



NORMATIVA

SEGURIDAD FÍSICA DEL EQUIPAMIENTO

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.06	DOCUMENTO:	NORMATIVA DE SEGURIDAD FÍSICA DEL EQUIPAMIENTO
---------	-------	------------	--

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/>

NORMATIVA	
SEGURIDAD FÍSICA DEL EQUIPAMIENTO	Fecha: Octubre 2019
	Edición: 1.0

1) OBJETO

El objeto de esta normativa es establecer los medios de seguridad física en los activos relacionados con el equipamiento de la entidad o sus instalaciones, siendo de aplicación para el Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento) y todo el personal relacionado con la misma.

2) ALCANCE

Esta normativa será de obligado cumplimiento para todo el personal adscrito al Ayuntamiento, y para aquellos terceros que, de alguna manera, manejen información propia de la entidad en sus equipamientos o instalaciones.

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

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

La responsabilidad de la puesta en marcha de esta normativa, de su cumplimiento y supervisión recaerá en el Responsable de Seguridad del Ayuntamiento.

La responsabilidad de poner en funcionamiento los posibles sistemas de información aplicables en esta norma recaerá en el Responsable de Sistemas del Ayuntamiento.

La implementación, gestión, configuración y mantenimiento de las medidas de seguridad aplicables en esta norma recaerá en el Administrador de seguridad del Ayuntamiento.

4) DESARROLLO NORMATIVO

4.1) EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS

Se deberán ubicar o proteger los equipos para reducir las amenazas y peligros ambientales y oportunidades de acceso no-autorizado. La ubicación de los servidores que almacenan información o son utilizados para explotación de los recursos y servicios del Ayuntamiento deben cumplir una serie de requerimientos tales como una Sala de Seguridad con acceso seguro. En esta sala debe estar terminantemente prohibido realizar actividades como fumar, comer, introducir materiales peligrosos o combustibles, cámaras o cualquier dispositivo de grabación.

4.2) INSTALACIÓN DE SUMINISTRO

Los equipos deberán estar protegidos ante fallos en el suministro de energía u otras anomalías eléctricas. El suministro de energía seguirá en todo momento las especificaciones del fabricante o proveedor de cada uno de los equipos contemplándose las siguientes medidas de control:

- Proveer de iluminación de emergencia en caso de producirse un fallo en el suministro principal de energía.
- Si se detectaran fallos continuos y prolongados del suministro eléctrico, se instalará un generador de respaldo o grupo electrógeno con el correspondiente suministro de combustible para garantizar que dicho generador pueda funcionar por un periodo amplio. Si el encendido del generador no fuera automático, se asegurará que el tiempo de funcionamiento de los SAI (Sistema de Alimentación Ininterrumpida) instalados permita el encendido manual del mismo.
- Revisar y probar periódicamente los generadores para asegurar que funcionan correctamente, en caso de disponer.

4.3) SEGURIDAD DEL CABLEADO

NORMATIVA	
SEGURIDAD FÍSICA DEL EQUIPAMIENTO	Fecha: Octubre 2019
	Edición: 1.0

Todas las instalaciones de cableado de datos deberán realizarse por empresas y personal debidamente certificado o personal técnico propio. Tras la instalación deberán realizarse mediciones y entregarse un certificado como prueba de que se cumplen todos los requisitos para su correcto funcionamiento.

Antes de realizar la instalación de cableado se realizará un estudio previo de trazado. Las canalizaciones de datos deben realizarse independientes de las de cableado de corriente eléctrica y lejos de las zonas con posibles interferencias electromagnéticas. Asimismo, debe evitarse que estén a la vista o fácilmente accesibles a personal no autorizado.

Los armarios de cableado y comunicaciones deben estar en zonas protegidas con acceso controlado, estando éstas controladas en todo momento.

4.4) MANTENIMIENTO DE LOS EQUIPOS

Todos aquellos equipos cuyo coste o necesidad de disponibilidad lo justifique deberán estar protegidos con un contrato de mantenimiento, reparación y/o sustitución en un tiempo máximo determinado con el proveedor o fabricante de los mismos.

Se recomienda el establecimiento de un sistema de renovación o actualización periódica con el proveedor o fabricante.

Sólo el personal autorizado, o bien de mantenimiento del proveedor, podrá manipular físicamente los equipos.

Toda salida de equipamiento para su mantenimiento que sea realizado fuera de las instalaciones del departamento deberá quedar perfectamente registrada. Se eliminará toda información confidencial que pueda contener el equipo, haciendo copia de seguridad si es necesario, previamente a la salida de las instalaciones.

4.5) RETIRADA DE MATERIALES PROPIEDAD DE LA ENTIDAD

Se habilitarán los métodos adecuados para retirar equipos. Se eliminarán tanto del software del inventario de activos como las etiquetas que dispongan.

Este proceso deberá realizarse junto el procedimiento de reutilización o eliminación segura de equipos.

4.6) SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

El uso de equipamiento para la realización de tratamiento de información fuera del ámbito del Ayuntamiento deberá quedar autorizado por el Responsable de Sistemas, informando éste además al Responsable de Seguridad.

En el caso de que se utilice información con datos de carácter personal deberá estar autorizado además por el responsable del Tratamiento afectado o en quién se delegue.

En cualquier caso, la seguridad a aplicar deberá ser equivalente a la proporcionada dentro del departamento para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera del mismo.

4.7) REUTILIZACIÓN O ELIMINACIÓN SEGURA DE EQUIPOS

Se habilitarán los métodos adecuados para eliminar, de forma no recuperable, toda la información sensible o crítica de los equipos o soportes que causen baja y vayan a ser desechados o destinados a otra finalidad. Se eliminarán tanto software como datos o posibles configuraciones lógicas existentes de acuerdo al Procedimiento de Baja de Equipos/Soportes y destrucción de su información.

4.8) POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA

Las principales razones para una política de escritorio y pantalla limpios son:

- Un escritorio limpio puede producir una imagen positiva cuando nuestros la ciudadanía acude al Ayuntamiento.
- Se reduce la amenaza de un incidente de seguridad con la información confidencial estando bajo llave cuando se dejan solos.
- Los documentos sensibles que se dejan al descubierto pueden ser robados.

Se debe aplicar las directrices de seguridad a todo el personal del Ayuntamiento, teniendo en cuenta las siguientes acciones:

- Bloquear el PC/Portátil cuando se ausente, incluso en muy breves periodos de tiempo.

NORMATIVA	
SEGURIDAD FÍSICA DEL EQUIPAMIENTO	Fecha: Octubre 2019
	Edición: 1.0

- Siempre limpie su área de trabajo antes de salir durante periodos más largos de tiempo.
- Utilizar las destructoras de papel para los documentos sensibles cuando ya no son necesarios.
- Cierre con llave su escritorio y archivadores al final de la jornada.
- Tratar a los dispositivos de almacenamiento masivo como CD-ROM, DVD o unidades USB como sensibles y guardarlos en un cajón cerrado con llave.
- En las salas de reuniones borre las pizarras al finalizar la reunión y nunca deje papeles en la sala.
- No se deben utilizar post-its visibles como recordatorios o carteles que contengan información sensible.

4.9) TRASLADO DE EQUIPOS

Antes de realizar el traslado de equipos se tomarán las adecuadas medidas de protección contra golpes, utilizando para ello embalajes con protección, identificación exterior de "muy frágil", transporte adecuado, etc.

Se respetarán en todo momento las instrucciones del fabricante respecto del cuidado del equipo, así como se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Ayuntamiento cuando sea conveniente.

Los dispositivos portátiles, cuando estén fuera de las instalaciones del Ayuntamiento o en lugares de acceso libre, no se abandonará en ningún momento.

Cuando la salida de los equipos sea por motivos de mantenimiento, se eliminará previamente toda su información almacenada, a menos que los discos se encuentren cifrados.

5) RESPONSABLE DEL CUMPLIMIENTO

El responsable de seguridad del Ayuntamiento será la persona responsable del control de dicha normativa y de verificar que se cumplen las medidas establecidas.

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