NORMATIVA DE CONTROL DE CONFORMIDAD LEGAL

Ayuntamiento de Martos

INFORMACIÓN DE USO INTERNO

DE ACCESO INTERNO AL PERSONAL DEL

AYUNTAMIENTO DE MARTOS

Cuadro de Control

Título:	Normativa de seguridad conformidad legal		
Tipo de documento:	Normativa		
Nombre del Fichero:	NOS-004 Normativa de Conformidad Legal.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 Conformidad Legal en 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 especificación de la normativa de control de acceso, 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.
LOPD	Ley Orgánica de Protección de Datos.
Dato de carácter personal	Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

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. Introducción

Los principales objetivos de este documento son:

- Identificar la legislación y normativa que la Organización ha de observar en el desarrollo de sus procesos de negocio en relación a la gestión de la seguridad de la información tratada en sus sistemas de información, así como dotar de los medios necesarios para el cumplimiento de dicha normativa y/o legislación identificada**.**
- Establecer y detallar las actividades necesarias para la revisión y mejora de las políticas de seguridad, normativa y procedimientos desarrollados.
- Evitar un posible incumplimiento de cualquier requerimiento legal, contractual o reglamentario que pueda ser aplicable a la Organización.

Es responsabilidad de los diferentes Departamentos y/o Áreas de la Organización la implantación de las medidas descritas en la presente Normativa.

5.2. Identificación de la legislación aplicable

Se debe identificar y documentar de forma explícita todos los requerimientos legales, regulatorios y contractuales que resulten aplicables a cada sistema de información, así como los controles, medidas y responsabilidades específicos para su cumplimiento. Estos requerimientos deben ser comunicados a las personas responsables de proceder a la implantación de los mismos.

5.3. Protección de datos de carácter personal

La Organización dentro del marco de sus actividades, trata información de carácter personal de empleados y de terceros (Ej: proveedores, colaboradores, etc.) y, por lo tanto, es Responsable del Fichero y/o Encargado del Tratamiento de estos datos de carácter personal.

La Organización, como Responsable del Fichero y/o Encargado del Tratamiento, deberá cumplir con las obligaciones que la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), impone a esta figura como son los deberes de información y de recabar el consentimiento del afectado para el tratamiento y cesión de sus datos de carácter personal o la facilitación de los derechos de acceso, rectificación, cancelación y oposición de los afectados.

En virtud de esta normativa, La Organización deberá declarar los ficheros que contengan datos de carácter personal ante el Registro General de Protección de Datos.

Por otra parte, se deberán implantar las medidas de seguridad de índole técnica y organizativa establecidas por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

La Organización deberá desarrollar uno o varios Documentos de Seguridad con el objetivo de establecer las medidas de índole técnica y organizativa acordes al nivel de los ficheros y la normativa vigente. Estos Documentos de Seguridad son de obligado cumplimiento para toda persona con acceso a datos de carácter personal.

Todos los ficheros que contengan datos de carácter personal deberán disponer de las medidas de seguridad que les correspondan dependiendo del tipo de datos, nivel de protección (básico, medio y/o alto) y conforme al ámbito de aplicación definido en los Documentos de Seguridad.

Todo usuario debe atenerse a las obligaciones definidas en La Organización, dependiendo de las funciones propias de su trabajo, debiendo tener acceso a la información exclusivamente necesaria para el desarrollo de sus funciones.

La Organización debe nombrar un Responsable de Seguridad LOPD al que se le asignen las funciones de definición, implantación y supervisión de las normas y procedimientos que afecten a los ficheros que contengan datos de carácter personal tratados por la Organización, así como los Documentos de Seguridad desarrollados para el tratamiento de este tipo de datos.

5.4. Propiedad intelectual

Dentro de las actividades de la Organización deben adoptarse diversas **medidas** para la adecuada protección de los activos de propiedad intelectual e industrial como las siguientes:

- Identificación de los derechos propios y de terceros en referencia a marcas e invenciones propias, obras originales y el alcance de los derechos generados o adquiridos y cesiones de ellos. Esto afecta a los derechos morales y de explotación generados sobre los libros, bases de datos, los derechos sobre marcas de la organización, software, etc.
- Clasificación y etiquetado de los activos susceptibles de protección.
- Adquisición de software a proveedores de reputada solvencia profesional y siempre bajo licencia legalmente adquirida y comprensiva de todos los usos a los que el software es destinado, todo ello incluido dentro de los respectivos contratos de licencia.
- Controles para la copia o instalación de software bajo licencia en los sistemas de la Organización.
- Revisiones periódicas para verificar que no ha sido instalado ningún software sin permiso de la Organización y que el número de instalaciones y en su caso usuarios, es acorde al número de licencias adquiridas.

- Celebración y archivo de contratos con cláusulas específicas sobre titularidad, transferencia o licencia de uso de los activos
- Registro de derechos dentro los registros oficiales de patentes y marcas y registros de propiedad intelectual
- Dentro de la normativa de Buen Uso de los Sistemas de Información se debe hacer referencia a la prohibición de los usuarios y administradores de sistemas de copiar o instalar copias ilegales de software dentro de los puestos o servidores de la Organización.
- Inclusión de disclaimers necesarios para la protección de la propiedad intelectual e industrial en el entorno web.

5.5. Recogida de evidencias

Cuando el seguimiento de una actuación contra una persona u organización, tras la ocurrencia de una incidencia grave o desastre, conlleve la interposición de acciones legales (civiles o penales), disciplinarias o de responsabilidad contractual, las evidencias relacionadas con la incidencia deben ser recabadas, archivadas y presentadas de acuerdo a legislación aplicable en cada caso para la admisibilidad de pruebas dentro del orden jurisdiccional aplicable o de los procesos contractualmente definidos.

Con el fin de asegurar y preservar la admisibilidad de las evidencias en un proceso judicial, estas deben recabarse de conformidad con los siguientes principios:

- Legitimidad: La evidencia debe poder ser usada y admitida en un proceso. Es imprescindible la utilización del procedimiento para la correcta extracción y custodia de las evidencias.
- Autenticidad: Es necesario garantizar la existencia de una relación directa entre la evidencia y la incidencia que se haya producido.
- Integridad: Con objeto de salvaguardar la admisibilidad de la evidencia es necesario durante todo el procedimiento de custodia preservar la integridad de los medios de almacenamiento originales.
- Claridad: Las evidencias electrónicas se deben presentar de forma comprensible.

Se deberán implantar las medidas de seguridad necesarias en el caso de realización de actividades ilícitas por parte de personal interno, con el fin de prevenir actuaciones de destrucción de pruebas o de represalias del personal investigado contra la Organización.

5.6. Protección de los registros

La Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante, LEC), establece las condiciones de admisibilidad de las pruebas en sede judicial, condiciones que pueden ser extrapoladas a otros ámbitos como las reclamaciones en actos de conciliación, arbitraje, etc. La LEC exige, para que las pruebas sean admitidas en Derecho que:

- La prueba consista en uno de los medios admitidos en Derecho para la práctica de la prueba y que se recogen el artículo 299 LEC.1
- Se garantice la integridad y exactitud de las pruebas presentadas para que las mismas puedan ser vinculantes para el juez. Para ello han de cumplir los requisitos establecidos en los artículos 314 y siguientes LEC.

La Organización deberá tener presente esta legislación a la hora de llevar a cabo las actividades de recolección y custodia de pruebas.

Se deberán proteger los registros importantes frente a su pérdida, destrucción y/o falsificación.

Estos registros deberán ser almacenados de forma segura, tanto para cumplir los requerimientos legales, como para soportar actividades esenciales del negocio. El almacenamiento de registros en soportes de información debe ajustarse a lo establecido en la Normativa de Gestión de Soportes de la Organización. El sistema de almacenamiento y manipulación debe asegurar la identificación clara de los registros y de su período de retención, en base a lo establecido en la legislación o las regulaciones nacionales, autonómicas o comunitarias aplicables. Este sistema debe garantizar la destrucción segura de los registros después de un período adecuado en caso de no ser necesarios para la Organización.

Para conseguir la admisibilidad de una prueba, previamente debe justificarse la necesidad de disponer de dicha información ante los servicios jurídicos de la Organización y ésta debe aprobarlo formalmente. Para asegurar una adecuada gestión y cumplimiento legal de cualquier proceso de monitorización implantado se debe informar previamente por escrito de la intención de proceder, motivación, identidad de las personas.

5.7. Responsabilidad por incumplimiento

Se considera un **incumplimiento grave o muy grave**, en función de las consecuencias y el ánimo del personal infractor, la inobservancia de las normativas y procedimientos establecidos por la Organización.

Se considera un **incumplimiento del Deber de Secreto y Confidencialidad** de la información, la acción de transmitir información contenida en los sistemas de información la Organización a terceros no autorizados, así como permitir su acceso a los mismos de forma directa o indirecta.

La valoración de las **consecuencias del incumplimiento** para el infractor, y las medidas a adoptar serán tomadas en base al Convenio Colectivo del trabajador o a las cláusulas de responsabilidad subsidiaria que se hayan firmado con la empresa proveedora del servicio, para el caso personal externo.

6. ANEXOS/FORMATOS

N/A

7. REFERENCIAS

- NOS – 005 Documento de Seguridad LOPD.