NORMATIVA DE CONTROL DE ACCESO LÓGICO

Ayuntamiento de Martos

INFORMACIÓN DE USO INTERNO

DE ACCESO INTERNO AL PERSONAL DEL

AYUNTAMIENTO DE MARTOS

Cuadro de Control

Título:	Normativa de control de acceso lógico		
Tipo de documento:	Normativa		
Nombre del Fichero:	NOS-002 Normativa de Control de Acceso Lógico.docx		
Clasificación:	Uso Interno		
Estado:	Documento		
Autor:	Consultor Externo		
Versión:	1.0	**Fecha:**	11/07/2016

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 Gestión de Accesos Lógicos 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 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

Autenticación	Procedimiento de comprobación de la identidad de un usuario.
Contraseña	Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.
ENS	Esquema Nacional de Seguridad.
Identificación	Procedimiento de reconocimiento de la identidad de un usuario.
LOPD	Ley Orgánica de Protección de Datos.
Puerto	Punto de acceso a un equipo informático a través de que tienen lugar transferencias (entradas y salidas) de información del equipo hacia el exterior y viceversa.
Recurso	Cualquier parte componente de un sistema de información.
Red	Conjunto de equipos y cableado que permite interconectar dos o más ordenadores.

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. ROLES Y RESPONSABILIDADES

Responsable de Seguridad	• Definir la normativa de control de acceso y velar por su cumplimiento.
Responsable del Sistema Administrador del Sistema	• Implantar la normativa de control de acceso en los diferentes recursos.
Usuarios	• Cumplir con la normativa de control de acceso en los casos en que les aplique

6. CUERPO DEL DOCUMENTO

6.1. Política de control de acceso lógico

a) Se deben aplicar controles de acceso en todos los niveles de la arquitectura y topología de los Sistemas de Información de la Organización. Esto incluye: redes, plataformas o sistemas operativos, bases de datos y aplicaciones. Los atributos de cada uno de ellos deben reflejar alguna forma de identificación y autenticación, autorización de acceso, verificación de recursos de información y registro y monitorización de las actividades.

b) Los usuarios tendrán acceso únicamente a aquellos recursos que sean necesarios para el desempeño de las labores propias de su puesto. Los derechos de acceso a los mismos también serán los mínimos posibles en función de dichas necesidades.

c) El conocimiento y formación de los usuarios en el uso correcto de los medios de control de acceso será fundamental para garantizar la efectividad de la presente política y su desarrollo. Se deben desarrollar actividades de formación y se deben establecer medios para comunicar a los usuarios y diferentes responsables sobre el uso correcto de los medios de acceso a sistemas y servicios.

d) El uso de la informática móvil y teletrabajo deberá tener un nivel de seguridad equiparable al existente en el uso de equipos locales. Las medidas de seguridad a adoptar deben tener en cuenta, en todo caso, los riesgos que este tipo de forma de trabajar lleva implícitos como, por ejemplo, el entorno de trabajo en que estas actividades se desarrollan que debe ser adecuadamente securizado y los procesos de autenticación de usuarios y máquinas.

e) La implementación de los controles de acceso deberá tener en cuenta los tipos de accesos posibles y sus riesgos, la criticidad de la información que resulta accedida a través de ellos y los requisitos legales aplicables

f) El acceso a los Sistemas de Información requerirá siempre de autenticación.

g) Los usuarios deben siempre autenticarse como usuarios no privilegiados del sistema, excepcionalmente y sólo con fines de administración podrán autenticarse como administradores del mismo.

h) Todas las contraseñas asignadas a las cuentas de usuario deben respetar la política de contraseñas detallada en el presente documento.

i) Los usuarios deben en todo momento hacer un uso responsable de la información y los sistemas de información accedidos, garantizando el nivel de seguridad adecuado de acuerdo a las directrices marcadas en las normas de uso de los sistemas de información.

j) Periódicamente se realizará una revisión de los derechos de acceso asignados a los usuarios. Los derechos de acceso privilegiados deben revisarse con una periodicidad menor. Además de lo anterior, deberá realizarse una revisión de los permisos de acceso correspondientes a un usuario siempre que hubiere sufrido modificación significativa de sus responsabilidades, posición o rol en la organización.

6.2. Gestión de acceso de usuarios

6.2.1. Registro de usuarios

La Organización debe implantar las pautas dictadas por esta normativa mediante procedimientos formales en materia de registro de usuarios y gestión de permisos que garantice el acceso de

los usuarios a la información y sistemas para los cuales estén autorizados. Como regla general, estos procedimientos deben hacer referencia a los siguientes aspectos:

- El uso de un identificador único por usuario, que permita identificarlo con claridad, así como atribuirle sus acciones. El uso de identificadores de usuarios genéricos deberá ser excepcional y estar justificado y documentado en todos los casos.
- Verificar que el usuario tiene la autorización del propietario del sistema para acceder a la información y/o sistema para su tratamiento antes de facilitarle el acceso. Siempre deberá ser el Responsable de usuario quien apruebe los cambios en derechos y permisos de acceso.
- Verificar que el nivel de acceso concedido es el adecuado para la actividad a realizar y cumple con lo establecido por la normativa de seguridad de la organización.
- Informar al usuario de la normativa aplicable sobre control de acceso a la información y/o sistema para su tratamiento.
- Garantizar de que el acceso no será efectivo hasta que se hayan completado los procedimientos de autorización y registro.
- Mantener un registro actualizado de todas las personas autorizadas para la utilización de un servicio concreto.
- Retirar de forma inmediata de los derechos de acceso para aquellos usuarios que han cambiado de puesto o han dejado la organización.
- Revisar de forma periódica y eliminar los identificadores de usuario y cuentas obsoletas por inactividad.
- Garantizar la inexistencia de identificadores de usuario duplicados.

6.2.1.1. Alta de usuarios

Deben desarrollarse procedimientos formales de alta de usuarios para cada sistema o entorno. Estos procedimientos deben respetar la normativa vigente en materia de control de accesos e incluir al menos los siguientes aspectos:

- Mecanismos de control en la asignación de permisos de acceso que permitan evitar los controles del sistema.
- Uso de identificadores de usuario únicos que permitan vincular a los usuarios con sus acciones y responsabilizarles de las mismas.
- Mecanismos para la verificación de la adecuación del nivel de acceso y su consistencia con la política de seguridad de la información vigente.
- Verificación constatada (Ej: mediante firma) de la entrega a los usuarios de sus permisos de acceso y reconocimiento de las condiciones.
- Garantía de que no se accede al servicio hasta que se hayan completado los procedimientos de autorización.
- El mantenimiento de un registro formalizado de todos los usuarios registrados para usar el servicio.

6.2.1.2. Baja de usuarios

Deben desarrollarse procedimientos formales de baja de usuarios para cada sistema o entorno. Estos procedimientos deben respetar la normativa vigente en materia de control de accesos e incluir al menos los siguientes aspectos:

- Eliminación inmediata de las autorizaciones de acceso a los usuarios que dejan la Organización o cambien de puesto de trabajo.
- Volcado de la información del usuario a un sistema de almacenado seguro con acceso restringido al Responsable de usuario.
- La revisión periódica y eliminación de identificadores y cuentas de usuario redundantes y/o inactivas.
- Registro de bajas de usuarios por sistema.

6.2.1.3. Modificación de permisos de usuarios

Algunos de los supuestos de modificación de permisos serán cambio de departamento, de puesto de trabajo o modificación del software o permisos de acceso asignados. Todas las demás modificaciones se tratarán como nuevas altas o bajas. Deben desarrollarse procedimientos formales de modificación de los permisos de acceso de los usuarios para cada sistema o entorno. Estos procedimientos deben respetar la normativa vigente en materia de control de accesos e incluir al menos los siguientes aspectos:

- Modificación inmediata de los permisos de acceso de los usuarios que cambien de departamento o puesto de trabajo dentro de la Organización.
- La revisión periódica de los permisos y privilegios de los usuarios por sistema.
- Registro de modificaciones de permisos de usuarios por sistema.

6.2.2. Gestión de privilegios

La Organización deberá implantar las pautas dictadas por esta normativa mediante procedimientos formales en materia de gestión de privilegios que garanticen el acceso de los usuarios a la información y sistemas para los cuales estén autorizados. Estos procedimientos deben respetar la normativa vigente en materia de control de accesos e incluir al menos los siguientes aspectos:

- Identificar los privilegios asociados a cada elemento del sistema, por ejemplo, el sistema operativo, el sistema gestor de base de datos y cada aplicación, así como las categorías de empleados que necesitan de ellos.
- Asignar privilegios a los individuos según los principios de "necesidad de su uso" y "caso por caso". Por ejemplo, el requisito mínimo para cumplir su función sólo cuando se necesite.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. No se otorgarán privilegios hasta que el proceso de autorización haya concluido.

- Promover el desarrollo y uso de rutinas del sistema para evitar la asignación de privilegios a los usuarios.

6.3. Control de acceso. General

6.3.1. Identificadores

- Todos los identificadores personales de la Organización deben estar normalizados, para posibilitar la identificación unívoca y personalizada de los usuarios.
- La creación de un identificador de usuario debe estar autorizada por su superior jerárquico, de acuerdo con el procedimiento de altas, bajas y modificaciones de permisos de usuarios.
- No se permitirá el uso de identificadores de grupo o genéricos, salvo cuando sea estrictamente necesario y por razones operacionales. Esta circunstancia deberá estar debidamente justificada y aprobada formalmente, aplicando los controles de seguridad precisos.
- Los identificadores de usuarios anónimos y los identificadores por defecto estarán siempre deshabilitados.
- Los identificadores no deben dar indicios de nivel de privilegio asociado.
- Siempre que sea posible, se deben establecer listas de control de acceso a los recursos de información.
- Los identificadores, siempre que sea posible, deben tener asignada una fecha de validez, tras la cual se deshabilitarán.
- Los usuarios son responsables de todas las actividades realizadas con sus identificadores, contraseñas y dispositivos de acceso. Por lo tanto, no deben permitir que otras personas los utilicen y conozcan.

6.3.2. Contraseñas

Las contraseñas (junto con el código de usuario o *user-id*) son el medio de acceso al sistema de información.

Es necesario que las contraseñas que se utilicen como mecanismo de autenticación sean robustas, es decir: difícilmente vulnerables.

En este sentido, se han definido las siguientes **reglas**, que deben ser seguidas por todos los usuarios a la hora de la definición o creación de contraseñas:

Generación de las contraseñas	
Longitud	Deben tener una longitud igual o superior a 7 caracteres
Complejidad	• No debe contener en parte o en su totalidad el nombre de usuario.

	• Debe estar compuesta por al menos 3 de entre los siguientes 4 conjuntos de caracteres:
	  ○ Caracteres alfanuméricos en mayúsculas.
	  ○ Caracteres alfanuméricos en minúsculas.
	  ○ Caracteres numéricos.
	  ○ Símbolos/caracteres especiales.

Repetición	No deberá ser igual a ninguna de las 3 últimas contraseñas usadas.

Semántica	Se deben evitar las contraseñas basadas en:
	  ○ Repetición de caracteres.
	  ○ Palabras del diccionario.
	  ○ Secuencias simples de letras, números o secuencias de teclado.
	  ○ Información fácilmente asociable al usuario como nombres de familiares o mascotas, números de teléfono, matrículas, fechas o en general información biográfica del usuario.

Precauciones	• Evitar apuntar las contraseñas en papel. • Evitar el envío de contraseñas por medios electrónicos o almacenarlas en ficheros de ordenador sin cifrar. • Es especialmente importante mantener el carácter secreto de la contraseña. No debe compartirse, entregarse ni comunicarse a nadie. En caso de haber tenido necesidad de hacerlo, el usuario deberá proceder a cambiarla de forma inmediata. • No utilizar la misma contraseña para distintos servicios web o dispositivos. • Cuanto más sensible, confidencial o protegida sea la información con la que se trabaja, más recomendable es el robustecimiento de las contraseñas y el aumento de la frecuencia de cambio de las mismas. • Deben ser fáciles de recordar. Se hace necesario, por tanto, encontrar una solución de compromiso entre la robustez de la contraseña y la facilidad con la que se puede recordar o memorizar. Para evitar dicha problemática, un mecanismo útil suelen ser los llamados acrósticos, que consisten en seleccionar un carácter de cada palabra de una frase conocida y fácilmente memorizable. Por ejemplo, la frase: “Mi nombre es Napoleón Bonaparte. Tengo 36 años.”, puede generar la siguiente contraseña: MneNB.T36a.

Distribución de las contraseñas	
Medio de entrega	• Las contraseñas iniciales se generan por sistemas cuando se da de alta un nuevo usuario y se le comunica verbalmente al mismo, informándole de la necesidad de cambiar la contraseña en el primer acceso
Contraseñas iniciales	• Las contraseñas se cambiarán en el primer acceso a los sistemas.

Uso de las contraseñas	
Renovación	• Las contraseñas deben renovarse al menos cada 3 meses. Este periodo será inferior de acuerdo a la sensibilidad de los sistemas y de la información gestionada por el mismo. Este es el caso de las contraseñas con privilegios especiales (administrador, root, system, dba, etc.) que deben renovarse, con una periodicidad inferior. • El sistema deberá forzar el cambio de contraseñas de acuerdo a los periodos de renovación establecidos. En caso de que no sea posible el usuario deberá realizar la renovación manualmente.
Cambio	• Los sistemas deben permitir a los usuarios modificar sus contraseñas (Ej: cuando se haya olvidado la contraseña, o cuando se haya bloqueado su acceso al sistema varios intentos fallidos). • Deberá cambiarse la contraseña cuando ésta haya quedado comprometida o se ha cedido a terceros autorizados por motivos de trabajo o mantenimiento, debiendo sustituirse de manera inmediata por otra que no hubiera sido comprometida. • Toda nueva contraseña será comunicada al usuario sin intermediarios, y deberá modificarse obligatoriamente en el primer inicio de sesión.
Custodia	• No deben ser incluidas en correos electrónicos o en otros medios de comunicación electrónica junto con el identificador, ni comunicadas por teléfono. • No se deben escribir o almacenar contraseñas en texto claro o en formas fácilmente reversibles.
Gestión	Para la gestión de contraseñas de acceso a los recursos, el personal de Sistemas debe utilizar una aplicación específica de gestión de contraseñas, como KeePass, PasswordSafe, Lastpass, etc. Estas bases de datos de contraseñas se mantendrán cifradas mediante algoritmos aceptados por la Normativa de Gestión de Claves Criptográficas (AES, TDEA, etc.).

Contraseñas en los sistemas	
Pantalla	Los sistemas no deben mostrar las contraseñas en claro por pantalla.
Salvapantalla	Los salvapantallas deben tener activada la protección por contraseña, bloqueándose tras un periodo de inactividad.
Contraseñas por defecto	Todas las contraseñas por defecto de los sistemas o aplicaciones deben ser cambiadas o desactivadas cuando no sean necesarias.
Recordar contraseña	Se debe evitar la característica “Recordar Contraseña” existente en algunas aplicaciones y formularios.
Expiración automática	Deben existir mecanismos de expiración y caducidad de contraseñas para obligar a los usuarios al cambio de la misma.

6.3.3. Certificados digitales

Sin perjuicio de lo estipulado en la Política de Firma Electrónica y de certificados, se deben seguir las siguientes normas generales:

- Cada certificado digital debe identificar inequívocamente a un solo usuario, y sólo deberá ser utilizado por él.
- El certificado digital debe haber sido emitido por un Prestador de Servicios de Certificación válido y de confianza.
- Cada certificado debe tener asignado un periodo de vida, tras el cual su uso se considerará ineficaz a todos los efectos, y deberá procederse a su renovación.
- En el supuesto de pérdida, robo o indicios de uso indebido por terceros, el certificado deberá ser revocado a la mayor brevedad posible.
- En autenticaciones basadas en certificado digital, su validez e identidad del usuario deberá ser verificada contra una infraestructura de PKI.

6.3.1. Monitorización de accesos

Se deben realizar labores periódicas de monitorización de los sistemas con el fin de detectar accesos no autorizados y desviaciones, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad. Así, se tendrán en cuenta:

Registro de eventos	• Intentos de acceso fallidos. • Bloqueos de cuenta. • Debilidad de contraseñas. • Normalización de identificadores. • Cuentas inactivas y deshabilitadas. • Últimos accesos a cuentas. • Etc.
Registro de uso de los sistemas	• Accesos no autorizados. • Uso de privilegios. • Alertas de sistema. • Etc.

6.4. Control de acceso a redes y servicios de red

La Organización establece las normas y mecanismos de protección para controlar los accesos a las redes que están dentro de su alcance y asegurar que no se hace un uso indebido de sus recursos de información.

Para ello se establecerán los siguientes controles:

- Interfaces apropiados entre la red corporativa de la Organización y las redes públicas.
- Mecanismos de autenticación apropiados en los equipos de los usuarios

- Sistemas de control de acceso para restringir el acceso de los usuarios a la información

6.4.1. Política de uso de los servicios de red

a) Los usuarios de la Organización únicamente tendrán acceso a aquellos servicios de red cuyo uso les haya sido específicamente autorizado conforme a correspondiente *procedimiento de Asignación de Permisos o Privilegios* establecido al efecto.

b) Los servicios de red únicamente podrán ser utilizados para la función para la que han sido dispuestos, estando prohibido su uso para otros cometidos o para llevar a cabo funciones fuera de las asociadas al puesto desempeñado.

c) Los privilegios asignados a los usuarios para el acceso a las redes de la Organización serán registrados y revisados por el responsable correspondiente de la Organización, si bien podrá solicitar información sobre los requisitos de acceso del usuario a los propietarios de las redes.

d) Se emplearán elementos de seguridad de red para garantizar las conexiones de los usuarios que se encuentran en redes internas como aquellas conexiones realizadas desde redes externas en base al riesgo existente en cada una de las conexiones a los servicios de red. En este sentido la Organización ha segregado sus redes de manera que se pueda restringir el acceso a los servicios proporcionados en los siete niveles de red definidos por el estándar OSI.

e) Las conexiones a través de redes públicas deben asegurarse mediante sistemas de cifrado o bien a través de redes privadas virtuales (VPN) de acuerdo al *riesgo* asociado a la conexión establecida.

f) Para los *accesos remotos a la red corporativa* de la Organización, se establecen controles y mecanismos para tratar convenientemente la información transmitida, los sistemas y recursos accedidos, la identidad de las personas que realizan dichos accesos y las posibles implicaciones que el acceso en global conlleva.

g) Los usuarios externos a la Organización solamente podrán acceder a los *servicios WEB* ubicados en la DMZ pública. Los accesos al resto de servicios de la red de la Organización se bloquean mediante la configuración de las reglas de acceso en los cortafuegos establecidos al efecto.

h) Los accesos a las redes y servicios proporcionados por la Organización serán registrados y monitorizados a fin de controlar y prevenir *accesos no autorizados* conforme al *procedimiento de Monitorización* establecido en la entidad.

6.4.2. Identificación de equipos en la red

Con el fin de identificar el origen y destino de las comunicaciones realizadas a través de la red interna de la Organización, todos los equipos se deben identificar de forma unívoca a través de su dirección IP. La identificación de los equipos permitirá llevar un control y filtrado más exhaustivo en los equipos de red, ya que es posible configurar filtros y reglas que permitan controlar dichas conexiones y los medios a través de los que se llevan a cabo.

La identificación de los equipos en la red es complementaria a la identificación y autenticación de los usuarios, y permite un seguimiento y registro de las actividades de los mismos cuando se llevan a cabo de forma remota.

Como regla general los equipos tendrán una dirección IP dinámica o fija.

Asimismo, se considerará la identificación automática de los equipos en aquellos casos en los que se requiera que la conexión se realice desde ubicaciones específicas. De esta forma el acceso a los servicios de red podrá ser restringida en base a unas reglas de filtrado establecidas a nivel de máquina. La identificación se efectúa por el usuario que está intentando acceder al sistema.

La autenticación de los equipos se realizará a través de la *dirección MAC*, *dirección IP* o incluso mediante el identificador de la *tarjeta GPRS* empleado por determinados usuarios de la Organización.

Los equipos pertenecientes a visitantes externos deben situarse en una VLAN determinada con acceso filtrado a los servicios de red.

6.4.3. Autenticación de usuarios desde redes externas

La Organización establecerá mecanismos de autenticación seguros para garantizar las conexiones realizadas desde redes externas a la misma.

Los accesos remotos a la red de la Organización, se establecerán mediante controles y mecanismos que permitan garantizar las personas que realizan dichos accesos de acuerdo a un estudio del riesgo asociado a la conexión y a los recursos empleados en dicha conexión.

La autenticación del usuario deberá garantizarse mediante el empleo de credenciales (usuario y contraseña) y deberá estar sustentado en mecanismos como servidores RADIUS, redes privadas virtuales (VPN), líneas privadas o a través de túneles SSL que garanticen la seguridad del canal de comunicaciones.

Como medida complementaría, los sistemas de autenticación del usuario podrán estar basados en dispositivos seguros tales como *tokens o smart cards* a fin de garantizar los procesos de autenticación de los usuarios de los sistemas de la Organización. Adicionalmente se podrán emplear sistemas OTP[1] (One Time Password) a fin de reforzar el sistema de autenticación.

[1] Se basa en la utilización de un dispositivo electrónico sincronizado con un servidor que muestra un número diferente cada cierta frecuencia. Este número junto con un PIN y el nombre de usuario, es el elemento de autenticación

6.4.4. Protección de los puertos de diagnóstico y configuración remota

Gran parte de los equipos informáticos, sistemas de red y comunicaciones disponen de funcionalidades para el diagnóstico y configuración remota. Si estos sistemas no están bien protegidos pueden convertirse en puntos de acceso incontrolado.

Los puertos de diagnóstico de los sistemas de la Organización deben estar controlados y protegidos frente accesos no autorizados tanto a nivel físico como lógico.

El acceso y configuración de los puertos estará restringido a los administradores y personal de mantenimiento de los sistemas según acuerdos establecidos.

Los armarios y racks en el que se encuentran estos equipos estarán cerrados con llave, con el fin de asegurar la imposibilidad de que se produzcan accesos físicos no permitidos.

Los servidores y sistemas de comunicación deben tener abiertos únicamente los puertos estrictamente necesarios para su uso en explotación. Los puertos, servicios y herramientas de configuración y diagnostico similares instalados en equipos o dispositivos de red cuyo uso no sea necesario para los propósitos de la Organización deben ser deshabilitados o eliminados.

6.4.5. Segregación de redes

Los sistemas de información de la Organización se deben segregar en diferentes redes mediante elementos de red para permitir únicamente el tráfico necesario y autorizado.

Para ello se deben implementar VLAN diferentes agrupando componentes con requisitos o características similares desde el punto de vista de seguridad de la información. A modo de ejemplo:

- Redes Internas: Redes propias de la Organización.
- Redes de Acceso Internas: Conexiones desde las diferentes instalaciones propias y/o autorizadas de la Organización.
- Redes de Acceso Externas (DMZ): Conexiones de usuarios externos a la Organización.

Debe establecerse un perímetro de seguridad. Los perímetros de seguridad entre cada VLAN deben ser controlados mediante el uso de dispositivos de red[2] que gestionen el acceso y tráfico de información entre redes, bloqueando los accesos no autorizados según la política de accesos aprobada.

Se deben establecer medidas de seguridad en las redes inalámbricas (WIFI) de la Organización a fin de garantizar la autenticidad, confidencialidad e integridad de la información que viaja a través de dicha red. La conexión a la red WIFI requerirá del uso de una clave robusta en cada momento para evitar accesos no autorizados al mismo. Asimismo el usuario deberá autenticarse

[2] Cortafuegos con ACL, switch o enrutadores.

a cada servicio proporcionado a través de la red WIFI. El acceso a través de la red WIFI es para invitados, a través de la red WIFI no se accede a la red corporativa.

6.4.6. Control de conexiones a la red

El control de las conexiones a la red se debe realizar utilizando dispositivos de filtrado, rutado, control a interconexión entre redes.

En el caso de redes compartidas, sobre todo las que se extienden a través de los límites de la Organización, el control se debe llevar a cabo mediante distintos dispositivos que regulan la capacidad de los usuarios de conectarse a y desde las redes de la Organización. Estos controles podrán comprender:

- Sistemas proxy de control, registro y/o prohibición del tráfico entrante y saliente a internet (principalmente servicios web y transferencia de ficheros).
- Filtros de correo que controlan la transferencia de correos electrónicos con el exterior.
- Limitación de tráfico hacia el exterior en la navegación y en el correo electrónico, y configuración de mecanismos de bloqueo o de alarmas que alerten de estas conductas.

6.4.7. Control de encaminamiento de red

Se deben realizar controles de ruta para garantizar que el tráfico trasmitido a través de las redes de la Organización sea el necesario y esté debidamente autorizado.

Estos controles de rutas estarán basados en sistemas que permiten realizar un filtrado de información en base a la dirección de origen y dirección de destino. (p.e firewalls, routers, etc.)

6.4.8. Control de la seguridad de la red

Las redes de la Organización deben estar permanentemente protegidas frente a amenazas. Para ellos la Organización podrá realizar controles como los siguientes:

- Realizar periódicamente escáneres de vulnerabilidades de las redes internas y externas a la Organización, y después de cualquier cambio significativo en la arquitectura de la red (Ej: instalación de nuevos componentes, cambios en la topología, modificación de reglas del Firewall, etc.)
- Realizar periódicamente pruebas de penetración de la infraestructura de red.
- Utilizar sistemas de detección de intrusos (IDS).
- Utilizar mecanismos de monitorización de la infraestructura de red.

6.5. Control de acceso al sistema operativo

6.5.1. Inicio seguro de sesión

El acceso a los sistemas operativos de la Organización estará controlado por un proceso de inicio de sesión seguro diseñado para minimizar los intentos de accesos no autorizados, y que contará con las siguientes características:

Información del sistema	Hasta que no se haya completado con éxito el proceso de autenticación, no se deberá mostrar ningún tipo de información relativa al sistema (tal como identificadores del sistema o versiones de software instalado), que puedan ayudar a identificarlo, así como cualquier otro tipo de información que pueda facilitar su acceso no autorizado.
Advertencia de seguridad	• En el momento de introducir los datos de acceso, se deberá visualizar una indicación de que el acceso al ordenador está restringido al personal autorizado (Ej: a través de una ventana emergente), sin que este mensaje permita revelar información del sistema al que está accediendo. • Una vez se haya accedido correctamente al sistema, se deberá mostrar un mensaje que advierta que el uso del sistema sólo está permitido a usuarios autorizados. Un ejemplo de tal mensaje podría ser el siguiente: "AVISO A LOS USUARIOS DEL SISTEMA *El uso de este sistema sólo está permitido a los usuarios autorizados.* *El acceso no autorizado está terminantemente prohibido y podrá ser objeto de acciones disciplinarias, sin perjuicio de las restantes acciones de naturaleza legal a las que hubiere lugar.* *Toda la actividad de este sistema se registra y es revisada periódicamente por el personal designado por la dirección del Ayuntamiento de Martos* *Cualquier usuario que acceda al sistema lo hace declarando conocer y aceptar íntegramente estas reglas y la Normativa de Uso de los Sistemas de Información de EL Ayuntamiento de Martos accesibles en <<URL>> y <<localización física>>. "*
Validación del acceso	La validación de la información de entrada se realizará únicamente cuando se hayan completado todos los datos de entrada. Si ocurre alguna condición de error, el sistema no deberá indicar en ningún caso la parte del dato que es incorrecta. (Por ejemplo, nunca deberá indicar si lo que se ha introducido de forma incorrecta es el nombre de usuario, o la contraseña, etc.).
Nº de intentos de acceso	El número de intentos de log-on en los sistemas estará limitado a un máximo de 5 intentos. Además se deberá: • Registrar los intentos de acceso tanto positivos como negativos. • La cuenta permanecerá bloqueada al menos entre 15 y 30 minutos desde el último intento fallido (en función de la criticidad del sistema).

	• Se enviará un mensaje de alarma a la consola del sistema si el máximo de intentos de acceso ha sido superado.
Tiempo de log-on	Deberá limitarse el *tiempo mínimo y máximo permitido* para el proceso de log-on a los sistemas. Si se excede el sistema debe finalizar el proceso de log-on.
Ocultación de contraseña	• Durante el proceso de inicio de sesión la contraseña permanecerá oculta mientras es introducida o estará oculta por asteriscos. • Las claves que vayan a viajar por la red para su validación durante el proceso de inicio de sesión irán ocultas durante su transmisión

6.5.2. Identificación y autenticación

Todos los usuarios dispondrán de un identificador único (ID) que permite trazar sus actividades en el sistema y hacerle responsable de las mismas.

Aquellos usuarios con privilegios especiales emplearán el identificador que les otorga dichos privilegios únicamente durante el desarrollo de las actividades que requieran de los mismos. Para el resto de las actividades cotidianas emplearán un identificador diferente.

Únicamente en caso excepcional y cuando sea realmente necesario, se podrá usar un único ID compartido para un grupo de usuarios o un trabajo específico. En todo caso dicho uso compartido deberá estar debidamente autorizado y documentado.

Por otro lado el uso de ID genéricos para el uso de los individuos únicamente será permitido cuando las actividades realizadas por ese usuario genérico no necesiten ser trazadas y controladas (Ej. Accesos con derechos solo de lectura) o cuando existen mecanismos adicionales para identificar al usuario (Ej. Password únicos asociados a usuarios)

6.5.3. Utilización de las prestaciones del sistema

La utilización de programas o utilidades que pueden eludir los controles de seguridad de los sistemas y aplicaciones, estará restringido y estrechamente controlado.

Deben establecerse controles que limiten el uso de estas prestaciones el sistema, por ejemplo los siguientes:

- Utilizar procesos de identificación, autenticación y autorización formales para el acceso a estas prestaciones.
- Limitar el uso de prestaciones del sistema al mínimo número de usuarios posible.
- Autorizar el uso de prestaciones con un propósito concreto.
- Registrar siempre el uso de las prestaciones del sistema mediante el uso de eventos del sistema adecuadamente protegidos.
- Definir y documentar los niveles de autorización para las prestaciones del sistema.

- Desactivar o eliminar todas las prestaciones basadas en software y el software de sistemas que no sean necesarios.

6.5.4. Desconexión automática de terminales

Al menos en los sistemas más sensibles y en los accesos privilegiados deben implantarse procedimientos que cierren las sesiones abiertas e inactivas durante un tiempo superior a 10 minutos. Deben incluir el borrado de la pantalla, el cierre de aplicaciones y el cierre de las sesiones de red.

En cada sistema se deben tener en cuenta los riesgos propios de la ubicación del terminal, el tipo de información que resulta accedida por dichas aplicaciones y los riesgos asociados al propio usuario.

6.5.5. Limitación del tiempo de conexión

Al menos en los sistemas más sensibles deben implantarse procedimientos que restrinjan el horario de conexión. Esta medida de seguridad deberá ser aplicada dentro de las áreas seguras y en las zonas de acceso al público. Como norma general, los tiempos de conexión de los usuarios deben limitarse al horario normal de oficina salvo excepciones autorizadas.

6.6. Control de acceso a las aplicaciones

6.6.1. Restricción de acceso a las aplicaciones

Deben tenerse en cuenta los siguientes aspectos de seguridad:

- El acceso a las aplicaciones y bases de datos debe ser independiente del acceso al sistema operativo.
- El acceso lógico a las aplicaciones y a la información tratada en ellas estará restringido únicamente a los usuarios autorizados.
- Los equipos de los usuarios únicamente deben tener instaladas las aplicaciones necesarias para la realización de sus tareas profesionales
- Los usuarios recibirán el mínimo nivel de acceso a la aplicación a sus funciones dentro de la Organización ya que un nivel de acceso por encima de dichas necesidades podría ocasionar un riesgo para la confidencialidad e integridad de la información. Para ello se establecerán restricciones de los derechos de acceso de los usuarios (ej. lectura, escritura, borrado, ejecución) a través de cada aplicación.

Por su parte, las aplicaciones empleadas en la Organización deben:

- Controlar el acceso de los usuarios a la información y aplicaciones de acuerdo con la política, normativa y procedimiento asociado de control de accesos.
- Protegerse de accesos no autorizados realizados por cualquier utilidad, aplicación y software malicioso que sean capaces de eludir los controles del sistema o aplicaciones.
- No comprometer la seguridad de otros sistemas con los que se compartan recursos de información.

7. ANEXOS/FORMATOS

N/A.

8. REFERENCIAS

- PRS-004 Procedimiento de gestión de usuarios (op.acc)
- Esquema de red y documento de detalle de la segregación de redes realizada.
- Documento de detalle de los sistemas y los mecanismos de autenticación utilizados. Todos los sistemas y/o servicios precisan contraseña.