UNIVERSIDAD D SEVILLA

# Procedimientos de Seguridad

## Procedimiento de gestión de la Identidad Digital y acceso lógico de la Universidad de Sevilla

# Índice

# 1. Introducción

La Gestión de la Identidad Digital permite automatizar los procesos asociados al ciclo de vida de los usuarios sincronizando los repositorios de datos y definiendo políticas genéricas para la institución.

El Usuario Virtual de la Universidad de Sevilla (en adelante, UVUS) es una tupla formada por un nombre de usuario y una clave que permite a los miembros de la Comunidad Universitaria el acceso a los Servicios de Tecnologías de la Información y las Comunicaciones (en adelante, TIC) de la Universidad de Sevilla (en adelante, US).

Dependiendo del tipo de relación mantenida con la US, es decir, dependiendo del perfil que tenga el usuario (Estudiante, Personal Docente e Investigador, Personal de Administración y Servicios, etc.) el usuario podrá acceder a unos servicios o a otros en función de los mecanismos de autorización que se realicen intrínsecamente en los mismos.

Por ello, es necesaria una correcta gestión de usuarios que garantice la integridad de la identidad de estos usuarios, la confidencialidad de la información que manejan los servicios TIC y la seguridad en el acceso a dichos servicios.

Con carácter general no se admite la modificación del UVUS.

El acceso a los servicios podrá realizarse utilizando otros mecanismos de autenticación como el Certificado Digital, el DNI electrónico o el carné universitario.

# 2. Objeto

El objeto del presente documento es la definición del procedimiento aplicable a la Gestión de la Identidad Digital: altas, bajas y modificación de usuarios, gestión de la contraseña, control de acceso lógico de los usuarios de los Sistemas de Información de la US, trazabilidad de los accesos dentro del alcance señalado en el Esquema Nacional de Seguridad (en adelante, ENS) y los roles y responsabilidades implicados en el procedimiento.

Se implantará el presente procedimiento atendiendo al nivel de seguridad de la información y los servicios prestados y a la categoría de los Sistemas de Información de la US 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 ENS en el ámbito de la administración electrónica, modificado por el RD 951/2015 de 23 de Octubre.

# 3. Ámbito de aplicación

Este procedimiento es de aplicación en todo el ámbito de actuación de la US, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la US.

El presente procedimiento es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, esté vinculado a la US, incluyendo al personal externo cuando sea usuario de los Sistemas de Información de la US.

En el ámbito del presente procedimiento, se entiende por usuario cualquier miembro de la Comunidad Universitaria, personal de organizaciones externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la US, que utilice o posea acceso a los Sistemas de Información de la US mediante su UVUS.

# 4. Vigencia

El presente procedimiento ha sido aprobado por la Comisión de Seguridad de la US con fecha 17 de julio de 2017, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la US pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la US. Las versiones anteriores quedan anuladas por la última versión de este procedimiento.

# 5. Revisión y evaluación

La gestión de este procedimiento corresponde al SIC, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.
- Tomar las medidas oportunas, si es necesario, para el correcto cumplimiento del mismo.

Cuando las circunstancias así lo aconsejen se revisará el presente procedimiento que se someterá, de haber modificaciones, a la aprobación del SIC.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica y organización general o cualquier otra cuestión que pueda provocarla.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

# 6. Referencias

La implantación de un procedimiento como el descrito requiere el examen previo de la siguiente documentación:

- Política de Seguridad de la Información de la Universidad de Sevilla
- Normativa General de Utilización de los Recursos y Sistemas de Información de la Universidad de Sevilla
- Normativas específicas de uso aceptable y seguridad básica de los servicios TIC de la Universidad de Sevilla
- Procedimiento de Gestión de Autorizaciones de la Universidad de Sevilla
- Política de contraseñas de la Universidad de Sevilla

# 7. Desarrollo del procedimiento

Cualquier persona que tenga una vinculación con la Universidad de Sevilla podrá disponer de un Usuario Virtual personal e intransferible que le identifica unívocamente dentro de la Universidad. El UVUS permitirá al usuario acceder a los servicios TIC de la US disponibles para su perfil concreto.

Es importante señalar que se mantendrá la unicidad del UVUS en el tiempo, es decir, un nombre de usuario que se haya utilizado alguna vez para alguna persona, nunca se volverá a utilizar en el tiempo.

## 7.1. Provisión de usuarios y generación de UVUS

La generación del UVUS dependerá de la vinculación que tenga el usuario con la US. En función de esto se podrán crear UVUS de manera automática, siguiendo procedimientos preestablecidos para tal fin, o se realizarán actuaciones puntuales manuales, ya sea de forma individual o por lotes.

### 7.1.1. Personal Docente e Investigador (PDI) y Personal de Administración y Servicios (PAS)

ALTA: los UVUS de PDI y PAS se generan automáticamente en un plazo máximo de 24 horas después de que la persona haya sido registrada en las bases de datos corporativas.

BAJA: en el momento que se produce un cambio de situación del PDI o PAS en las bases de datos corporativas, ya sea por jubilación o porque deja de prestar servicios para la US, la relación con la US pasa a ser EX Personal Docente e Investigador y/o EX Personal de Administración y Servicios en las bases de datos corporativas. El UVUS se modifica en este mismo momento de manera automática para recoger el cambio en su relación con la universidad y se mantiene activo. Solamente se procederá a la BAJA de un UVUS de este tipo si previamente se realiza una BAJA del registro del usuario en las bases de datos corporativas.

RENOVACIÓN: estos usuarios no requieren renovación en tanto no cambie su vínculo con la US. Cuando el usuario deja de tener vínculo con la US, los UVUS pasan a pertenecer al colectivo de EXPDI y EXPAS y son de carácter vitalicio.

### 7.1.2. Estudiantes de centros propios

ALTA: al igual que en el caso anterior, los UVUS cuya relación con la US es ALUMNO se generan automáticamente en un plazo máximo de 24 horas después de que el alumno haya sido dado de alta en las bases de datos corporativas.

BAJA: en el momento que se produce un cambio en las bases de datos corporativas relativo a la vinculación con la US de un estudiante perteneciente a este colectivo, la relación de esta persona pasa a ser del tipo EXALUMNO. Con un margen de 24 horas respecto al cambio de situación

académica, se actualizará el perfil relativo a su UVUS de manera automática, convirtiéndolo en EXALUMNO.

Se producirá una BAJA del UVUS de un usuario con perfil ALUMNO sólo si previamente se produce una baja del usuario en las bases de datos corporativas, realizándose de manera automática en un plazo de 24 horas después del cambio. En el caso del perfil de EXALUMNO se podrá producir una BAJA cuando el UVUS no se renueve por parte del interesado.

RENOVACIÓN: los usuarios con perfil ALUMNO no requieren renovación en tanto no cambie su vínculo con la US. Al pasar a tener perfil EXALUMNO, el periodo de validez es de dos años, renovables por el propio usuario a través de la plataforma de Gestión de la Identidad (https://identidad.us.es). Antes de que llegue la fecha de validez o expiración de este tipo de UVUS y de manera automática, los sistemas que gestionan la identidad en la Universidad de Sevilla enviarán por correo electrónico tres avisos de renovación de cuenta (30, 15 y 7 días antes de que caduque) a la dirección de correo facilitada por el estudiante como dirección de contacto en el proceso de automatrícula. Llegada dicha fecha, si el usuario no renueva su cuenta, ésta se desactiva automáticamente y se borra 90 días después, de manera automática.

### 7.1.3. Docentes de Enseñanzas Propias no oficiales

Son los docentes de las enseñanzas impartidas por el Centro de Formación Permanente.

ALTA: los UVUS para este colectivo se generan automáticamente en un plazo máximo de 24 horas después de que la persona haya sido registrada en las bases de datos asociadas a enseñanzas no oficiales. Estos UVUS se crean con perfil PDIEXTERNO.

BAJA: Se producen automáticamente en un plazo de 24 horas a partir de que los usuarios son dados de baja de las bases de datos de enseñanzas no oficiales.

RENOVACIÓN: no tienen posibilidad de renovación.

### 7.1.4. Personal de Investigación

ALTA: los UVUS para este colectivo se crean con perfil PDIEXTERNO también y se solicitan a través de un tutor, responsable de departamento u organización de la US desde https://listas.us.es/main, teniendo asociada una validez de uno a cuatro años, a petición del responsable o tutor de la misma.

BAJA: se produce cuando finaliza el vínculo definido a través del periodo de validez de la persona con la US. Los sistemas que gestionan la identidad en la Universidad de Sevilla enviarán por correo electrónico un aviso de caducidad al usuario.

RENOVACIÓN: no tienen posibilidad de renovación por el propio usuario, aunque sí es viable por el tutor que la solicitó.

### 7.1.5. Personal temporal, cuentas institucionales, asociaciones y personal externo

Los UVUS de personas en estos colectivos se crean con perfil MISCELANEA.

ALTA: el UVUS debe solicitarlo el tutor y/o responsable interno de la US. Estas cuentas tienen una duración temporal y se dan de alta bajo demanda.

BAJA: la fecha de caducidad es el parámetro que define cuando se produce la BAJA de este tipo de usuarios, que depende de las necesidades de la cuenta y así lo solicita el responsable de la misma. Llegada dicha fecha, si el responsable no solicita la renovación de la cuenta, ésta se borra automáticamente.

RENOVACIÓN: antes de que llegue la fecha de validez o expiración de estos tipos de UVUS y de manera automática, los sistemas que gestionan la identidad en la Universidad de Sevilla enviarán por correo tres avisos de caducidad (30, 15 y 7 días antes de que caduque) a la dirección de correo asociada a la misma y a la de su responsable. En el caso particular de las cuentas de personal externo, asociaciones y algún otro colectivo, la solicitud de renovación sólo la podrá realizar el responsable y/o tutor. En otro caso, el propio usuario podrá renovar su propia cuenta directamente a través de la plataforma de Gestión de Identidad.

### 7.1.6. Estudiantes de Bachillerato

ALTA: los UVUS asociados a los estudiantes de segundo de bachillerato se dan de alta de manera semiautomática (por lotes) a través del Servicio de Alumnos de forma transparente para los mismos. Por defecto se dan de alta inactivos y deben activarlo a través de la plataforma de Gestión de la Identidad.

BAJA: llegada la fecha de validez de estas cuentas, se borran automáticamente, sin previo aviso.

RENOVACIÓN: estas cuentas no son renovables por el usuario.

### 7.1.7. Profesores de Enseñanza Secundaria

ALTA: los miembros de este colectivo obtienen su UVUS de forma transparente para ellos a través del Área de Orientación y Atención a Estudiantes, si pertenecen al colectivo de calificadores de Pruebas de Acceso a la Universidad (PAU) o son administradores de los centros que participan en la PAU. En otro caso, el usuario puede solicitar cuenta de manera individual directamente.

BAJA: estos UVUS son temporales y llegada la fecha de validez (un año, normalmente) se borran automáticamente sin previo aviso.

RENOVACIÓN: estas cuentas no son renovables por el usuario.

## 7.2. Sincronización de repositorios de datos

La gestión de identidad sincroniza información sobre un numeroso grupo de aplicaciones heterogéneas, directorios, bases de datos y otros repositorios de datos, proporcionando una vista virtual única de toda la información de identidad de cada usuario y estableciendo un punto central de administración para todos los usuarios, grupos y organizaciones.

La consolidación de la información se realiza utilizando en cada caso el mismo protocolo de gestión que es propio de cada uno de los repositorios de datos, lo que permite que la implantación sea no-invasiva, al no requerir de la instalación de agentes en los sistemas en que reside dicha información.

## 7.3. Gestión de la contraseña

La gestión de la contraseña asociada al UVUS se realiza desde el punto de entrada único https://identidad.us.es.

### 7.3.1. Obtención y/o cambio de contraseña

En cualquiera de los casos enumerados en el apartado 7.1 los usuarios podrán obtener la contraseña, si la desconocen, de las siguientes formas:

- Accediendo a la plataforma de Gestión de la Identidad de la US mediante Certificado de la FNMT.
- Personándose y acreditando su condición de usuario en las Aulas de Informática de los distintos centros de la US.

- Personándose y acreditando su condición de usuario en el Servicio de Informática y Comunicaciones de la US.

Si el usuario conoce su contraseña, puede cambiarla accediendo a la plataforma de Gestión de la Identidad de la US con el UVUS o mediante el Certificado de la FNMT.

### 7.3.2. Política de Seguridad de la contraseña

La implantación de la Gestión de Identidad permite la gestión de la contraseña desde un único punto de entrada. Los cambios de contraseña realizados por el propio usuario o por las Administraciones Delegadas son realizados en todos los recursos. Las Administraciones Delegadas son aplicativos para la administración de la plataforma de gestión de identidad basados en roles.

Se aplica a todos los usuarios de los Servicios TIC de la Universidad de Sevilla la “Política de contraseñas de la Universidad de Sevilla” vigente.

## 7.4. Bloqueo/Desbloqueo del UVUS

Existen dos casos en los que se puede bloquear el UVUS:

- Uso indebido: se bloqueará automáticamente desde el SIC sin previo aviso si se detecta un mal uso del UVUS o de cualquiera de los recursos a los cuales el usuario tiene acceso, conforme a la Normativa General de Utilización de los Recursos y Sistemas de Información de la US y a las Normativas de uso aceptable y seguridad básica específicas de los distintos servicios TIC.
- Solicitud de bloqueo por parte del propio usuario: en este caso la solicitud se formulará a través del Servicio de Atención a Usuarios SOS por parte del responsable del UVUS.

En cualquiera de los casos en los que el UVUS haya sido bloqueado, para proceder a su desbloqueo es necesario que el usuario responsable del mismo se ponga en contacto con el Servicio de Atención a Usuarios SOS de la US.

# 8. Privilegios

Los privilegios de acceso de los usuarios a los Sistemas de Información de la US deben ser gestionados y controlados adecuadamente para evitar accesos o usos no autorizados de la información y de los sistemas que la soportan. Por ello, los privilegios asignados requieren de

revisiones periódicas acordes a las normativas vigentes que posibiliten la adopción de las medidas correctivas en su caso. Sólo y exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su propietario.

Todos los accesos deben estar basados en la necesidad de conocer, es decir, que el usuario sólo accederá a la información requerida para cumplir con sus obligaciones. Por otro lado, los permisos otorgados a cada usuario deberán ser los mínimos para el desarrollo de sus funciones.

## 8.1. Gestión de privilegios

La asignación, modificación o revocación de privilegios en los Sistemas de Información de la US será solicitada por los responsables del departamento o área a la que pertenezca el destinatario de dichos privilegios.

Los sistemas de información que manejen datos personales con nivel de protección alto mantendrán un Inventario para Control de Accesos, en el que se identifiquen los usuarios y los privilegios autorizados y denegados.

En la US existen privilegios asociados a:

- Usuarios: en función de su perfil (Estudiantes, PDI o PAS) o rol (Responsables de unidades administrativas, centros o departamentos, administradores de sistemas informáticos, desarrolladores de aplicaciones, personal de soporte informático, etc.)
- Recursos: sistemas operativos, aplicaciones, bases de datos, equipos de red, sistemas de almacenamiento, etc.
- Permisos: de consulta, modificación, delegación, etc.

Los responsables de los Servicios de la US serán los encargados de registrar, mantener y custodiar los permisos otorgados a los usuarios mediante un Inventario de Privilegios de Acceso, que contendrá información relativa a cada usuario y los privilegios de acceso concedidos. La información se creará al dar de alta a un usuario por primera vez en alguno de los sistemas afectados y deberá mantenerse actualizada, registrándose todas aquellas modificaciones que se produzcan en los privilegios de acceso hasta el momento en que el usuario haya causado baja en todos los sistemas incluidos en el alcance.

Los sistemas deben estar diseñados o configurados de tal forma que sólo se acceda a las funciones permitidas.

Los soportes y documentos que contengan datos de carácter personal serán accesibles únicamente por el personal autorizado en el correspondiente Documento de Seguridad, conforme a lo dispuesto en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

## 8.2. Revisión de privilegios

Periódicamente el responsable de cada servicio realizará una revisión de los privilegios de acceso de todos los usuarios.

Cuando se trate de privilegios especiales (administrador, *root*, etc.) y los sistemas manejen información con nivel de protección alto según la LOPD, tal revisión de privilegios se deberá realizar, al menos, cada seis meses, y, en cualquier caso, siempre que existan:

- Alta de nuevos usuarios
- Baja de usuarios
- Cambios en las funciones o responsabilidades de los usuarios.

Para ello se tendrán en cuenta, al menos, las siguientes cuestiones:

- Necesidad de nuevos permisos
- Cancelación de antiguos permisos
- Segregación de funciones
- Devolución de activos y modificación o cancelación de permisos de accesos físicos
- Modificación de contraseñas de acceso
- Notificación al personal implicado de su baja o cambio
- Necesidad de retención de registros

IMPORTANTE: todos los privilegios de acceso de usuarios tanto internos como externos deben ser cancelados en el momento de la finalización de su vínculo o prestación de servicios a la US.

# 9. Gestión de acceso a los servicios TIC

Uno de los requerimientos primordiales de los sistemas informáticos que desempeñan tareas importantes son los mecanismos de seguridad adecuados a la información que se intenta proteger; el conjunto de tales mecanismos ha de incluir al menos un sistema que permita identificar a los

usuarios que intentan acceder a los mismos, mediante procesos tan simples como una contraseña o tan complejos como un dispositivo analizador de patrones de retina.

En este apartado trataremos tres aspectos fundamentales de la gestión de accesos: Autenticación, Autorización y Auditoría (AAA).

Los usuarios de la US tendrán acceso a los Servicios TIC de la US en función de su relación con la Universidad, lo que determinará su perfil o perfiles de usuario y los servicios a los que podrá tener acceso con su UVUS o con otros mecanismos de autorización disponibles en la US.

## 9.1. Mecanismos de autenticación

La autenticación es el proceso de verificación de la identidad digital del remitente de una comunicación como petición para conectarse. Es un modo de asegurar que los usuarios son quienes ellos dicen ser.

Los mecanismos de autenticación definen de qué manera pueden realizarse los procesos de autenticación de usuarios de forma segura. En la US hay cuatro procedimientos de autenticación de usuarios:

1. Autenticación basada en usuario y contraseña, UVUS.
2. Autenticación basada en Certificado Electrónico de la FNMT.
3. Autenticación basada en DNI-e
4. Carné universitario

### 9.1.1. UVUS

Mediante este mecanismo de autenticación, los usuarios pueden hacer uso de su UVUS, es decir, de un nombre de usuario y una contraseña asociada, mediante los que pueden realizar el proceso de *login* en los diferentes sistemas o aplicativos.

### 9.1.2. Certificado digital

La US admite el uso de certificados digitales personales para la realización de firma electrónica reconocida, de acuerdo a lo establecido por la Política de Firma Electrónica de la Universidad de Sevilla, así como para el acceso a algunos servicios TIC. La utilización de dichos certificados se deberá llevar a cabo de acuerdo a lo establecido por la legislación vigente.

### 9.1.3. DNI electrónico

La US pone a disposición de toda la comunidad universitaria la posibilidad de poder hacer uso del DNI-e para realizar el proceso de autenticación en determinados servicios y aplicaciones. Para ello, el puesto desde el que se realiza la autenticación debe disponer de infraestructura adecuada que permita hacer uso del DNI-e.

http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_001

### 9.1.4. Carné universitario

El Carné de la Universidad de Sevilla es una tarjeta inteligente que acredita al usuario como miembro de la Comunidad Universitaria. Contiene un chip donde están grabados sus datos identificativos protegidos por un código secreto (PIN) que sólo el usuario conoce.

http://institucional.us.es/vrelinstitu/carne-universitario

## 9.2. Mecanismos de autorización

La autorización es el proceso por el cual se permite al usuario identificado a acceder a determinados recursos de la aplicación, por tanto es un proceso que se realiza después del proceso de autenticación del que hemos hablado en el párrafo anterior.

Con el objeto de realizar procesos de autorización en las aplicaciones y servicios integrados con el sistema SSO, éste pone a disposición de los responsables de aplicaciones y servicios integrados un conjunto de datos del usuario autenticado. De esta manera el responsable de la aplicación dispone de la información necesaria para realizar internamente un proceso de autorización de acuerdo a sus necesidades y requerimientos. En la URL http://sic.us.es/servicios/cuentas-y-accesos-los-servicios/integracion-con-sso/sso-atributos se puede consultar este conjunto de atributos.

## 9.3. Auditorías

Las auditorías son los procesos por los que los distintos sistemas registran todos y cada uno de los accesos a los recursos que realiza el usuario autorizados o no.

Estos procesos complementan a los anteriores de autenticación y autorización, permitiendo realizar un seguimiento exhaustivo del uso de un sistema en los casos que sean necesarios.

Tanto la gestión de la identidad de la US, como los propios servicios, disponen de estos mecanismos de auditorías sin los que sería completamente imposible realizar seguimientos y actuaciones que en determinadas circunstancias se hacen absolutamente necesarias.

## 9.4. Gestión de sesiones de conexión a los servicios

Se describen seguidamente los aspectos que deben tenerse en cuenta de cara a minimizar el número de accesos no autorizados a los sistemas de información.

- 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. La integración de aplicaciones con el sistema SSO facilita mantenerse en la línea de esta indicación puesto que su funcionamiento impide que se realice de otra forma.
- Una vez que se haya accedido correctamente al sistema, se deberá mostrar un mensaje que advierta que el uso del sistema sólo está permitido a usuarios autorizados.
- Respecto del proceso de validación de entrada, los sistemas deberán tener en cuenta los siguientes puntos:
  - La validación de los datos de acceso (UVUS y contraseña) se realizará únicamente cuando se hayan completado todos los datos. Si ocurre alguna condición de error, el sistema no deberá indicar en ningún caso la parte del dato que es incorrecta.
  - Una vez completado con éxito el proceso de autenticación en el sistema, deberá mostrarse la información de la última entrada satisfactoria.
  - Como norma general, se utilizarán protocolos de comunicación que permitan el envío de las credenciales de usuario de forma cifrada para evitar que sean capturadas en algún punto intermedio de la comunicación. La integración de aplicaciones con el sistema SSO de la US es acorde a este principio básico de seguridad.
- Siempre que sea posible, las sesiones tendrán configurado un *time-out*, de modo que una vez transcurrido un determinado tiempo de inactividad la sesión se cerrará automáticamente.

NOTA: el cierre de sesión por razones de *time-out* puede tener como consecuencia la cancelación de todo lo que el usuario no haya consolidado en las aplicaciones que estuvieran abiertas en el momento del cierre.

## 9.5. Control de acceso a la red

Se debe establecer un control de acceso a la red, tanto interna como externamente, implantando medidas de seguridad y procedimientos de autorización de acceso.

- El acceso a la red cableada se solicitará mediante formulario a través del Servicio de Atención a Usuarios SOS.
- El acceso a la red inalámbrica se realizará mediante el UVUS.
- El acceso desde el exterior será vía VPN mediante UVUS para los usuarios de la US, y mediante usuario/contraseña para externos que no dispongan de UVUS

Se protegerán los servicios de red, puertos de configuración y diagnóstico remoto con estas medidas de seguridad:

- Cuando no sean necesarios los servicios de red estarán deshabilitados.
- La red debe estar segmentada si los sistemas son de categoría ALTA. En cualquier otro caso la segmentación de redes es una recomendación de seguridad.
- Se debe contar con controles de conexión a la red (filtros, reglas, etc.), de enrutamiento y de identificación del equipamiento en la red.

## 9.6. Control de acceso a otros recursos TIC

El acceso a los sistemas y aplicaciones para su administración y a las bases de datos corporativas para el tratamiento de datos, se realizará con cuentas locales que, en todo caso, cumplirán con las medidas de seguridad establecidas para el UVUS, incluida la política de contraseñas.

## 9.7. Revisión del control de acceso a los servicios

Cuando las circunstancias así lo aconsejen el responsable de cada servicio realizará una revisión de los derechos de acceso asignados a los usuarios. La revisión debería realizarse en los siguientes términos:

- A intervalos regulares y tras cualquier cambio en la situación de la persona que posea los derechos, sea una promoción o fin de un contrato o relación con la US.
- Cuando haya un cambio de rol de una persona dentro de la misma organización.
- Si los derechos de accesos son privilegiados el periodo de revisión ha de ser mas frecuente.
- Verificación periódica de que no se han obtenido privilegios no autorizados.

# 10. Auditoría e informes

La Gestión de la Identidad proporciona un sistema completo de auditoría y reporte del perfil de datos de identidad, histórico de cambios y roles de usuarios. Los riesgos de seguridad son detectados de forma que los administradores pueden responder proactivamente.

De igual forma, aquellos sistemas o recursos que utilicen cuentas locales para la autenticación, deben disponer de sistemas de auditoría similares.

## 10.1. Registro de sucesos en los SI

Los sistemas de información que procesen, transmitan o almacenen información deben generar un registro de los accesos lógicos producidos, siempre que técnicamente sea posible, y bajo las siguientes condiciones:

- Este registro recogerá los sucesos en orden cronológico, posibilitando la reconstrucción, revisión y examen de la secuencia de actividades relacionadas con un determinado evento.
- El registro de sucesos será siempre obligatorio en todos los sistemas que contengan información confidencial, así como en aquellos que conforman el perímetro de seguridad como los cortafuegos, con el objeto de aportar las pruebas necesarias para el seguimiento de los mismos, en el caso de accesos no autorizados.
- El registro de accesos lógicos y su auditoria deben proporcionar trazabilidad sobre los accesos al sistema, actividades de administración y otros eventos críticos.
- Tipo de actividades que se recomienda registrar:
  - I. Actividad sospechosa.
  - II. Intentos de acceso no autorizado.
  - III. Excepciones y otro tipo de actividad inusual.
  - IV. Conexiones establecidas con éxito.
  - V. Intentos de conexión denegados y rechazados.
  - VI. Inicios de sesión válidos y erróneos.
  - VII. Mensajes de error y alertas
  - VIII. Tiempos de conexión elevados.
  - IX. Uso concurrente de identificadores de usuario duplicados.
  - X. Acceso remoto de proveedores para tareas de mantenimiento y diagnóstico.
  - XI. Actividad de los cortafuegos.

  - XII. Actividad del administrador.
  - XIII. Inicio y apagado del sistema. Válido o fallido.
  - XIV. Acceso fallido a ficheros u objetos.
  - XV. Cambios en la política de seguridad. Logrados y fallidos.
  - XVI. Cambios en los ficheros del sistema o en el registro.
  - XVII. Copias de seguridad y restauración de las mismas.
  - XVIII. Actividad del antivirus.
  - XIX. En general, todas las actividades de administración de seguridad.
- Para facilitar la monitorización y la investigación de sucesos, los registros de conexiones y otros eventos relativos a la seguridad serán almacenados durante, al menos, 12 meses (excepto los sujetos a la LOPD, que se custodiarán por el periodo señalado en dicha ley).
- Dichos registros contendrán la información necesaria para identificar las conexiones y su naturaleza.
- El responsable del área o departamento correspondiente, o la persona que designe a tal fin, revisarán el contenido de los registros de sucesos con una periodicidad mínima de seis meses.
- El acceso a los registros estará restringido al responsable del área o departamento correspondiente y a las personas designadas por este. Se evitará el acceso de personas no autorizadas que puedan ver, alterar o eliminar registros.
- Los registros deberán ser protegidos y custodiados adecuadamente puesto que podrán usarse en el seguimiento y obtención de pruebas de eventos o incidentes.
- Se usarán herramientas o utilidades que faciliten la revisión de los registros de sucesos. Todas las redes y sistemas operativos dependientes de cada área o departamento, deberán contar con medios para monitorizarlos y generar alarmas o alertas.
- Los responsables de cada área o departamento deberán ser informados cuando los registros de sucesos muestren evidencias de problemas en la seguridad de los sistemas monitorizados.
- Todos los equipos que cuenten con un reloj interno estarán sincronizados entre sí para garantizar la precisión de los sucesos registrados y permitir la correlación de los diferentes eventos.
- Los registros de sucesos serán almacenados siguiendo lo establecido en la planificación que establezca cada área o departamento sobre los sistemas monitorizados de su responsabilidad y protegidos según el nivel de clasificación de la información tratada.
- En el caso de los servidores de ficheros los registros de sucesos serán almacenados durante, al menos, 1 mes. En aquellos equipos que contengan información sensible los registros de sucesos serán almacenados durante un periodo no inferior a 1 año. No

obstante, el periodo mínimo de almacenamiento podrá aumentar cuando así lo exija la legislación vigente.

- La rotación de los registros de sucesos se realizará en base a los criterios propuestos por la propia aplicación/producto/herramienta y en el tamaño de los ficheros de registro de sucesos.
- Los ficheros de registro de sucesos estarán protegidos física y lógicamente para prevenir su acceso no autorizado.
- Los sistemas de registro de sucesos no deben ser configurados para sobrescribir registros antes de su rotación y archivado.
- Si la rotación automática de los ficheros de registro de sucesos no es posible, el sistema deberá avisar cuando los ficheros de registro de sucesos se encuentren en el límite de su almacenamiento y no sea posible registrar sucesos adicionales. Los ficheros de registro de sucesos deberán ser archivados antes del restablecimiento o borrado derivado de su rotación.

## 10.2. Monitorización de los sistemas

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.

A tal efecto, se tendrán en cuenta, en los sistemas:

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

# 11. Roles y responsabilidades

Los roles y las responsabilidades de la Gestión de Identidad son los siguientes:

| Roles | Responsabilidades |
|---|---|
| Usuarios | • Aplicar el presente procedimiento |
| Responsable de Seguridad (RSEG) | • Determinar la categoría del sistema.<br>• Realizar el análisis de riesgos.<br>• Elaborar la declaración de aplicabilidad.<br>• Establecer las medidas de seguridad para proteger la identidad y el acceso seguro a los SI<br>• Aprobar Procedimientos de seguridad.<br>• Elaborar planes de mejora de la seguridad.<br>• Elaborar planes de concienciación y formación. |
| Responsable del sistema (RSIS) | • Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente.<br>• Elaborar los Procedimientos de seguridad.<br>• Elaborar el Plan de mejora de la seguridad a partir de auditorías.<br>• Planificar la implantación de las salvaguardas en el sistema.<br>• Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema.<br>• Aplicar de los Procedimientos de seguridad aprobados y verificar su cumplimiento.<br>• Informar al RSEG de cualquier anomalía.<br>• Colaborar en la investigación y resolución de incidentes de seguridad.<br>• Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves. |
| Responsable de los usuarios | • Comunicar el alta, baja o modificación de usuarios, a través de los procedimientos descrito en el presente documento.<br>• Establecer el perfil del usuario a fin de que se puedan asignar, modificar o revocar acceso y privilegios en los Sistemas de Información |

| | |
|---|---|
| | • Registrar, mantener y custodiar los permisos otorgados a los usuarios |
| Responsable de la Gestión de la Identidad | • Gestionar la identidad de cada uno de los usuarios<br>• Gestionar el ciclo de vida alta/baja/renovación de los usuarios<br>• Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema.<br>• Auditar y reportar el perfil de datos de identidad, histórico de cambios y permisos de los usuarios.<br>• Revisión mensual de los intentos de acceso a los sistemas con acceso a datos de nivel alto LOPD<br>• Aplicación de los Procedimientos de seguridad y verificación de su cumplimiento.<br>• Gestionar las contraseñas desde un único punto de entrada. |

Cada usuario con implicación en las TIC velará, dentro de su ámbito, por el cumplimiento del procedimiento y revisará su correcta implantación o cumplimiento.

# Apéndice: Lenguaje de género

Este procedimiento ha sido redactado con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.