UNIVERSIDAD D SEVILLA

Normas de Seguridad

Normativa general de utilización de los Recursos y Sistemas de Información de la Universidad de Sevilla

Índice

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: GLOSARIO

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.