UNIVERSIDAD Ð SEVILLA

Normas de Seguridad

Normativa de uso de portátiles corporativos

Índice

1. Introducción

La Universidad de Sevilla (en adelante, US) dispone de equipos portátiles corporativos que, por su naturaleza, necesitan una protección especial.

2. Objeto

El presente documento tiene por objeto establecer las normas de uso de los equipos portátiles corporativos, con especial atención a las mismas cuando dichos equipos se utilicen fuera de las instalaciones de la organización y no puedan beneficiarse de la misma protección física y lógica.

3. Ámbito de aplicación

Esta normativa es de aplicación para todo el personal PAS y PDI de la Universidad de Sevilla que de manera permanente o eventual tenga asignado un equipo portátil corporativo, ya sea como puesto de trabajo o con carácter de préstamo, independientemente de que haga uso de él únicamente dentro de las instalaciones de la US o se conecte desde fuera de la US o desde su domicilio particular con el portátil.

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 que la US pone a disposición de los usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Esta normativa entrará en vigor inmediatamente después de su publicación y difusión 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 Servicio de Informática y Comunicaciones (en adelante, SIC) 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

Sin perjuicio de las medidas generales de las normativas de protección de equipos frente a código dañino y de acceso local y remoto, para equipos portátiles se adoptarán, además, las siguientes medidas.

7.1. Portátiles usados como puesto de trabajo

Los ordenadores portátiles corporativos utilizados como puestos de trabajo son administrados directamente por los usuarios responsables de los mismos. Dichos equipos pueden contener información corporativa y acceder, en algunos casos, a los Sistemas de Información (en adelante, SI) corporativos: deberán, por tanto, estar sujetos a estrictos controles de seguridad y contar con las medidas de protección descritas en esta normativa.

- La US establecerá los requisitos y las condiciones específicas a cumplir por el personal PAS o PDI, para que se le asigne un portátil como puesto de trabajo.
- En todos los casos, la propiedad de los ordenadores portátiles es de la US, y podrán ser retirados si se verifica un uso inadecuado.
- Se establecerá un sistema de protección perimetral (cortafuegos –*firewall*-) en el equipo que minimice la visibilidad exterior.
- El usuario es responsable de mantener los elementos de seguridad operativos, las aplicaciones instaladas en el equipo y el estado y uso del mismo.
- Se controlará el acceso a la red de la US cuando el equipo se conecte desde fuera de las instalaciones de la Universidad mediante Red Privada Virtual (VPN).
- Se evitará que el equipo contenga claves de acceso remoto a la US capaces de habilitar un acceso a otros equipos de la US u otros de naturaleza análoga.
- Los usuarios son responsables de proteger adecuadamente los accesos (usuario y contraseña) de los servicios corporativos a los que tienen acceso desde el ordenador portátil corporativo.
- Si el portátil contiene información de los sistemas corporativos y/o datos personales, ni el equipo ni sus copias de seguridad podrán salir de las instalaciones de la Universidad de Sevilla sin autorización expresa.
- La salvaguarda y confidencialidad de los datos del ordenador portátil corporativo son responsabilidad del usuario.
- Los usuarios notificarán al Servicio de Atención a Usuarios SOS cualquier alteración en el estado de funcionamiento del equipo que pueda afectar a la seguridad o información del mismo.
- Finalizado el plazo de asignación del portátil, cuando se produzca un cambio de destino de usuario, baja definitiva o jubilación, el usuario realizará la devolución del mismo a la US y se procederá a la eliminación de toda la información del usuario.
- Para los equipos obsoletos se procederá a su baja y retirada o reciclaje de acuerdo al procedimiento de retirada de equipos informáticos vigente en la US.

Debido a que los equipos portátiles tienen un riesgo manifiesto de pérdida o robo, se tomarán las siguientes medidas de precaución cuando los equipos portátiles corporativos se utilicen fuera de la US:

- Vigilancia permanente. Los equipos portátiles deben estar vigilados y bajo control para evitar extravíos o hurtos que comprometan la información almacenada en ellos o que pueda extraerse de ellos. En los desplazamientos en medios de transporte, tales como avión, ferrocarril, autobús, barco, etc., este tipo de equipamiento no debe facturarse y deberá viajar siempre con el usuario. En caso de pérdida o hurto de cualquier equipo portátil propiedad de la US se debe abrir, inmediatamente, una incidencia al Servicio de Atención a Usuarios SOS.
- Evitar el acceso no autorizado. El trabajo en lugares públicos debe realizarse con la mayor cautela y precaución, evitando conexiones *wifi* abiertas o en general conexiones inalámbricas, de forma que personas no autorizadas vean o escuchen información.
- Transporte seguro. Los equipos portátiles corporativos que salgan de las instalaciones de la US se deben transportar de manera segura, evitando proporcionar información sobre el contenido en los mismos y utilizando, en su caso, maletines de seguridad que eviten el acceso no autorizado.
- Mantenimiento de los equipos. Los equipos portátiles corporativos se mantendrán de acuerdo a las especificaciones técnicas de uso, almacenamiento, transporte, etc., proporcionadas por el fabricante. En particular, se evitará su uso en condiciones de temperatura o humedad inadecuadas, o en entornos que lo desaconsejen (mesas con alimentos y líquidos, entornos sucios, etc.)

Cuando un portátil contenga información corporativa y/o datos personales protegidos por la LOPD, el usuario responsable de dicho portátil observará rigurosamente la Normativa de intercambio de información y uso de soportes de la US, así como las medidas de seguridad establecidas en el Documento de Seguridad de la Información de la US.

7.2. Equipos en préstamo

Aplican, además de las normas anteriores, las siguientes:

- La US establecerá y comunicará al PDI y PAS los requisitos y las condiciones específicas del “Servicio de préstamo de portátiles”.
- Todos los ordenadores portátiles entregados, tanto al PAS como al PDI, estarán maquetados y configurados con elementos básicos de seguridad y no podrán ser alterados por el usuario:

- El programa antivirus y el firewall deben estar siempre activos.
- Los portátiles dispondrán de una herramienta de gestión remota y control de programas instalados que podrá ser usada por el Servicio de Atención a Usuarios SOS en caso necesario y previa petición del usuario.
- En caso de que el portátil se utilice para acceder a la red de la Universidad desde el exterior, emulando una conexión local, utilizará una Red Privada Virtual.

- Finalizado el plazo estipulado para el préstamo o asignación del portátil, el usuario realizará la devolución del mismo al Servicio de Atención a Usuarios SOS y se procederá a la eliminación de toda la información del usuario.
- Queda prohibida la cesión de portátiles entre usuarios.

8. Responsabilidades

Todos los usuarios son responsables de cumplir con las directrices de protección de equipos portátiles corporativos, dispuestas a través de esta normativa y el resto de normativas referenciadas.

Cualquier persona que administre o use un equipo informático portátil propiedad de la US es responsable de mantener correctamente instalados y actualizados los sistemas de protección del equipo como requisito para el acceso a la Red Informática de la Universidad de Sevilla (RIUS), ya sea desde la propia red de la US o accediendo desde redes externas.

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

Antivirus

Programa informático que analiza continuamente el equipo en busca de alguno de los virus registrados en su base de datos. Es importante tener siempre actualizada la base de datos del antivirus. Dependiendo de cada antivirus y de su configuración, éste actuará avisándonos, poniéndolo el virus en cuarentena o eliminándolo directamente.

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.

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.

SOS

Soporte de Operaciones y Sistemas. Es el Servicio de Atención a Usuarios SOS, responsable de la recepción de todas las incidencias informáticas y de resolver las incluidas en su catálogo de servicios.

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.