UNIVERSIDAD Ð SEVILLA

Normativa de Seguridad

Normativa general de utilización de los Recursos y Sistemas de Información de la Universidad de Sevilla. Acceso local y remoto.

1. Objeto

Establecer las normas y criterios generales para el uso de recursos informáticos y servicios de información de la Universidad de Sevilla (en adelante US) en consonancia con lo establecido en la Política de Seguridad de la Información.

2. Ámbito de aplicación

Esta normativa es de obligado cumplimiento y aplicable a todos los usuarios de los servicios y recursos de Tecnología de la Información (en adelante TI) de la US.

3. Referencias legales

La legislación vigente está disponible en la web de Seguridad de la Información y Protección de Datos, opción de menú "Marco legal".

4. Lenguaje de género

Las referencias a personas o colectivos figuran en el presente documento en género masculino como género gramatical no marcado. Cuando proceda, será válida la cita de los preceptos correspondientes en género femenino.

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.
- Actualizar la normativa, sometiendo los cambios a la aprobación de la Comisión de Seguridad de la US, cuando:
  - Se identifiquen oportunidades de mejora en la gestión de la seguridad.
  - Se produzcan cambios legales, en las infraestructuras tecnológicas o cambios organizativos.
  - Se cumpla el plazo establecido para su revisión.

- Verificar su efectividad.

6. Términos y condiciones de acceso y uso

La US presta servicios de información a los usuarios para facilitar la realización de sus tareas. La utilización de los servicios se rige por la aplicación de la Política de seguridad de la US, por lo establecido en el presente documento y por lo establecido con carácter particular en la normativa específica de cada uno de los servicios.

La creación de nuevos servicios de información deberá contar con la aprobación previa de la Comisión de Seguridad de la US.

6.1. Registro del usuario

Todos los usuarios con carácter previo al acceso y utilización de los servicios de la US deberán ser identificados, registrados y aceptar la Política de Seguridad de la Información y las normas de uso.

6.2. Condiciones de uso

La US, en cumplimiento de lo dispuesto por la legislación vigente, guarda un registro del uso realizado por cada usuario de los recursos y servicios ofrecidos, durante el tiempo necesario.

Los usuarios tienen conocimiento y aceptan que por la US se utilicen todos los mecanismos de que disponga para garantizar la seguridad de los servicios ofertados.

El SIC, como responsable de los servicios debe asegurar:

- La disponibilidad del servicio ofertado por la US conforme a los compromisos adquiridos de conformidad con el Acuerdo de Nivel de Servicio (SLA).
- La salvaguardia de la información y datos mediante la realización de las copias de seguridad adecuadas.
- Evitar la interrupción de los servicios que ofrece.
- Evitar situaciones que afecten a la seguridad del servicio y de los usuarios

Los usuarios se comprometen a:

- Aceptar y cumplir las normas de seguridad aplicables a cada servicio en la US.
- Comunicar los problemas que surjan al Servicio de Atención de Usuarios del SIC para su resolución.

- Comunicar cualquier incumplimiento de estas normas al Servicio de Atención a Usuarios SOS para la apertura de la oportuna incidencia de seguridad (véase incidente de seguridad).
- Eximir a la US de cualquier responsabilidad que pueda derivarse por la realización de un uso no aceptable.
- 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.
- Proteger los equipos de usuario con contraseñas acordes a la Política de Contraseñas de la US.
- Hacer un uso aceptable:
  - Se entiende uso aceptable aquel uso que se ajusta la finalidad del servicio.
- Evitar un uso no aceptable. Se entiende por uso no aceptable:
  - Difundir mensajes con contenidos contrarios a los principios enunciados en los Estatutos de la US, 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 legislación sobre protección de datos de carácter personal 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.
  - Utilizar los servicios para fines privados comerciales no autorizados por la US.
  - Desarrollar 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.

6.3. Incidente de seguridad

Cuando un usuario detecte cualquier anomalía o incidente de seguridad deberá informar inmediatamente al Servicio de Atención a Usuarios SOS que lo registrará debidamente y elevará, en su caso.

Cuando el incidente de seguridad afecte a datos de carácter personal deberá ser notificado de forma inmediata el Delegado de Protección de Datos y se aplicará el protocolo de información establecido por la legislación vigente.

6.4. Datos sensibles, confidenciales, protegidos o de carácter personal

Todos los datos e información contenida en las bases de datos de la US, así como todos los tratamientos de datos de carácter personal que se desarrollen por la US deberán estar protegidos por la legislación vigente y contar con las medidas de seguridad que les sean de aplicación.

Los usuarios de la US que tengan acceso a datos de carácter personal están obligados a guardar la confidencialidad, el secreto sobre los mismos, respetar las normas de seguridad establecidas y hacer un uso conforme a la legislación vigente. Este deber se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la US.

No está permitido 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.

Normas sobre políticas de privacidad:

- La información personal relativa a los usuarios que esté disponible en cualquier recurso de la US solo podrá utilizarse para los fines adecuados quedando expresamente prohibido su uso para fines distintos salvo que se cuente 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 o en espacios colectivos como foros, chat, webs o blogs. El entorno de la US incluye por defecto el nombre de usuario UVUS, correo profesional, teléfono corporativo, nombre y apellidos. Cualquier otro dato incluido en perfiles del usuario se publican bajo la exclusiva responsabilidad de su titular.
- La inclusión de referencias de datos personales sensibles no está permitida, sin el previo consentimiento expreso del usuario y con los requisitos que marca la legislación vigente.
- El uso de fotografías no es obligatorio, pudiendo ser retirada aquellas que no se ajusten a la normativa de la US. El profesor solo podrá, si lo estima relevante para su actividad, sugerir a los alumnos que incorporen la misma.
- Cualquier archivo, fotografía o video que con carácter docente se publique en el entorno de la US contará con permiso expreso de las personas que aparezcan en él, sin límite geográfico y por tiempo limitado, o se tomarán las medidas necesarias para impedir su identificación. En cualquier caso, la publicación será respetuosa con la imagen personal de quienes aparezcan en tales ficheros. 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 de la Universidad revelará ni facilitará a terceros sus credenciales de acceso a los Servicios Corporativos. 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, éste procederá a cambiar su contraseña en la plataforma de Gestión de Identidad de la US.

6.5. Normas de seguridad para el personal de la US

- PRIMERO. PUESTOS DE TRABAJO.
  - Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que almacenan 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, a bloquear o apagar el equipo según proceda, y a reiniciar la sesión cuando vuelva a ocupar el puesto de trabajo.
  - En el caso de las impresoras, el usuario 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 que no están autorizados para acceder a la información de los documentos impresos, 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 al Servicio de Atención a Usuarios SOS.
- CUARTO. COPIA DE DATOS EN SOPORTES PROPIOS.
  - No se recomienda la copia de documentos que contengan datos personales en soportes externos 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 utilizar documentos que contengan datos personales o contenidos protegidos en soporte papel, será responsable de su custodia de modo que se evite que terceros no autorizados accedan a la información 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 este tipo de documentos se encuentra expresamente prohibido.
- Las papeleras de reciclado sólo podrán utilizarse previa destrucción segura de los documentos.

6.6. Normas específicas de protección de la propiedad intelectual

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.

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 la US, 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.

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.

Ningún usuario del sistema podrá introducir en el entorno de US documentos, materiales, software o cualesquiera recursos con incumplimiento de la legislación vigente sobre propiedad intelectual y patentes.

Sólo se insertarán 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 entorno 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.

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 o trabajos elaborados por usuarios de la Universidad.

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 cualquier plataforma de publicación o enseñanza virtual 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 usuarios:

Que la inclusión de materiales de cualquier tipo en el entorno de la US 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».

El entorno de la US 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.

6.7. Responsabilidad

La US no se hace responsable de la mala utilización que se realice por los usuarios de los servicios quedando facultada para adoptar las medidas que correspondan a fin de restablecer la legalidad vigente y la calidad de los servicios.

Las acciones que se tomen y la duración de estas dependerán de la incidencia detectada y de los perjuicios que la misma esté causando o pueda llegar a causar. Con carácter general se procederá con la mayor diligencia posible a la suspensión de la prestación del servicio o servicios afectados por el incumplimiento.

El servicio será restablecido al usuario cuando se considere que se dan las condiciones que garanticen un adecuado funcionamiento del servicio y un uso aceptable por parte del usuario.

7. Acceso local y remoto a TI

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 con 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. [por defecto el administrador del sistema establecerá una política de bloqueo en todos los equipos]
- 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.

8. Glosario y acrónimos

Todas las definiciones y acrónimos de los conceptos recogidos en esta y el resto de las normativas están publicadas en el enlace "Glosario y acrónimos".