# I. DISPOSICIONES Y ACUERDOS GENERALES

## I.3. Rector

**Resolución Rectoral de fecha 9 de febrero de 2017 por la que se aprueban las normativas de desarrollo de la política de seguridad de la información de la Universidad de Sevilla.**

Mediante Acuerdo del Consejo de Gobierno de 26 de febrero de 2014, se aprobó la Política de Seguridad de la Información de la Universidad de Sevilla, que dispone, en su artículo 9, que la citada Política "será revisada anualmente por la Comisión de Seguridad de la Información y será aprobada por Resolución Rectoral".

La Comisión de Seguridad de la Información en sesión de 16 de diciembre de 2016 acordó proponer al Rector de la Universidad de Sevilla la modificación de la Política vigente desde febrero de 2014, para su aprobación por Resolución Rectoral.

Por Resolución Rectoral de 16 de enero de 2017 se aprobó el Texto integrado de la Política de Seguridad de la Información de la Universidad de Sevilla conforme a la revisión propuesta por la Comisión de Seguridad de la Información.

El Artículo 5.1 de la Política de Seguridad de la Información dispone que entre las funciones y responsabilidades propias de la Comisión de Seguridad de la Información se encuentra proponer al Rector la aprobación de las normativas y reglamentos de seguridad relacionados con la aplicación del Esquema Nacional de Seguridad.

En la citada sesión de 16 de diciembre de 2016 la Comisión de Seguridad de la Información acordó proponer al Rector la aprobación de dichas normativas, cuyos textos se incorporan al acta de la sesión.

En su virtud, mediante la presente Resolución acuerdo:

1. Aprobar las siguientes Normativas de la Universidad de Sevilla, que se incluyen como Anexos a la misma:

- Normativa de Acceso local y remoto.
- Normativa de Clasificación y tratamiento de la información.
- Normativa de Control de acceso físico.
- Normativa de Generación de copias de seguridad y recuperación de la información.
- Normativa de Intercambio de información y uso de soportes.
- Normativa de Protección de equipos frente a código dañino.
- Normativa de Uso aceptable y seguridad básica del Servicio de atención a usuarios (SOS).
- Normativa de Uso aceptable y seguridad básica del Correo institucional.
- Normativa de Uso aceptable y seguridad básica del Servicio de enseñanza virtual.
- Normativa de Uso de portátiles corporativos.
- Normativa general de Utilización de los recursos y sistemas de la información.
- Normativa de Uso aceptable y seguridad básica de las Redes de comunicación.
- Normativa de Uso aceptable y seguridad básica del Servicio de alojamiento de páginas web.
- Normativa de Uso aceptable y seguridad básica del Portal Institucional.
- Política de contraseñas.

2. Las citadas normativas entrarán en vigor desde el día de la fecha, no obstante serán publicadas en el Boletín Oficial de la Universidad de Sevilla.

EL RECTOR,
Miguel Ángel Castro Arroyo.

## ANEXO 1

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.

## ANEXO 2

NORMAS DE SEGURIDAD
NORMATIVA DE CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN EN LA UNIVERSIDAD DE SEVILLA

Índice

**1. Introducción**

La Universidad de Sevilla (en adelante, US) maneja información de diversa índole. Gran parte de esta información es de uso interno y puede tener distintos grados de confidencialidad. Para el manejo seguro de la información es requisito indispensable clasificar la información según su naturaleza y su nivel de confidencialidad. La clasificación de la información afecta al tratamiento de los documentos y los Sistemas de Información (en adelante, SI) y a los medios de almacenamiento y transferencia de la información.

Por ello, es de suma importancia regular el manejo de la información corporativa y dar a conocer esta normativa a toda la comunidad universitaria.

**2. Objeto**

Este documento tiene el propósito de normalizar el manejo de la información por parte de la comunidad universitaria cuando accede a ella o la trata.

La presente normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica cuando la información contenga datos personales protegidos por la Ley de Protección de Datos de Carácter Personal (en adelante, LOPD).

**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.

Aplica a la clasificación y tratamiento de la información que manejan los SI de la US afectados por el ENS. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el ENS deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará 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, que la US articula a través del Documento de Seguridad.

**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 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. Normas de clasificación**

La clasificación de la información que maneja la US la realizan las personas responsables de cada información y lo harán conforme al "Procedimiento de clasificación y tratamiento de la información de la Universidad de Sevilla".

La valoración de la información que maneja la US se realiza en torno a las diferentes dimensiones de la seguridad: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

La clasificación de la información determina cómo la información se asegura, maneja, retiene y dispone. La información de la US se clasifica en una de las siguientes categorías:

- Pública: información que la organización pone a disposición del público dentro de su página Web, o que la organización ha hecho pública a través de medios de comunicación.
- Restringida de nivel básico: información sensible de la US cuya pérdida pudiera tener como consecuencia un menoscabo leve en la reputación o en las finanzas de la organización.
- Restringida de nivel alto (confidencial o reservada): información sensible de la US cuya pérdida pudiera tener como consecuencia un menoscabo grave en la reputación o en las finanzas de la organización. Se incluyen dentro de este grupo los ficheros de carácter personal declarados con nivel medio y alto.

**7.2. Normas aplicables en función de la categoría**

**7.2.1. Información pública**

- Cualquier información que se publicite a través de los medios que la US tenga establecidos para ello, debe haber pasado por una clasificación previa que asegure que no se expone información confidencial o reservada al público en general.
- Debido a la gran diversidad de información que la US maneja y a la dificultad de clasificarla en su totalidad, inicialmente toda la información sin valoración se considerará información pública, salvo que exista regulación expresa en otro sentido.
- No podrá publicarse en Internet sin restricciones de acceso la información catalogada como información restringida, sea de nivel alto o bajo.

### 7.2.2. Información restringida de nivel básico

Para el manejo de información clasificada de uso interno de nivel básico se observarán las siguientes medidas de seguridad, además de las establecidas en el punto 7.2.1:

- Se debe respetar de forma escrupulosa la política de escritorios limpios según establece la Normativa de control de acceso físico.
- Los responsables de cada entorno en los que se ubique o trate información de este nivel de confidencialidad deben gestionar las autorizaciones de acceso a dichos entornos, revisándolas periódicamente, y monitorizando los accesos, conforme a la Normativa de control de acceso físico, al Procedimiento de gestión de usuarios y acceso lógico y al Procedimiento de gestión de autorizaciones de la US.
- La información de este nivel de confidencialidad que deba utilizarse fuera de las dependencias de la Universidad ha de ser mínima y cumplir con las medidas de seguridad establecidas en la Normativa de intercambio de información y uso de soportes, a fin de evitar pérdidas de confidencialidad de la misma.
- Se deberán minimizar los cambios sobre la información publicada en entornos abiertos de acceso restringido cuando requieran la parada de un servicio y realizarlos, preferentemente, en los periodos de menor acceso a dichos entornos de acuerdo a las estadísticas de uso disponibles.
- Cualquier incidencia asociada con la indisponibilidad de la información deberá ser inmediatamente reportada al responsable de la información y/o del servicio.

### 7.2.3. Información restringida de nivel alto

Para el manejo de información clasificada como confidencial o reservada se deben observar, además de las medidas de seguridad para la información de uso interno de nivel básico del punto 7.2.2, las siguientes medidas adicionales:

- La información confidencial deberá ser tratada mediante plataformas de gestión de contenidos, gestión de documentos, gestión de versiones o similares, que permitan el registro automático de los cambios sufridos por la información y/o de los distintos estados por los que va pasando.
- Cuando la información confidencial deba ser compartida, no se hablará sobre ella en lugares públicos ni en zonas abiertas, ni siquiera dentro de las dependencias de la Universidad. Estas conversaciones deberán tener lugar en departamentos convenientemente cerrados y privados, con el fin de que no se produzcan escuchas de terceros.
- Durante el trabajo con información de este nivel de confidencialidad, se deberá prestar especial atención a que nadie ajeno a la misma puede ver dicha información. Por tanto, será necesario cubrir o proteger adecuadamente todos los documentos, en papel o electrónicos, con el fin de evitar "miradas indiscretas".
- Los documentos electrónicos con información de este nivel de confidencialidad deberán estar convenientemente protegidos, de modo que sólo puedan acceder a ellos los usuarios expresamente autorizados. La información en papel deberá guardarse adecuadamente, en lugares donde como mínimo sea necesario poseer una llave o conocer una contraseña para acceder a ellos.
- Se deberá aplicar la Política de Certificación de Firma Electrónica de @FIRMA aplicada a la US para firmar la información clasificada con este nivel de confidencialidad.
- Habrá que prestar especial atención a la realización de copias de la información de este nivel de confidencialidad, que deberán ser las mínimas posibles y tener las mismas medidas de protección que los originales. Se eliminarán todas las copias de la información de este nivel de

confidencialidad que no sean necesarias, especialmente las almacenadas de forma local en los equipos de los usuarios.

- Toda la información confidencial o reservada que contenga datos personales de nivel alto o información corporativa clasificada como restringida de nivel alto, se deberá cifrar tanto en su almacenamiento como en su transmisión. Para ello se utilizarán los mecanismos de cifrado dispuestos por la Universidad a tal efecto en los diferentes entornos:
  - Utilización de redes privadas virtuales en comunicaciones que discurran fuera del dominio de seguridad de la Universidad de Sevilla.
  - Cifrado de disco en ordenadores portátiles.
  - Herramientas de cifrado de archivos, carpetas y/o unidades en PCs, soportes extraíbles y servidores.
  - Cifrado implementado por las propias aplicaciones que lo requieran, como el e-mail. gestor documental, páginas Web, etc.

### 7.3. Normas de tratamiento de la información

#### 7.3.1. Etiquetado

- La información pública no requiere ningún tipo de marca.
- El etiquetado de la información restringida depende del tipo de soporte utilizado y se realizará conforme al "Procedimiento de clasificación y tratamiento de la información".

#### 7.3.2. Normas de acceso

- Solo los usuarios autorizados tendrán acceso a la información de uso interno. Las personas responsables de la información deberán otorgar códigos únicos de seguridad que identifiquen a los usuarios y sus contraseñas.
- La autorización de acceso a la información confidencial o reservada deberá basarse en un requisito de la Universidad, como el Usuario Virtual de la US (en adelante, UVUS), conforme establecen el "Procedimiento de gestión de la identidad y acceso lógico de la Universidad de Sevilla" y el "Procedimiento de gestión de autorizaciones de la Universidad de Sevilla".
- Los usuarios que accedan a un sistema de información no deberán dejar la sesión desatendida para evitar que alguien no autorizado pueda acceder al sistema.
- La información restringida de la US deberá utilizarse exclusivamente durante el desempeño de las tareas de la Universidad. Se prohíbe su uso para otros propósitos que estén fuera del interés de la organización.

#### 7.3.3. Normas de protección

- La información de la Universidad se protegerá en función de su clasificación y su valor. El coste de la seguridad de la información deberá corresponder al valor de la información asegurada conforme al principio de medidas proporcionadas.
- La información pública de la Universidad, sin importar el medio o naturaleza, será divulgada por los medios o vías oficiales establecidos por la propia Universidad de Sevilla.
- De ser requerido por ley o regulación, la Universidad informará acerca de las violaciones de seguridad de la información a las autoridades externas correspondientes, de inmediato.
- Los usuarios responsables de información corporativa deberán cumplir con la Normativa de generación de copias de seguridad y recuperación de información de la Universidad de Sevilla.

- Cuando la información ya no sea necesaria se procederá a su borrado y destrucción segura teniendo en cuenta que se han cumplido los requerimientos de retención de datos en cada Sistema de Información (en adelante, SI) de cara a la realización de acciones administrativas, disciplinarias, civiles o penales. Se seguirán las normas de borrado y destrucción de soportes de la Normativa de intercambio de información y uso de soportes.

### 7.4. Uso inapropiado de la información restringida

El uso inadecuado de información restringida está prohibido en la Universidad. Los usuarios autorizados no utilizarán los sistemas de información para uso no apropiado, teniendo en cuenta los siguientes puntos:

- Se prohíbe el acceso no autorizado a cualquier información de naturaleza restringida.
- Se prohíbe a los usuarios tener acceso a la información, de cualquier naturaleza o medio, para la que no hayan sido autorizados.
- Se prohíbe compartir información restringida de cualquier índole con personas que no estén autorizadas a conocer dicha información.
- Los usuarios autorizados tienen la responsabilidad de saber que si hacen un uso inapropiado de la confidencialidad de la información universitaria, puede negárseles el acceso futuro a la información y estarán sujetos a las sanciones disciplinarias establecidas.

## 8. Responsabilidades

Cada responsable de Servicios, Aplicaciones, Sistemas de Información o Responsable Propietario de Fichero en la US, dentro de su ámbito, velará por el cumplimiento de la normativa y revisará su correcta implantación o cumplimiento.

## 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

**Documento de Seguridad de la Universidad de Sevilla**

Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 1720/2007 de 13 de Diciembre), que recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

**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.

**LOPD**

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (cualquier información concerniente a personas físicas identificadas o identificables).

**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.

**UVUS**

Usuario Virtual de la Universidad de Sevilla.

## ANEXO 3

NORMAS DE SEGURIDAD
NORMATIVA DE CONTROL DE ACCESO FÍSICO

Índice



### 1. Introducción

La presente normativa establece las condiciones y acciones a realizar para el acceso físico a las ubicaciones de Tecnologías de la Información y las Comunicaciones (en adelante, TIC) de acceso restringido de la Universidad de Sevilla (en adelante, US) estableciendo tanto el protocolo de autorización como los procedimientos de acceso específicos para cada caso.

### 2. Objeto

Esta normativa trata de determinar las medidas de seguridad que se deben aplicar para llevar a cabo un correcto seguimiento y control del acceso físico en relación a la seguridad física y del entorno,

como son los controles físicos de entrada y las áreas de acceso restringido.

**3. Ámbito de aplicación**

Esta normativa será aplicable al control de acceso físico a todas las ubicaciones seguras y las áreas de acceso restringido de la US.

Esta normativa es de aplicación para todo el personal, que de manera permanente o eventual, preste sus servicios en la US, incluyendo el personal de organizaciones externas cuando sean usuarias o posean acceso a los Sistemas de Información de la US.

**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 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. Marco de aplicación**

La presente normativa regula el acceso físico a las ubicaciones que albergan Tecnologías de la Información y las Comunicaciones en la US que, por sus características especiales, requieren un acceso restringido. Todo el personal de la US y de organizaciones externas que disponga del permiso correspondiente, debe conocer y seguir las directrices de control de acceso que le afecten.

A cada local se le aplican unas medidas de seguridad de control de acceso que dependen de sus características. Con el fin de establecer unas medidas homologables, a cada local se le asigna una de las siguientes categorías:

- Centros de Proceso de Datos (en adelante CPDs): salas de equipamiento TIC en las que se ubican los Sistemas de Información de la US. Requieren unas características técnicas particulares, infraestructura específica, medidas concretas de seguridad y mantenimiento continuo para su correcto funcionamiento.
- Cuartos Técnicos de Telecomunicaciones: locales donde se ubican los racks de telecomunicaciones del edificio y/o la central telefónica del edificio o Campus.
- Salas de operación: salas, normalmente anejas a los CPDs, donde se desarrollan tareas de operación de los CPDs.
- Almacenes: locales donde se guarda material informático y de telecomunicaciones y/o copias de seguridad.
- Otros espacios TIC: el resto de espacios de trabajo que no se encuadran en las categorías anteriores como aulas TIC, laboratorios, salas de videoconferencia, seminarios, salas de servidores, etc.
- Despachos: espacios en los que desarrolla su trabajo el personal de la US y que están dotados de las infraestructuras TIC requeridas por el puesto de trabajo.

El inventario de áreas de acceso restringido, con su clasificación, se relaciona en el Anexo II de esta normativa.

En cada área restringida hay una persona encargada del control y registro de accesos a los que se refiere esta normativa. Estas personas se encargan de la identificación en primera instancia del personal autorizado. Ante cualquier duda sobre la identidad de las personas que soliciten acceso, se requerirá su autenticación a los servicios de seguridad.

### 7.2. Procedimientos de acceso

#### 7.2.1.Acceso a Centros de Proceso de Datos

Todos los CPDs deben disponer de un sistema informatizado de registro y control de acceso basado en lectores de tarjeta de proximidad. El acceso se realiza utilizando una tarjeta corporativa proporcionada por la US y, dependiendo del CPD, tecleando adicionalmente un PIN. En cada acceso queda registrado de forma automática la tarjeta, la fecha y hora en la que se produce el acceso. Sólo puede acceder a los CPDs el personal autorizado por el responsable de explotación del área restringida.

Existen tres tipos de perfiles de acceso:

- Acceso permanente: personal que realiza tareas habituales en las salas de operación y en los CPDs, y que dispone de tarjeta de acceso propia, asignada a su nombre, la cual es personal e intransferible. Aunque el acceso sea permanente, si el sistema de control de acceso lo permite, podrían existir limitaciones horarias en función del grupo al que pertenezcan. Los grupos de personas con acceso permanente son los siguientes:
  - Personal de sistemas: explotación, comunicaciones y atención a usuarios.
  - Limpieza: personal de limpieza destinado al edificio.
  - Seguridad: vigilantes de Campus y Responsable de seguridad.
  - Personal responsable de evacuación en caso de emergencia.
  - Personal de Mantenimiento de la US.

- Acceso temporal: personal interno o externo de la US que debe realizar tareas ocasionales durante un periodo de tiempo definido, y a los que se debe proveer de autorización temporal, ya sea asignando el permiso sobre su tarjeta corporativa, o en caso de no disponer de tarjeta, proporcionándole una tarjeta de cortesía a la que se asigna el permiso de acceso correspondiente y cuyo uso debe quedar registrado. Esta tarjeta podrá ser de uso diario, en cuyo caso se recogerá al inicio de la jornada de trabajo y se devolverá al finalizar, o bien permanente si es una tarjeta para un centro que dispone de instalaciones TIC. En este caso el centro será el responsable de registrar los usos de la tarjeta. Una persona con acceso permanente indicará a la persona con acceso temporal la ubicación del rack, equipo o sistema sobre el que ha de actuar.
- Visitas: personal interno o externo de la US que realiza tareas puntuales sin supervisión, visitas supervisadas o visitas guiadas a las instalaciones.
  - Visitas sin supervisión: personal que ha de acceder para realizar tareas puntuales y que no es necesario que estén acompañados mientras realizan sus tareas, por ejemplo, reparación de averías, instalaciones de cableado y de equipos, etc. Una persona con acceso permanente indicará al visitante la ubicación del rack, equipo o sistema sobre el que ha de actuar. Una vez finalizado el trabajo, lo notificará a la persona que le ha acompañado en el acceso y a la persona para la que ha realizado el trabajo, para registrar el fin de la visita.
  - Visitas supervisadas: personal que ha de acceder puntualmente y han de estar acompañados en todo momento. Si se trata de visitas de replanteo de instalaciones, transportistas, etc. el acceso al área restringida se realizará acompañado de una persona que dispone de acceso permanente, quien le acompañará hasta el rack, equipo o sistema sobre el que ha de actuar, y permanecerá acompañado en todo momento hasta la finalización de la visita.
  - Visitas guiadas a las instalaciones: se rigen por el protocolo elaborado por el Servicio de Prevención de Riesgos Laborales de la Universidad de Sevilla (en adelante SEPRUS) que recoge el documento "Recepción de Grupos de Visitantes en Instalaciones de la Universidad de Sevilla". Dada la naturaleza de estas instalaciones cada Centro podrá disponer de consideraciones particulares que deberán ser consultadas al solicitar la visita.

El procedimiento de solicitud y asignación de permisos de acceso, así como el protocolo detallado de acceso al CPD estará descrito en la normativa particular de cada instalación. El SIC dispone de una normativa propia, aprobada y disponible dentro del marco del Proceso de Gestión de la Continuidad.

En todo caso, el personal ajeno a la US que tenga que realizar cualquier tipo de trabajo en sus instalaciones, deberá ajustarse a la normativa publicada por el SEPRUS en cuanto a subcontratación de servicios externos, debiendo estar dado de alta en Portal GESPREM (coordinación de actividades empresariales en la Universidad de Sevilla) para poder realizar los trabajos en cualquier instalación objeto de este documento.

En general, el trabajo en el interior de los CPDs se regirá por la normativa básica de buenas prácticas que se especifica en el Anexo III.

Cualquier trabajador de la US que observe un incumplimiento de estas normas deberá comunicarlo al Servicio de Atención a Usuarios SOS para la apertura del oportuno incidente de seguridad.

#### 7.2.2. Acceso a Cuartos Técnicos de Telecomunicaciones

Los cuartos técnicos están siempre cerrados bajo llave o con cerradura electrónica. Sólo puede acceder a los cuartos técnicos el personal autorizado por la persona responsable. En caso de que el cuarto técnico disponga de cerradura electrónica, el procedimiento de acceso será el mismo que para los CPDs.

Los armarios de comunicaciones que estén ubicados en pasillos o en espacios de uso compartido (no exclusivos de comunicaciones) permanecerán siempre cerrados con llave.

En general, el trabajo en el interior de los cuartos técnicos de telecomunicaciones se regirá por la normativa básica de buenas prácticas que se especifica en el Anexo III.

Cualquier trabajador de la US que observe un incumplimiento de estas normas deberá comunicarlo al Servicio de Atención a Usuarios SOS para la apertura del oportuno incidente de seguridad.

**7.2.3. Acceso a Salas de Operación**

El acceso a las salas de operación se realizará en las mismas condiciones que a los CPDs, a excepción del personal externo que no dispone de tarjeta de la US y debe acceder a esta sala con DNI + PIN. Se podrán disponer video-porteros para facilitar el acceso a personal ajeno, por ejemplo, para entrega de material, para solicitud de tarjeta de cortesía, etc. La entrega de paquetes no quedará registrada.

Las visitas guiadas a las salas de operación se rigen por el mismo protocolo que los CPDs.

Cuando una persona con acceso autorizado a un CPD acceda por una sala de operación, se entiende autorizada a esta última con los permisos de acceso al CPD.

Cualquier trabajador de la US que observe un incumplimiento de estas normas deberá comunicarlo al Servicio de Atención a Usuarios SOS para la apertura del oportuno incidente de seguridad.

**7.2.4. Acceso a otros espacios TIC**

Los espacios TIC de trabajo que no se encuadran en las categorías anteriores como aulas TIC, laboratorios, seminarios, salas de servidores, salas de videoconferencia, etc. deben considerarse sensibles desde el punto de vista de la seguridad porque disponen de equipos con software y, en muchos casos, acceso a los Sistemas de Información de la US.

Deben seguirse los siguientes principios mínimos de seguridad:

- Permanecerán cerrados cuando no haya nadie trabajando en ellos.
- Fuera del horario de trabajo sólo accederán a ellos personal autorizado de limpieza y seguridad.

El procedimiento de solicitud y asignación de permisos de acceso, así como el protocolo detallado de acceso a los espacios TIC estará descrito en la normativa particular de cada instalación.

En general, el trabajo en el interior de los espacios TIC se regirá por la normativa básica de buenas prácticas que se especifica en el Anexo III.

Cualquier trabajador de la US que observe un incumplimiento de estas normas deberá comunicarlo al Servicio de Atención a Usuarios SOS para la apertura del oportuno incidente de seguridad. Cualquier presencia sospechosa se pondrá en conocimiento de los servicios de seguridad de la US.

**7.2.5. Acceso a despachos**

En general, los despachos del personal de la US están dotados de las infraestructuras TIC requeridas por el puesto de trabajo. Cada miembro de la Comunidad Universitaria será responsable del acceso restringido a su despacho y velará por la seguridad de los equipos e información del mismo. Tiene autorización de acceso a los despachos el personal de servicios de limpieza y de seguridad.

En particular, los despachos del personal que trabaja directamente con las TIC deben considerarse especialmente sensibles desde el punto de vista de la seguridad por diversas razones:

- Guardan información sobre estructura y funcionalidad de distintos sistemas de información.

- Pueden disponer de equipos con software y permisos de acceso privilegiado a sistemas de información críticos.
- En algunos casos son lugares que dan acceso a otros de idéntica o similar naturaleza.

En todos los casos deben seguirse los siguientes principios mínimos de seguridad:

- Permanecerán cerrados cuando no haya nadie trabajando en ellos.
- Fuera del horario de trabajo sólo accederán a ellos personal autorizado de limpieza y seguridad.
- En caso de ausencia, el puesto de trabajo estará bloqueado y el monitor presentará la pantalla de bloqueo.
- Se seguirá una política de escritorios limpios cuando deba abandonarse el lugar de trabajo, aunque sea de manera temporal. Se guardará bajo llave en cajones y armarios toda información que pueda considerarse sensible.

Cualquier presencia sospechosa en los despachos se pondrá en conocimiento de los servicios de seguridad de la US.

**8. Responsabilidades**

Cada persona responsable del acceso restringido a ubicaciones TIC velará, dentro de su ámbito, por el cumplimiento de la normativa y revisará su correcta implantación o cumplimiento.

**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 I: Acrónimos y glosario de términos**

**CPD**

Centro de Proceso de Datos. Espacio equipado para albergar Sistemas de Información de la US que ofrecen Servicios TIC.

**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.

**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

**Anexo II: Áreas de acceso restringido**

| Denominación | Responsable del acceso | Tipo |
|---|---|---|
| CPD Edificio Rojo y sala de operación | SIC | CPD/Sala de operación |
| Centro de Cálculo Edificio Blanco y sala de operación | ETSI Informática | CPD/Sala de operación |

| Denominación | Responsable del acceso | Tipo |
|---|---|---|
| Centro de Cálculo de Cartuja y sala de operación | ETS Ingeniería | CPD/Sala de operación |
| Cuartos de telecomunicaciones | SIC | Cuarto Técnico |
| Aulas TIC, laboratorios, seminarios,… | SIC/Centros/ Departamentos | Otros espacios TIC |
| Sala de Servidores | SIC/Centros/ Dptos/Unidades | Otros espacios TIC |
| Despachos del personal de la US | Personal de la US | Despachos |

## Anexo III: Buenas prácticas

### Normativa de trabajos en CPDs, Cuartos Técnicos de Telecomunicaciones y espacios TIC

### Normativa básica

Los CPDs, Cuartos Técnicos de Telecomunicaciones y Espacios TIC son áreas de acceso restringido donde se ubica equipamiento TI muy sensible, a las que solamente deben entrar personas previamente autorizadas y únicamente a hacer la labor encomendada.

Disponen de una infraestructura eléctrica particular, por lo que se debe consultar al operador antes de conectar móviles, portátiles, taladros, en cualquiera de las tomas eléctricas.

Son espacios climatizados para mantener la óptima refrigeración de los equipos TI y no con criterios de confort. Para su eficiente funcionamiento se debe evitar tener la puerta abierta. En el CPD no se deben retirar simultáneamente más de 6 losetas del suelo técnico.

El CPD tiene un sistema de detección y extinción automática de incendios. Los detectores son muy sensibles por lo que está prohibido hacer trabajos con llama, chispa o que generen polvo o humo. Todas estas operaciones: soldaduras, cortes, taladros,… se deben realizar fuera del CPD. En el caso que no pueda realizarse en el exterior se debe solicitar autorización para hacerlo dentro, poniendo todas las medidas necesarias para minimizar la emisión de polvo y suciedad.

Tanto en el CPD como en los Cuartos Técnicos de Telecomunicaciones y otros espacios TIC se debe tener especial sensibilidad con el orden y la limpieza:

- Ensuciar y desordenar lo mínimo al realizar los trabajos.
- Dar un acabado pulcro y de calidad a los trabajos.
- Recoger y limpiar todo cuando se finalizan los trabajos.
- Los embalajes y las basuras se retiraran como mínimo al finalizar cada jornada.
- NO se podrá dejar NADA (documentación, CD-s, cables, conectores,…) en las mesas o en los racks.
- Las conexiones eléctricas y de red se harán con cables y/o fibras de longitud adecuada.

Es responsabilidad del trabajador traer las herramientas necesarias para hacer su trabajo, guardar las medidas de seguridad y atender los consejos del Servicio de Prevención de Riesgos Laborales.

### Acceso a salas de servidores y/o sala de explotación

La tarjeta de acceso al CPD y a los Cuartos Técnicos de Telecomunicaciones es personal e intransferible. No se puede acceder acompañado de otras personas que no dispongan a su vez de tarjeta de acceso con los permisos de acceso a dichas salas.

Una vez dentro del CPD, se deben seguir las siguientes directrices:

- Queda PROHIBIDO abrir las ventanas y/o levantar las persianas.
- Queda PROHIBIDO manipular los sistemas de climatización, de incendios y cuadros eléctricos.
- Queda PROHIBIDO levantar las losetas, salvo permiso concedido expresamente para dicha visita o acceso.
- Asímismo queda PROHIBIDO enchufar o desenchufar equipos en los enchufes dispuestos bajo las losetas, salvo que se disponga de permiso expreso.
- Queda PROHIBIDO manipular cualquier otro equipo del que no sea titular.
- Queda PROHIBIDO beber y comer en las instalaciones.

Cualquier duda sobre estas normas o sobre cualquier necesidad que surja mientras se trabaja en el CPD deberá ser consultada con los operadores.

Se debe avisar de cualquier anormalidad observada a los técnicos de las salas de explotación, o bien al servicio de seguridad, sobre todo si se encuentra en la instalación fuera de las horas habituales de trabajo del personal de la US.

## ANEXO 4

NORMAS DE SEGURIDAD
NORMATIVA DE GENERACIÓN DE COPIAS DE SEGURIDAD
Y RECUPERACIÓN DE INFORMACIÓN

Índice



### 1. Introducción

La información de la Universidad de Sevilla (en adelante, US) debe estar protegida frente a posibles pérdidas o daños. Es necesario disponer de normas adecuadas para la realización de copias de seguridad de la información que garanticen la recuperación de la misma.

### 2. Objeto

El objetivo del presente documento es definir las directrices para garantizar el respaldo, la protección

y la disponibilidad de la información corporativa, contenga o no datos personales, para restaurarlos en caso de pérdida o daño de los datos originales. Se aplicarán las medidas de seguridad necesarias que permitan el almacenamiento y recuperación de los datos atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas 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 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 el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de la US.

La presente normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la US, especialmente, los responsables del Servicio de Informática y Comunicaciones (en adelante, SIC) y los propios usuarios, como actores ambos, en sus respectivas competencias, de la generación de copias de respaldo y su ulterior recuperación, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información de la US.

En el ámbito de la presente normativa, se entiende por usuario cualquier empleado público perteneciente o ajeno a la US, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la US y que utilice o posea acceso a los Sistemas de Información (en adelante, SI) de la US.

**4. Vigencia**

La presente Normativa ha sido aprobada por el Comité 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 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.

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**

Se realizarán copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada. Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de respaldo deberán abarcar:

a. Información de trabajo de la organización.
b. Aplicaciones en explotación, incluyendo los sistemas operativos.
c. Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
d. Claves utilizadas para preservar la confidencialidad de la información.

**7.1. Copias de respaldo de los SI y recuperación**

Para garantizar la continuidad de los servicios, todos los datos almacenados en los servidores y dispositivos de almacenamiento de los SI corporativos que gestiona la US se deben copiar de manera regular. De esta forma, se establecen los mecanismos necesarios para garantizar la continuidad de los servicios en caso de pérdida de datos.

- Todos los datos del ámbito de aplicación del ENS a la US serán periódicamente respaldados en soportes de backup.
- Los Responsables correspondientes de la Información y los Servicios, asesorados por el Responsable del Sistema y el Responsable de Seguridad, establecerán los ciclos de copia más adecuados para cada tipo de información.
- Las copias de respaldo deben abarcar todos los datos necesarios para recuperar el servicio en caso de corrupción o pérdida de datos.
- Las copias de seguridad estarán guardadas en un lugar seguro con medidas de seguridad físicas, de forma que el personal no autorizado no tenga acceso. Deben estar identificadas y etiquetadas con la información útil que se considere necesaria.
- Siempre debe existir una copia adicional almacenada en un armario ignífugo o procedimiento alternativo como medida de recuperación ante desastres y, dependiendo del nivel de seguridad de la información y los servicios prestados, se debe mantener un segundo juego de copias offsite, en otro edificio y en armario ignífugo.
- El traslado de los volúmenes de las copias se debe realizar conforme a la Normativa de intercambio de información y uso de soportes.
- Se debe definir un procedimiento de recuperación de las copias de seguridad, de forma que incluya las pautas para los diferentes sistemas operativos.
- Cuando la información que manejan los SI contengan datos personales protegidos por la LOPD

se aplicarán, además, las normas establecidas en el Documento de Seguridad de la US.

- Cada SI dispondrá de un procedimiento de copias de respaldo que incluirá, al menos, estos elementos:
  a. Nivel de seguridad de la información
  b. Periodicidad de las copias de respaldo acorde al tipo de dato o servicio
  c. Ventana de backup más adecuada
  d. Periodos de retención de las copias
  e. Ubicación de los soportes de respaldo
  f. Procedimientos de recuperación de la información
  g. Procedimientos de restauración de los servicios y verificación de la integridad de la información respaldada
  h. Procedimientos de inventario y gestión de soportes para backup
  i. Procedimiento de revisión de logs de copias de seguridad

### 7.2. Copia de respaldo de los equipos de usuario

Los usuarios son responsables de la realización de copias de respaldo periódicas de la información de sus puestos de trabajo, especialmente cuando haya cambios significativos en la información que manejan.

- En ningún caso se deberán almacenar copias de respaldo en dependencias de terceros ajenas a la US si no existe un acuerdo institucional previamente suscrito con el tercero en el que se expliciten las cautelas debidas respecto de la custodia de la información almacenada.
- Si el usuario trata información corporativa en su puesto de trabajo, los responsables de las unidades administrativas de la US deberán asegurarse de que los empleados a su cargo salvaguardan dicha información de forma satisfactoria dentro de las dependencias de la US de acuerdo a los recursos disponibles.
- En caso de uso de ordenadores portátiles corporativos, el usuario se atendrá a la "Normativa de uso de portátiles corporativos de la Universidad de Sevilla".

### 7.3. Tipos de copias de respaldo

En función del tipo de información, como parte de la estrategia de copias de seguridad, se podrán utilizar los siguientes tipos de copias de respaldo:

- Copia completa o FULL: copia completa de todos los datos principales, ficheros y bases de datos.
  a. Requiere mayor espacio de almacenamiento y ventana de backup.
  b. Ofrece la seguridad de tener una imagen de los datos en el momento de la copia.
- Copia incremental: copia de los datos modificados desde la anterior copia completa o incremental.
  a. Siempre se debe partir de una copia total o completa inicial.
  b. Si se realiza con frecuencia, el proceso no consumirá un tiempo excesivo, debido al bajo volumen de datos a copiar.
  c. La restauración completa es lenta: se requiere recuperar una copia completa y todas las incrementales realizadas hasta el momento en el cual se quiera restaurar el sistema.
- Copia diferencial: copia de los datos que hayan sido modificados respecto a una copia completa anterior.

a. Requiere menor espacio de almacenamiento y ventana de backup.
b. Se ejecutará con mayor rapidez en función de la frecuencia con que se realice.
c. La restauración suele ser más rápida que la incremental, ya que basta con recuperar una copia completa y una copia diferencial.

### 7.4. Verificación y comprobación de las copias

Se deben comprobar los registros de logs de las copias de seguridad de forma que, ante una incidencia, sea posible relanzar de nuevo la copia de seguridad.

Los responsables de los SI deben realizar pruebas periódicas de restauración de las copias realizadas, de forma que se garantice la integridad de las mismas. La información del ámbito de aplicación del ENS, almacenada en un medio informático durante un período prolongado de tiempo, deberá ser verificada al menos una vez al año, para asegurar que la información es recuperable.

### 7.5. Retención de las copias

Los documentos originales y los ficheros en formato electrónico deben ser retenidos durante el tiempo que en cada caso el ordenamiento jurídico prescriba. Los Responsables de la Información y los Servicios, asesorados por el Responsable de Seguridad y el Gabinete Jurídico, en su caso, se encargará de definir los periodos de retención de la información en función de la naturaleza de la misma y del ordenamiento jurídico vigente en cada momento.

- El procedimiento de copias de respaldo de cada SI definirá el periodo de retención de las copias que se realizan.
- Hay que tener en cuenta los requerimientos de retención de datos en cada SI de cara a la realización de acciones administrativas, disciplinarias, civiles o penales (por ejemplo, logs para auditorías). Se implantarán los medios necesarios para poder revisar las actividades de los usuarios que manejan este tipo de información.
- Cuando la información deje de ser necesaria, deberá ser destruida o eliminada de manera segura. Los soportes de información que se desechen serán eliminados conforme a la Normativa de intercambio de información y uso de soportes.

## 8. Responsabilidades

Cada Responsable de Información o de SI de la US, dentro de su ámbito, velará por el cumplimiento de esta normativa y revisará su correcto cumplimiento, asegurándose de la existencia de un procedimiento de copias de respaldo y recuperación y su implantación efectiva.

## 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

**Backup**

Palabra inglesa utilizada habitualmente para hacer referencia a la copia de seguridad o copia de respaldo en tecnologías de la información. Es la copia de datos que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida parcial o total.

**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.

**Offsite**

En el ámbito de las Tecnologías de la Información y las Comunicaciones, la palabra inglesa offsite hace referencia a la localización alternativa al lugar de producción primario (Centro de Proceso de Datos principal o de producción), en la que se almacenan copias de seguridad y documentación vitales para su uso durante la recuperación de un desastre que implique pérdida total o parcial de datos en los Sistema de Información.

**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.

## ANEXO 5

NORMAS DE SEGURIDAD
NORMATIVA DE INTERCAMBIO DE INFORMACIÓN Y USO DE SOPORTES

Índice

**1. Introducción**

En la estructura y organización de la seguridad de los Sistemas de Información (en adelante, SI) de la Universidad de Sevilla (en adelante, US), se prestará especial atención a la información corporativa en tránsito, contenga o no datos personales, independientemente de que para ello se utilicen soportes físicos, servicios electrónicos o papel.

Las medidas de seguridad aplicadas deben garantizar:

- El control permanente del medio en el que está la información a lo largo de su ciclo de vida.
- El control del acceso a la información contenida como garantía para preservar su confidencialidad e integridad.

**2. Objeto**

La presente normativa establece las condiciones generales para preservar la autenticidad, integridad, confidencialidad y disponibilidad del almacenamiento, transmisión y procesamiento de la información de los SI de la US entre los usuarios que deban manejar los datos.

El objetivo es regular, en función del medio utilizado, la protección de información en tránsito para preservarla en todas sus dimensiones, especialmente si es información reservada, confidencial o contiene datos de carácter personal protegidos por la Ley Orgánica de Protección de Datos (en adelante, LOPD).

**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.

Aplica a la información en tránsito que manejan los SI de la US afectados por el Esquema Nacional de Seguridad (en adelante, ENS) independientemente del medio utilizado, sea éste un soporte (objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos), una comunicación electrónica (correo electrónico, aplicaciones de intercambio de información, etc.) o papel.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el Esquema Nacional de Seguridad deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará 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, que la US articula a través del Documento de Seguridad.

Los procedimientos de salvaguarda y conservación de los documentos electrónicos producidos por la US en el ámbito de sus competencias se regulan en el "Procedimiento de copias de seguridad de la información de la US".

**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 de las Tecnologías de la Información y las Comunicaciones (en adelante, 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**

La entrada y salida de información de los SI de la US en cualquier soporte, por cualquier medio de comunicación o en papel, contengan o no datos personales, deberá ser realizada exclusivamente por personal autorizado por la propia Universidad.

Como norma general, los usuarios se abstendrán de sacar al exterior cualquier información de los SI de la US en cualquier soporte, comunicación electrónica o papel, salvo autorización expresa.

Cuando se trate de SI categorizados de nivel bajo o de datos personales de nivel básico, las operaciones con soportes serán autorizadas por el responsable del SI, en su caso, o por el responsable del fichero de datos personales. En este caso podrán estar autorizadas en el Documento de Seguridad de la US.

Los SI categorizados de nivel medio y los datos personales a partir del nivel medio, requieren una gestión más exhaustiva de la información en tránsito y los soportes utilizados para ello.

La entrada y salida de datos sensibles, confidenciales o protegidos, y los datos pertenecientes a ficheros de datos registrados con nivel alto en la Agencia Española de Protección de Datos, requerirán el cifrado de la información o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte.

**7.1. Gestión de soportes físicos**

**7.1.1. Inventario de soportes**

Cualquier soporte con información corporativa de los SI de la US o que contenga datos de nivel medio

en adelante protegidos por la LOPD debe estar inventariado. Los responsables de la información serán los encargados de gestionar el inventario de los soportes físicos. El inventario de los soportes físicos debe contener, al menos:

- Código del soporte
- Tipo de soporte físico utilizado
- Fecha de alta/baja
- Tipo de información que contiene
- Nivel de seguridad de la información que contiene
- Responsable del soporte
- Personas autorizadas para acceder al soporte
- Estado: activo/baja/extraviado/averiado
- Observaciones

**7.1.2. Etiquetado de soportes**

Los soportes que contengan información corporativa o datos personales se deben etiquetar utilizando códigos que, sin revelar el contenido del soporte, permitan identificar el tipo de información que contienen a los usuarios autorizados.

Los usuarios han de estar capacitados para entender el significado de las etiquetas, bien mediante simple inspección, bien mediante el acceso a un repositorio que lo explique.

**7.1.3. Registro de operaciones con soportes**

Los soportes que contengan información de los SI de nivel medio de la US o datos protegidos por la LOPD a partir de nivel medio, deben permanecer bajo control. Para ello:

- Se dispondrá de un registro de entrada/salida de información que identifique los soportes y las personas que van a transportar la información.
- Se dispondrá de un procedimiento rutinario que levante las alarmas pertinentes cuando se detecte algún incidente con la información en tránsito.
- Se utilizarán los medios de protección criptográfica correspondientes al nivel de calificación de la información contenida de mayor nivel y se protegerán las claves criptográficas durante todo su ciclo de vida.

El responsable de la información garantizará que se satisfacen los requisitos de seguridad mientras los datos están siendo desplazados de un lugar a otro:

- Si la información es relativa a servicios, corresponde al Responsable del Servicio con el que está relacionada.
- Si se trata de información con datos de aplicación propia o ajena, corresponde al Responsable de la Aplicación.
- Si la información contiene datos de carácter personal, corresponde al responsable propietario del fichero aplicar las medidas físicas/lógicas acordes al nivel de protección exigido por la LOPD, recogidas en el Documento de Seguridad de la US.

Cuando el personal que maneja los soportes es personal ajeno a la Universidad, ya sea trabajando en ella o en las dependencias de una empresa externa, se observarán las siguientes normas:

- La empresa deberá firmar un acuerdo de tratamiento de datos con la Universidad de Sevilla.

- Si se trata de datos personales será preciso que exista una autorización previa del responsable del fichero registrada en el Documento de Seguridad. Dicha autorización podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez de la misma.
- En todo caso, deberá garantizarse el nivel de seguridad de los datos tratados.

Los registros de entrada/salida de información en soporte físico deben contener, al menos, la siguiente información:

- Código del soporte (el asignado en el inventario)
- Operación (entrada/salida)
- Fecha y hora de la operación
- Emisor o receptor autorizado
- Forma de envío
- Comentarios

#### 7.1.4. Borrado y destrucción de los soportes

Todos los usuarios deben garantizar un uso responsable de los soportes que contienen información de los SI de la US, contengan o no datos personales, debiendo eliminar de forma segura la información corporativa contenida en ellos una vez finalizada su función.

- En caso de reutilizar un soporte para otra información, el borrado será proporcionado a la clasificación de la información que ha contenido. Se borrará el soporte utilizando productos certificados siempre que sea posible y siguiendo las recomendaciones del NIST SP 800-88 conforme a la Guía CCN-STIC 804. El responsable de la información borrada registrará la baja del soporte y el responsable de la nueva información registrará el alta con un nuevo código.
- En caso que se detecte la necesidad de destrucción del soporte extraíble (por avería, porque el soporte no permita un borrado seguro o por mandato legal como en el caso de datos personales según la LOPD) el usuario debe avisar al responsable de la información correspondiente. El responsable debe registrar la baja del soporte y proceder a su destrucción segura siguiendo las directrices de la Guía CCN-STIC 804, con el fin de evitar un posible acceso indebido a la información contenida.
- En caso de obsolescencia, el responsable procederá a la destrucción del soporte y anotará su baja.

#### 7.1.5. Control de acceso a los soportes

El control de acceso a los SI de la US se regula mediante la "Normativa de control de acceso físico" a las dependencias de la US que disponen de Tecnologías de la Información y de las Comunicaciones y mediante el "Procedimiento de gestión de usuarios y acceso lógico".

El "Procedimiento de autorizaciones de la Universidad de Sevilla" regula la gestión de autorizaciones e identifica a los responsables de la gestión de accesos.

Si el soporte contiene datos de carácter personal, la autorización para su uso deberá ser otorgada por el responsable del fichero cuyos datos vayan a ser almacenados en el soporte. El responsable del fichero o la persona en la que delegue será quien gestione el control de acceso mediante el registro habilitado a tal fin. En todo caso, el procedimiento a seguir dependerá del nivel de protección de los datos y queda establecido en el Documento de Seguridad de la US, en su apartado "Medidas y normas para la Gestión de soportes".

#### 7.1.6. Custodia de la información albergada en soportes

El personal de la US debe ser consciente de la responsabilidad en la custodia del soporte físico que contenga información de los SI de la US, especialmente si dicha información es sensible.

A estos efectos, el usuario deberá:

- Asegurar la custodia de dichos soportes y evitar dejarlos conectados a los equipos informáticos o sobre la mesa de trabajo cuando no se utilicen, debiendo quedar siempre a resguardo del acceso de cualquier otra persona no autorizada.
- Garantizar que se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.

En el caso de pérdida de un soporte o de cualquier otro incidente ocurrido con la información almacenada en el mismo, se deberá poner inmediatamente en conocimiento del responsable de la información, quien lo anotará en el registro de incidentes de seguridad y procederá a ejecutar un plan de respuesta al incidente, tomando las acciones oportunas.

### 7.2. Servicios electrónicos corporativos

Para la entrada/salida de información corporativa de los SI de la US a través de redes de comunicación, especialmente si la información es reservada, confidencial o contiene datos de carácter personal protegidos por la LOPD, sólo deben utilizarse los servicios electrónicos corporativos dispuestos por la US, tales como correo electrónico, carpetas compartidas o servicios de gestión documental y colaborativos, quedando totalmente prohibida la utilización de soluciones ajenas a la US.

Se puede utilizar indistintamente una solución corporativa u otra para el almacén o el intercambio de información, teniendo en cuenta que existen límites en los tamaños de los ficheros o documentos a intercambiar.

La autorización de intercambio de información entre emisores y receptores de información corporativa constará en los acuerdos de servicio entre unidades administrativas de la US, o en los contratos con las empresas prestatarias de servicios si son externos. Los logs de los servicios electrónicos corporativos harán las funciones de registro de transferencias de información.

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al nivel correspondiente a los accesos en modo local, cumpliendo, en todo caso, las medidas y normas para la información en tránsito por vía electrónica conforme al Documento de Seguridad de la US.

### 7.3. Cifrado de la información

Los SI de la US, al estar categorizados como sistemas de nivel medio, no requieren de cifrado de la información en soporte físico en tanto que no contengan datos personales de nivel alto.

Si la información que manejan los SI de la US contiene datos personales de nivel alto, los responsables de los ficheros deberán adoptar las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en los dispositivos o a través del intercambio de información por medios electrónicos:

- La información se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.

- Para proteger la confidencialidad en las comunicaciones, se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad y se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
- Para el uso de criptografía en los soportes de información, se aplicarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida y que estén acreditados por el Centro Criptológico Nacional y, preferentemente, productos conformes a normas europeas o internacionales que estén certificados por entidades independientes de reconocida solvencia.

En todo caso, siempre que la información contenga datos de carácter personal, se actuará conforme a lo establecido en el Documento de Seguridad de la US.

NOTA: tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas. Tendrán la consideración de entidades independientes de reconocida solvencia las recogidas en los acuerdos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información u otras de naturaleza análoga.

**8. Responsabilidades**

Los responsables de Servicios, Aplicaciones, Sistemas de Información o Responsables Propietarios de Fichero en la US, dentro de su ámbito, velarán por el cumplimiento de la normativa y revisarán su correcta implantación.

El responsable adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones y las consecuencias en caso de incumplimiento.

**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**

**AUTENTICIDAD**

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

**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.

**CONFIDENCIALIDAD**

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

**DATOS DE CARÁCTER PERSONAL**

Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

**DISPONIBILIDAD**

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Documento de Seguridad de la Universidad de Sevilla

Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 1720/2007 de 13 de Diciembre), que recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

**INTEGRIDAD**

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

**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.

**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.

## ANEXO 6

NORMAS DE SEGURIDAD
NORMATIVA DE PROTECCIÓN DE EQUIPOS FRENTE A CÓDIGO DAÑINO

Índice

**1. Introducción**

La utilización de los Servicios de Tecnologías de Ia 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.

## ANEXO 7

NORMAS DE SEGURIDAD
NORMATIVA DE USO ACEPTABLE Y SEGURIDAD BÁSICA DEL SERVICIO DE ATENCIÓN A USUARIOS SOS DE LA UNIVERSIDAD DE SEVILLA

Índice



### 1. Introducción

Este documento define las normas de uso y seguridad que deben seguir todos los usuarios del Servicio de Atención a Usuarios SOS en su relación con las Tecnologías de la Información y las Comunicaciones (en adelante, TIC) que presta la Universidad de Sevilla (en adelante, US). Las normas han sido elaboradas con el objetivo de conseguir un uso más eficiente, correcto y seguro de los recursos destinados a dicho Servicio.

### 2. Objeto

El objeto de la presente normativa es definir y regular la prestación del Servicio de Atención a Usuarios SOS en su relación con las TIC desde las distintas sedes de la Universidad de Sevilla o a través de ellas, posibilitando la homogeneización de criterios dentro de sus unidades administrativas y definiendo

unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

**3. Ámbito de aplicación**

Esta normativa será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, pertenezca a la comunidad universitaria y tenga acceso al Servicio de Atención a Usuarios SOS de la US por cualquiera de las vías habilitadas para ello en función de su categoría de Estudiante, Personal Docente e Investigador (en adelante, PDI) o Personal de Administración y Servicios (en adelante, PAS).

Los usuarios serán informados de esta normativa de uso aceptable y seguridad básica y aceptarán que el Servicio de Informática y Comunicaciones (en adelante, SIC) sea el garante del cumplimiento de las mismas. Así mismo podrán proponer al órgano pertinente las modificaciones a este documento que consideren oportunas para ajustarlo a la lógica evolución tecnológica y legislativa que se produzca, manteniendo el espíritu del mismo en lo que respecta a los objetivos y finalidades del Servicio de Atención a Usuarios SOS. Los usuarios serán puntualmente informados de cualquier modificación que fuera preciso introducir.

**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 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 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.

Cuando las circunstancias así lo aconsejen, el SIC 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. Términos y condiciones de acceso y uso

Estos términos y condiciones de acceso y uso regulan el uso del Servicio de Atención a Usuarios SOS de la US.

### 7.1. Registro del usuario

El acceso al Servicio de Atención a Usuarios SOS de la US requiere de un Usuario Virtual de la Universidad (en adelante, UVUS) para el acceso a la Plataforma de Gestión de Incidencias a través de la cual Estudiantes, PDI y PAS podrán realizar su petición de servicio.

El usuario se compromete a usar sus claves de acceso (nombre de usuario y contraseña) de acuerdo con las restricciones que aparecen en este documento y la normativa asociada.

### 7.2. Condiciones de uso

Para garantizar y optimizar el mejor funcionamiento del Servicio de Atención a Usuarios SOS se hace necesaria una serie de compromisos entre los usuarios y los responsables del Servicio.

El SIC, como responsable de este servicio, debe asegurar:

- La disponibilidad del Servicio de Atención a Usuarios SOS de la US conforme a los compromisos de calidad adquiridos en la Carta de Servicios del SIC.
- La salvaguarda de la información relacionada con las peticiones de servicio.
- Los compromisos por parte de los usuarios del Servicio de Atención a Usuarios SOS de la US son los siguientes:
- Hacer un uso aceptable del Servicio, respetando los fines para los que ha sido creado y utilizando correctamente los recursos del mismo.
- Acreditar que el equipo para el que solicita el servicio está inventariado por la Universidad de Sevilla en los casos en que así se requiera.
- Cumplir las normas de seguridad definidas en el presente documento.

### 7.3. Uso aceptable

Los usuarios del Servicio de Atención a Usuarios SOS de la US utilizarán el mismo para:

- Solicitar la atención y resolución de consultas e incidencias relacionadas con las TIC según el alcance del Servicio de Atención a Usuarios SOS publicado en el Portal Institucional de la Universidad de Sevilla.

En general los usuarios del Servicio de Atención a Usuarios SOS de la US deberán utilizar eficientemente el servicio con el fin de evitar perjuicios al resto de usuarios.

### 7.4. Uso no aceptable

El Servicio de Atención a Usuarios SOS de la US no debe usarse para:

- Fines privados o personales.
- Peticiones de servicios no proporcionados por el SIC.

### 7.5. Aceptación y compromiso de cumplimiento

El uso del Servicio de Atención a Usuarios SOS de la US implica el conocimiento y plena aceptación de las advertencias legales y condiciones vigentes en cada momento en que el usuario acceda al mismo y que se especifican en este documento.

Cualquier usuario que incumpla alguno de los términos especificados en este documento deberá asumir las responsabilidades derivadas de la utilización incorrecta del Servicio de Atención a Usuarios SOS de la US.

**8. Desarrollo de la normativa**

- A fin de reducir el riesgo en el uso del servicio de Atención a Usuarios SOS, el usuario de este servicio deberá cumplir las normas que se incluyen a continuación:
- El usuario deberá hacer llegar su petición a través de las vías establecidas para ello que se podrán consultar en el Portal Institucional de la Universidad de Sevilla, en el apartado "Utilidades", "Solicitud de Ayuda al SOS".
- Como norma general no se atenderá más de un portátil o más de un puesto de trabajo fijo, aun estando inventariados.
- El usuario utilizará los puestos de trabajo únicamente para fines institucionales y como herramienta de apoyo a sus competencias profesionales.
- Todo el software que se utilice estará licenciado conforme a la legislación vigente en materia de Propiedad Intelectual.
- El usuario respetará las recomendaciones que se hagan en cuanto a Navegadores, versiones de Java, etc., para el uso de las aplicaciones corporativas.
- El usuario debe ser consciente de las amenazas provocadas por código malicioso (malware) para no contribuir a su propagación mediante dispositivos removibles (CDs/DVDs, memorias USB u otros de naturaleza análoga), mensajes de correo electrónico o instalación de programas descargados desde Internet cuyo origen es desconocido.
- Como norma general, no se utilizarán aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.).
- Cualquier material cedido por la Universidad estará bajo la custodia del usuario que lo utilice y deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- La sustracción de estos equipos se ha de poner inmediatamente en conocimiento de la Universidad para la adopción de las medidas que correspondan.
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático por parte de la US el usuario lo devolverá al objeto de proceder al borrado seguro de la información almacenada y para que pueda ser asignado a un nuevo usuario.

Además de las anteriores normas, se recomienda:

- Mantener actualizados los sistemas operativos de equipos y dispositivos móviles, y los programas que tengan instalados, al menos en cuanto a parches de seguridad, así como mantenerlos correctamente configurados.
- Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.
- Realizar copias de seguridad periódicas de los equipos. La información almacenada en los puestos de trabajo de los usuarios no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad.

- Avisar al Servicio de Atención a Usuarios SOS de cualquier incidencia que pueda surgir y que se estime pueda afectar al normal comportamiento de los Servicios de Tecnología de la Información y las Comunicaciones (en adelante, TIC) de la US.

**9. Responsabilidades**

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, el SIC, dependiendo de la gravedad y reiteración del incidente, procederá a aplicar una de estas medidas:

**Suspensión temporal del acceso al Servicio de Atención a Usuarios SOS**

Esta medida se tomará cuando se produzca la violación de los términos de este documento de forma premeditada, cuando se esté causando una degradación en los recursos del Servicio de Atención a Usuarios SOS o se implique a la US en algún tipo de responsabilidad que conlleve perjuicio para sus usuarios.

**Suspensión indefinida del acceso al Servicio de Atención a Usuarios SOS**

Esta medida se aplicará cuando se incurra en infracciones de especial gravedad o en una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por el cauce adecuado.

En ambos casos el servicio podrá restablecerse cuando se considere que las medidas adoptadas por el usuario garanticen un uso aceptable del Servicio en el futuro.

**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**

**SERVICIO DE INFORMÁTICA Y COMUNICACIONES**

Servicio de la Universidad responsable de atender las necesidades de apoyo informático para las tareas de docencia, investigación y gestión, de todos los miembros de la comunidad universitaria.

**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.

**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.

**SOPORTE DE OPERACIONES Y SISTEMAS (SOS)**

Servicio responsable de la recepción de todas las incidencias informáticas y de resolver aquellas de 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.

**USUARIOS DEL SERVICIO DE ATENCIÓN A USUARIOS SOS**

Estudiantes, profesores, investigadores, personal de la administración y servicios, usuarios de las instituciones conectadas a la red de la US y, en general, cualquier persona que, por su relación con la US, sea autorizada para usar cualquier servicio TIC que esta presta.

**UVUS**

Usuario Virtual de la Universidad de Sevilla.

**P2P**

Una red peer-to-peer, red de pares (red entre iguales o red entre pares) es una red de ordenadores en la que todos actúan simultáneamente como clientes y servidores respecto a los demás, permitiendo el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

**PORTAL INSTITUCIONAL DE LA US**

Página oficial de la Universidad de Sevilla que proporciona el acceso a la mayor parte de los contenidos Web institucionales, académicos y de investigación existentes en la Universidad.

**Salvaguardas**

Medidas aplicadas para protección de la información contenida en su alojamiento.

## ANEXO 8

NORMAS DE SEGURIDAD
NORMATIVA DE USO ACEPTABLE Y SEGURIDAD BÁSICA DEL CORREO INSTITUCIONAL DE LA UNIVERSIDAD DE SEVILLA

Índice

**1. Introducción**

Este documento define las normas de uso y seguridad que deben seguir todos los usuarios que dispongan de una cuenta de correo corporativa en la Universidad de Sevilla (en adelante US). Las normas han sido elaboradas con el objetivo de conseguir un uso más eficiente, correcto y seguro de los recursos destinados a dicho Servicio.

**2. Objeto**

El objeto de la presente normativa es regular el acceso y utilización del correo electrónico (e-mail) por parte de los usuarios de los Sistemas de Información de la US, desde los distintos Campus o cualquier ubicación posible, posibilitando la homogeneización de criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

**3. Ámbito de aplicación**

La presente normativa será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, pertenezca a la comunidad universitaria, incluyendo el personal de organizaciones externas cuando sean usuarios o posean acceso al Servicio de Correo de la US.

En particular, las normas contenidas en este documento serán de aplicación para todos los usuarios que dispongan de un buzón de correo corporativo o hagan uso de buzones en estafetas secundarias de correo de la US.

Los usuarios serán informados de esta Normativa de uso aceptable y seguridad básica y aceptarán que el Servicio de Informática y Comunicaciones (en adelante, SIC) sea el garante del cumplimiento de las mismas. Así mismo podrán proponer al órgano pertinente las modificaciones a este documento que consideren oportunas para ajustarlo a la lógica evolución tecnológica y legislativa que se produzca, manteniendo el espíritu del mismo en lo que respecta a los objetivos y finalidades del correo institucional. Los usuarios serán puntualmente informados de cualquier modificación que fuera preciso introducir.

**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 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 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.

Cuando las circunstancias así lo aconsejen, el SIC 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. Términos y condiciones de acceso y uso**

Estos Términos y condiciones de acceso y uso regulan el uso del sistema de correo de la US.

**7.1. Registro del usuario**

El acceso y utilización del correo electrónico de la US por parte del usuario requiere de la existencia de un buzón de correo para el mismo. Este espacio depende directamente de la creación del Usuario Virtual de la US (UVUS). La información sobre estos servicios se encuentra accesible vía Web a través de la página del Servicio de Informática y Comunicaciones (en adelante SIC) de la US (http://sic.us.es).

La utilización de los sistemas de estafetas primarias por parte de las estafetas secundarias definidas depende de la viabilidad y coordinación entre los responsables de las mismas y el SIC.

El usuario se compromete a usar sus claves de acceso (nombre de usuario y contraseña) de acuerdo con las restricciones que aparecen en este documento.

**7.2. Condiciones de uso**

Para garantizar y optimizar el mejor funcionamiento del correo electrónico institucional se hace necesaria una serie de compromisos entre los usuarios y los responsables del Servicio de Correo Electrónico.

El SIC, como responsable de este servicio, debe asegurar:

- La disponibilidad del correo electrónico de la US conforme a los compromisos adquiridos de conformidad con el Acuerdo de Nivel de Servicio (SLA).
- La salvaguardia de la información almacenada en los buzones de correo electrónico.

Los compromisos por parte de los usuarios del correo electrónico de la US son los siguientes:

- Hacer un uso aceptable del correo de la US, respetando los fines para los que ha sido creado y utilizando correctamente los recursos que se le suministran.
- Evitar la interrupción de los servicios que ofrece.
- Evitar situaciones que afecten a la seguridad del correo y de sus usuarios
- Cumplir las normas de seguridad definidas en el presente documento.
- Comunicar los problemas que surjan al Servicio de Atención de Usuarios del SIC para su resolución.

**7.3. Uso aceptable**

Los usuarios del Correo electrónico de la US utilizarán el mismo para:

- La comunicación con otros usuarios, siempre que se trate de información cuyo contenido sea de investigación, académico, educacional o necesario para el desempeño de la función administrativa.

En general los usuarios del correo de la US deberán utilizar eficientemente el servicio con el fin de evitar perjuicios al resto de usuarios.

### 7.4. Uso no aceptable

El Correo Institucional de la US no debe usarse para:

- Difundir mensajes con contenidos contrarios a los principios enunciados en los Estatutos de la US: mensajes con contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o que actúen en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.
- Enviar información que viole los derechos de propiedad intelectual, la LOPD o cualquier otra legislación vigente.
- Enviar información que cause cualquier tipo de molestia a otros usuarios, incluida la información difamatoria de cualquier tipo, ya sea contra entidades o personas.
- Fines privados comerciales no autorizados por la US.
- El desarrollo de actividades que produzcan:
  - La congestión de la red de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
  - La destrucción, modificación o apropiación indebida de la información de otros usuarios.
  - La violación de la privacidad e intimidad de otros usuarios.
  - El uso y obtención de cuentas ajenas.

### 7.5. Aceptación y compromiso de cumplimiento

El uso del correo electrónico de la US implica el conocimiento y plena aceptación de las advertencias legales y condiciones vigentes en cada momento en que el usuario acceda al mismo y que se especifican en este documento.

Cualquier usuario que incumpla alguno de los términos especificados en este documento deberá asumir las responsabilidades derivadas de la utilización incorrecta del correo corporativo de la Universidad de Sevilla.

## 8. Desarrollo de la normativa

El correo electrónico es un servicio de red que permite a los usuarios de la US enviar y recibir mensajes y, en ocasiones, estos pueden incluir ficheros adjuntos. Las características peculiares de este medio de comunicación (universalidad, bajo coste o anonimato) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades.

### 8.1. Enunciado de las normas generales

A fin de reducir riesgos en el uso del correo electrónico, el usuario de este servicio deberá cumplir las normas que se incluyen a continuación:

- Utilizar el correo electrónico para propósitos profesionales.
- Utilizar el correo electrónico para comunicaciones interpersonales: en ningún momento debe usarse como un medio de difusión masiva e indiscriminada de información.
- Usar protocolos seguros en los clientes de correo (SSL o TLS) para la conexión a los buzones.

- Utilizar protocolos seguros en las conexiones por SMTP para envío de correo autenticado y cifrado.
- Usar contraseñas seguras conforme a la política de contraseñas de la US.
- No ceder el uso de las cuentas de correo a terceros: las cuentas de correo son personales e intransferibles ya que esto provoca la suplantación de identidad y el acceso a información confidencial.
- No responder a mensajes de SPAM
- Utilizar mecanismos de cifrado de la información cuando los mensajes contengan información sensible, confidencial o protegida.
- No ejecutar archivos adjuntos sin analizarlos previamente con la herramienta corporativa contra código malicioso (antivirus).
- No reenviar correos en los que se haya detectado virus o código malicioso para evitar su posible propagación: todo incidente de seguridad se notificará a través del Servicio de Atención a Usuarios SOS sin reenviar el correo.
- No responder a solicitudes que pidan el usuario y/o contraseña.
- No manipular las cabeceras del correo electrónico saliente.
- Respetar el contenido de las leyes y demás disposiciones que sean de aplicación con especial atención al cumplimiento de la Ley Orgánica 15/1999 de Protección de Datos Personales (LOPD).

Además de las anteriores normas, se recomienda:

- No utilizar el correo electrónico como espacio de almacenamiento.
- Asegurar la identidad del remitente antes de abrir un mensaje: con carácter general, si no se conoce el remitente de un correo, y/o el asunto del mismo es extraño a pesar de haber traspasado el filtro de SPAM, se recomienda borrar el mensaje o situarlo en cuarentena hasta disponer de más datos, especialmente si contiene ficheros adjuntos.
- Revisar la barra de direcciones antes de enviar un mensaje para comprobar que no hay destinatarios erróneos y evitar una brecha en la confidencialidad de la información.
- Desactivar la visualización HTML de los mensajes: esto ayuda a evitar que el código malicioso se ejecute.
- Usar las listas de distribución para la difusión de la información, evitando el envío de documentos pesados a través de las mismas, para lo cual se recomienda usar enlaces a páginas web.
- Usar el campo Copia Oculta (CCO o BCC) para evitar la visibilidad de direcciones de correo a todos los receptores de un mensaje cuando el usuario tenga necesidad de enviarlo a un conjunto de destinatarios.
- Mantener actualizados los sistemas operativos de equipos, los sistemas operativos de dispositivos móviles y los clientes pesados de escritorio a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.
- Ante cualquier incidencia que pueda surgir y afecte al normal comportamiento del servicio de correo, contactará con el Servicio de Atención de Usuarios del SIC.

Recomendaciones para acceso al correo vía web:

- Mantener actualizados los navegadores a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.

- Cerrar la conexión al servidor una vez finalizada la sesión web.
- Desactivar la característica "recordar contraseñas" en el navegador.
- Activar en el navegador la opción de borrado automático de la información sensible al cerrar: histórico de navegación, caché, cookies, contraseñas, sesiones autenticadas, etc.
- No instalar addons (extensiones) para el navegador que puedan alterar el normal funcionamiento del acceso web al correo.

### 8.2. Normas específicas de uso de estafetas secundarias

La Universidad de Sevilla permite el uso de Estafetas Secundarias de correo siempre y cuando tengan razón de ser en cuanto a número de buzones afectados, responsabilidad del servicio, coordinación con el grupo de personas que administran las estafetas primarias de la Universidad de Sevilla y aceptación de la política de correo universitaria.

### 8.3. Normas específicas de prevención contra correo basura (SPAM)

Además de las medidas técnicas de prevención y eliminación de SPAM ya instaladas en la US a través del SIC, se detallan seguidamente las normas que todo usuario deberá seguir para hacer frente a este problema:

- Con carácter general, sólo se proporcionará la dirección de correo electrónico profesional de la US a personas de confianza y del entorno profesional.
- Se debe evitar introducir la dirección de correo de la US en foros de noticias o listas de correo a través de Internet, salvo en los casos necesarios y con proveedores de confianza.
- Si a pesar de las medidas de prevención instaladas el usuario recibe un mensaje de SPAM:
  - No accederá a los enlaces o adjuntos que pudieran contener.
  - Lo comunicará al SIC a través del Servicio de Atención a Usuarios SOS inmediatamente.

## 9. Responsabilidades

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, cuando se detecten envíos masivos o cualquier otra actividad abusiva que pudiera perjudicar el correcto funcionamiento del Servicio de Correo, o cuando se reciba un aviso de incidencia de los organismos encargados de ello (CCN-Cert, RedIris), el SIC procederá, dependiendo de la gravedad y reiteración del incidente, a aplicar una de estas medidas:

**Suspensión temporal del buzón de correo de un usuario**

Esta medida se tomará cuando se produzca la violación de los términos de este documento de forma premeditada o cuando se esté causando una degradación en los recursos de nuestra institución o implique a la US en algún tipo de responsabilidad que conlleve perjuicio para sus usuarios. La acción a tomar y la duración de la misma dependerán de la incidencia, si bien, como medida de precaución se procederá a deshabilitar la cuenta del usuario, no permitiendo el acceso al correo universitario.

**Suspensión temporal del acceso de la estafeta secundaria al puerto 25 de mail.us.es**

Se tomará esta medida cuando se produzca un mal uso del servicio que ofrece la estafeta secundaria de correo.

**Suspensión indefinida del usuario o la estafeta secundaria**

Esta medida se aplicará cuando se incurra en infracciones de especial gravedad o en una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por el cauce

adecuado.

En todos los casos el servicio podrá restablecerse cuando se considere que las medidas adoptadas por el responsable de la cuenta de correo o estafeta secundaria garanticen un uso aceptable en el futuro.

**Exención de responsabilidades de la US por los contenidos**

La Universidad de Sevilla no se hace responsable del contenido de los mensajes enviados por los usuarios a través de cualquiera de las formas de utilización del correo universitario. En cualquier caso, la Universidad de Sevilla se compromete a actuar con diligencia para evitar cualquier uso indebido del servicio.

**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**

**Addons**

Extensiones, también llamados plugins o complementos: son programas que sólo funcionan anexados a otro y que sirven para incrementar o complementar sus funcionalidades

**CCN-Cert**

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Tiene responsabilidad en ciberataques sobre sistemas de las Administraciones Públicas.

**ESTAFETAS PRIMARIAS DE CORREO DE LA US**

Sistemas que gestionan todo el tráfico de correo entrante y saliente de la US administradas por el SIC.

**ESTAFETAS SECUNDARIAS DE CORREO EN LA US:**

Sistemas que gestionan subdominios bajo el dominio de correo @us.es. Administradas por el SIC, Centros o Departamentos.

**LOPD**

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (cualquier información concerniente a personas físicas identificadas o identificables).

**MX DE LA US (buzon.us.es)**

Mail eXchange record (registro de intercambio de correo). Es un tipo de registro en el Servidor de Nombres, DNS, que especifica cómo debe ser encaminado un correo electrónico en internet. Los registros MX apuntan a los Sistemas que reciben todo el correo dirigido al dominio @us.es y todos los subdominios que dependen de él.

**mail.us.es (correo autenticado)**

Nombre del servidor de correo de la US: es el sistema de estafetas primarias diseñado para enviar correo autenticado y cifrado, única forma de envío permitida en la US.

**RedIris**

Red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional.

**SERVICIO DE INFORMÁTICA Y COMUNICACIONES**

Servicio de la Universidad responsable de gestionar el Correo Institucional de la US.

**SLA**

Service Level Agreement o "Acuerdo de Nivel de Servicio" (ANS) en castellano. Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel de calidad de dicho servicio.

**SMTP**

Simple Mail Transfer Protocol o "protocolo para transferencia simple de correo" en castellano. Es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre dispositivos.

**SPAM**

Correo electrónico masivo no solicitado.

**SSL**

Secure Sockets Layer (capa de puertos seguros) es un protocolo criptográficos que proporciona comunicaciones seguras por red.

**TLS**

Transport Layer Security (seguridad de la capa de transporte) es una versión actualizada y más segura del protocolo SSL.

**UVUS**

Usuario Virtual de la Universidad de Sevilla.

**PORTAL INSTITUCIONAL DE LA US**

Página oficial de la Universidad de Sevilla que proporciona el acceso a la mayor parte de los contenidos Web institucionales, académicos y de investigación existentes en la Universidad.

**USUARIOS DE CORREO CORPORATIVO DE LA US**

Estudiantes, profesores, investigadores, personal de la administración y servicios, resto de miembros de la Comunidad Universitaria y, en general, cualquier persona externa a la Universidad de Sevilla que disponga de un buzón de correo corporativo en la misma por su relación con la US.

## ANEXO 9

NORMAS DE SEGURIDAD
NORMATIVA DE USO ACEPTABLE Y SEGURIDAD BÁSICA DEL SERVICIO DE ENSEÑANZA VIRTUAL DE LA UNIVERSIDAD DE SEVILLA

Índice

**1. Introducción**

La Universidad de Sevilla (en adelante, US) mantiene, como centro de enseñanza superior, una plataforma de enseñanza digital en la que se recogen materiales docentes elaborados por su profesorado y puestos a disposición de los alumnos en régimen de red privada (con exigencia de identificación y autentificación) para complementar las actividades docentes presenciales impartidas en el aula o para generar nuevas modalidades de formación, apoyadas en las nuevas Tecnologías de la Información y las Comunicaciones (en adelante, TIC).

La Plataforma de Enseñanza Virtual (en adelante, EVIRTUAL) es el nombre con el que se refiere al conjunto de herramientas informáticas basadas en la red con la que se da apoyo a las actividades docentes oficiales y no oficiales de la Universidad de Sevilla.

Este documento define las normas de uso y seguridad que deben seguir todos los usuarios de la Plataforma de Enseñanza Virtual. Las normas han sido elaboradas con el objetivo de conseguir un uso más eficiente, correcto y seguro de los recursos destinados a dicho Servicio.

**2. Objeto**

El objeto de la presente normativa es regular el acceso y utilización del Servicio de Enseñanza Virtual de la US, desde los distintos Campus o cualquier ubicación posible, posibilitando la homogeneización de criterios entre Centros y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

**3. Ámbito de aplicación**

La presente normativa será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, pertenezca a la comunidad universitaria, incluyendo el personal de organizaciones externas cuando sean usuarios o posean acceso al Servicio de Enseñanza Virtual de la US.

Los usuarios serán informados de esta Normativa de uso aceptable y seguridad básica y aceptarán que el Servicio de Informática y Comunicaciones (en adelante, SIC) sea el garante del cumplimiento de las mismas. Así mismo podrán proponer al órgano pertinente las modificaciones a este documento que

consideren oportunas para ajustarlo a la lógica evolución tecnológica y legislativa que se produzca, manteniendo el espíritu del mismo en lo que respecta a los objetivos y finalidades del Servicio de Enseñanza Virtual. Los usuarios serán puntualmente informados de cualquier modificación que fuera preciso introducir.

**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 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 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.

Cuando las circunstancias así lo aconsejen, el SIC 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. Términos y condiciones de acceso y uso**

Estos Términos y condiciones de acceso y uso regulan el uso del Servicio de Enseñanza Virtual de la US.

**7.1 Registro del usuario**

El acceso y utilización de la Plataforma de Enseñanza Virtual de la US por parte del usuario requiere que éste disponga de un Usuario Virtual de la Universidad de Sevilla (en adelante, UVUS) y estar inscrito en los sistemas de gestión administrativa de la actividad docente.

El usuario se compromete a usar sus claves de acceso (nombre de usuario y contraseña) de acuerdo con las restricciones que aparecen en este documento y en la normativa asociada.

Para garantizar y optimizar el mejor funcionamiento de la Plataforma de Enseñanza Virtual se hace necesaria una serie de compromisos entre los usuarios y los responsables del Servicio.

El SIC, como responsable de este servicio, debe asegurar:

- La disponibilidad del Servicio de Enseñanza Virtual de la US conforme a los compromisos de calidad adquiridos en la carta de servicios del SIC.
- El uso de la información disponible de los estudiantes para los fines propios de la Enseñanza Virtual en virtud de lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, garantizando en todo caso la confidencialidad de la misma. Los usuarios podrán ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos recopilados y archivados.
- El tratamiento de los datos de tráfico generados por el uso y la navegación en el entorno de EVIRTUAL para fines estrictamente técnicos por personal vinculado por el deber de secreto y confidencialidad. En los espacios abiertos del aula como foros, noticias, etc., sin perjuicio del respeto a los derechos de estudiantes y profesores en relación con los contenidos, opiniones y trabajos publicados, los datos de uso y tráfico podrán ser tratados con fines estadísticos y de investigación al servicio del objetivo de calidad en la docencia universitaria.
- La salvaguardia de la información almacenada en los espacios del usuario en la Plataforma.

Los compromisos por parte de los usuarios del Servicio de Enseñanza Virtual de la US son los siguientes:

- Hacer un uso aceptable de la Plataforma, respetando los fines para los que ha sido creada y utilizando correctamente los recursos que se le suministran.
- Evitar actuaciones que provoquen la interrupción de los servicios que ofrece la Enseñanza Virtual.
- Evitar situaciones que afecten a la seguridad del Servicio de Enseñanza Virtual y de sus usuarios.
- Cumplir las normas de seguridad definidas en el presente documento.
- Comunicar los problemas que surjan al Servicio de Atención de Usuarios para su resolución.
- Cumplir la Ley de la Propiedad Intelectual.

Derechos de los estudiantes:

- En el entorno de EVIRTUAL los estudiantes son titulares de los derechos que les otorgan los estatutos y demás normas de desarrollo.

### 7.3 Uso aceptable

Los usuarios de la Plataforma de Enseñanza Virtual de la US utilizarán el mismo para:

- Complementar las actividades docentes presenciales impartidas en el aula o para generar nuevas modalidades de formación apoyadas en las nuevas tecnologías.

En general los usuarios de la Plataforma de Enseñanza Virtual de la US deberán utilizar eficientemente el servicio con el fin de evitar perjuicios al resto de usuarios.

### 7.4 Uso no aceptable

El Servicio de Enseñanza Virtual de la US no debe usarse para:

- Difundir mensajes con contenidos contrarios a los principios enunciados en los Estatutos de la US: mensajes con contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología

del terrorismo o atentatorio contra los derechos humanos, o que actúen en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.

- Difundir información con cualquier fin comercial, político, ideológico o religioso.
- Enviar información que viole los derechos de propiedad intelectual, la Ley Orgánica de Protección de Datos (en adelante, LOPD) o cualquier otra legislación vigente.
- Enviar información que cause cualquier tipo de molestia a otros usuarios, incluida la información difamatoria de cualquier tipo, ya sea contra entidades o personas.
- Difundir información o material que pueda perjudicar a otros usuarios de la red (virus, correo publicitario, cadenas de correo, correos spam, etc.).
- Fines privados comerciales no autorizados por la US.
- El desarrollo de actividades encaminadas a entorpecer el uso de EVIRTUAL:
  - La congestión de la red de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
  - La denegación del Servicio.
  - La destrucción, modificación o apropiación indebida de la información de otros usuarios.
  - La violación de la privacidad e intimidad de otros usuarios.
  - El uso y obtención de cuentas ajenas con el fin de usurpar la personalidad de otro usuario del Campus Virtual.
  - Simular o falsificar la relación del usuario con cualquier otra persona o entidad.

### 7.5 Aceptación y compromiso de cumplimiento

El uso de la Plataforma de Enseñanza Virtual de la US implica el conocimiento y plena aceptación de las advertencias legales y condiciones vigentes en cada momento en que el usuario acceda al mismo y que se especifican en este documento.

El usuario manifiesta y declara que asume de forma total y exclusiva toda la responsabilidad en los siguientes casos:

- Cuando vulnere los términos y condiciones de uso especificados en este documento.
- Cuando, por un tercero, la Universidad de Sevilla sea objeto de cualquier tipo de reclamación, o requerimiento judicial o extrajudicial, relacionada con la información o material que el usuario tenga publicado o enviado a través de EVIRTUAL. En consecuencia, el usuario se obliga a mantener a la Universidad de Sevilla indemne por cualquier reclamación, obligación, pérdida, daño, perjuicio, gasto, violación, usurpación o infracción de derechos de propiedad intelectual o industrial o cualquier otro tipo de derecho protegido por las leyes españolas.

Cualquier usuario que incumpla alguno de los términos especificados en este documento deberá asumir las responsabilidades derivadas de la utilización incorrecta del Servicio de Enseñanza Virtual de la US.

## 8. Desarrollo de la normativa

A fin de reducir el riesgo en el uso del Servicio de Enseñanza Virtual, el usuario de este servicio deberá cumplir las normas que se incluyen a continuación.

### 8.1 Normas sobre políticas de privacidad

- La información personal disponible relativa a los usuarios en cualquier recurso del entorno de EVIRTUAL podrá utilizarse para los fines propios del Aula.

- Queda expresamente prohibido a todos los miembros de la comunidad universitaria, y en general a cualquier usuario, su uso para fines distintos salvo que cuenten con autorización legalmente válida del titular de los datos.
- Cada usuario puede decidir el grado de información que muestra a los demás a través de la configuración de su perfil. El entorno de EVIRTUAL incluye por defecto el nombre de usuario UVUS, el nombre y apellidos. Los datos incluidos en el perfil del usuario se publican bajo la exclusiva responsabilidad del titular de los mismos.
- Cualquier información personal revelada en espacios colectivos como foros, chat o blog se publica bajo la exclusiva responsabilidad del titular de la misma.
- El uso de fotografías en EVIRTUAL se encuentra regido por el derecho a la propia imagen establecido en el artículo 18.1 de la Constitución. En aquellos casos en los que el profesor considere que disponer de tal información resulta relevante podrá sugerir a los estudiantes que la incluyan. No obstante, en ningún caso será obligatoria la inclusión.
- El usuario podrá incluir una fotografía, preferentemente de carné y que reproduzca únicamente su efigie, cuando lo desee. Cuando la fotografía incluida contravenga las Normas de uso personal de los recursos informáticos y telemáticos de la Universidad de Sevilla, podrá ser retirada por la Universidad.
- Cualquier archivo, fotografía o video que con carácter docente se publique en EVIRTUAL será respetuoso con la imagen personal de quienes aparezcan en tales ficheros, se contará con permiso expreso de las personas que aparezcan en él, sin límite geográfico y por tiempo ilimitado, o se tomarán las medidas necesarias para impedir su identificación. En caso de que se reciba comunicación fehaciente de un agente activo en cualquiera de esos materiales, o de quién ejerza en su nombre sus derechos, se deberá proceder a su supresión.
- En ningún caso el usuario del Servicio revelará ni facilitará a terceros sus credenciales de acceso a la Plataforma. Los daños y/o perjuicios que dicha revelación pudiera causar se atribuirán al usuario titular de la misma.
- Ante cualquier incidente relacionado con el usuario y/o contraseña que pudiera afectar a la seguridad del Servicio o del propio usuario, este procederá a cambiar su contraseña en la plataforma de Gestión de Identidad de la US.

Además de las anteriores normas, se recomienda:

- No incluir datos relativos a la ideología, afiliación sindical, religión y creencias, origen racial, salud y vida sexual en los espacios de la Plataforma de Enseñanza Virtual. La inclusión de referencias de este tipo se realizará bajo la exclusiva responsabilidad del usuario.

### 8.2 Normas de seguridad para el personal docente

La gestión de los recursos de EVIRTUAL comporta el acceso a datos de carácter personal de los estudiantes dentro de un marco de actividades docentes reguladas por las normativas correspondientes según la tipología de la Docencia. Esto supone la adopción por parte del profesorado y de los gestores y administradores del sistema de las siguientes medidas.

PRIMERO. PUESTOS DE TRABAJO.

- Los puestos de trabajo desde los que se acceda a EVIRTUAL estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

- Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Para ello procederá a abandonar la aplicación y a reiniciar la sesión de trabajo cuando vuelva a ocupar el puesto de trabajo.
- En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

SEGUNDO. SALVAGUARDA Y PROTECCIÓN DE LAS CONTRASEÑAS PERSONALES.

- Cada usuario será responsable de la confidencialidad de su contraseña, no debiendo revelarla ni facilitarla a terceros. Los daños y/o perjuicios que dicha revelación pudiera causar se atribuirán al usuario titular de la misma.

TERCERO. GESTIÓN DE INCIDENCIAS.

- Cualquier usuario que tenga conocimiento de una incidencia deberá comunicarla inmediatamente a evirtual@us.es.

CUARTO. COPIA DE DATOS EN SOPORTES PROPIOS.

- No se recomienda la copia de documentos que contengan datos personales en soportes externos a EVIRTUAL salvo que resulte estrictamente necesario. En tal caso y siempre que el tipo de soporte empleado para la copia lo permita se bloqueará el acceso mediante usuario y contraseña. Cuando el soporte por su naturaleza no permita esta medida de seguridad se custodiará debidamente por el usuario que lo generó.
- Aquellos soportes que sean reutilizables, y que hayan contenido copias de datos personales, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

QUINTO. SOPORTE PAPEL.

- Cuando el usuario tenga necesidad de imprimir documentos que contengan datos personales o contenidos protegidos y/o utilizarlos en soporte papel será responsable de su custodia de modo que se evite que terceros no autorizados accedan a la información personal contenida en los mismos.
- Una vez finalizado su uso, y salvo que exista obligación de conservación, el soporte papel será destruido de modo que la información que contenga resulte ininteligible para cualquier tercero ajeno. El uso de la cara en blanco de un documento se encuentra expresamente prohibido.
- Asimismo, el de estos soportes en papeleras de reciclado sólo podrá realizarse previa destrucción.

### 8.3 Normas específicas de protección de la propiedad intelectual

PRIMERO. LA UNIVERSIDAD.

- La Universidad tiene derechos exclusivos de propiedad intelectual sobre el contenido de las páginas web y sobre cualquier creación intelectual, información y documentación elaboradas por la misma. Se prohíbe la reproducción, distribución, comunicación pública o transformación no autorizadas de estos contenidos, datos y documentos sin perjuicio de los derechos que correspondan a profesores o estudiantes sobre los materiales de producción propia.

SEGUNDO. ESTUDIANTES.

- Los estudiantes tienen derecho a que sea respetada la propiedad intelectual y la de autoría de sus trabajos, estudios y otras realizaciones desarrolladas en el entorno de EVIRTUAL de la Universidad, de acuerdo con lo que establece la legislación vigente en materia de propiedad intelectual, patentes y marcas.
- El uso del material bibliográfico, apuntes, exposiciones, intervenciones de los profesores etc., se reserva para finalidades académicas, docentes y de formación. Queda rigurosamente prohibida la reproducción total o parcial de los mismos por cualquier medio, así como su difusión y distribución a terceras personas.

TERCERO. PROFESORES.

- No se incluirán en el entorno virtual fotocopias digitalizadas de obras, documentos, materiales, software o cualquier otro recurso cuando ello constituya una vulneración de la legislación vigente en materia de propiedad intelectual.

CUARTO. LOS USUARIOS.

- Ningún usuario del sistema podrá introducir en el entorno de EVIRTUAL documentos, materiales, software o cualesquiera recursos con incumplimiento de la legislación vigente sobre propiedad intelectual y patentes.
- Sólo se insertarán en EVIRTUAL ficheros que reproduzcan total o parcialmente libros, artículos o documentos protegidos por la Ley de Propiedad Intelectual cuando se haya obtenido previa autorización de uso por parte del titular de los derechos intelectuales.
  - Si una vez publicado el documento, el usuario recibiera una petición de su autor solicitando su retirada, deberá proceder a eliminar dicho texto de entre los materiales educativos del curso virtual.
- Las revistas y otros contenidos licenciados por la Biblioteca de la Universidad podrán ser utilizados por el personal docente en los cursos virtuales, dentro de los términos establecidos en cada licencia.
- Son documentos de libre acceso y, como tales, pueden comunicarse libremente y sin restricciones los siguientes:
  - El contenido de los periódicos oficiales como el DOCE, BOE, Boletines oficiales de las Comunidades Autónomas, etc.
  - El texto de las resoluciones de los órganos jurisdiccionales, recomendándose en este punto que se utilicen preferentemente los textos recogidos en las bases de datos públicas (por ejemplo, el CENDOJ).
  - El contenido publicado bajo la protección de licencias "creative commons" u otras similares y el recogido en repositorios "open access", siempre que se realice dentro de los límites que en cada caso se establezca en la respectiva licencia.
  - Las tesis doctorales publicadas por las universidades conforme a lo establecido en el art. 14.5 del Real Decreto 99/2011.
  - Cuando el texto que se considere de interés para la asignatura pueda encontrarse tanto en una tesis doctoral como en una obra posterior del mismo autor, deberá reproducirse la tesis original, citando el nombre del autor. El derecho de cita limita los derechos de un creador intelectual respecto al uso de parte de su obra para fines docentes o de investigación, conforme al art. 32 del Texto Refundido de la Ley de Propiedad Intelectual (Real Decreto Legislativo 1/1996, de 12 de abril).

- Obras que se hallen en el dominio público.

QUINTO. HIPERENLACES.

- Las referencias a materiales disponibles en Internet se realizarán mediante indicación del hiperenlace correspondiente. Asimismo, en la edición de noticias, o cualquier otro texto, en las que se acuda a fuentes externas se realizará con cita de autoría y con pleno respeto a la legislación sobre propiedad intelectual. Cuando tal información se encuentre accesible en la red se incluirá una referencia a la fuente mediante hiperenlace.
- En caso de que se reciba una comunicación fehaciente del autor, o de quien ejerza en su nombre sus derechos, de que el enlace incluido en ese concreto material docente referencia una obra cuya publicación no está debidamente autorizada, deberá procederse a su supresión.
- La Universidad no se responsabiliza de los contenidos incluidos en las páginas a las que se enlace desde textos elaborados por usuarios de EVIRTUAL.

SEXTO. USO DEL DERECHO DE CITA Y DE ILUSTRACIÓN PARA LA ENSEÑANZA.

El derecho de cita consiste, de acuerdo con la Ley de propiedad intelectual en «la inclusión en una obra propia de fragmentos de otras ajenas de naturaleza escrita, sonora o audiovisual, así como de obras aisladas de carácter plástico, fotográfico figurativo o análogo, siempre que se trate de obras ya divulgadas y su inclusión se realice a título de cita o para su análisis, comentario o juicio crítico. Tal utilización sólo podrá realizarse con fines docentes o de investigación en la medida justificada por el fin de esa incorporación e indicando la fuente y el nombre del autor de la obra utilizada».

De lo anterior se desprende que la utilización de material ajeno en el seno de los materiales virtuales deberá ajustarse a lo siguiente:

- Cuando el texto escrito que se pretende recoger proceda de obras ajenas publicadas en papel y escaneadas se transformará en un documento de texto a través de los programas OCR y su incorporación a EVIRTUAL deberá realizarse de manera elaborada con referencia precisa de la fuente y nombre del autor, conforme a los criterios metodológicos de aplicación en cada caso, intercalando entre los distintos párrafos recopilados, acotaciones del profesor ponente en donde se realicen aclaraciones, precisiones, valoraciones o, al menos, se la concuerde con otras referencias.
- Deberá realizarse una utilización proporcionada, no debiendo reproducirse más material que el necesario para ilustrar la cuestión objeto de explicación o análisis, procurando no reproducir la totalidad de una obra.

Además de las anteriores normas, se recomienda a los profesores:

- Que la inclusión de materiales de cualquier tipo en el entorno de EVIRTUAL se realice en formatos que dificulten su copiado. En todo caso deberá figurar con claridad en la página inicial y preferentemente en los encabezados o pies de página el lema: «Queda rigurosamente prohibida la reproducción total o parcial por cualquier medio, así como su difusión y distribución a terceras personas».

### 8.4 Libertad de expresión

El entorno de EVIRTUAL dispone de espacios que facilitan el ejercicio del derecho de información y la libertad de expresión.

- Tales derechos se ejercerán con pleno respeto a los principios constitucionales de veracidad e interés público, la legalidad vigente y en particular el derecho al honor, a la intimidad, a la propia

imagen y a la protección de la juventud y de la infancia.

- El uso de los recursos de EVIRTUAL para esta finalidad se halla sujeto a lo dispuesto por la normativa general de utilización de los recursos y Sistemas de Información de la Universidad de Sevilla.

**9. Responsabilidades**

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, cuando se detecten actividades abusivas que pudieran perjudicar el correcto funcionamiento del Servicio de Enseñanza Virtual, o cuando se reciba un aviso de incidencia de los organismos encargados de ello (CCN-Cert, RedIris), el SIC procederá, dependiendo de la gravedad y reiteración del incidente, a aplicar una de estas medidas:

**Suspensión temporal del acceso de un usuario a la Plataforma de Enseñanza Virtual**

Esta medida se tomará cuando se produzca la violación de los términos de este documento de forma premeditada o cuando se esté causando una degradación en los recursos de nuestra institución o implique a la US en algún tipo de responsabilidad que conlleve perjuicio para sus usuarios. La acción a tomar y la duración de la misma dependerán de la incidencia, si bien, como medida de precaución se procederá a deshabilitar la cuenta del usuario, no permitiéndole el acceso a la Plataforma.

**Suspensión indefinida del acceso de un usuario a la Plataforma de Enseñanza Virtual**

Esta medida se aplicará cuando se incurra en infracciones de especial gravedad o en una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por el cauce adecuado.

En todos los casos el servicio podrá restablecerse cuando se considere que las medidas adoptadas por el usuario de la Plataforma garanticen un uso aceptable en el futuro.

**Exención de responsabilidades de la US por los contenidos**

La Universidad de Sevilla no se hace responsable de la licitud del contenido suministrado por los usuarios a través de cualquiera de las maneras de utilización de la Plataforma de Enseñanza Virtual ni de los contenidos incluidos en las páginas a las que se enlace desde textos elaborados por usuarios de EVIRTUAL. En cualquier caso, la Universidad de Sevilla se compromete a actuar con diligencia para evitar cualquier uso indebido del servicio.

**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-Cert**

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Tiene responsabilidad en ciberataques sobre sistemas de las Administraciones Públicas.

**LOPD**

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (cualquier información concerniente a personas físicas identificadas o identificables).

**RedIris**

Red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional.

**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.

**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.

**UVUS**

Usuario Virtual de la Universidad de Sevilla.

**USUARIOS DEL SERVICIO DE ENSEÑANZA VIRTUAL DE LA US**

Estudiantes, profesores y resto de miembros de la Comunidad Universitaria que disponga de acceso a la Plataforma de Enseñanza Virtual por su relación con la US.

## ANEXO 10

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.

## ANEXO 11

NORMAS DE SEGURIDAD
NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD DE SEVILLA

Índice

APÉNDICE: LENGUAJE DE GÉNERO
ANEXO: GLOSARIO

**APROBACIÓN Y ENTRADA EN VIGOR**

Texto aprobado por la Comisión de Seguridad de la Universidad de Sevilla de fecha 16 de diciembre de 2016.

Esta Norma de Seguridad es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Norma.

**EXPOSICIÓN DE MOTIVOS**

La Política de Seguridad de la Universidad de Sevilla (en adelante US), aprobada por Consejo de Gobierno, supone un marco general sobre el tratamiento de la Seguridad de la Información en el ámbito de nuestra Universidad que debe ser desarrollado con normativas más específicas. La presente normativa desarrolla lo expuesto en la Política de Seguridad y aporta una serie de recomendaciones y obligaciones sobre el uso correcto de los Sistemas de Información, así como para el desarrollo de las buenas prácticas necesarias para la prevención, detección, respuesta y recuperación ante incidentes de seguridad.

La creciente importancia de los Sistemas de Información, en todas las actividades de la vida universitaria, incide en la relevancia de la Seguridad de la Información. Por ello, deben adoptarse las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada o de los servicios prestados, garantizando al mismo tiempo la disponibilidad continuada de estos servicios.

En la actualidad, los servicios y recursos a que se refiere esta normativa son prestados y desarrollados en su mayor parte por el Servicio de Informática y Comunicaciones (en adelante, SIC), que asume las tareas descritas en el artículo 125 de los Estatutos, en tanto no se opte por otra forma de organización:

- Fomentar el desarrollo, aplicación y uso de las tecnologías de la información y la comunicación para la construcción de la sociedad del conocimiento y la información, destinando para ello los medios materiales y humanos adecuados.
- Atender las necesidades de apoyo informático a las tareas de estudio, docencia, investigación y gestión de todos los miembros de la comunidad universitaria.

Ello abarca fundamentalmente la organización general de los sistemas automatizados de información para el apoyo a las tareas universitarias, la planificación y gestión de la red informática de la Universidad y de los equipos conectados a la misma, y la atención a los usuarios -profesores, alumnos y personal de administración y servicios-, a quienes se les debe facilitar además el acceso al conocimiento y la utilización de dichos medios.

**Artículo 1. Objeto y ámbito de aplicación**

**1.1.** La presente normativa tiene por objeto la regulación del uso de los recursos informáticos y servicios de red que la Universidad de Sevilla proporciona a la Comunidad Universitaria para su utilización en actividades académicas, de investigación, desarrollo e innovación y de proyección social, incluyendo las tareas administrativas asociadas, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

**1.2.** La presente regulación es aplicable a todos los miembros de la Comunidad Universitaria, tanto a nivel individual como colectivo (departamentos, servicios, etc.) en cuanto que hagan uso de

recursos informáticos o servicios de red, así como a cualquier otra persona o entidad externa a la Universidad que coyunturalmente los utilice.

**1.3.** Quedan sujetos a las normas y condiciones contenidas en este documento todos los equipos y Sistemas de Información y Comunicaciones de la US, ya sean personales o compartidos, y estén o no conectados a la red. Aquellos equipos que no sean propiedad de la Universidad, pero que se conecten a la red de la Universidad o usen los servicios y recursos de la misma, también deberán cumplir con esta normativa de uso. Los servicios y recursos ofrecidos por la Universidad a sus usuarios, serán utilizados en las condiciones previstas en cada caso. Dichas condiciones estarán recogidas en normativas específicas de uso o, en su defecto, por la normativa que con carácter general define el presente documento.

**Artículo 2. Vigencia**

**2.1.** La presente normativa general de utilización de los recursos y Sistemas de Información de la US ha sido aprobada por la Comisión de Seguridad de la Información de la US, 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.

**2.2.** La Comunidad Universitaria será informada de estas normas de uso y seguridad y aceptará el cumplimiento de las mismas. Con objeto de dar la mayor publicidad a esta normativa, el SIC de la US dispondrá de los medios necesarios para permitir su consulta de forma fácil, teniendo en cuenta que el desconocimiento de esta normativa no exime de su cumplimiento.

**2.3.** Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación.

**Artículo 3. Revisión y evaluación**

**3.1.** La gestión de esta normativa general 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.

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

**3.3.** 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.

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

**Artículo 4. Referencias legales**

**4.1.** Son de aplicación las leyes y normativas españolas, así como las que dimanen de la Unión Europea y de la Junta de Andalucía en relación con protección de datos personales, propiedad

intelectual y uso de herramientas telemáticas, así como las que puedan aparecer, en un futuro, a este respecto.

Esta normativa se sitúa dentro del marco jurídico definido por las leyes y reales decretos siguientes:

- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y sus normas de desarrollo.
- Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
- Instrucción 1/1998, De 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
- Ley Orgánica 1/1982, de Protección Civil del Derecho al Honor, a la intimidad Personal y Familiar y a la Propia Imagen.
- Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- Ley 34/2002, de Servicios de la Sociedad de la Información (LSSI) y de Comercio Electrónico.
- Ley 11/2007, de Acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, por el que se desarrolla parcialmente la Ley 11/2007 de Acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 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.

**Artículo 5. Utilización de los equipos informáticos de la US**

**5.1.** Los datos, dispositivos, programas y servicios informáticos que la US pone a disposición de los usuarios para el desarrollo de su actividad deben utilizarse para las funciones encomendadas. Cualquier uso de los recursos con fines distintos a los autorizados no está permitido.

**5.2.** Los usuarios deberán utilizar dichos equipos informáticos para usos compatibles con las funciones que les competen.

**5.3.** Los usuarios deberán cuidar los equipos informáticos que les sean facilitados, no procediendo a su alteración ni modificación.

**5.4.** No está permitida la instalación de aplicaciones informáticas sin la correspondiente licencia o no adecuándose a la legislación vigente. Asimismo, no está permitida la instalación o visualización de salvapantallas, fotos, vídeos, comunicaciones u otros medios con contenidos ofensivos, violentos, amenazadores, obscenos o, en general, aquellos que agredan la dignidad de la persona.

**5.5.** No está permitida la instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

**5.6.** Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores

de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos los problemas.

**Artículo 6. Conexión a la Red Informática de la US (RIUS)**

**6.1.** RIUS es el conjunto de todos los recursos tanto físicos como lógicos que permiten el transporte de información de los distintos ordenadores existentes en la Universidad que estén conectados a la misma.

**6.2.** Se considera que un ordenador o dispositivo es miembro de RIUS y está sujeto a esta normativa si:

a. Se encuentra conectado a RIUS desde cualquiera de los puntos de acceso que se facilitan a este efecto en los campus universitarios, ya sean aquellos cableados o inalámbricos.

b. Está conectado a la US usando alguno de los métodos de acceso remoto que ésta proporciona.

**6.3.** Todos los equipos que se conecten a RIUS deberán estar correctamente identificados en las condiciones que, para cada caso, se determine en la normativa de acceso correspondiente. Deben tener la configuración de red indicada por el SIC, además de ser incluidos en el registro correspondiente, junto con la identidad de los responsables del equipo. Cualquier modificación de un equipo registrado debe ser comunicada al SIC.

**6.4.** Los responsables de los equipos conectados a RIUS deben asegurarse de tener instalados los parches de seguridad y actualizaciones de sistemas operativos y software que desde la US se les recomiende.

**6.5.** Se considera aceptable usar RIUS para acceder a, u ofrecer información, siempre que esté de alguna forma relacionada con el entorno universitario, que no viole derechos de propiedad intelectual, y que este uso se realice de forma eficiente a fin de evitar perjuicios a terceros.

**6.6.** No se considera aceptable y no puede ser usada RIUS bajo ningún concepto para:

a. Cualquier acto que viole la legislación vigente o las normativas de las redes en las que RIUS está integrada (RICA, RedIRIS).

b. Fines privados comerciales no autorizados por la US.

c. La búsqueda de claves de acceso de otros usuarios o cualquier intento de encontrar y explotar fallos en la seguridad de los sistemas informáticos de la US o de fuera de ella, o hacer uso de aquellos sistemas para atacar cualquier sistema informático. No está permitido utilizar analizadores del tráfico que circula por RIUS ni herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está autorizado a los administradores de RIUS y bajo situaciones especiales que lo justifiquen (incidentes de seguridad, denuncias de usuarios, etc.).

d. Intentar acceder a la información de otro usuario que no haya sido facilitada explícitamente como de acceso público.

e. La creación, utilización y difusión de cualquier tipo de material que ponga en peligro la seguridad de RIUS, que esté destinado a sabotear su uso o que cause molestias o daños a otros usuarios.

f. La conexión a red de cualquier elemento físico o lógico que modifique la topología de RIUS ni la utilización de direcciones de red sin que hayan sido previamente autorizadas.

g. La manipulación de los componentes de RIUS, tanto activos como pasivos o los mecanismos que les proporcionan suministro eléctrico.

h. Facilitar el acceso a la infraestructura RIUS y a los servicios ofertados a personas u organizaciones ajenas a la Universidad fuera de los cauces que se establezcan sin autorización expresa.

**6.7.** Cuando se detecte un uso incorrecto, se podrá decidir la suspensión del servicio a cualquier usuario o entidad conectada a ella en una de las dos formas siguientes:

a. Suspensión temporal o de emergencia del servicio, cuando la violación de las normas indicadas en este documento esté causando o pueda estar causando una degradación de los servicios de RIUS y/o implique a la US en algún tipo de responsabilidad, así como cuando suponga una modificación de la topología de la red o una conexión no autorizada. Esta decisión se tomará por el administrador de RIUS y se restablecerá la conexión en el momento en que se compruebe que el motivo de la suspensión se ha eliminado.

b. Si se producen infracciones de una especial gravedad, o una reiteración de las mismas, la US podrá suspender indefinidamente la conexión a RIUS de un usuario, restableciéndose el servicio cuando se considere que se dan las condiciones necesarias para ello.

**Artículo 7. Acceso a los Sistemas de Información y a los datos tratados**

**7.1.** Los datos gestionados por la US y tratados por cualquier Sistema de Información de la US deben tener asignado un responsable, que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de los usuarios.

**7.2.** La autorización del acceso establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

**7.3.** Es responsabilidad del usuario hacer buen uso de su cuenta de usuario o cualquier otro mecanismo de acceso. El acceso podrá ser desactivado por el SIC en caso de una incorrecta utilización.

**7.4.** Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso intransferibles.

**7.5.** Cuando un usuario deje de atender un PC durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar el salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizados.

**7.6.** La baja o cambio en la relación del usuario con la US será comunicado en su caso al SIC para proceder a la modificación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.

**7.7.** Todo el personal de la US que por su trabajo tenga acceso a información de carácter personal debe cumplir con la obligación de secreto y confidencialidad, lo que no excluye la posibilidad

de que, en estricto cumplimiento de los pertinentes requerimientos judiciales o, en su caso, autoridad legalmente autorizada, deban revelarse estos contenidos.

**Claves de acceso**

**7.8.** Los usuarios dispondrán de un código de Usuario Virtual de la US (en adelante UVUS) y una contraseña (password) o bien un certificado digital reconocido, para el acceso a los Sistemas de Información de la US, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del dispositivo o terminal desde el que se realiza el acceso.

**7.9.** Dado que la credencial es llave de acceso a datos protegidos, y se podría usar para hacer responsable a su propietario de acciones que no ha realizado, los usuarios no deben revelar o entregar, bajo ningún concepto, su clave de acceso o certificado digital a otra persona.

**7.10.** Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

**7.11.** Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al SIC el correspondiente incidente de seguridad.

**7.12.** Los usuarios deben utilizar contraseñas seguras y deberán cambiarse periódicamente o cuando se sospeche que pueda ser conocida.

**7.13.** El acceso a todos los servicios identificados se hará mediante protocolos cifrados.

**7.14.** Se proveerá a los usuarios de mecanismos para cambiar la clave y generar una nueva en caso de olvido.

**Artículo 8. Acceso y permanencia de terceros en los edificios, instalaciones y dependencias de la US**

Los terceros ajenos a la US que, eventualmente, permanecieran en sus edificios, instalaciones o dependencias, deberán observar las siguientes normas:

**8.1.** El personal ajeno a la US que temporalmente deba acceder a los Sistemas de Información de la US, deberá hacerlo siempre bajo la supervisión de algún miembro acreditado de la US que actuará como enlace, y previa autorización del Servicio responsable del Sistema de Información.

**8.2.** Cualquier incidencia que surja antes o en el transcurso del acceso a la US deberá ponerlo en conocimiento de su enlace. La función del enlace será dar asesoramiento, atender consultas o necesidades, transmitir instrucciones, ponerle al corriente de sus cometidos, objetivos, etc.

**8.3.** Para los accesos de terceros a los sistemas de información de la US, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo en la US. Si, de manera excepcional, tuvieran que utilizar identificadores de usuarios ya existentes, una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas de los usuarios utilizados.

**8.4.** Tales personas, en lo que les sea de aplicación, deberán cumplir puntualmente la presente normativa general, así como el resto de normativas de seguridad de la US, especialmente en lo referente a los apartados de salida y confidencialidad de la información.

**8.5.** Para acceder a los edificios, instalaciones o dependencias de la US deberá estar en posesión de la correspondiente documentación de identificación personal admitida en Derecho (DNI,

pasaporte, etc.), debiendo estar incluido en la relación nominal proporcionada previamente por la empresa a la que perteneciere. La primera vez que acceda físicamente deberá identificarse al personal de Control de Acceso y solicitar la presencia de la persona responsable de la US, que constituirá su enlace durante su estancia en él.

**8.6.** Los terceros atenderán siempre los requerimientos que le hiciere el personal de control y seguridad de los edificios, instalaciones o dependencias a los que tuvieren acceso.

En todo caso, se cumplirá la Normativa vigente en materia de Prevención y Riesgos Laborales.

**Artículo 9. Protección de datos de carácter personal y deber de secreto**

**9.1.** La información contenida en las bases de datos de la US que comprenda datos de carácter personal está protegida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su normativa derivada o de desarrollo.

**9.2.** Los Ficheros o Tratamientos de datos de carácter personal gestionados por la US han de adoptar las medidas de seguridad que se correspondan con las exigencias previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

**9.3.** Todo usuario de la US o de terceras organizaciones que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la US.

**9.4.** No está permitido, asimismo, transmitir o alojar información sensible, confidencial o protegida propia de la US en servidores externos a la US salvo autorización expresa del SIC, que comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre la US y la empresa responsable de la prestación del servicio, incluyendo los Acuerdos de Nivel de Servicio que procedan, el correspondiente Acuerdo de Confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

**9.5.** Las empresas proveedoras con acceso a los Sistemas de Información, deberán cumplir con el presente reglamento así como con las indicaciones que en materia de seguridad les haga la Universidad y, especialmente, con las contempladas para este tipo de accesos en la LOPD.

**Artículo 10. Condiciones en que se prestan los servicios**

**10.1.** La US presta servicios telemáticos a los miembros de la Comunidad Universitaria para facilitar la realización de sus tareas.

**10.2.** La creación de nuevos servicios telemáticos deberá contar con la aprobación previa de la Comisión de Seguridad de la US.

**10.3.** La US, a través de sus órganos de gobierno de carácter general, y de acuerdo con las normativas específicas establecidas al efecto, podrá establecer condiciones específicas de uso asociadas a las características particulares de cada servicio.

**10.4.** Independientemente de esta normativa de carácter general, la utilización de los servicios corporativos lleva asociada unas condiciones específicas asociadas a las características particulares de cada servicio. Estas condiciones de uso se reflejarán en documentos anexos a esta normativa general.

**10.5.** La US, en cumplimiento de lo dispuesto por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), guarda registro del uso de las cuentas de los usuarios y de

los recursos y servicios de RIUS por un periodo de tiempo ajustado, en cada caso, a la legislación vigente, para poder determinar en caso de un mal uso las posibles responsabilidades de sus usuarios.

**10.6.** Se respetará en los términos establecidos por las normas la privacidad del contenido de los mensajes de correo electrónico, sin menoscabo de la capacidad de la US para la aplicación sistemática de programas de detección y eliminación de virus y programas de filtro anti-spam a los mensajes que llegan a la estafeta de la Universidad.

**10.7.** En cumplimiento de lo dispuesto por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), se hará un seguimiento de los accesos que sus usuarios realicen o intenten realizar a los ficheros con datos personales cuya titularidad corresponda a la Universidad.

**10.8.** La US utilizará todos los mecanismos de que disponga para garantizar la seguridad de los servicios ofertados. En virtud de los principios de responsabilidad y autoprotección, los usuarios deberán adoptar todas aquellas medidas que se establezcan para garantizar la seguridad de los Sistemas Informáticos de la Universidad.

**Artículo 11. Correo electrónico**

**11.1.** La US facilita una cuenta de correo electrónico corporativa a cada uno de sus miembros que sirve como medio de comunicación básico, eficiente, homogéneo y gratuito para apoyar la realización de las actividades universitarias.

**11.2.** El servicio institucional de correo electrónico tiene como elemento principal la Estafeta Central por la que se encamina todo el correo entrante y saliente de la US. La US dispone también de servidores para contener los buzones personales que se asignan a cada miembro de la Universidad cuando ingresa en ella, y los buzones institucionales que puedan crearse.

**11.3.** Los usuarios deben ser conscientes de que la dirección de correo electrónico @us.es y sus subdominios informan de su relación con la institución universitaria a diferencia de las direcciones ofrecidas por cualquier proveedor de Internet.

**11.4.** Los usuarios son responsables legales de cualquier actividad que se pueda realizar desde las cuentas asociadas a sus buzones de correo, por lo que no deben permitir que nadie más que ellos pueda utilizarlas.

**11.5.** Está terminantemente prohibido suplantar la identidad de un usuario de la US, de correo electrónico o de cualquier otra herramienta colaborativa.

**11.6.** Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.

**11.7.** No está permitida la utilización de las cuentas de correo personales de la US para el envío de publicidad ni para enviar correo a personas que han expresado su deseo de no recibirlo.

**11.8.** No está permitido el envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad o discapacidad. Tampoco los que contengan programas informáticos (software) sin licencia y los envíos que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.

**11.9.** En ningún caso se podrá utilizar el servicio de correo electrónico de forma que interfiera con el rendimiento del servicio o con las labores propias de los gestores del servicio. Este apartado engloba la prohibición explícita de prácticas mencionadas en los tipos definidos de Abuso de Correo Electrónico (ACE).

**11.10.** Con carácter general, la estafeta central de la US sólo admitirá mensajes dirigidos a los dominios propios de la US y sus subdominios registrados, no redirigiendo mensajes a estafetas externas a la Universidad.

**Artículo 12. Publicación de contenidos en la WEB**

**12.1.** En el uso del servicio de alojamiento de contenidos web, deberá tenerse en cuenta lo dispuesto por la Ley Orgánica de Protección de Datos de Carácter Personal en todos aquellos contenidos que presenten datos de carácter personal. En especial, se evitará hacer públicos mediante este servicio datos personales salvo que esté legalmente establecido. En cualquier caso, se recomienda que sólo se permita el acceso a información personal al interesado. Es también necesario caducar estos documentos cuando haya concluido el período razonable de exposición.

**12.2.** Los Departamentos, Centros, Grupos de investigación, Servicios, asociaciones o colectivos universitarios debidamente reconocidos y autorizados por la US que deseen hacer uso de los recursos del SIC para publicar sus contenidos web deberán solicitar el servicio mediante el formulario que a tal efecto se disponga.

**12.3.** Los contenidos de aquellas páginas web que pertenezcan a entidades y no a usuarios individuales, estarán bajo la responsabilidad de la persona designada en el formulario de solicitud de alta en el servicio. El cese o sustitución del responsable de contenidos deberá ser comunicado al SIC.

**12.4.** Los responsables de contenidos deberán velar por el cumplimiento de la presente normativa para la publicación de los contenidos web, quedando sometidos a la responsabilidad disciplinaria o de otra índole a que hubiere lugar como consecuencia de su incumplimiento.

**12.5.** Será obligatorio incluir en los contenidos los datos que permitan identificar al usuario responsable, expresando asimismo que su contenido es responsabilidad exclusiva de dicho usuario.

**12.6.** Las páginas personales tienen que ser diseñadas de manera que no induzcan a error respecto a su carácter no institucional. La utilización de logotipos o imágenes de la US está permitida siempre que no induzca a considerar la existencia de relación o apoyo a los contenidos de la página personal del usuario por parte de la US.

**12.7.** El Servicio de Alojamiento de Páginas Personales tiene como finalidad exclusiva la publicación de información relacionada con la actividad académica, investigadora o de gestión en el ejercicio de las actividades profesionales dentro de la Universidad de Sevilla.

**Artículo 13. Dominios específicos distintos del corporativo 'us.es'**

**13.1.** La US tiene asociado el dominio us.es como dominio corporativo.

**13.2.** La creación de dominios alternativos, subdominios bajo us.es y asignación de nombres a servicios, requerirá autorización previa de la US mediante el procedimiento que se regule en la normativa correspondiente. La persona designada en el formulario de solicitud de este servicio asumirá asimismo las responsabilidades que la titularidad de dicho dominio lleva consigo. Asimismo, el responsable técnico del dominio debe garantizar que los recursos presentan un funcionamiento seguro que no interfiera en el uso del resto de RIUS.

**Artículo 14. Incidentes de seguridad**

**14.1.** Cuando un usuario detecte cualquier anomalía o incidente de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la US o su imagen, deberá informar inmediatamente al Servicio de Atención a Usuarios SOS que lo registrará debidamente y elevará, en su caso.

**Artículo 15. Usos incorrectos de los recursos**

**15.1.** Se considerará uso incorrecto de los recursos cuando se viole la legislación vigente o se actúe en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.

**15.2.** Las normativas de uso específicas que defina la US podrán concretar qué se considera uso incorrecto de los recursos para cada uno de los servicios.

**15.3.** El uso de los recursos informáticos de la US debe circunscribirse principalmente a actividades docentes e investigadoras o a actividades necesarias para el desempeño de la función administrativa.

**15.4.** El uso de los Servicios y Sistemas de Información estará debidamente controlado para todos los usuarios. Si se hiciese un uso abusivo o inapropiado de estos servicios, la US podrá adoptar las medidas disciplinarias que considere oportunas, sin perjuicio de las acciones civiles o penales a las que hubiere lugar.

**Artículo 16. Medidas a aplicar en caso de incumplimiento**

**16.1.** El incumplimiento de las presentes Normas y Condiciones de Uso o de cualesquiera otras establecidas por la US, comportará de forma preventiva la inmediata suspensión del servicio prestado y/o bloqueo temporal de sistemas, cuentas o acceso a RIUS, con el fin de garantizar el buen funcionamiento de los servicios.

**16.2.** Los órganos competentes de la US decidirán las acciones a tomar en el caso de incumplimiento de la presente normativa de utilización de los recursos y sistemas de información de la US y de la normativa complementaria asociada a cada servicio. Todo ello sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, a las personas presuntamente implicadas en dicho incumplimiento.

**Artículo 17. Monitorización y aplicación de esta normativa**

**17.1.** La US, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

a. Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
b. Monitorizará los accesos a la información contenida en sus sistemas.
c. Auditará la seguridad de las credenciales y aplicaciones.
d. Monitorizará los servicios de Internet, correo electrónico y otras herramientas de colaboración.

**17.2.** La US llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que pudieran atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento legal e investigación sobre

un uso ilegítimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales de los usuarios.

**17.3.** Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. El SIC, con la colaboración de las restantes unidades de la US, velará por el cumplimiento de la presente Normativa General e informará a la Comisión de Seguridad de la Información sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

**17.4.** El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

**17.5.** El sistema que proporciona el servicio RIUS podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar al SIC sobre usos prolongados e indebidos del servicio.

**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**

**ACE** (Abuso de Correo Electrónico)

Actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios. Algunos de los términos habitualmente asociados en Internet a estos tipos de abuso son spamming, mail bombing, unsolicited bulk email (UBE), unsolicited commercial email (UCE), junk mail, etc., abarcando un amplio abanico de formas de difusión.

**AUTENTICIDAD**

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

**CONFIDENCIALIDAD**

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

**DATOS DE CARÁCTER PERSONAL**

Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

**DISPONIBILIDAD**

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

**DOMINIO**

Identificación asociada a un grupo de dispositivos o equipos conectados a internet (us.es).

**DOMINIO ALTERNATIVO**

Dominio distinto a us.es gestionado por la US.

**INCIDENTE DE SEGURIDAD**

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

**INFORMACIÓN INSTITUCIONAL**

Información surgida de los procesos de gestión universitaria.

**INTEGRIDAD**

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

**MEDIDAS DE SEGURIDAD**

Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

**SEGURIDAD DE LA INFORMACIÓN**

Protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas, con el fin de proporcionar confidencialidad, integridad y disponibilidad.

**SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN**

Es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

**SERVICIOS TELEMÁTICOS INSTITUCIONALES**

Servicios telemáticos ofertados a la comunidad universitaria que contribuyen al cumplimiento de los objetivos de la institución.

**SISTEMAS DE INFORMACIÓN INSTITUCIONAL UNIVERSITARIOS**

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

**SUBDOMINIO**

Dominio que forma parte de otro dominio más general. Por ejemplo centro.us.es.

**TRAZABILIDAD**

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

**UVUS**

Usuario Virtual de la Universidad de Sevilla. Mecanismo de autentificación basado en usuario+contraseña del que disponen los miembros de la Comunidad Universitaria para acceder a los Servicios Telemáticos de la Universidad de Sevilla.

## ANEXO 12

NORMAS DE SEGURIDAD
NORMATIVA DE USO ACEPTABLE Y SEGURIDAD BÁSICA DE LAS REDES DE COMUNICACIONES DE LA UNIVERSIDAD DE SEVILLA

Índice



### 1. Introducción

Este documento define las normas de uso y seguridad que deben seguir todos los usuarios que dispongan de acceso a la Redes de Comunicaciones de la Universidad de Sevilla (en adelante, US). Las normas han sido elaboradas con el objetivo de conseguir un uso más eficiente, correcto y seguro de los recursos destinados a dicho Servicio.

### 2. Objeto

El objeto de la presente normativa es regular el acceso y utilización de las redes de datos e infraestructuras de comunicaciones por parte de los usuarios de los Sistemas Informáticos de la US, desde sus distintas sedes o a través de ellas, posibilitando la homogeneización de criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

**3. Ámbito de aplicación**

La presente normativa es de aplicación a 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.

La presente normativa será de aplicación y de obligado cumplimiento para toda la comunidad universitaria y para el personal de organizaciones externas cuando sean usuarios o posean acceso a los Sistemas de Información conectados a las Redes de Comunicaciones de la US.

Los usuarios serán informados de esta Normativa de uso aceptable y seguridad básica y aceptarán que el Servicio de Informática y Comunicaciones (en adelante, SIC) sea el garante del cumplimiento de las mismas. Así mismo podrán proponer al órgano pertinente las modificaciones a este documento que consideren oportunas para ajustarlo a la lógica evolución tecnológica y legislativa que se produzca, manteniendo el espíritu del mismo en lo que respecta a los objetivos y finalidades de las Redes de Comunicaciones. Los usuarios serán puntualmente informados de cualquier modificación que fuera preciso introducir.

**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 transmisión 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 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, el SIC 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. Términos y condiciones de acceso y uso

Estos términos y condiciones de acceso y uso regulan el uso de las Redes de Comunicaciones de la US.

### 7.1. Condiciones de uso

Para garantizar y optimizar el mejor funcionamiento de las Redes de Comunicaciones de la US, son necesarios una serie de compromisos entre los usuarios y los responsables de la red.

El SIC, como responsable de este servicio, debe asegurar:

- La mayor conectividad posible a las Redes de Comunicaciones de la US a todos los usuarios, cumpliendo siempre con las normas de uso y seguridad.
- Acceso a los servicios detallados en la Carta de Servicios del SIC en los términos recogidos en dicho Carta, conforme a los compromisos adquiridos de Acuerdo de Nivel de Servicio (SLA).
- La salvaguardia del espectro de radiofrecuencias en las bandas de 2.4 y 5 GHz que utiliza la red inalámbrica.
- Los compromisos por parte de los usuarios de la Red de Comunicaciones de la US son los siguientes:
- Hacer un uso aceptable de la Red de Comunicaciones de la US en los términos definidos más adelante.
- No interferir con el espectro de radiofrecuencias en las bandas de 2.4 y 5 GHz que utiliza la red inalámbrica.
- Cumplir las normas de seguridad definidas en el presente documento.
- No utilizar su conexión a las Redes de Comunicaciones de la US para proporcionar tráfico a terceras personas o entidades, salvo por expreso consentimiento de los organismos responsables del SIC.
- No solicitar más recursos de los que vayan a ser utilizados.
- Comunicar los problemas que surjan al Servicio de Atención de Usuarios para su resolución.
- Utilizar correctamente los recursos que se le suministran.
- Actualizar los datos asociados al Servicio de DNS cuando se produzcan cambios en ellos, ya sea por alta o baja de equipos o por modificación de alguno de los campos de los mismos.

### 7.3. Uso aceptable

Los usuarios de las Redes de Comunicaciones de la US utilizarán la infraestructura de red para:

- El intercambio de información cuyo contenido sea de investigación, académico, educacional o necesario para el desempeño de la función administrativa o para el acceso a los servicios que a través de ellas se suministran.

En general los usuarios de las Redes de Comunicaciones de la US deberán utilizar eficientemente el servicio con el fin de evitar perjuicios al resto de usuarios.

### 7.4. Uso no aceptable

La infraestructura y servicios ofrecidos por las Redes de Comunicaciones de la US no deben usarse para:

- Cualquier transmisión de información o acto que viole la legislación vigente.
- Fines privados comerciales no autorizados por la US.

- La creación o transmisión de material que cause cualquier tipo de molestia a los usuarios de la US.
- La circulación de información difamatoria de cualquier tipo, ya sea contra entidades o personas.
- La distribución de material que viole derechos de propiedad intelectual.
- El desarrollo de actividades que produzcan:
  - La congestión de la Red de Comunicaciones o Sistemas Informáticos mediante el envío de información o programas concebidos para tal fin.
  - La destrucción, manipulación o apropiación indebida de la información que circula por la red o de la información de otros usuarios.
  - La violación de la privacidad e intimidad de otros usuarios.
  - El deterioro del trabajo de otros usuarios.
  - El uso y obtención de cuentas de Sistemas Informáticos ajenas.
- La comunicación de contraseñas u otro tipo de información que permita a otros usuarios entrar en el sistema.
- Proporcionar acceso remoto a las Redes de Comunicaciones de la US distinto del que el SIC ofrece.
- La conexión de equipos de red activos (hubs, switches, routers, modems, firewalls, puntos de acceso inalámbricos, etc.) que previsiblemente perturbe el correcto funcionamiento de la red o comprometa su seguridad, salvo expresa autorización del SIC.
- La conexión de equipos con nombres o direcciones no registrados en el DNS o asignadas específicamente.
- El empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red, salvo expresa autorización del SIC.
- El uso de analizadores del tráfico, salvo expresa autorización del SIC.
- La conexión, desconexión o reubicación de equipos sin la autorización expresa del SIC.
- El alojamiento de dominios distintos de us.es salvo expresa autorización del SIC.

### 7.5. Aceptación y compromiso de cumplimiento

Los usuarios de los Sistemas Informáticos y/o Sistemas de Información de la Universidad de Sevilla tendrán acceso libre y permanente, durante el tiempo de vinculación con la Universidad de Sevilla, al uso de las Redes de Comunicaciones a las que se refiere la presente normativa.

El uso de las Redes de Comunicaciones de la US implica el conocimiento y plena aceptación de las advertencias legales y condiciones vigentes en cada momento en que el usuario acceda a las mismas y que se especifican en este documento.

Cualquier usuario de las Redes de Comunicaciones de la US que incumpla alguno de los términos especificados en este documento deberá asumir las responsabilidades derivadas de la utilización incorrecta de la infraestructura de Redes de Comunicaciones de la US.

## 8. Desarrollo de la normativa

A fin de reducir el riesgo en el uso de las Redes de Comunicaciones de la US el usuario de este servicio deberá, inexcusablemente, cumplir las normas que se incluyen a continuación:

- Respetar los fines para los que han sido creadas las infraestructuras de red.
- Evitar la interrupción de los servicios que ofrecen o de otros equipos que formen parte de ellas.

- Evitar interferencias e interrupciones en el trabajo de otros usuarios: estas circunstancias pueden producirse especialmente en la red inalámbrica ReInUS, por la presencia de equipos de usuarios no correctamente configurados que generan interferencias en las bandas de emisión de la red o bien por el uso de estos equipos en zonas en las que su uso debe ser restringido.
- Evitar situaciones que afecten a la seguridad de las redes y a sus usuarios.
- Respetar el contenido de las leyes y demás disposiciones que sean de aplicación con especial atención al cumplimiento de la Ley Orgánica 15/1999 de Protección de Datos Personales (LOPD).
- Respetar, dentro de los campus de la US, el rango de radiofrecuencias entre los 2.4 y 5 GHz para uso de la red inalámbrica de la Universidad (ReInUS) y la normativa específica de uso que de este documento se desprenda.

La conexión de un Sistema Informático a las Redes de Comunicaciones de la US conlleva ciertos riesgos desde el momento en que dichas redes están conectadas a Internet. Desde Internet llegan diariamente ataques, virus, gusanos, etc. y, para minimizar los riesgos, los usuarios de la US deben cumplir las siguientes normas de seguridad:

- El usuario del Sistema debe estar protegido por una contraseña acorde a la Política de Contraseñas de la US.
- Deben aplicarse periódicamente todas las actualizaciones de seguridad para el sistema operativo que esté usando. Esta tarea es fácilmente automatizable en la mayoría de los casos.
- No compartir carpetas sin contraseña.
- Como norma general, se utilizarán protocolos seguros que permitan el cifrado y guardado de las contraseñas.

Además de las anteriores normas, se recomienda:

- Instalar únicamente el software que se vaya a necesitar, lo que mejorará las prestaciones del equipo.
- No instalar servicios de red que no se vayan a usar o que interfieran con los ofrecidos por la US, en especial la configuración de los equipos móviles como puntos de acceso inalámbricos.
- Mantener la seguridad de servidores de cualquier tipo (FTP, Web, NTP, etc.) de los que sean responsables.

**9. Responsabilidades**

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, o cuando se reciba un aviso de incidencia de los organismos encargados de ello (CCN-Cert, RedIris), el SIC procederá a la suspensión o interrupción del servicio en el ordenador o dispositivo de red, dependiendo de la gravedad y reiteración del incidente.

**Suspensión temporal o de emergencia del servicio**

Esta medida se tomará cuando se produzca la violación de los términos de este documento de forma premeditada o cuando se esté causando una degradación en los recursos de las Redes de Comunicación de la US o implique a la US en algún tipo de responsabilidad que conlleve perjuicio para sus usuarios. La acción consistirá en la desconexión física de la red de Comunicaciones de la US, del Sistema Informático o dispositivo causante del incidente, hasta resolver la causa que ha llevado a tomar esta medida. Como medida de precaución se procederá al filtrado del tráfico del Sistema Informático o dispositivo implicado, que podrá ser local o general. En el primer caso no permitiendo el acceso al

exterior de la US pero sí a la Red Informática de la Universidad de Sevilla (en adelante, RIUS) y en el segundo caso no permitiendo el acceso a RIUS.

**Suspensión indefinida del servicio**

Esta medida se aplicará cuando se incurra en infracciones de especial gravedad o en una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por el cauce adecuado.

En todos los casos el servicio podrá restablecerse cuando se considere que las medidas adoptadas por el responsable del Sistema Informático o dispositivo causante del incidente garanticen un uso aceptable en el futuro.

**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-Cert**

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Tiene responsabilidad en ciberataques sobre sistemas de las Administraciones Públicas.

**DNS**

Domain Name System (Sistema de Nombres de Dominio) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

**FTP**

File Transfer Protocol (Protocolo de Transferencia de Archivos) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

**LOPD**

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (cualquier información concerniente a personas físicas identificadas o identificables).

**NTP**

Network Time Protocol, es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

**RedIris**

Red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional.

**SERVICIO DE INFORMÁTICA Y COMUNICACIONES**

Servicio responsable de gestionar las Redes de Comunicaciones de la Universidad de Sevilla.

**SLA**

Service Level Agreement o "Acuerdo de Nivel de Servicio" (ANS) en castellano. Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel de calidad de dicho servicio.

**REDES DE COMUNICACIONES O DATOS DE LA US**

Redes de Comunicaciones, tanto cableadas (RIUS) como inalámbricas (ReInUS), que conectan entre sí y con Internet todos los Sistemas Informáticos de la US con interfaz de red, permitiendo a los usuarios el acceso a la red de datos.

**USUARIOS DE LAS REDES DE COMUNICACIONES DE LA US**

Estudiantes, profesores, investigadores, personal de la administración y servicios, usuarios de las instituciones conectadas y, en general, cualquier persona que, por su relación con la US, sea autorizada para dicho uso.

**USO ACEPTABLE**

Uso permitido de las Redes de Comunicaciones de la US.

**USO NO ACEPTABLE**

Uso no permitido de las Redes de Comunicaciones de la US.

**NORMATIVA DE USO DE LAS REDES DE COMUNICACIONES DE LA US**

Este documento que recoge la normativa orientada a lograr el uso aceptable, correcto y seguro de las Redes de Comunicaciones de la US, sean del tipo que sean.

**INSTITUCIONES CONECTADAS A TRAVÉS DE LAS REDES DE COMUNICACIONES DE LA US**

Toda institución que, por un motivo u otro, se encuentre directamente conectada a las Redes de Comunicaciones de la US, ya sea integrante de ésta o externa.

## ANEXO 13

NORMAS DE SEGURIDAD
NORMATIVA DE USO ACEPTABLE Y SEGURIDAD BÁSICA DEL SERVICIO DE ALOJAMIENTO DE PÁGINAS WEB DE LA UNIVERSIDAD DE SEVILLA

Índice

**1. Introducción**

Este documento define las normas de uso y seguridad que deben seguir todos los usuarios que hagan uso del Servicio de Alojamiento de Páginas Web de la Universidad de Sevilla (en adelante, US). Las normas han sido elaboradas con el objetivo de conseguir un uso más eficiente, correcto y seguro de los recursos destinados a dicho Servicio.

**2. Objeto**

La presente normativa tiene por objeto regular el acceso y la utilización del Servicio de Alojamiento de Páginas Web de la Universidad de Sevilla por parte de los usuarios del mismo definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

**3. Ámbito de aplicación**

Esta normativa será aplicable a todos los usuarios de la US en tanto en cuanto hagan uso del Servicio de Alojamiento de Páginas Web.

Los miembros de la Comunidad Universitaria que soliciten alojamiento de página Web y reciban la autorización pertinente, podrán tener sus propias normas de uso y seguridad de la información que publiquen en su página Web, dentro del contexto de la finalidad de dicha información. Estas normas deberán ser compatibles con las condiciones y términos expresados en el presente documento y deberán aparecer publicadas en la página Web del usuario.

Los usuarios serán informados de esta normativa de uso aceptable y seguridad básica y aceptarán que el Servicio de Informática y Comunicaciones (en adelante, SIC) sea el garante del cumplimiento de las mismas. Así mismo podrán proponer al órgano pertinente las modificaciones a este documento que consideren oportunas para ajustarlo a la lógica evolución tecnológica y legislativa que se produzca, manteniendo el espíritu del mismo en lo que respecta a los objetivos y finalidades para los que se crearon el Servicio de Alojamiento de Páginas Web y los servicios añadidos que se mencionan en la Carta de Servicios del SIC. Los usuarios serán puntualmente informados de cualquier modificación que fuera preciso introducir.

**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 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, el SIC 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. Términos y condiciones de acceso y uso**

Estos términos y condiciones de acceso y uso regulan el uso del Servicio de Alojamiento de Páginas Web de la Universidad de Sevilla.

La existencia de los presentes términos y condiciones de acceso y uso no excluye la presencia de otras disposiciones o condiciones de acceso a la información publicada en los alojamientos.

**7.1. Registro del usuario**

Con carácter general, el acceso al Servicio de Alojamiento de Páginas Web de la Universidad de Sevilla exige la previa inscripción o registro de los usuarios en las bases de datos de la Universidad de Sevilla. En estos casos, los datos de carácter personal facilitados a la Universidad serán objeto de tratamiento por parte de la misma, en las condiciones y términos especificados en la presente normativa de uso aceptable y seguridad básica.

El usuario se compromete a usar sus claves de acceso (nombre de usuario y contraseña) de acuerdo con las restricciones que aparecen en este documento y con las normativas en que se basa.

**7.2. Condiciones de uso**

Para garantizar y optimizar el mejor funcionamiento del Servicio de Alojamiento de Páginas Web de la US es necesaria una serie de compromisos entre los usuarios y los responsables del Servicio de Alojamientos.

El SIC, como responsable de este servicio, debe asegurar:

- La disponibilidad del Servicio de Alojamiento de Páginas Web conforme a los compromisos adquiridos mediante Acuerdo de Nivel de Servicio (en adelante SLA).
- El acceso a los servicios añadidos que están detallados en la Carta de Servicios del SIC, en los términos recogidos en dicha Carta.

Los compromisos por parte de los usuarios del Servicio de Alojamiento de Páginas Web de la US son los siguientes:

- Cumplir las normas de seguridad definidas en el presente documento y respetar las leyes de aplicación con especial atención al cumplimiento de los Derechos de Autor y de la LOPD (Ley Orgánica de Protección de Datos).
- Utilizar el alojamiento exclusivamente para el fin por el que fue solicitado: cualquier cambio de uso del alojamiento deberá ser comunicado a los responsables del Servicio de Alojamientos por parte del usuario.
- Gestionar correctamente los recursos que se le suministran conforme a la Normativa aceptada en el proceso de solicitud de alojamiento.
- Comunicar los problemas que surjan al Servicio de Atención de Usuarios para su resolución.

### 7.3. Uso aceptable

Los usuarios del Servicio de Alojamiento de Páginas Web de la Universidad de Sevilla utilizarán las páginas Web para la publicación de información cuyo contenido sea de investigación, académico, educacional o necesario para el desempeño de la función administrativa.

En general los usuarios del Servicio de Alojamiento de Páginas Web de la Universidad de Sevilla deberán utilizar eficientemente sus alojamientos web con el fin de evitar perjuicios al resto de usuarios.

### 7.4. Uso no aceptable

El Servicio de Alojamiento de Páginas Web de la Universidad de Sevilla no debe usarse para:

- Publicar información que viole los derechos de propiedad intelectual, la LOPD o cualquier otra legislación vigente.
- Publicar información que cause cualquier tipo de molestia a otros usuarios, incluida la información difamatoria de cualquier tipo, ya sea contra entidades o personas.
- Fines privados comerciales no autorizados por la US.
- La inclusión de publicidad comercial, así como cualquier tipo de actividad lucrativa.
- Desarrollo de actividades que produzcan:
  - La congestión de la red de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
  - La destrucción, modificación o apropiación indebida de la información de otros usuarios.
  - La violación de la privacidad e intimidad de otros usuarios.
  - Uso y obtención de cuentas ajenas.

### 7.5. Aceptación y compromiso de cumplimiento

Todos los usuarios del Servicio de Alojamiento de Páginas Web de la Universidad de Sevilla deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente normativa, debiendo suscribirla durante el procedimiento electrónico de solicitud del servicio. La aceptación implica que el usuario declara haber leído y comprendido las normas de uso y se compromete a su cumplimiento.

Cualquier usuario que incumpla alguno de los términos especificados en este documento deberá asumir las responsabilidades derivadas de la utilización incorrecta del Servicio de Alojamiento de Páginas Web de la US.

## 8. Desarrollo de la normativa

### 8.1. Enunciado de las normas generales

Para minimizar los riesgos en el uso del Servicio de Alojamiento de Páginas Web de la US los usuarios

deben cumplir las normas que se incluyen a continuación:

- Utilizar la página Web exclusivamente para propósitos relacionados con su vinculación a la Universidad de Sevilla.
- Proteger las credenciales de acceso al alojamiento.
- No ceder el uso de las cuentas de alojamiento a terceros.
- Utilizar conexiones cifradas cuando se deba transmitir información sensible.
- Comprobar la no vulnerabilidad del código de la página alojada.
- Mantener actualizados los programas utilizados por las páginas Web a las últimas versiones disponibles, en particular si se usa un gestor de contenidos.
- Asegurar la actualidad y veracidad de los contenidos publicados de los que sean responsables los usuarios.
- Ajustarse al nivel Doble-A de las Directrices de Accesibilidad para el Contenido Web 1.0 del W3C, incluyendo todos los puntos de verificación de Prioridad 1 y Prioridad 2 definidos en las Directrices.
- Informar debidamente al usuario del uso de cookies, si las hubiera, en virtud del cumplimiento de las leyes vigentes.
- No utilizar el alojamiento como espacio de almacenamiento.
- Disponer la medidas de seguridad básicas necesarias en los ordenadores utilizados para la conexión al Servicio de Alojamiento a fin de evitar el compromiso de la seguridad del servidor de alojamientos.

### 8.2. Normas específicas de protección de datos de carácter personal

Cuando un usuario del Servicio de Alojamiento de Páginas Web publique en su página datos de carácter personal definidos como "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo concerniente a personas físicas identificadas o identificables", deberá cumplir la Ley de Protección de Datos (LOPD), el RD 1720/2007 que la desarrolla y el Documento de Seguridad de la Universidad de Sevilla.

En concreto el usuario observará las siguientes normas:

- Se compromete explícitamente a formar e informar al personal con acceso de publicación en la página en las obligaciones que de tales normas dimanan.
- Declarará los datos de carácter personal que vaya a publicar si no se encuentran previamente declarados en los correspondientes ficheros de datos personales inscritos en la Agencia Española de Protección de Datos por la Universidad de Sevilla o si no está autorizado a disponer de ellos.
- El acceso será únicamente a aquellos datos que precisen para las funciones requeridas y legalmente permitidas. Si a los datos personales accedieran terceros, habría que formalizar el correspondiente contrato de prestación de servicios con acceso a datos.
- Una vez finalizadas las tareas que el adjudicatario del alojamiento tuviera previstas, deberá borrar toda la información de datos personales utilizada o que se derive de la ejecución del correspondiente alojamiento, mediante el procedimiento técnico adecuado.

## 9. Responsabilidades

Si bien, en principio, la duración de este servicio es indeterminada, la Universidad de Sevilla se reserva el derecho a suspender o dar por terminada la prestación del mismo. Esta decisión podrá ser comunicada con antelación a los usuarios de los servicios según estime oportuno la Universidad de

Sevilla.

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento o cuando se reciba un aviso de incidencia de los organismos encargados de ello (CCN-Cert, RedIris), el SIC procederá, dependiendo de la gravedad y reiteración del incidente, a aplicar una de estas medidas:

**Suspensión temporal del acceso de un usuario al Servicio de Alojamiento**

Esta medida se tomará cuando se produzca la violación de los términos de este documento de forma premeditada o cuando se esté causando una degradación en los recursos de nuestra institución o implique a la US en algún tipo de responsabilidad que conlleve perjuicio para sus usuarios.

**Suspensión indefinida de acceso del usuario al Servicio de Alojamiento**

Esta medida se aplicará cuando se incurra en infracciones de especial gravedad o en una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por el cauce adecuado.

En todos los casos el servicio podrá restablecerse cuando se considere que las medidas adoptadas por el responsable del alojamiento garantizan un uso aceptable en el futuro.

**Exención de responsabilidades de la US por los contenidos publicados por los alojamientos**

La Universidad de Sevilla no se hace responsable de la licitud del contenido publicado por los alojamientos de los usuarios. En cualquier caso, se compromete a actuar con diligencia para evitar la existencia de contenidos ilícitos en los alojamientos y, en caso de que tome conocimiento efectivo de estos contenidos, eliminarlos o impedir el acceso a los mismos.

Los documentos publicados podrían contener inconsistencias técnicas o errores tipográficos involuntarios de los cuales la Universidad de no se hace responsable, pero se compromete a comunicarlo, a la mayor brevedad posible, al responsable del alojamiento desde el momento en que tenga conocimiento de los mismos.

La US no se hace responsable de los contenidos a los que se acceda en virtud de enlaces externos a la propia Universidad, ni de las modificaciones que se lleven a cabo en los mismos, ni del uso que de aquellos se realice, ni de la disponibilidad técnica de los mismos. En cualquier caso, la US se compromete a hacer lo posible por evitar la existencia en sus alojamientos de enlaces a sitios de contenido ilegal, que promuevan actividades ilícitas y, en general, susceptibles de atentar contra los principios de libertad y de dignidad humana o vulneren los valores y derechos reconocidos por la Constitución española y por la Declaración Universal de los Derechos Humanos. Asimismo, en caso de que tome conocimiento de la existencia de los antedichos enlaces a sitios de contenido ilegal, el Servicio de Informática y Comunicaciones se compromete a actuar con diligencia para suprimirlos de forma inmediata y comunicarlo al responsable del alojamiento.

**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-Cert**

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Tiene responsabilidad

en ciberataques sobre sistemas de las Administraciones Públicas.

**LOPD**

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (cualquier información concerniente a personas físicas identificadas o identificables).

**Salvaguardas**

Medidas aplicadas para protección de la información contenida en su alojamiento.

**SERVICIO DE INFORMÁTICA Y COMUNICACIONES**

Servicio de la Universidad responsable de gestionar los Alojamiento de Páginas Web de la US.

**SERVICIO DE ALOJAMIENTO DE PÁGINAS WEB DE LA US**

Proporciona a todos los miembros de la Comunidad Universitaria los medios para publicar sus propios contenidos Web institucionales, académicos o de investigación.

**USUARIOS DEL SERVICIO DE ALOJAMIENTO DE PÁGINAS WEB DE LA US**

Estudiantes Universitarios de la US , Estudiantes de Secundaria y Bachillerato de la provincia de Sevilla, Personal Docente e Investigador y Personal de Administración y Servicios de la US, en tanto en cuanto hagan uso del Servicio y, en general, cualquier persona en la que los responsables deleguen y esté autorizada para la administración y el mantenimiento de una página Web.

**NORMATIVA DE USO ACEPTABLE Y SEGURIDAD BÁSICA DEL SERVICIO DE ALOJAMIENTO**

Este documento, que recoge la normativa orientada a lograr el uso correcto y seguro de la información proporcionada al usuario a través de Internet, sea del tipo que sea, en un determinado ámbito.

**RedIris**

Red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional.

**Vulnerabilidad**

Defecto de un activo informático que lo expone a un daño potencial, es decir, un fallo conocido que alguien puede utilizar para acceder sin autorización a nuestro ordenador o a nuestra información.

**W3C**

El Consorcio World Wide Web (W3C) es una comunidad internacional donde las organizaciones Miembro, el personal a tiempo completo y el público en general trabajan conjuntamente para desarrollar estándares Web.

## ANEXO 14

NORMAS DE SEGURIDAD
NORMATIVA DE USO ACEPTABLE Y SEGURIDAD BÁSICA DEL PORTAL INSTITUCIONAL DE LA UNIVERSIDAD DE SEVILLA

Índice

**1. Introducción**

Este documento define las normas de uso y seguridad que deben seguir todos los usuarios que hagan uso del Portal Institucional de la Universidad de Sevilla (en adelante, US). Las normas han sido elaboradas con el objetivo de conseguir un uso más eficiente, correcto y seguro de los recursos destinados a dicho Servicio.

**2. Objeto**

La presente normativa tiene por objeto regular el acceso y la utilización del Portal Institucional de la US por parte de los usuarios del mismo definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

**3. Ámbito de aplicación**

Esta normativa será aplicable a todos los usuarios del Portal Institucional de la US en tanto en cuanto hagan uso de él.

Los miembros de la Comunidad Universitaria que soliciten la publicación de información en el Portal Institucional y reciban la autorización pertinente podrán tener sus propias normas de uso y seguridad de la información que publiquen, dentro del contexto de la finalidad de dicha información. Dichas normas deberán ser compatibles con las condiciones y términos expresados en el presente documento y deberán aparecer publicadas junto a la información del usuario.

Los usuarios serán informados de esta normativa de uso aceptable y seguridad básica y aceptarán que el Servicio de Informática y Comunicaciones (en adelante, SIC) sea el garante del cumplimiento de las mismas. Así mismo podrán proponer al órgano pertinente las modificaciones a este documento que se consideren oportunas para ajustarlo a la lógica evolución tecnológica y legislativa que se produzca, manteniendo el espíritu del mismo en lo que respecta a los objetivos y finalidades para los que se creó el Portal Institucional. Los usuarios serán puntualmente informados de cualquier modificación que

fuera preciso introducir.

**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 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.

Cuando las circunstancias así lo aconsejen, el SIC 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. Términos y condiciones de acceso y uso**

Estos términos y condiciones de acceso y uso regulan el uso del sitio web de la Universidad de Sevilla, al que se accede mediante la dirección URL http://www.us.es.

La existencia de los presentes términos y condiciones de acceso y uso no excluye la presencia de otras disposiciones o condiciones de acceso a las diversas secciones que componen el sitio de la Universidad de Sevilla.

**7.1. Registro del usuario**

Con carácter general, el acceso y utilización del Portal Institucional de la Universidad de Sevilla no exige la previa inscripción o registro de los usuarios. No obstante, el acceso a determinados servicios de la Universidad de Sevilla accesibles a través del sitio oficial está supeditado al registro del usuario en las bases de datos de la Universidad de Sevilla. En estos casos, los datos de carácter personal facilitados a la Universidad serán objeto de tratamiento por parte de la misma, en las condiciones y términos especificados en la presente normativa de uso aceptable y seguridad básica.

El usuario se compromete a usar sus claves de acceso (nombre de usuario y contraseña) a los servicios de acuerdo con las restricciones que aparecen en la normativa específica de cada servicio.

### 7.2. Condiciones de uso

Para garantizar y optimizar el mejor funcionamiento del Portal Institucional de la US es necesaria una serie de compromisos entre los usuarios y los responsables del Portal.

El SIC, como responsable de este servicio, debe asegurar:

- La disponibilidad del Portal Institucional de la US conforme a los compromisos adquiridos mediante Acuerdo de Nivel de Servicio (en adelante SLA).
- La actualidad y veracidad de los contenidos publicados en el Portal Institucional.
- La conformidad por parte de la US de ajustarse al nivel Doble-A de las Directrices de Accesibilidad para el Contenido Web 1.0 del W3C, incluyendo todos los puntos de verificación de Prioridad 1 y Prioridad 2 definidos en las Directrices.
- El acceso a los servicios que están detallados en el Catálogo de Servicios del SIC en los términos recogidos en dicho Catálogo.

Los compromisos por parte de los usuarios del Servicio Portal Institucional de la US son los siguientes:

- Hacer un uso aceptable del Portal Institucional de la US, respetando los fines para los que ha sido creado y utilizando correctamente los recursos que se le suministran.
- Evitar la interrupción de los servicios que ofrece.
- Evitar situaciones que afecten a la seguridad del Portal Institucional y de sus usuarios.
- Actualizar puntualmente los contenidos de los que sean responsables.
- Cumplir las normas de seguridad definidas en el presente documento y respetar las leyes de aplicación con especial atención al cumplimiento la propiedad intelectual, los derechos de autor y la protección de datos personales.
- Comunicar los problemas que surjan al Servicio de Atención de Usuarios para su resolución.

### 7.3. Uso aceptable

Los usuarios del Portal Institucional de la Universidad de Sevilla utilizarán el sitio web oficial de esta institución para:

- Consulta y publicación de información cuyo contenido sea de investigación, académico, educacional o necesario para el desempeño de la función administrativa.
- Acceso a los servicios que a través del Portal se suministran.

En general los usuarios del Portal Institucional de la US deberán utilizar eficientemente el sitio web con el fin de evitar perjuicios al resto de usuarios.

### 7.4. Uso no aceptable

El Portal Institucional de la Universidad de Sevilla no debe usarse para:

- Publicar información que viole los derechos de propiedad intelectual, la LOPD o cualquier otra legislación vigente.
- Publicar información que cause cualquier tipo de molestia a otros usuarios del Portal Institucional, incluida la información difamatoria de cualquier tipo, ya sea contra entidades o personas.
- Fines privados comerciales no autorizados por la US.
- Desarrollo de actividades que produzcan:

- La congestión de la red de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
- La destrucción, modificación o apropiación indebida de la información de otros usuarios.
- La violación de la privacidad e intimidad de otros usuarios.
- Uso y obtención de cuentas ajenas.

### 7.5. Aceptación y compromiso de cumplimiento

Todos los usuarios del Portal Institucional de la US deberán tener acceso permanente a la presente normativa. Su uso implica el conocimiento y plena aceptación de las advertencias legales y condiciones vigentes en cada momento en que el usuario acceda al Portal y que se especifican en este documento.

Cualquier usuario que incumpla alguno de los términos especificados en este documento deberá asumir las responsabilidades derivadas de la utilización incorrecta del Portal Institucional de la Universidad de Sevilla.

## 8. Desarrollo de la normativa

### 8.1. Enunciado de las normas generales

Para minimizar riesgos, los usuarios del Portal Institucional de la US deberán cumplir las normas que se incluyen a continuación:

- Proteger las credenciales de acceso a los servicios ofrecidos a través del Portal Institucional.
- Utilizar conexiones cifradas cuando se deban transmitir datos personales protegidos por la Ley.
- Configurar correctamente las cookies en los navegadores.
- Asegurar la actualidad y veracidad de los contenidos publicados de los que sean responsables.
- Disponer la medidas de seguridad básicas necesarias en los ordenadores utilizados para la conexión al Portal Institucional y a los servicios que a través del él ofrece la Universidad de Sevilla, como pueden ser antivirus, software mínimo imprescindible, etc. a fin de evitar el compromiso de la seguridad.

### 8.2. Normas específicas de protección de la propiedad intelectual y derechos de autor

En cumplimiento de lo previsto en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, se informa que el sitio web www.us.es ha sido creado, es mantenido y es propiedad de la Universidad de Sevilla, por lo que el usuario del Portal Institucional deberá observar las siguientes normas:

- La denominación "Universidad de Sevilla", así como otros signos distintivos (gráficos o denominativos) que aparecen en este sitio web, son propiedad exclusiva de la Universidad de Sevilla. Queda prohibida su utilización por parte de terceros que carezcan de autorización.
- La eventual presencia en este sitio de signos distintivos de titularidad ajena a la US se efectúa sin finalidad comercial y con la autorización de sus legítimos propietarios. Queda prohibida su utilización por parte de terceros que carezcan de la autorización de sus titulares.
- El nombre de dominio "www.us.es" y todos aquellos que sirvan para acceder de forma directa al presente sitio oficial son de titularidad exclusiva de la Universidad de Sevilla. La indebida utilización de los mismos en el tráfico económico supondría una infracción de los derechos conferidos por su registro y será perseguido por los medios previstos en la Ley.
- Los contenidos (textos, fotografías, diseños y en general, cualquier creación intelectual existente en este sitio oficial), así como el propio sitio en su conjunto como obra artística multimedia

están protegidos como derechos de autor. El usuario queda expresamente autorizado por la Universidad de Sevilla a visualizar, imprimir, copiar o almacenar, las creaciones intelectuales protegidas siempre que ello se efectúe para fines personales y privados del usuario, sin finalidad comercial o de distribución y sin modificar, alterar o descompilar los antedichos derechos y contenidos.

- Esta facultad de uso personal se entiende reconocida siempre y cuando se respeten intactas las advertencias a los derechos de autor y de propiedad industrial aquí realizadas y no supone la concesión de licencia alguna al usuario.
- Quedan exceptuados de esta protección aquellos archivos o programas de ordenador que no sean de titularidad de la Universidad de Sevilla y de acceso gratuito (freeware) que el usuario puede descargarse desde diversas páginas de este sitio con el fin de posibilitar el acceso a las mismas. Se trata, en todo caso, de aplicaciones que tienen el carácter de dominio público por expresa voluntad de sus autores.
- Los museos, bibliotecas, fonotecas, filmotecas, hemerotecas o archivos, de titularidad pública o integradas en instituciones de carácter cultural o científico, quedan exentos de requerir la autorización de la Universidad de Sevilla por la reproducción del material contenido y, en general, de cualquier creación intelectual existente en este sitio oficial o activo amparado o no por un derecho de exclusiva, cuando aquella se realice sin finalidad lucrativa y exclusivamente para fines de investigación.
- Cualquier otra utilización requerirá la autorización expresa y por escrito de la Universidad de Sevilla.

**8.3. Normas específicas de protección de datos de carácter personal**

La Universidad de Sevilla pone en conocimiento de los usuarios del Portal Institucional que podrá crear un archivo automatizado con los datos personales que sean facilitados a la misma como consecuencia de la utilización del presente sitio web y en estricto cumplimiento con lo preceptuado en la legislación en materia de protección de datos. En este supuesto, el usuario se compromete a:

- Garantizar la veracidad y autenticidad de las informaciones y datos que comuniquen en virtud de la utilización de este sitio web. Los usuarios podrán ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos recopilados y archivados.
- Aceptar plenamente y sin reservas el tratamiento, por parte de la Universidad de Sevilla, de los datos de carácter personal facilitados.

**9. Responsabilidades**

Si bien, en principio, la duración de este servicio es indeterminada, la Universidad de Sevilla se reserva el derecho a suspender o dar por terminada la prestación del mismo. Esta decisión podrá ser comunicada con antelación a los usuarios de los servicios según estime oportuno la Universidad de Sevilla.

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento o cuando se reciba un aviso de incidencia de los organismos encargados de ello (CCN-Cert, RedIris), el SIC procederá, dependiendo de la gravedad y reiteración del incidente, a aplicar una de estas medidas:

**Suspensión temporal del acceso de un usuario al Portal y servicios ofrecidos a través del él**

Esta medida se tomará cuando se produzca la violación de los términos de este documento de forma premeditada o cuando se esté causando una degradación en los recursos de nuestra institución o

implique a la US en algún tipo de responsabilidad que conlleve perjuicio para sus usuarios. La acción a tomar y la duración de la misma dependerán de la incidencia, si bien, como medida de precaución se procederá al filtrado del tráfico del ordenador o dispositivo implicado, no permitiendo el acceso al Portal Institucional y/o a los Servicios ofrecidos a través del mismo.

**Suspensión indefinida de acceso del usuario al Portal y servicios ofrecidos a través del él**

Esta medida se aplicará cuando se incurra en infracciones de especial gravedad o en una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por el cauce adecuado.

En ambos casos el servicio podrá restablecerse cuando se considere que las medidas adoptadas por el responsable del ordenador o dispositivo causante del incidente garantizan un uso aceptable en el futuro.

**Exención de responsabilidades de la Universidad de Sevilla por los contenidos publicados por terceros**

La Universidad de Sevilla no se hace responsable de la licitud del contenido suministrado por los proveedores, usuarios y otros terceros a través de cualquiera de las maneras de utilización de este sitio web. En cualquier caso, la Universidad de Sevilla se compromete a actuar con diligencia para evitar la existencia en su sitio web de contenidos ilícitos y, en caso de que tome conocimiento efectivo de estos contenidos, eliminarlos o impedir el acceso a los mismos.

Los documentos publicados podrían contener inconsistencias técnicas o errores tipográficos involuntarios de los cuales la Universidad de Sevilla no se hace responsable, pero se compromete a subsanarlos, a la mayor brevedad posible, desde el momento en que tenga conocimiento de los mismos.

La Universidad de Sevilla no se hace responsable de los contenidos a los que se acceda en virtud de enlaces externos a la propia Universidad, ni de las modificaciones que se lleven a cabo en los mismos, ni del uso que de aquellos se realice, ni de la disponibilidad técnica de los mismos. En cualquier caso, la Universidad de Sevilla se compromete a hacer lo posible por evitar la existencia en su sitio web de enlaces rotos o a sitios de contenido ilegal, que promuevan actividades ilícitas y, en general, susceptibles de atentar contra los principios de libertad y de dignidad humana o vulneren los valores y derechos reconocidos por la Constitución española y por la Declaración Universal de los Derechos Humanos. Asimismo, en caso de que tome conocimiento de la existencia de los antedichos enlaces a sitios de contenido ilegal, la Universidad de Sevilla se compromete a actuar con diligencia para suprimirlos de forma inmediata.

La información, la presentación y los servicios que ofrece este sitio pueden ser sometidos a cambios periódicos o puntuales, susceptibles de ser efectuados libremente por la Universidad de Sevilla sin que esté obligada a comunicarlo a los usuarios.

**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-CERT**

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro

Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Tiene responsabilidad en ciberataques sobre sistemas de las Administraciones Públicas.

**LOPD**

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (cualquier información concerniente a personas físicas identificadas o identificables).

**PORTAL INSTITUCIONAL DE LA UNIVERSIDAD DE SEVILLA**

Sitio web oficial de la Universidad de Sevilla que proporciona el acceso a la mayor parte de los Servicios de la US y de los contenidos Web institucionales, académicos y de investigación existentes en la Universidad.

**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.

**SLA**

Service Level Agreement o "Acuerdo de Nivel de Servicio" (ANS) en castellano. Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel de calidad de dicho servicio.

**NORMATIVA DE USO ACEPTABLE Y SEGURIDAD BÁSICA DEL SERVICIO DE ALOJAMIENTO**

Este documento, que recoge la normativa orientada a lograr el uso correcto y seguro de la información proporcionada al usuario a través de Internet, sea del tipo que sea, en un determinado ámbito.

**RedIris**

Red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional.

**USUARIOS DEL PORTAL INSTITUCIONAL DE LA US**

Estudiantes, profesores, investigadores, personal de la administración y servicios, resto de miembros de la Comunidad Universitaria y, en general, cualquier persona externa a la Universidad de Sevilla, en tanto en cuanto hagan uso de este Servicio.

**W3C**

El Consorcio World Wide Web (W3C) es una comunidad internacional donde las organizaciones Miembro, el personal a tiempo completo y el público en general trabajan conjuntamente para desarrollar estándares Web.

## ANEXO 15

POLÍTICAS DE SEGURIDAD
POLÍTICA DE CONTRASEÑAS DE LA UNIVERSIDAD DE SEVILLA

Índice

5. Referencias
6. Desarrollo de la política
7. Responsabilidades

Apéndice: Lenguaje de género

ANEXO: Acrónimos y glosario de términos

**1. Introducción**

La Universidad de Sevilla (en adelante, US) establece una Política de Contraseñas acorde a los requisitos legales vigentes que debe ser aplicada a cualquier mecanismo de autentificación que utilicen los miembros de la Comunidad Universitaria para acceder a los Servicios de Tecnologías de la Información y las Comunicaciones (en adelante, TIC) de la US.

Concretamente se aplica al Usuario Virtual de la Universidad de Sevilla (en adelante, UVUS), que es el mecanismo de acceso a los servicios más extendido, así como a los usuarios locales de las aplicaciones informáticas que no utilizan el UVUS como medio de autenticación y a los usuarios externos que acceden a la Red Informática de la Universidad de Sevilla (RIUS) a través de Redes Privadas Virtuales (VPN).

**2. Ámbito de aplicación**

La presente política es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, esté vinculado la US, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la US y tengan que utilizar contraseñas para acceder a ellos.

**3. Vigencia**

Esta política 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 ella.

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 política.

**4. Revisión y evaluación**

La gestión de esta política 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 política, 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.

**5. Referencias**

La presente política 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.

**6. Desarrollo de la política**

Se aplica a todos los usuarios de los Servicios TIC de la Universidad de Sevilla la siguiente política de contraseñas:

- La longitud de la contraseña debe ser como mínimo de 8 caracteres, si bien se recomienda usar contraseñas más largas.
- La contraseña debe contener al menos 4 caracteres alfabéticos de los cuales serán, al menos, dos letras mayúsculas y dos minúsculas.
- La contraseña debe contener al menos 2 caracteres numéricos.
- El número máximo de repeticiones de caracteres adyacentes de la contraseña será 4.
- El número máximo de caracteres numéricos en secuencia de la contraseña será 4.
- La contraseña no podrá contener el nombre o apellido del usuario, ni el documento de identidad del mismo o su UVUS.
- No compartir la contraseña bajo ningún concepto con otras personas, aunque sean de su mismo entorno.
- Guardar la información de contraseñas en un lugar seguro.
- Cambiar la contraseña al menos una vez al año.
- No utilizar para generar la contraseña palabras o nombres comunes que puedan figurar en diccionarios.
- No se podrán utilizar las tres últimas contraseñas empleadas.

Además de la anterior política de contraseñas aplicada a los UVUS, el usuario podrá observar las siguientes recomendaciones:

- Modificar la contraseña que le entreguen antes de hacer uso de ella aunque no esté obligado a hacerlo.
- Tener al menos un símbolo (cualquier otro carácter que no sea alfabético o numérico: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).

**7. Responsabilidades**

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, o cuando se reciba un aviso de incidencia de los organismos encargados de ello (CCN-Cert, RedIris), el SIC podrá proceder al bloqueo temporal o indefinido del usuario dependiendo de la gravedad y reiteración del incidente, siendo responsable el usuario titular.

**Apéndice: Lenguaje de género**

Esta política 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-Cert**

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Tiene responsabilidad en ciberataques sobre sistemas de las Administraciones Públicas.

**RedIris**

Red académica y de investigación española que proporciona servicios avanzados de comunicaciones a la comunidad científica y universitaria nacional.

**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.

**UVUS**

Usuario Virtual de la Universidad de Sevilla.

**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.

***