olvidemos de que aunque el servicio lo preste un tercero, el servicio es de la propia entidad local y la información es de la propia entidad local.

Por tanto, la no adecuación al ENS de los servicios prestados por tras admon Podría dar lugar a una no conformidad.

# Es responsabilidad de la Administración exigirlo

**Modelo de cláusula administrativa particular**

«Cláusula administrativa particular.–En cumplimiento con lo dispuesto en el artículo 99.4 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, y el artículo 18 del Real Decreto ……/……, de …… de …… por el que se regula el Esquema Nacional de Seguridad, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes, han sido previamente certificados por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

En el caso de que no exista la certificación indicada en el párrafo anterior, o esté en proceso, se incluirá, igualmente, referencia precisa, documentada y acreditativa de que son los más idóneos.

Cuando estos sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre.»

# ¿Tenemos que certificar nuestro sistema de información?

Auditoria BIENAL

**NIVEL BÁSICO (Opcional)**

**NIVEL MEDIO Y ALTO (obligatoria y por entidad acreditada)**

Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.


## Gestión Propia

- Nomi
- Pers
- Ce
- 
- 
- Fies


## Gestión Terceros

- Empresa Privada
  - Contabili
  - Padró
  - W
  - 
- Otras A
  - FAC
  - ORVE

## Diputaciones

- adrón
- Contabilidad
- Recaudación
- eAdministración
- Central compras
- Inventarios bienes
- Servicios sociales
- Etc

# Sistemas de gestión propia


**Antivirus**

**Control de acceso / copia de seguridad**

**Identificación y autenticación de los usuarios**

**Seguridad en la Red LAN**

**Configurar adecuadamente el Router**

**Cortafuego**

**Separar la conexión wifi del Ayuntamiento**

**Instalación de software legal**

**Gestión de soportes y documentos**

**Uso de correo corporativo**

# Sistemas de gestión propia


**Principales vectores de ataque:**

**Correo electrónico**

**Equipos personales (de un PC a otro)**

**Navegación web / accesos externos**

**Pendrive**

**BYOD (portátiles, móviles,etc)**

**Redes insecuras (LAN/WIFI)**

**Servicios en la nube no controlados (el usuario si no dispone de un servicio, se busca la vida)**

**En definitiva personas…**

# Formación y concienciación

20% medidas son técnicas , el 80% son organizativas, de personal y seguridad perimetral.

- INAP / CCN CERT
- INCIBE
- FEMP
- ESCUELAS DE ADMNISTRACIÓN PÚBLICA REGIONALES (EJ. ECLAP JCYL)
- PLANES PROVINCIALES DE FORMACIÓN

# Muchas gracias