PROCEDIMIENTO DE CONTROL DE ACCESO

Diputación de Soria

GESTIÓN Y CONTROL DE DOCUMENTOS Y REGISTROS

ELABORADO POR:	REVISADO POR:	APROBADO POR:

FECHA	EDICIÓN	REVISIÓN	CAMBIOS REALIZADOS
19/08/2019	01		Versión inicial del documento
30/01/2020	01	02	Adaptación al funcionamiento interno

ÍNDICE

1. Objeto

El objeto del presente documento es la definición del procedimiento aplicable a la Gestión de Accesos de DIPUTACIÓN DE SORIA (en adelante, también 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. En el presente caso estarán comprendidos en este concepto las instalaciones físicas tales como los edificios, CPDs, despachos, o salas, así como los accesos lógicos.
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.
- 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".
- Real Decreto 951/2015, de 23 de octubre, de modificación 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
- Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Público.
- La Jurisprudencia existente en materia de protección de datos de carácter personal. Se tendrán en cuenta también los informes y resoluciones de la AEPD.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), en vigor desde el 24 de mayo de 2016 pero no será aplicable hasta el 25 de mayo de 2018.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

5. Roles y Responsabilidades

Responsable del usuario	• Solicitar acceso de un usuario a un recurso • Retirar el mecanismo de acceso a los recursos • Revisar periódicamente la relación de sus usuarios a los recursos
Responsable del sistema o Administrador del sistema	• Implantar este procedimiento • Otorgar o denegar el acceso al recurso. • Asignar el perfil de acceso al recurso. • Facilitar el mecanismo de acceso al recurso. • Gestionar el registro con las altas y bajas de personas con acceso al recurso. • Gestionar el inventario de recursos bajo su competencia y personas con acceso a los mismos. • Determinar y controlar las condiciones de acceso a los correspondientes recursos.
Responsable de	• Interpretar las dudas que puedan surgir en la aplicación de este procedimiento.

Seguridad	• Proceder a la revisión de este procedimiento cuando sea necesario para actualizar su contenido. • Verificar la efectividad de este procedimiento. • Custodiar y divulgar la versión aprobada de este procedimiento.
Usuarios	• Cumplir con dichas normas
DPD	• Interpretar las dudas que puedan surgir en la aplicación de este procedimiento, y que tengan relación con la protección de datos. • Aprobar, en el ámbito del Comité de Seguridad, este procedimiento. • Verificar su cumplimiento.

6. Control de acceso lógico

6.1. Altas, bajas y modificaciones de usuarios

Inicio del proceso

Las altas, bajas y modificaciones lógicas de usuarios en el sistema se inician por parte del Responsable de Área correspondiente (único personal con competencia para autorizar la concesión, modificación o anulación de los accesos a los recursos), quién envía una solicitud al departamento de informática indicando, al menos, la siguiente información del nuevo usuario:

- Nombre y apellidos
- Departamento
- Id de usuario (para bajas y modificaciones)
- Teléfono de contacto
- Aplicaciones e Información para las que se solicita el acceso, que serán los mínimos imprescindibles que el usuario requiera para llevar a cabo su trabajo.

Este registro se conservará como registro de solicitud de alta, baja o modificación de permisos de usuario.

Con la asignación de perfiles de usuario se consigue que el usuario acceda solamente a aquellas aplicaciones, datos y archivos necesarios para el correcto desarrollo de su actividad. El proceso de asignación de perfiles de usuario debe contemplar las funciones del personal de la DIPUTACIÓN DE SORIA, la sensibilidad de las aplicaciones y datos a los que tiene acceso y la correcta configuración de las contraseñas que limitan el acceso a las mismas.

Atención del pedido

El departamento de informática o sistemas (único personal con competencia para conceder, modificar o anular los accesos a los recursos) dará de alta al usuario en el directorio activo con los permisos

indicados en la solicitud. Cuando se asigne la contraseña al usuario, debe seleccionarse la opción de cambio de contraseña en el primer inicio de sesión, de manera que se fuerce al usuario a cambiar la contraseña que se le facilita inicialmente.

El proceso de alta de usuario se realiza de acuerdo a los siguientes pasos:

1. Solicitud de alta, por los medios que indique el departamento de sistemas de forma que se garantice el registro y conservación, iniciada por el Responsable de Área correspondiente.
2. Determinación de necesidades de usuario y concesión de autorizaciones.
3. Creación de identificadores y asignación de permisos.
4. Comunicación al usuario de clave de acceso inicial.
5. Formación inicial al usuario y entrega de las políticas/manuales de seguridad.
6. Firma de un acuse de recibo de políticas/manuales/obligaciones de seguridad con la entrega de las credenciales.
7. Cambio de contraseña en el primer inicio de sesión.

El proceso de modificación de permisos de usuario se realiza de acuerdo a los siguientes pasos:

1. Solicitud de modificación de permisos, por los medios que indique el departamento de sistemas, iniciada por el Responsable de Área correspondiente.
2. Determinación de necesidades de usuario y concesión de autorizaciones.
3. Modificación de permisos.

El proceso de baja de usuarios se realiza de acuerdo a los siguientes pasos:

1. Notificación de baja usuario por parte del Responsable de Área correspondiente por los medios que indique el departamento de sistemas.
2. Modificación de la contraseña de acceso del usuario y/o deshabilitar la cuenta de usuario.
3. Tras un periodo de retención de 1año, se deben eliminar los identificadores de las aplicaciones.

6.2. 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.

6.3. Control de acceso. General

3.3.1 Identificadores

- Todos los identificadores personales de la Organización deben estar normalizados, y deben posibilitar la identificación unívoca y personalizada de los usuarios. Estos identificadores deben

permitir saber quién ha hecho algo y qué ha hecho, además de encontrarse registrado quién recibe y qué derechos recibe.

- 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. Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.
- 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.
- Los identificadores, siempre que sea posible, deben tener asignada una fecha de validez, tras la cual se deshabilitarán. Estos identificadores se deshabilitarán, en todo caso, cuando un usuario deje la organización, cuando el usuario cesa en la función para la cual se requerían dichos privilegios o cuando la persona que lo autorizó da orden en sentido contrario.
- 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.
- Las credenciales se activarán una vez que estén bajo el control del propio usuario, y éste reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia.
- Se registrarán los accesos realizados con éxito y los fallidos, y el sistema informará al usuario sobre sus obligaciones inmediatamente después de obtener acceso al sistema.
- Se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración mediante permisos de administración.
- Las cuentas se retendrán durante un periodo mínimo de 1 año de forma a atender las necesidades de trazabilidad asociadas a las mismas.

3.3.2 Contraseñas

Las contraseñas (junto con el código de usuario o *user-id*) son el medio de acceso principal 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 8 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: o Caracteres alfanuméricos en mayúsculas. o Caracteres alfanuméricos en minúsculas. o Caracteres numéricos. o Símbolos/caracteres especiales.
Repetición	No deberá ser igual a ninguna de las 3 últimas contraseñas usadas.
Semántica	Se deben evitar las contraseñas basadas en: o Repetición de caracteres. o Palabras del diccionario. o Secuencias simples de letras, números o secuencias de teclado. o 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 2 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, los usuarios pueden 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 determinado por el departamento de sistemas.
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.

3.3.3 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.

3.3.4 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.

3.3.5 Doble Factor de autenticación

Pueden utilizarse los siguientes mecanismos de autenticación frente al sistema (de manera aislada o combinarse para generar mecanismos de autenticación fuerte):

- "algo que se sabe": contraseñas o claves concertadas.
- "algo que se tiene": componentes lógicos (como certificados software) o dispositivos físicos (tokens).
- "algo que se es": elementos biométricos (huella digital).

Los mecanismos de autenticación se adecuarán al nivel del sistema atendiendo a las siguientes consideraciones:

- Para los controles de acceso de los subsistemas de Nivel Bajo, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor. Por ejemplo, usuario y contraseña.
- Para los controles de acceso de los subsistemas de Nivel Medio, se exigirá el uso de al menos dos factores de autenticación. Por ejemplo, DNIe y el PIN asociado, o el certificado de empleado público y el PIN asociado. Además, las credenciales utilizadas deberán haber sido obtenidas tras un registro previo.

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

3.4.1 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.

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 administradores 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.

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.

3.4.2 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* u otro identificador que permita esta autenticación.

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

3.4.3 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.

3.4.4 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.

3.4.5 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. Acceso Local.

3.5.1 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. Además, se informará al usuario del último acceso realizado con su identidad en su sistema.
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, y de las obligaciones de éstos. 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 de la DIPUTACIÓN DE SORIA.* *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 la DIPUTACIÓN DE SORIA, accesibles en la intranet de DIPUTACIÓN DE SORIA.*
Validación del	La validación de la información de entrada se realizará únicamente cuando se hayan completado todos los datos de entrada. Si ocurre alguna condición de

acceso	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

3.5.2 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 60 minutos o el que determine el departamento de sistemas. 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.

3.5.3 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

3.6.1 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.

6.7. Segregación de funciones y tareas

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita

De esta forma, en caso de realizarse desarrollo de sistemas, los entornos de desarrollo y de operación se encontrarán en entornos independientes. El personal con permisos en uno de los entornos no tendrá acceso al otro.

Además, el personal asignado a la explotación de los sistemas no puede tener permisos de administración para la configuración y mantenimiento de los mismos.

Por último, la responsabilidad de la supervisión y auditoría debe recaer en personal o entidades que no intervengan en ninguna otra función.

De cualquier forma, y ante limitaciones de recursos para asumir todas estas responsabilidades de forma específica, la entidad intentará mantener estas incompatibilidades, aunque también se reconoce que será necesario, especialmente por motivos de sustitución u otros similares, que cada usuario del departamento de informática sepa desarrollar labores de todo tipo.