



## **NORMATIVA**

### **ACEPTACIÓN DE NUEVOS SISTEMAS Y PRODUCTOS**

Excmo. Ayuntamiento de Baeza

Octubre 2019

**CONTROL DE DOCUMENTACIÓN:**

CÓDIGO:	NR.15	DOCUMENTO:	NORMATIVA DE ACEPTACIÓN DE NUEVOS SISTEMAS Y PRODUCTOS
---------	-------	------------	--

REVISIÓN NÚMERO:	1.0	FECHA DE ENTRADA EN VIGOR:	31 – Octubre - 2019
------------------	-----	----------------------------	---------------------

ES ORIGINAL:	<input checked="" type="checkbox"/>	ES COPIA CONTROLADA:	<input type="checkbox"/>	ES COPIA NO CONTROLADA:	<input type="checkbox"/>
--------------	-------------------------------------	----------------------	--------------------------	-------------------------	--------------------------

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
[ ÁREA ]	[ ÁREA ]	Comité de Seguridad de la Información
[ NOMBRE – INICIALES ]	[ NOMBRE – INICIALES ]	[ NOMBRE – INICIALES ]
FECHA:	FECHA:	FECHA:
FIRMA:	FIRMA:	FIRMA:

**CONTROL DE CAMBIOS:**

REVISIÓN Nº:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:

DOCUMENTACIÓN OBSOLETA:	<input type="checkbox"/>	FECHA:	
-------------------------	--------------------------	--------	--

**CLASIFICACIÓN DE LA INFORMACIÓN:**

## SEGURIDAD

PÚBLICA:	<input type="checkbox"/>	PUBLICABLE	<input type="checkbox"/>	USO INTERNO	<input checked="" type="checkbox"/>	CONFIDENCIAL:	<input type="checkbox"/>	SECRETA:	<input type="checkbox"/>
----------	--------------------------	------------	--------------------------	-------------	-------------------------------------	---------------	--------------------------	----------	--------------------------

## PRIVACIDAD

NO IP	<input type="checkbox"/>	IP A	<input checked="" type="checkbox"/>	IP B	<input type="checkbox"/>	IP C	<input type="checkbox"/>
-------	--------------------------	------	-------------------------------------	------	--------------------------	------	--------------------------

## **Confidencialidad Acerca de este documento**

---

AVISO: Este documento está protegido por la legislación referente a propiedad intelectual e industrial y por tratados internacionales. La utilización permitida de esta documentación queda limitada exclusivamente en relación con el Ayto. de Baeza, y todo uso no autorizado será perseguido de acuerdo con la legislación aplicable. Se prohíbe su copia, modificación, reproducción o distribución sin permiso del titular.

### **Excmo. Ayuntamiento de Baeza**

Pje. Cardenal Benavides, 10

23440 Baeza, Jaén

ESPAÑA

<http://www.baeza.es/baeza/extranet/>

<b>NORMATIVA</b>	
<b>ACEPTACIÓN DE NUEVOS SISTEMAS Y PRODUCTOS</b>	Fecha: Octubre 2019
	Edición: 1.0

## 1) OBJETO

Esta normativa tiene como objeto establecer los parámetros de seguridad a implantar previo a la puesta en marcha, modificación o mejora de nuevos sistemas desarrollados por el Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento) o adquiridos de un tercero.

## 2) ALCANCE

Esta normativa es de obligado cumplimiento para todo el personal de desarrollo en particular, y personal del Ayuntamiento en particular. Dichos parámetros de seguridad tendrán que cumplirse igualmente para aquellos sistemas que se adquieran de un tercero o no hayan sido desarrollado por el Ayuntamiento.

Esta normativa ha sido aprobada por el Comité de Seguridad, atendiendo a las recomendaciones del Responsable de la Información, Responsable de la Entidad, Responsable de Seguridad, Responsable del Sistema y de todos los actores intervinientes en la misma.

Cualquier modificación posterior entrará en vigor al día siguiente de su aprobación y publicación por parte del Comité de Seguridad. En este caso, la versión anterior quedará anulada por la última versión de esta normativa.

## 3) RESPONSABILIDADES

El responsable de la puesta en marcha y verificación del cumplimiento de los requisitos definidos en esta normativa recae sobre el Responsable del Sistema.

Los desarrolladores tendrán que cumplir lo estipulado en la presente normativa antes de la puesta en marcha de los sistemas.

## 4) DESARROLLO NORMATIVO

Cuando se pongan en marcha los proyectos para el desarrollo e implantación de nuevos sistemas, o ampliación/mejora de los ya existentes, además de las actividades tradicionales de cada una de las fases de éstos, se llevarán a cabo igualmente las actividades para determinar e implementar los requerimientos de seguridad necesarios.

Cuando se vaya a adquirir un producto se establecerán igualmente los requerimientos de seguridad que debe cumplir y se revisará dicho cumplimiento antes de su compra.

### 4.1) DESARROLLO DE NUEVOS SISTEMAS. ANÁLISIS Y ESPECIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD

Se determinarán los requerimientos de seguridad que se van a necesitar, dependiendo de la naturaleza del sistema a desarrollar. Se establecerán teniendo en cuenta las leyes, políticas de la organización, las amenazas que puedan afectarle y su posible impacto. Se establecerá, por tanto, el nivel de seguridad necesario para el hardware, software, documentación, etc.

En la fase de diseño se introducirán los controles de seguridad identificados. Esta actividad es primordial en esta fase del proyecto, ya que el coste de implementación de las medidas de seguridad se reduce considerablemente cuando se tienen en cuenta en la fase de diseño. Se llevará a cabo la definición de la arquitectura de seguridad a utilizar en el sistema.

Tras la implementación de los controles de seguridad, y siempre que sea posible, se llevará a cabo un test para comprobar la eficacia de cada uno de ellos.

### 4.2) ADQUISICIÓN DE NUEVOS SISTEMAS/PRODUCTOS

Se determinarán los requerimientos de seguridad que debe cumplir el producto dependiendo de su naturaleza. Los requerimientos se establecerán teniendo en cuenta las leyes, políticas de la organización, las amenazas que puedan afectarle y su posible impacto. Se establecerá, por tanto, el nivel de seguridad necesario para el hardware, software, documentación, etc.

Se llevará a cabo un de test de seguridad sobre el producto para comprobar que se cumplen los requerimientos antes identificados.

<b>NORMATIVA</b>	
<b>ACEPTACIÓN DE NUEVOS SISTEMAS Y PRODUCTOS</b>	Fecha: Octubre 2019
	Edición: 1.0

Se realizará un informe en el que se incluyan los tests de seguridad realizados y el resultado de los mismos.

Cuando el producto no cumpla los requerimientos, sólo se adquirirá cuando se haya aceptado el riesgo (por parte del Responsable de Seguridad y el Responsable del Sistema) o se hayan definido los controles compensatorios que se pueden implementar (y la conveniencia de ello) para mitigarlo.

#### **4.3) APROBACIÓN DEL SISTEMA O APLICACIÓN**

Una vez finalizadas las pruebas, y antes de la compra en su caso, y de la puesta en marcha del sistema, el Responsable del Sistema y el Responsable de Seguridad deberán aprobar la seguridad de éste, teniendo en cuenta los riesgos residuales que hayan resultado.

Esta medida no será necesaria cuando los productos estén certificados.

#### **5) RESPONSABLE DEL CUMPLIMIENTO**

El responsable del cumplimiento de la presente normativa será el Responsable de Seguridad, que podrá delegar en el Responsable del Sistema la verificación y vigilancia de dicho cumplimiento.

#### **6) REFERENCIAS**

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Guía de Seguridad CCN-STIC 821: Normas de Seguridad.
- Guía de Seguridad de las TIC CCN-STIC 883: Guía de Implantación del ENS para Entidades Locales.
- Guía de Seguridad CCN-STIC 804: Guía de Implantación
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- RGPD (UE) 2016/679, del parlamento europeo y del consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de derechos digitales.

#### **7) REGISTROS/ANEXOS**