



# BANCO DE BUENAS PRÁCTICAS

**TITULO DE LA EXPERIENCIA:** : Aprobación Plan de Adecuación a los esquemas nacionales de seguridad e interoperabilidad

**NOMBRE DE LA ENTIDAD LOCAL:** Ayuntamiento de Sant Feliu de Llobregat

**ÁREA DE LA ENTIDAD QUE SE HA DESARROLLADO:** Tecnología y Gestión del Conocimiento

**OTRAS ÁREAS IMPLICADAS EN LA ORGANIZACIÓN**

**AÑO:** 2011-212

## PERSONA DE CONTACTO

**NOMBRE Y APELLIDOS:** Mario Alguacil Sanz

**CARGO:** Director de Tecnologías y Gestión del Conocimiento

**DEPARTAMENTO:**

**DIRECCIÓN:** Pl. Vila, 1

**CÓDIGO POSTAL:** 08980

**LOCALIDAD:** Sant Feliu de Llobregat

**PROVINCIA:** Barcelona

**TELÉFONO:** 936858000

**FAX:** 936858003

**E-MAIL:** [alguacilsm@santfeliu.cat](mailto:alguacilsm@santfeliu.cat)

**WEB:** [www.santfeliu.cat](http://www.santfeliu.cat)

## DESCRIPCIÓN:

Análisis e identificación de las medidas de seguridad e interoperabilidad que el Ayuntamiento ha de desarrollar para adecuar sus sistemas y actividades a los principios y requisitos establecidos en los esquemas nacionales de Seguridad e Interoperabilidad, de acuerdo con una política de seguridad en la utilización de medios



electrónicos que permita la protección adecuada de la información tal y como se establece en el artículo 42.2 de la ley 11/2007, de 22 de junio

### **OBJETIVOS:**

Creación de las condiciones necesarias de 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 a los ciudadanos y a las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Integrar la Seguridad como un proceso transversal que afecta a la totalidad de la actividad administrativa.

Acciones:

1. Establecimiento de la política de seguridad.
2. Identificación de activos, en especial, los expedientes electrónicos afectados por la Administración electrónica, y de los servicios de tramitación electrónica correspondientes, mediante un **marco de referencia de eAdministración**.
3. Análisis de riesgos de los expedientes identificados, y determinación de categorías de seguridad de los sistemas afectados. El análisis de riesgo se ha ampliado con **criterios específicos de seguridad documental electrónica**.  
Identificación de las medidas de seguridad a implementar, y de las auditorías a realizar, alineado con el Esquema Nacional de Seguridad.
5. Selección de controles y estándares de seguridad en la actuación administrativa, especialmente desde la perspectiva de su formalización documental.
6. Ampliación de los controles aplicables, a partir de la política-modelo de seguridad documental electrónica de Astrea (licencia Creative Commons BY-NC-ND).  
Determinación de recomendaciones e impacto, para identificar las tareas a abordar en la implantación, configuración y operación de las plataformas y sistemas afectados.
7. Aplicación de las medidas técnicas, en particular mediante el establecimiento de configuraciones adecuadas y, en su caso, de modificaciones programáticas.

Y en el futuro, medición, auditoría y mejora constante.

### **RESULTADOS:**

Aprobación de la documentación en el marco de aplicación del Esquema Nacional de Seguridad y del Esquema Nacional de Interoperabilidad:

- Plan de Adecuación
- Política de Seguridad
- Política de Firma Electrónica.

