UNIVERSIDAD D SEVILLA

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.