NORMATIVA DE SEGURIDAD DE LOS EQUIPOS

Ayuntamiento de Martos

INFORMACIÓN DE USO INTERNO

DE ACCESO INTERNO AL PERSONAL DEL

AYUNTAMIENTO DE MARTOS

Cuadro de Control

Título:	Normativa de seguridad de los equipos		
Tipo de documento:	Normativa		
Nombre del Fichero:	NOS-007 Normativa de Seguridad de los Equipos.docx		
Clasificación:	Uso Interno		
Estado:	Documento		
Autor:	Consultor Externo		
Versión:	1.0	**Fecha:**	01-07-2016

Revisión y aprobación			
Revisado por:	Responsable de Seguridad		
Aprobado por:	Comité de Seguridad	**Fecha:**	22-03-2017

Lista de distribución	

Control de Cambios

Versión	Fecha	Autor	Descripción del Cambio

INDICE

1. OBJETO

El objeto del presente documento es la definición de la normativa aplicable a la seguridad de los equipos de Ayuntamiento de Martos (en adelante la Organización), dentro del alcance señalado en el Esquema Nacional de Seguridad.

Se ha implantado la siguiente normativa atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de la Organización, que resulten de la aplicación de las previsiones contempladas en los Anexos I y II 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 (ENS).

2. ALCANCE

Esta normativa es de aplicación a todo el ámbito de actuación de la Organización, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de la Organización.

La presente normativa es de aplicación a todas las instalaciones de la Organización en las que se desarrollen actividades, y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Organización, especialmente, el Responsable de Seguridad, los responsables de Sistemas de Información y los propios usuarios, como actores ambos, en sus respectivas competencias, de la implantación técnica de dicha normativa, y del cumplimiento de la misma, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información de la Organización.

3. DEFINICIONES Y SIGLAS

ENS	Esquema Nacional de Seguridad.
Recurso/Activo	Cualquier elemento que tiene valor para la Organización (conjunto de datos estructurados, bases de datos, software, sistemas, personas, aplicaciones, documentación, instalaciones, imagen corporativa, etc.) y que soporta un determinado proceso de negocio.
Servicio	Cada una de las funciones lógicas completas prestadas por un equipo informático.
Usuario	Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

4. LEGISLACIÓN Y NORMATIVA APLICABLE

Las referencias tenidas en cuenta para la redacción de esta normativa han sido:

- 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.
- Ley 15/1999, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD.
- Documentos y Guías CCN-STIC, en especial la Guía "CCN-STIC-821 Normas de seguridad en el ENS" y el Anexo I de la Guía "CCN-STIC-822" – Procedimientos de seguridad en el ENS".

5. CUERPO DEL DOCUMENTO

5.1. Emplazamiento y protección de equipos

Los sistemas de información y comunicaciones deben estar físicamente protegidos frente a posibles amenazas del entorno para evitar accesos no autorizados o pérdidas u otros daños en los sistemas que puedan afectar a la integridad, confidencialidad o disponibilidad de la información.

La ubicación física de los equipos debe cumplir una serie de requerimientos que permitan:

- Garantizar el buen funcionamiento de los mismos.
- Reducir la posible existencia de incidentes que puedan comprometer su seguridad.
- Que sólo pueda acceder personal debidamente autorizado.

Las áreas seguras deberán disponer de medidas adicionales de seguridad como las siguientes:

- Techos y suelos falsos.
- Sistema de control de acceso (Ej: tarjetas RFID).
- Sistemas automáticos de detección y protección contra daños por fuego, agua, temperatura, humedad, fallos del suministro eléctrico o accesos no autorizados.

5.2. Instalaciones de suministro

Las instalaciones de suministro deberán disponer de medidas como las siguientes:

- Los sistemas de información y comunicaciones deberán están protegidos contra fallos relativos al suministro (Ej: agua, electricidad, etc.).

- Todos los equipos de suministros de agua, electricidad, aire acondicionado, etc. deben ser regularmente revisados y probados por el proveedor de mantenimiento correspondiente para asegurarse que cumplen con las necesidades de suministro

requeridas así como con las especificaciones del fabricante, y de esta forma reducir el riesgo de fallos por fallo o mal funcionamiento.

- Las especificaciones de los equipos deberán cumplir con las especificaciones establecidas en la legalidad vigente y ser adecuados a las necesidades de los equipos a los que sirven de apoyo.

- Si fuera necesario se instalarán sistemas de alarma que detectarán fallos de funcionamiento en los equipos de suministros esenciales.

5.3. Seguridad del cableado

La infraestructura del cableado eléctrico y de comunicaciones deberá estar protegida por medio de medidas de seguridad como las siguientes:

- Se utilizarán falsos suelos y techos, y sus correspondientes canaletas para dotarse de un cableado estructurado dentro de las instalaciones.

- Los cables y equipos de telecomunicaciones y alimentación deberán estar bien identificados, etiquetados y listados para evitar errores en la gestión o manipulación de los mismos.

- El cableado de red deberá estar protegido contra interceptación no autorizada o daño (Ej: mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas).

- Los cables de energía estarán separados de los cables de comunicaciones para evitar interferencias.

- Existirán mecanismos de control de acceso a las salas donde se gestionan los sistemas de cableado de manera que se restrinja el acceso al personal debidamente autorizado.

5.4. Mantenimiento de equipos

El mantenimiento de los equipos deberá realizarse siguiendo medidas de seguridad como las siguientes:

- El mantenimiento de los equipos se deber realizar por personal debidamente autorizado y capacitado, siguiendo en todo caso las recomendaciones del fabricante.

- Dentro del inventario de activos de información de la Organización deberán estar relacionados los proveedores de mantenimiento, el servicio que prestan y las personas de contacto.
- Se debe guardar registro documental de todas las acciones correctivas o preventivas de mantenimiento dentro de los equipos, así como cualquier fallo real o sospechado de los mismos.
- Se deberán adoptar medidas adecuadas de protección de los equipos cuando estos salgan fuera de las instalaciones para su mantenimiento. En caso de que el equipo contenga información o datos de carácter personal, el equipo no debe salir de las instalaciones o, en todo caso, deben adoptarse medidas para proteger la información contenida en el mismo (ej: encriptación)

5.5. Seguridad de los equipos fuera de las dependencias de la Organización

Cuando los equipos deban ser utilizados de forma puntual, periódica o permanente fuera de las oficinas de la Organización, se habrán de contemplar medidas de seguridad como las siguientes:

- La salida de equipos fuera de las dependencias de la Organización deberá estar debidamente autorizada por el responsable del usuario o propietario de la información, conforme al procedimiento que se haya definido.
- Los equipos portátiles fuera de las dependencias de la Organización deberán estar controlados en todo momento. Durante los viajes deberán ser facturados como equipaje de mano.
- Se deben establecer medidas de seguridad basadas en técnicas de cifrado que garanticen la confidencialidad de la información de los equipos en caso de que el equipo contenga información confidencial.
- Los propietarios de los activos deberán observar las instrucciones del fabricante en lo referente a la protección de los equipos contra diversas amenazas como campos electromagnéticos.
- Las actividades de teletrabajo estarán reguladas de acuerdo a los controles establecidos al efecto. Los controles establecidos en estos sistemas estarán basados en una

evaluación previa de los riesgos y se aplicarán aquellos controles que sean convenientes. No salen equipos de las instalaciones del Ayuntamiento.

5.6. Reutilización o retirada segura de dispositivos de almacenamiento

En la reutilización o retirada de dispositivos de almacenamiento, deberán tenerse en cuenta las siguientes medidas de seguridad:

- Todo dispositivo que contenga *información confidencial* deberá ser destruido físicamente o deberá realizarse un borrado seguro antes de ser eliminado o reutilizado.
- La eliminación o borrado de soportes con información deberá estar autorizado por el responsable del dispositivo o propietario de la información.
- En caso de que empresas externas participen en las labores de eliminación o mantenimiento de equipos, deberán comprometerse contractualmente:
    - A no consultar, almacenar, o distribuir la información confidencial contenida en los equipos que quedan bajo su custodia.
    - A emitir un certificado conforme han destruido el dispositivo, cuando se les haya requerido este tipo de servicios.

6. ANEXOS/FORMATOS

N/A.

7. REFERENCIAS