UNIVERSIDAD D SEVILLA

Procedimientos de Seguridad

Procedimiento de bastionado de equipos informáticos y Sistemas de Información

Índice

1. Objeto

El objeto de este procedimiento es determinar los pasos a seguir para asegurar la configuración de los sistemas en la Universidad de Sevilla previo a su puesta en producción, a fin de reducir las vulnerabilidades de los mismos.

El artículo 19 del RD 3/2010 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, lleva por título "Seguridad por defecto" y establece que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto: mínima funcionalidad y seguridad por defecto.

2. Ámbito de aplicación

Este procedimiento es de aplicación a todo el equipamiento informático utilizado en la Universidad de Sevilla ya sea un ordenador personal para un puesto de trabajo, una impresora en red, un equipo multifunción, una cámara, almacenamiento externo o cualquier otro dispositivo con conexión a red.

De igual forma, aplica a los Sistemas de Información que la Universidad utiliza para la prestación de Servicios de Tecnología de la Información.

Toda persona relacionada con la administración de un equipo informático o Servicio TI está obligada a seguir lo dispuesto en este procedimiento, incluyendo el personal de organizaciones externas, cuando sean administradores.

La documentación de instalación y/o implantación de los diferentes productos deberá hacer referencia a este documento para llevar a cabo el bastionado del mismo. El Servicio de Informática y Comunicaciones facilitará una guía de apoyo para el bastionado de los principales sistemas y aplicaciones utilizados en la Universidad de Sevilla.

3. Configuración de seguridad de equipos informáticos

Se deberá de llevar a cabo una instalación "personalizada" de los sistemas de forma que proporcionen únicamente la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra.

Este apartado describe aspectos de bastionado generales aplicables a cualquier sistema informático previo a su entrada en producción. Aplican las medidas de configuración de seguridad del Anexo II del Real Decreto ENS, en concreto:

1. Se deberán eliminar y/o cambiar las cuentas de usuario estándar y las credenciales por defecto en el equipo o las aplicaciones.
2. Se utilizará, en la medida de lo posible, la política de la US para la generación de contraseñas.
3. Se eliminará todo aquel servicio o funcionalidad que no sea estrictamente necesario. Esto implica desactivación de servicios que se no se vayan a usar, cierre de puertos, limitación de accesos, etc.
4. Se configurará el sistema de forma que por defecto sea seguro no permitiendo claves vacías, previniendo la revelación de información sobre el sistema, generando informes de error comunes para evitar la obtención de información de los sistemas que no sea necesaria, etc.
5. Se actuará de la manera más restrictiva posible a la hora de otorgar privilegios a los usuarios.
6. Se utilizarán, en la medida de lo posible, protocolos que cifren las comunicaciones, como SSL, HTTPS, evitando el envío de información en texto claro, como con los protocolos HTTP, FTP, Telnet, etc.
7. Se sincronizarán las fechas y horas de todos los sistemas/dispositivos.
8. Se evitará el uso de algoritmos de cifrado inseguros o débiles (MD5, SHA-1, RC3, RC4,...)
9. Se activarán las actualizaciones automáticas del SO del equipo siempre que sea posible.
10. Se dispondrá siempre de un antivirus activo y actualizado y, cuando sea necesario, de un cortafuegos correctamente configurado.

Se adjunta como anexo en este documento un *cheklist* para el cumplimiento de estas medidas.

Es responsabilidad del usuario la custodia segura de los identificadores y claves asignados para el uso del equipamiento y los servicios de la US (dirección IP, UVUS y contraseñas locales) evitando guardar credenciales en ficheros de texto plano. Toda la información confidencial, además de las credenciales, debería de ser cifrada y solo accesible para los usuarios que estrictamente lo requieran.

La información relativa al bastionado seguro de los sistemas debe quedar registrada siguiendo buenas prácticas de seguridad en la redacción de los documentos:

- Evitar que aparezcan contraseñas de usuarios, y en general cualquier tipo de credencial.
- Revisar la documentación al menos una vez al año para actualizarla o cuando haya un cambio importante en el sistema.

4. Configuración de seguridad de Sistemas de Información

Cuando el equipamiento informático forme parte de un Sistema de Información que presta un Servicio se tendrán en cuenta, además de las medidas del apartado anterior, las medidas que le apliquen para el cumplimiento del Esquema Nacional de Seguridad (ENS).

El Responsable de la Información que maneja el Sistema de Información lo categorizará en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de dicha información con perjuicio para la autenticidad, integridad, confidencialidad o trazabilidad siguiendo el procedimiento establecido en el Anexo I del RD 3/2010.

El Responsable del Servicio prestado por el Sistema de Información lo categorizará en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de dicho servicio con perjuicio para la disponibilidad del mismo siguiendo el procedimiento establecido en el Anexo I del RD 3/2010.

El Responsable del Sistema aplicará las medidas de seguridad del ENS en función de la categorización del Sistema de Información determinada por los Responsable de la Información y el Servicio. Para ello podrá solicitar al Servicio de Informática y Comunicaciones un documento Excel con *checklist* de las medidas que le aplican, a través de la dirección de correo seguridadtic@us.es.

Si la información que contiene el sistema maneja datos personales, estos se tratarán conforme a lo establecido en el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDyGDD), siguiendo los procedimientos relacionados con la Protección de Datos Personales de la Universidad de Sevilla y el asesoramiento del Delegado de Protección de Datos.

El responsable del Sistema elaborará un procedimiento que permita la gestión de la configuración de forma continua tras la entrada en producción del sistema.

5. Anexo: *cheklist* para el bastionado del equipo

Medidas de seguridad	Aplicado (SI/NO)	Observaciones
¿Se han eliminado/desactivado las cuentas innecesarias y claves por defecto?		
¿Ha utilizado la política de la US para la generación de contraseñas?		
¿Ha eliminado los servicios o funcionalidades que no sean estrictamente necesarios y ha revisado el cierre de puertos?		
¿Ha revisado la configuración por defecto para que sea segura no permitiendo claves vacías y previniendo la revelación de información sobre el sistema?		
¿Ha revisado los privilegios de los usuarios para que sean los mínimos necesarios?		
¿Utiliza siempre protocolos seguros para la conexión y el envío de información?		
¿Ha sincronizado la fecha y la hora del equipo?		
¿Evita el uso de algoritmos de cifrado inseguros o débiles (MD5, SHA-1, RC3, RC4, etc...)?		
¿Ha establecido una política para las copias de seguridad del equipo?		
¿Ha establecido un procedimiento para la creación, revisión y almacenamiento de logs?		
¿Están activadas las actualizaciones automáticas del SO del equipo?		
¿Dispone de un antivirus activo y actualizado?		
¿Necesita un cortafuegos?		

NOTA: el *checklist* de medidas del ENS aplicables a Sistemas que presten Servicios debe ser solicitado al SIC a través de la dirección de correo electrónico seguridadtic@us.es.