NORMATIVA DE GESTIÓN DE INCIDENCIAS

INFORMACIÓN DE USO INTERNO

DE ACCESO INTERNO AL PERSONAL DEL

AYUNTAMIENTO DE MARTOS

Cuadro de Control

Título:	Normativa de gestión de incidencias		
Tipo de documento:	Normativa		
Nombre del Fichero:	NOS-009 Normativa de Gestión de Incidencias.docx		
Clasificación:	Uso Interno		
Estado:	Documento		
Autor:	Consultor Externo		
Versión:	1.0	**Fecha:**	01-09-2016

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 Gestión de Incidencias 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 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.
Incidencia	Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de negocio y amenazan la seguridad de la información.
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

En relación a la gestión de incidencias, la Organización deberá:

- Desarrollar un Procedimiento de Gestión de Incidencias en el que se detallen los pasos a seguir para la notificación, valoración y respuesta ante las incidencias y debilidades de seguridad de la información.
- Implantar una plataforma o sistema para la gestión de incidencias que permita su recogida, registro y gestión conforme al Procedimiento de Gestión de Incidencias. Este sistema permitirá garantizar una respuesta adecuada, organizada y eficaz a las incidencias que se puedan producir, mejorando su control e impidiendo que alguna incidencia pueda quedar sin respuesta.
- Gestionar las incidencias de seguridad de la información que transciendan los límites de la Organización. En base a ello, se debería incluir, dentro de los Contratos de Prestación de Servicios con terceros (Ej: proveedores de software, comunicaciones u otros servicios), cláusulas donde se establezcan los medios de comunicación y respuesta de incidentes y debilidades de seguridad, de forma tal forma que se pueda proporcionar una respuesta coordinada y una distribución de información que permita una eficaz gestión y resolución de las mismas.

5.1. Notificación

Cuando se produzca una incidencia de seguridad de la información, habrá que tener en cuenta las siguientes consideraciones:

- Todos los usuarios (tanto internos como externos a la Organización) deben ser informados y concienciados sobre la responsabilidad de notificar las incidencias de seguridad de forma inmediata, así como sobre los procedimientos y canales de comunicación disponibles para ello.
- Cualquier usuario que tenga conocimiento de una incidencia o debilidad de seguridad deberá notificarla de forma inmediata a través de los canales y destinatarios establecidos por la Organización.

- Adicionalmente a la notificación de incidencias y debilidades de seguridad por parte de los usuarios, existen otras fuentes para la detección de incidencias de seguridad, como puede ser la monitorización de los sistemas de información, las alertas del sistema y otras vulnerabilidades que puedan ser detectadas dentro de los sistemas de información de la Organización.
- Los canales establecidos y el sistema de notificación de incidencias deben presentar el formato adecuado para incluir toda la información necesaria para facilitar la gestión y trazabilidad de la incidencia, sirviendo de herramienta de apoyo para el desarrollo de las actividades de reporte y resolución de incidencias.

5.2. Registro

En el registro de las incidencias de seguridad, habrá que tener en cuenta las siguientes consideraciones

- Todas las incidencias de seguridad deben tener un número único que permita su identificación y trazabilidad a lo largo del proceso de gestión. Este número facilitará tanto el almacenamiento y registro de la incidencia como la búsqueda de incidencias.
- Toda la información relacionada con las causas, tratamiento y resolución de incidencias de seguridad debe estar correctamente registrada junto con las evidencias, logs y trazas que hayan sido obtenidos sobre la misma.
- La información registrada debe ser almacenada y protegida de forma que no pueda ser modificada (incluso por los administradores del sistema).
- El registro de los logs y trazas, así como otros registros y evidencias adjuntos a la incidencia deben cumplir con los requerimientos legales, contractuales y los relativos la normativa interna de la Organización.
- En caso de que la incidencia afecte a ficheros que contengan datos de carácter personal, se debe garantizar que el Registro de Incidencias contiene, al menos, los siguientes campos de información:
  - Tipo de incidencia.
  - Momento en que se ha producido, o en su caso detectado.
  - Persona que realiza la notificación.
  - Persona que recibe la notificación.
  - Persona a quién se comunica la notificación.
  - Efectos de la Incidencia.
  - Medidas correctoras aplicadas.
  - Persona que ejecutó el proceso de recuperación de datos, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente (esto aplicará cuando la incidencia afecte a datos de nivel medio o alto).

5.3. Gestión

En la gestión de las incidencias de seguridad, habrá que tener en cuenta las siguientes consideraciones:

- Las incidencias deben ser clasificadas de acuerdo a los criterios de clasificación que se consideren más adecuados para la Organización, para permitir ofrecer la respuesta más adecuada en cada caso.
- Los responsables de la gestión de las incidencias deberán recabar de los usuarios toda la información necesaria para gestionar la incidencia.
- Deben establecerse las responsabilidades y procesos necesarios para garantizar una repuesta rápida, efectiva y ordenada a las incidencias y debilidades de seguridad.
- En determinados casos será necesario adoptar medidas para la contención de la incidencia que eviten daños mayores. En aquellos casos en que la adopción de estas medidas de contención conlleve una paralización de los sistemas de usuario se debe informar con la mayor antelación posible a los usuarios afectados mediante los canales de comunicación que hayan sido formalmente establecido.
- En los casos de incidencias graves o en las que sea necesario activar el Plan de Contingencias, las incidencias deben ser comunicadas de forma inmediata al Responsable de Seguridad, que debe decidir las acciones a adoptar en cada caso (entre ellas la activación del Plan de Contingencias o la convocatoria del Comité de Seguridad para informar de los hechos).
- La resolución de la incidencia debería ser comunicada a los usuarios que la han reportado o que fueron afectados durante su gestión, para proceder al cierre definitivo de la misma.

5.4. Aprendizaje

En el aprendizaje de las incidencias de seguridad, habrá que tener en cuenta las siguientes consideraciones:

- La gestión y registro de las incidencias de seguridad deben ser revisados periódicamente, con objeto de identificar la causa raíz o problema subyacente de las mismas y las soluciones adoptadas, identificar posibles deficiencias de seguridad o proponer las soluciones más adecuadas. Se debería revisar y elaborar un informe donde se establezcan las conclusiones de las revisiones realizadas.
- La evaluación de las incidencias de seguridad de la información puede indicar la necesidad de aumentar o añadir nuevos controles que limiten la frecuencia, daño o coste

de futuras incidencias o pueden ser tenidos en cuenta como fuente de información dentro de los procesos de revisión de las políticas de seguridad.

- El responsable y los operadores de incidencias, así como en su caso los usuarios afectados deben ser formados y prevenidos sobre la base de conocimiento adquirido, y sobre posibles incidencias que puedan repetirse en el futuro para prevenir que estas vuelvan a producirse. De este modo, salvando los aspectos de confidencialidad propios de la gestión de incidencias, las incidencias deben ser utilizadas dentro de los procesos de mejora continua como ejemplo para la concienciación y formación de los usuarios y administradores del sistema ante incidencias similares de modo que puedan prevenirse su reaparición en el futuro.

5.5. Recopilación de evidencias

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

Con el fin de asegurar y preservar la admisibilidad de las evidencias en un proceso judicial se han de tener en cuenta las siguientes consideraciones:

- Se debe desarrollar un procedimiento interno de recolección de evidencias que determine los pasos a seguir por la Organización para la recolección y presentación de evidencias que tienen como fin facilitar el desarrollo y defensa de las acciones disciplinarias, judiciales o de reclamación de responsabilidades que puedan emprenderse por la Organización. Este procedimiento debe contener:
    - Las pautas más importantes a seguir tanto en la recogida de las evidencias, estableciendo los controles necesarios para la trazabilidad de las actuaciones realizadas en esta etapa, así como los controles a implementar dentro del proceso posterior de custodia de las evidencias de tal manera que se pueda contrastar la integridad y completitud de las mismas a la hora de su aportación como prueba en los procesos correspondientes.
    - Las medidas de seguridad a adoptar en el caso de la aparición de actividades ilícitas por parte de personal interno y de cara a prevenir actuaciones de destrucción de pruebas o de represalias del personal investigado contra la Organización.

- Se debería disponer de herramientas de monitorización y gestión y registro de evidencias que cuentan con los requisitos necesarios para monitorizar, registrar y almacenar toda actividad dentro de los sistemas de información de la Organización desde el primer momento en que una evidencia se genera, permitiendo así establecer una cadena de custodia que garantice la integridad y completitud de las evidencias recogidas de cara a posibles procesos que puedan surgir posteriormente. No obstante lo anterior, la Organización también podrá solicitar los servicios de consultores de seguridad y asesores legales expertos en la materia, que le asesoren de cara a poder llevar una investigación del hecho de forma eficaz, así como para facilitar la admisibilidad de las evidencias provistas dentro de las diferentes jurisdicciones aplicables.

6. ANEXOS/FORMATOS

N/A.

7. REFERENCIAS