UNIVERSIDAD D SEVILLA

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.