NORMATIVA DE CONTROL DE SEGURIDAD EN LA OPERATIVA

INFORMACIÓN DE USO INTERNO

DE ACCESO INTERNO AL PERSONAL DEL

AYUNTAMIENTO DE MARTOS

Cuadro de Control

Título:	Normativa de seguridad en la operativa		
Tipo de documento:	Normativa		
Nombre del Fichero:	NOS-006 Normativa de Seguridad en la Operativa.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 la Operativa de Seguridad en el 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.
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. Introducción

El siguiente documento establece las normas básicas a seguir en la operativa de los sistemas de información.

5.2. Segregación de tareas

Las principales tareas y responsabilidades dentro de la Organización deben estar segregadas a fin de evitar un riesgo de mal uso, deliberado o intencionado, de sus activos de información, de tal forma que una misma persona no pueda acceder, modificar y usar activos sin previa autorización o monitorización de su actividad. Por todo ello será necesario adoptar medidas de seguridad como las siguientes:

- Segregar siempre y cuando sean posible las tareas de autorización y ejecución a fin evitar accesos o cambios no autorizados sobre los sistemas de información de la Organización.

- Segregar las tareas de desarrollo y operación.

- El rol de Responsable de Sistemas de acuerdo al ENS no podrá coincidir con el Responsable de Información, con el Responsable de Servicio ni con el Responsable de Seguridad Corporativa o de la Información.

- Se deben monitorizar las actividades de los usuarios, administradores y operadores de sistemas mediante la elaboración de procedimientos asociados para la gestión de la monitorización, así como la activación de pistas o registros de auditoría.

5.3. Separación de entornos

Los entornos de desarrollo, prueba y producción de los sistemas de la Organización deben estar separados para reducir los riesgos de accesos no autorizados o cambios en los sistemas en producción. Además, se deberán adoptar medidas de seguridad como las siguientes

- El software en desarrollo y el software de producción debe alojarse en diferentes sistemas o servidores y en diferentes dominios o directorios.

- Las herramientas de compilación, edición y otras utilidades de desarrollo no deben estar accesibles desde los sistemas de producción cuando no se necesiten.

- Se deberán definir y documentar reglas para la migración del software del entorno de desarrollo al entorno de producción.

- Se establecerán entornos de preproducción además de entornos de pruebas en virtud de la criticidad del sistema que se ponga en producción. El entorno de preproducción ha de emular el entorno de producción lo más ajustadamente posible

- Se establecerán diferentes identificadores de usuario para diferenciar los entornos de pruebas y producción a fin de reducir el riesgo de error.

- Para acceder al entorno de pruebas es preferible autenticarse con un usuario diferente al de desarrollo para reducir de esta manera el riesgo de error.

- Se evitará el empleo de *datos sensibles* dentro de los entornos de pruebas. En todo caso, si se utilizan datos operativos (reales) con fines de prueba, se aplicarán las siguientes directrices para protegerlos:

    - Los datos empleados en la fase de pruebas deberán contener los mismos controles de seguridad que los datos en producción.

    - El procedimiento de asignación de permisos de acceso aplicable a los sistemas en producción también debería aplicarse en la fase de pruebas

    - Debería obtenerse una autorización independiente cada vez que se copie información operativa a un sistema de aplicación de prueba.

    - Los datos de prueba deberán ser eliminados del entorno de pruebas cuando éstas se hayan completado.

(No obstante, en el Ayuntamiento no se realiza desarrollo por lo que no existe un entorno de pruebas)

5.4. Gestión de la capacidad

En relación a la gestión de la capacidad, habrá que tener en cuenta medidas de seguridad como las siguientes:

- El uso de los recursos internos de la Organización y el uso que pueden hacer terceros debe ser monitorizado y medido para poder establecer las necesidades actuales y futuras de capacidad de los sistemas.

- Las proyecciones de los requisitos de capacidad de los sistemas deben tener en cuenta las especificaciones de los nuevos sistemas necesarios dentro de la Organización, así como aquellos requerimientos derivados del uso de recursos por parte de terceros (Ej: clientes o proveedores).
- Se debe desarrollar un procedimiento de monitorización a través del cual se establezcan:
  - Que recursos y/o actividades se deben monitorizar.
  - Quienes realizarán las actividades de monitorización.
  - Con qué periodicidad se revisarán los resultados de estas actividades.

- Se deben implantar mecanismos de monitorización que permitan controlar la capacidad disponible de los sistemas en todo momento, detectar problemas a su debido tiempo y poder tener un margen de actuación para resolver los posibles problemas que puedan ir apareciendo sin comprometer la disponibilidad del sistema.

5.5. Aceptación del sistema

Se deben establecer los criterios de aceptación de nuevos sistemas, en los que se tengan en cuenta medidas de seguridad como las siguientes:

- Disponer de un **inventario de recursos hardware y software** homologado por la Organización, que contenga, al menos, la siguiente información:
  - Nombre del recurso.
  - Marca, modelo.
  - Características técnicas.
  - Manuales.
  - Responsables (del recurso, de la operación y del mantenimiento).
  - Usuarios.
  - Software instalado y versión.
  - Configuración de seguridad.
  - Operaciones de mantenimiento realizadas (Ej: actualizaciones, modificaciones, etc.).

- Disponer de un **proceso de homologación de nuevos recursos**, en el que se contemplen aspectos como los siguientes:
  - La realización de un análisis de los requerimientos funcionales (será importante asegurarse de que las necesidades se expresen en términos puramente funcionales y no en términos de soluciones o términos técnicos, entendiendo, por necesidad funcional, aquella que tiene el usuario o cliente para el normal desarrollo de su trabajo o una mejora en el mismo, independientemente de la tecnología o soluciones).
  - La realización de un análisis de los requerimientos técnicos (Ej: rendimiento, fiabilidad, seguridad, portabilidad, etc.).

- La selección de un proveedor en el que se tengan en cuenta aspectos como precio, calidad, garantía, solvencia, nivel de servicio, certificaciones que posee, prestigio, experiencia.
- La selección de recursos homologados, certificados o que hayan sido evaluados en base a normas europeas o internacionales (Ej: ISO/IEC 15408 Common Criteria.
- La realización de pruebas reales con el fin de:
  - Comprobar que el dispositivo funciona correctamente dentro de las plataformas corporativas para las que ha sido seleccionado.
  - Comprobar que cubre los requerimientos funcionales deseados, evaluar si se deben actualizar.
  - Comprobar que se cumplen los requerimientos técnicos esperados y las descritas por el fabricante.
  - Elaborar propuesta de guía de configuración (si es necesario) y/o propuesta de modificación de la documentación existente implicada.
  - Elaborar propuesta de guía de usuario (si es necesario) y/o propuesta de modificación de la existente
- La formación previa del personal que deberá trabajar con el nuevo recurso.
- El almacenamiento y difusión de la documentación del nuevo recurso (Ej: manual de configuración o usuario), entre las personas afectadas (Ej: administradores, operadores, etc.).
- La actualización de la documentación, en concreto del inventario de recursos, así como aquellos otros documentos que se pueden ver afectados como el Plan de Continuidad de Negocio.
- La aceptación formal por parte del responsable correspondiente antes del paso a producción.

5.6. Configuración segura

Deben establecerse las **pautas para la configuración segura de sistemas y recursos**, de forma que se detallen las actividades previas a la puesta en producción y se garantice la protección previa del equipamiento y el deshabilitado de todas las opciones y servicios que no sean necesarios.

Con el fin de garantizar dicha puesta en marcha, se deberá elaborar un ***checklist* de verificaciones y bastionado de equipos**, el cual pueda servir de guía y normalización del conjunto de aspectos a revisar, siguiendo en todo caso pautas como las siguientes:

- Todo recurso previo a su puesta en servicio debe disponer de mecanismos de control de acceso que requiera la identificación y autenticación de usuarios.
- Todo recurso previo a su puesta en servicio debe disponer de mecanismos de protección de los archivos de sistema y configuración que puedan comprometer la seguridad del equipo.

- Deben asignarse sólo los mínimos privilegios al personal técnico que requiera acceso para gestión, mantenimiento u operación del equipo.
- Deben ser revisadas y deshabilitadas las cuentas y contraseñas del sistema por defecto, así como de servicios, opciones y puertos que no vayan a ser empleados.

Debe existir un ***checklist* para cada grupo de activos** (equipos de usuario, servidores, bases de datos, dispositivos de comunicaciones, dispositivos de almacenamiento, etc.), cada uno de ellos debería validar al menos lo siguiente:

- Incluir el equipo en el dominio, de tal forma que se apliquen todas las directivas de dominio a nivel de cuenta de equipo y usuario: caducidad y otras opciones de seguridad de contraseñas, impedir acceso a zonas administrativas del equipo (panel de control, red, etc.), bloqueo de pantalla por contraseña tras un tiempo de inactividad…
- Habilitar las actualizaciones críticas y de seguridad a nivel de sistema operativo y aplicativos instalados (suite ofimática, lector PDF, navegadores, cliente de correo electrónico, cliente java, etc.). Realizar las actualizaciones correspondientes antes de la puesta del equipo en producción.
- Instalar y configurar el antivirus.
- Deshabilitar o cambiar cuentas y contraseñas por defecto.
- Deshabilitar servicios, opciones y puertos no necesarios.
- En su caso, configurar Firewall.
- En su caso, configurar Proxy.
- En su caso, configurar acceso remoto por VPN segura.

En el caso de que se decida **no aplicar todas las restricciones** y opciones de bastionado sobre el equipo, debe quedar documentado asumiendo el nivel de riesgo derivado de dicha decisión.

5.7. Gestión de cambios

En el ámbito de la seguridad de la información el concepto de cambio puede ser aplicado a cualquier elemento de la Organización (procesos de negocio, objetivos, personas, infraestructura, instalaciones, estructura organizativa, proveedores, suministros, metodologías, normativa, etc.). En el presente caso, entenderemos como cambio cualquier modificación en los sistemas de información y, en concreto, en cualquier de los siguientes elementos:

- Cambios en la topología de red.
- Cambios en los sistemas de información (hardware y software).
- Cambios en la configuración.
- Cambio en los procedimientos operativos de soporte.

Los cambios en los sistemas de información de la Organización deben ser gestionados mediante procesos formalmente establecidos y revisados. El control inadecuado de los cambios en los sistemas es una causa común de fallo tanto en el sistema como en la seguridad, por lo que será necesario adoptar medidas de seguridad como las siguientes:

- Establecer las **funciones y responsabilidades** para garantizar el control satisfactorio de todos los cambios en los sistemas y aplicaciones
- Establecer un **proceso formal de actuación** que tengan en cuenta aspectos como los siguientes:
    - El inicio del proceso mediante una solicitud formal de cambio.
    - La clasificación, priorización y asignación del cambio.
    - La evaluación de impacto y riesgo del cambio.
    - La aceptación formal del cambio.
    - La asignación de los recursos necesarios.
    - La comunicación de los cambios a las personas que corresponda proporcionando la formación correspondiente en caso de que fuera necesario.
    - La realización de pruebas en un entorno diferente.
    - El seguimiento de los cambios realizados.
    - El mantenimiento de un registro de los cambios efectuados.
    - La actualización de la documentación afectada.

5.8. Protección contra código malicioso

En relación a la protección contra el código malicioso, habrá que tener en cuenta medidas de seguridad como las siguientes:

- Mecanismos de prevención:
    - Desactivación de los permisos de administrador sobre los equipos de los usuarios.
    - Verificación de la inexistencia de código malicioso en el software desarrollado por terceros.
    - Acciones de formación y concienciación de los usuarios.
    - Prohibición de la realización de determinadas actividades:
        - Descarga, instalación y uso de software no autorizado.
        - Apertura de archivos adjuntos al correo electrónico de destinatario desconocido.
    - Definición e implantación de Planes de Contingencia que incluyan la recuperación de los sistemas en caso de ataque de un código malicioso.
- Mecanismos de detección y eliminación.
    - Instalación y actualización automática del sistema antivirus.

5.9. Registros de actividad

Con la finalidad de detectar y reaccionar ante comportamientos sospechosos o inesperados, se deben establecer medidas de seguridad como las siguientes:

- Implantar mecanismos de registro de actividades (logs) que almacenen los datos generados por las actividades de sistemas, redes, aplicaciones en relación a los administradores, operadores y usuarios base de los sistemas de información de la Organización. Estos mecanismos de registro deben permanecer activos siempre que dichos sistemas, redes, aplicaciones e identificadores de usuario se encuentren operativos.

- El tipo de información que deberá registrarse se incluirá:
    - Eventos de red, de sistemas, de procesos, de aplicaciones, modificaciones de ficheros y directorios.
    - Actividades de los usuarios.
    - Resultados de tratamiento de los propios registros de actividad.

- El registro de actividad deberá guardar (siempre que sea posible) la siguiente información:
    - Identificación de código de usuario.
    - Identificación de nodo.
    - Fecha y hora de entrada y salida de cada sesión del sistema.
    - Aplicaciones invocadas.
    - Cambios en los datos de los archivos de configuración de las aplicaciones críticas.
    - Adiciones o cambios de los privilegios de los usuarios.
    - Modificaciones en los controles del sistema.
    - Fecha y hora de inicio y fin del acceso al sistema de información.
    - Intentos de acceso no autorizados.
    - Uso de comandos privilegiados y de software del sistema.

- En el caso de que se traten datos de carácter personal de nivel alto, deberá registrarse la siguiente información:
    - Identificación del usuario.
    - Fecha y hora.
    - Fichero accedido.
    - Tipo de acceso.
    - Si el acceso ha sido autorizado o denegado.
    - En caso de accesos autorizados, la información que permita identificar el registro accedido.

5.10. Respaldo y recuperación

La Organización debe disponer los **medios físicos, soportes y procedimientos** necesarios para la realización de copias de respaldo de la información esencial y de la configuración de los equipos, de tal forma que permitan la recuperación ante cualquier contingencia o desastre. Para ello deberán tenerse en cuenta medidas de seguridad como las siguientes:

- Se debe elaborar un procedimiento de realización de copias de respaldo y recuperación, en el que se establezcan las funciones y responsabilidades asociadas al procedimiento a fin de garantizar la correcta ejecución del mismo. Este procedimiento debe contener, al menos:
    - La descripción del sistema de respaldo y recuperación, con detalle de:
        - Los diferentes tipos de copia que se realice.
        - La determinación de la información objeto de respaldo.
        - La periodicidad de la realización de la copia.
        - El lugar de almacenamiento y traslado de las copias.
        - El mecanismo de protección de las copias (Ej: cifrado).
    - La descripción de las tareas a realizar por el operador de copia. Entre ellas:
        - Revisión del proceso de respaldo y de los logs generados por el sistema.
        - Revisión periódica de las cintas.
        - Actuación en caso de incidencias.
    - La descripción del proceso de etiquetado, rotación, traslado y almacenamiento local y remoto de las cintas de respaldo, de acuerdo a los requerimientos legales o de negocio.
- Se debe establecer un registro de entrada y salida de cintas de respaldo en línea con el procedimiento de entrada y salida de soportes. (En la actualidad, no se generan cintas de respaldo)
- Se deben elaborar las Instrucciones técnicas necesarias para el manejo del sistema de respaldo y recuperación.
- Se debe probar regularmente la correcta ejecución del proceso de respaldo y recuperación, a fin de garantizar que éstos son eficaces y que permitirán recuperar la información cuando sea preciso. Durante estas pruebas se seguirán los procedimientos e instrucciones técnicas elaborados, con el fin de determinar que los mismos son efectivo y se encuentran en todo momento actualizados.

5.11. Gestión de las vulnerabilidades técnicas

En relación a la gestión de las vulnerabilidades técnicas, habrá que tener en cuenta medidas de seguridad como las siguientes:

- Se debe disponer de un **inventario actualizado de todos los recursos** de la Organización, que contenga, al menos, la siguiente información:
  - Nombre del recurso.
  - Marca, modelo.
  - Características técnicas.
  - Manuales.
  - Responsables (del recurso, de la operación y del mantenimiento).
  - Usuarios.
  - Software instalado y versión.
  - Configuración de seguridad.
  - Operaciones de mantenimiento realizadas (Ej: actualizaciones, modificaciones, etc.).

- Establecer las **funciones y responsabilidades** asociadas a la gestión de las vulnerabilidades técnicas (Ej: supervisión, evaluación de riesgos, parcheo, seguimiento de activos, registro, etc.).

- Establecer los mecanismos de **identificación o conocimiento** de las vulnerabilidades:
  - Suscripción a boletines de proveedores o noticias.
  - Revisiones periódicas internas a través de herramientas automáticas o pruebas manuales.
  - Contratación de un servicio de hacking ético a un proveedor externo.

- Establecer un **proceso de actuación** que tengan en cuenta aspectos como los siguientes:
  - Detección y conocimiento de la vulnerabilidad y de sus consecuencias.
  - Evaluación de impacto de la resolución de la vulnerabilidad.
  - Evaluación de riesgos del parche.
  - Prueba del parche.
  - Aprobación del cambio.
  - Puesta en producción.
  - Actualización del inventario.
  - Cierre de la vulnerabilidad.

6. ANEXOS/FORMATOS

6.1. Registros

Nombre	Responsable del registro	Contenido	Periodo de Conservación	Ubicación
Solicitud de cambio.	Responsable de Sistemas	Solicitud de cambio	Indefinido	Herramienta gestión incidencias o carpeta
Registro de cambios.	Responsable de Sistemas	Registro de cambios	Indefinido	Herramienta gestión incidencias o carpeta
Inventario de Activos.	Responsable de Sistemas.	Inventario de activos	Indefinido	

7. REFERENCIAS

- PRS-009 Procedimiento de Gestión del Cambio
- PRS-007 Procedimiento de respaldo y recuperación