UNIVERSIDAD Ð SEVILLA

Normas de Seguridad

Normativa de protección de equipos frente a código dañino

Índice

1. Introducción

La utilización de los Servicios de Tecnologías de la Información y las Comunicaciones (en adelante, TIC) por parte de la Universidad de Sevilla (en adelante, US) es cada vez más amplia y la disponibilidad permanente de estos servicios es esencial para el buen funcionamiento de la institución. Por ello, es necesario proteger la seguridad e integridad de los sistemas de información (servicios, aplicaciones, infraestructuras TIC, etc.) y de los puestos de trabajo.

Los Sistemas de Información de la US dispondrán de sus propios mecanismos de seguridad para los Servicios que ofrecen, aplicaciones que manejan e infraestructuras TIC que los soportan y serán responsables de ellos los administradores de dichos sistemas.

Los equipos informáticos utilizados como puestos de trabajo por el personal de la Universidad de Sevilla para realizar sus funciones, necesitan herramientas especializadas. Para ello la US dispone de diversos contratos con empresas suministradoras de soluciones de antivirus y seguridad de contenidos.

2. Objeto

El presente documento tiene por objeto establecer las pautas de utilización de soluciones de seguridad para minimizar la probabilidad de ocurrencia de riesgos y vulnerabilidades por código dañino (virus, gusanos, troyanos, *spyware*, y en general, todo lo conocido como *malware*), con el fin de preservar la confidencialidad, integridad y disponibilidad de la información, las aplicaciones informáticas y las redes de comunicaciones de la US.

3. Ámbito de aplicación

Esta normativa es de aplicación para todo el personal de la Universidad de Sevilla y el personal de organizaciones externas que de manera permanente o eventual utilice o administre equipos informáticos o dispositivos móviles conectados a la red corporativa, ya sea desde la propia Universidad o desde su domicilio particular.

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 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

7.1. Protección de los Sistemas de información de la US

Todos los Sistemas de información que presten Servicios TIC a la US deberán disponer de un sistema de protección en los servidores y aplicaciones que lo componen. Se trata de *software* que analiza el código malicioso, que detecta y limpia los virus encontrados.

Los responsables de estos servidores deben asegurarse de tener instalados los parches de seguridad y actualizaciones de sistemas operativos y *software* de aplicación.

7.2. Protección de equipos personales

Todo usuario que conecte un dispositivo a la red de la US es responsable de tener instalado y operativo un programa antivirus, siempre que la tecnología lo permita, con las últimas actualizaciones (patrones de virus, motores de antivirus) disponibles de dicho programa o *software*, así como cualquier otro *software* que se establezca desde la Universidad de Sevilla, para mejorar la seguridad informática.

La US dispone de varias soluciones de seguridad, de antivirus, seguridad de contenidos y código malicioso, gestionadas desde el SIC y a disposición de los usuarios en diferentes modalidades.

Los procedimientos de uso de las diferentes soluciones corporativas de protección de equipos están recogidos en el catálogo de servicios del SIC accesible vía web.

7.3. Reacción ante un virus

Los virus detectados por las soluciones antivirus instaladas en servidores de aplicaciones y equipos personales suelen ser limpiados en el momento de su detección.

En los servidores de aplicaciones de la US se pueden dar casos de falsos positivos. Si el usuario sospecha que es así deberá notificarlo al Servicio de Atención a Usuarios SOS para la corrección, si procede, del comportamiento del sistema por parte del personal TIC de la US.

En el caso de los ordenadores personales, si el antivirus, en sus revisiones periódicas o en el acceso a un fichero, notifica la existencia de virus, el usuario debe seguir las instrucciones del programa en la medida de sus posibilidades. Si aun así, se tiene la sospecha de que el equipo está infectado o tiene algún problema, se debe poner inmediatamente en contacto con el Servicio de Atención a Usuarios SOS para abrir un incidente de seguridad. Hasta el diagnóstico y resolución del problema por parte del técnico especialista, el usuario debe evitar el uso del equipo y su conexión a la red, o en su caso seguir las instrucciones indicadas desde el Servicio de Atención a Usuarios SOS.

En los casos en los que el usuario sea administrador de un equipo servidor, y se encuentre infectado con un virus, el propio usuario es responsable de resolver el problema causado.

En los casos en que el SIC considere que pueden estar en peligro la integridad y/o continuidad de los servicios TIC de la US debido a la infección de un equipo de usuario, puede proceder a tomar medidas preventivas temporales como deshabilitar la conexión a la red del equipo infectado o potencialmente peligroso.

8. Responsabilidades

Todos los usuarios son responsables de cumplir con las directrices de protección de equipos 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

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.

Malware

Del inglés "*malicious software*", hace referencia a código maligno o *software* dañino. Se trata de un tipo de virus que tiene como objetivo infiltrarse o dañar un ordenador o un Sistema de Información sin el consentimiento de su propietario. Incluye una gran variedad de código dañino (virus, gusanos, troyanos, *spyware*, etc.)

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.

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 la resolución de aquellas que se encuentran incluidas en su catálogo de servicios.

Virus

Programa informático que tiene por objeto alterar el funcionamiento normal del ordenador sin el permiso o el conocimiento del usuario propietario del equipo. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también pueden tratar de robar información sin que el usuario sea consciente de ello, o atacar a otros equipos desde el ordenador infectado.