UNIVERSIDAD Ð SEVILLA

Normas de Seguridad

Normativa de acceso local y remoto

Índice

1. Introducción

La Universidad de Sevilla (en adelante, US) debe controlar adecuadamente los accesos que se realizan a sus sistemas informáticos con el fin de garantizar su seguridad. Para ello debe gestionar el acceso a los Sistemas de Información (en adelante, SI), tanto si el acceso se realiza desde dentro de la US, como si el acceso es desde fuera de sus instalaciones.

2. Objetivo

La presente normativa pretende regular los principios generales del acceso a los SI desde la propia red de la Universidad y del acceso de los usuarios cuando, por su actividad profesional, se conectan a los SI desde fuera de las dependencias o instalaciones de la Universidad, accediendo a la red interna de la US utilizando redes externas.

La presente normativa resulta de la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la administración electrónica, modificado por el RD 951/2015 de 23 de Octubre.

3. Ámbito de aplicación

Esta normativa es de aplicación a todo el ámbito de actuación de la US, y sus contenidos derivan de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la US. La presente normativa será de aplicación y de obligado cumplimiento para todos los usuarios que utilicen credenciales de acceso a los diferentes servicios, sistemas y demás recursos de Tecnología de la Información y las Comunicaciones (en adelante, TIC) gestionados por el Servicio de Informática y Comunicaciones (en adelante, SIC).

4. Vigencia

La presente normativa ha sido aprobada por la Comisión de Seguridad de la US con fecha 16 de diciembre de 2016, 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 esta normativa.

5. Revisión y evaluación

La gestión de esta normativa corresponde al Secretariado TIC de la US, 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.

Cuando las circunstancias así lo aconsejen se revisará la presente normativa, que se someterá, de haber modificaciones, a la aprobación de la Comisión de Seguridad de la US.

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 presente normativa se fundamenta en la legislación vigente en materia de seguridad de las Tecnologías de la Información y las Comunicaciones de ámbito europeo, estatal y autonómico, así como en las normas y procedimientos internos que resulten de aplicación a la Universidad en el marco de la Política de Seguridad de la Información.

7. Desarrollo de la normativa

El acceso a los SI de la US requiere distintas medidas de seguridad en función del origen de la conexión. A continuación se incluye un conjunto de normas de obligado cumplimiento, que tienen como objetivo reducir el riesgo cuando se accede a los SI tanto desde dentro como desde fuera de las instalaciones, ya sea con equipos corporativos o con equipos personales del usuario, portátiles o de sobremesa.

7.1. Acceso local

Se considera acceso local al realizado desde puestos de trabajo dentro de las propias instalaciones de la organización a través de las redes corporativas de la Universidad (cableada o inalámbrica). De acuerdo al nivel de las dimensiones de seguridad de los SI de la US, aplican las siguientes medidas:

- La configuración de los SI debe prevenir la revelación de información acerca de los servidores o servicios cuando aún no se ha accedido a los mismos.
    - La información revelada a quien intenta acceder a los servicios debe ser la mínima imprescindible: los diálogos de acceso proporcionarán solamente la información indispensable.
    - Se configurarán debidamente los mensajes de error de las aplicaciones para limitar la información que se ofrece al usuario sobre el servicio prestado.
- Siempre que sea posible, el número de intentos de acceso permitidos a los SI de la US será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.
- Se registrarán los accesos con éxito y los fallidos.
- Siempre que sea posible, se informará al usuario del último acceso efectuado con su identidad.

- Siempre que sea posible el sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.

7.2. Acceso remoto

Se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros.

El acceso desde fuera de las instalaciones de la US conlleva el riesgo de trabajar en entornos de acceso desprotegidos, esto es, sin las barreras de seguridad físicas y lógicas implementadas en las instalaciones de la US. Fuera de este perímetro de seguridad aumentan las vulnerabilidades y la probabilidad de materialización de las amenazas, por lo que se hace necesario adoptar medidas de seguridad adicionales que aseguren la confidencialidad, autenticidad e integridad de la información.

Además de estas medidas de seguridad de acceso local, la US aplica las siguientes medidas:

- Prevención de ataques activos desde el exterior, garantizando que al menos serán detectados y que se activarán los procedimientos previstos de tratamiento del incidente. Los ataques activos incluyen:
    - La alteración de la información en tránsito
    - La inyección de información espuria
    - El secuestro de la sesión por una tercera parte
- Para asegurar la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información es obligatorio el uso de contraseñas acordes a la Política de Contraseñas de la US.
- Uso de redes privadas virtuales (VPN) teniendo en cuenta las siguientes consideraciones:
    - Siempre que sea posible, la autenticación del usuario se realizará en el directorio corporativo de la US mediante mecanismos que no gestionen directamente las contraseñas (sistema Single Sign On, SSO)
    - Cerrar siempre la sesión al terminar el trabajo.
    - Bloquear siempre la sesión, ante cualquier ausencia temporal, aunque sea por poco espacio de tiempo.
- Uso de algoritmos acreditados por el Centro Criptológico Nacional (en adelante, CCN)

Cuando la conexión desde el exterior se realice con equipos portátiles corporativos, el usuario tendrá en cuenta:

- Que dichos equipos son para uso exclusivo del trabajador y sólo serán utilizados para fines profesionales. No deben prestarse a terceros salvo autorización expresa que incluirá, en todo caso, la definición de las condiciones de uso.
- Que es necesario aplicar las medidas de seguridad indicadas en la Arquitectura de Seguridad y, de forma más específica, en la Normativa de uso de portátiles corporativos para utilizar el equipo en el acceso a recursos o sistemas de información de la US o en el tratamiento de la información de la Universidad.

Si la conexión se realiza desde equipos de trabajo personales que no estén bajo la responsabilidad de la US, los usuarios deben considerar:

- Que los equipos estén configurados con los requisitos de software necesarios que permiten trabajar en los mismos entornos y versiones que requieren los SI de la US.

En cualquier caso, los equipos desde los que se realiza la conexión remota deben disponer de las siguientes medidas de seguridad, estén o no bajo la responsabilidad del SIC:

- Antivirus instalado y actualizado junto con sus patrones de virus.
- Cortafuegos activado.
- Versión del sistema operativo actualizada con los últimos parches de seguridad.
- Copias de seguridad periódicas de la información contenida en los equipos. Es necesario adoptar las medidas adecuadas para la protección de dichas copias.

Cuando el acceso remoto a los servicios internos de la US se realice vía Web, se aplicarán las siguientes medidas de seguridad:

- Los navegadores utilizados deben estar adecuados a las versiones oficiales que dan cobertura a los sistemas de la US, así como tener los parches de seguridad correspondientes instalados y configurados.
- Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.
- Desactivar las características de recordar contraseñas en el navegador.
- Activar la opción de borrado automático al cierre del navegador de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.
- No instalar *addons* (extensiones) para el navegador que puedan alterar el normal funcionamiento de las aplicaciones.

7.3. Cumplimiento de las normativas internas

Durante la actividad profesional fuera de las instalaciones de la US se seguirán las políticas, normativas, procedimientos y recomendaciones internas existentes en la US, atendiendo de manera especial a las siguientes:

- Política de contraseñas de la US: las contraseñas deberán ser robustas y renovarse periódicamente o cuando se sospeche que pueden estar comprometidas.
- Normativa de intercambio de información y soportes extraíbles: el uso de los soportes físicos extraíbles (CDs, DVDs, memorias USB, etc.) debe limitarse. El almacenamiento de la información en soportes físicos extraíbles debe caracterizarse por no ser accesible para usuarios no autorizados. Para ello, es necesario aplicar claves de acceso o algoritmos de cifrado cuando la naturaleza de la información así lo aconseje.
- Normativa de protección de equipos frente a código dañino: no se desactivarán las herramientas de seguridad habilitadas en los dispositivos móviles (ordenadores portátiles, móviles, tabletas, etc.) y se mantendrán siempre actualizadas. No descargarán ni se instalarán contenidos no autorizados en los equipos.
- Procedimiento de gestión de incidentes de seguridad: comunicar cualquier incidente, con la mayor rapidez posible, a través del Servicio de Atención a Usuarios (SOS).
- Medidas preventivas y buenas prácticas: cifrar y/o firmar los correos electrónicos con información sensible, confidencial o protegida que vayan a ser transmitidos a través de correo electrónico o de cualquier otro canal que no proporcione la confidencialidad adecuada.

8. Responsabilidades

Todos los usuarios vinculados a la US (PAS, PDI, terceros…) afectados por esta normativa son responsables de conocer las normas que afectan al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.

Todos los usuarios son responsables de cumplir con las directrices de la normativa de acceso local y remoto dispuestas a través de esta normativa y el resto de normativas asociadas. Cualquier persona que administre un equipo informático, aplicación o servicio, es responsable de mantener correctamente instalado y actualizado el sistema de protección del equipo como requisito para el acceso a la Red Informática de la Universidad de Sevilla (RIUS).

Apéndice: Lenguaje de género

Esta Normativa ha sido redactada con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.

ANEXO: Acrónimos y glosario de términos

CCN

Centro Criptológico Nacional. Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

Cortafuegos

Del inglés “firewall”, es una parte de un sistema o una red que está diseñada para permitir, limitar, cifrar, descifrar, el tráfico entre distintas redes sobre la base de un conjunto de políticas de seguridad.

ENS

Esquema Nacional de Seguridad. 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, modificado por el RD 951/2015 de 23 de Octubre.

SI

Sistema de Información. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

SIC

Servicio de Informática y Comunicaciones. Servicio cuyo objetivo es atender las necesidades de apoyo informático a las tareas de estudio, docencia, investigación y gestión en la Universidad de Sevilla.

SSO

Single sign-on (autenticación única) es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

SOS

Soporte De Operaciones y Sistemas: servicio responsable de la recepción de todas las incidencias informáticas y de la resolución de aquellas que se encuentran en su catálogo de servicios.

TIC

Tecnologías de la Información y las Comunicaciones. Dispositivos que permiten trabajar el ciclo de vida completo de la información, es decir, crear, almacenar, tratar, enviar o borrar información.

VPN

Virtual Private Network (Red Privada Virtual) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que los ordenadores que usan esta tecnología envíen y reciban datos sobre redes públicas con toda la funcionalidad, seguridad y políticas de gestión de una red privada.