UNIVERSIDAD D SEVILLA

Normas de Seguridad

Normativa de generación de copias de seguridad y recuperación de información

Índice

1. Introducción

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

2. Objeto

El objetivo del presente documento es definir las directrices para garantizar el respaldo, la protección y la disponibilidad de la información corporativa, contenga o no datos personales, para restaurarlos en caso de pérdida o daño de los datos originales. Se aplicarán las medidas de seguridad necesarias que permitan el almacenamiento y recuperación de los datos atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de la US que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica, modificado por el RD 951/2015 de 23 de Octubre.

3. Ámbito de aplicación

Esta normativa es de aplicación a todo el ámbito de actuación de la US, y sus contenidos derivan de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de la US.

La presente normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la US, especialmente, los responsables del Servicio de Informática y Comunicaciones (en adelante, SIC) y los propios usuarios, como actores ambos, en sus respectivas competencias, de la generación de copias de respaldo y su

ulterior recuperación, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información de la US.

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

4. Vigencia

La presente Normativa ha sido aprobada por el Comité de Seguridad de la US con fecha 16 de diciembre de 2016, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la US pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la US. Las versiones anteriores quedan anuladas por la última versión de esta normativa.

5. Revisión y evaluación

La gestión de esta normativa corresponde al SIC, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario, para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

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

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica y organización general o cualquier otra cuestión que pueda provocarla.

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

6. Referencias

La presente normativa se fundamenta en la legislación vigente en materia de seguridad de las Tecnologías de la Información y las Comunicaciones de ámbito europeo, estatal y autonómico, así como en las normas y procedimientos internos que resulten de aplicación a la Universidad en el marco de la Política de Seguridad de la Información.

7. Desarrollo de la normativa

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

Las copias de respaldo deberán abarcar:

a) Información de trabajo de la organización.

b) Aplicaciones en explotación, incluyendo los sistemas operativos.

c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.

d) Claves utilizadas para preservar la confidencialidad de la información.

7.1. Copias de respaldo de los SI y recuperación

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

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

- Periodos de retención de las copias
- Ubicación de los soportes de respaldo
- Procedimientos de recuperación de la información
- Procedimientos de restauración de los servicios y verificación de la integridad de la información respaldada
- Procedimientos de inventario y gestión de soportes para *backup*
- Procedimiento de revisión de *logs* de copias de seguridad

7.2. Copia de respaldo de los equipos de usuario

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

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

7.3. Tipos de copias de respaldo

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

- Copia completa o *FULL*: copia completa de todos los datos principales, ficheros y bases de datos.

- Requiere mayor espacio de almacenamiento y ventana de *backup*.
- Ofrece la seguridad de tener una imagen de los datos en el momento de la copia.

- Copia incremental: copia de los datos modificados desde la anterior copia completa o incremental.
  - Siempre se debe partir de una copia total o completa inicial.
  - Si se realiza con frecuencia, el proceso no consumirá un tiempo excesivo, debido al bajo volumen de datos a copiar.
  - La restauración completa es lenta: se requiere recuperar una copia completa y todas las incrementales realizadas hasta el momento en el cual se quiera restaurar el sistema.
- Copia diferencial: copia de los datos que hayan sido modificados respecto a una copia completa anterior.
  - Requiere menor espacio de almacenamiento y ventana de *backup*.
  - Se ejecutará con mayor rapidez en función de la frecuencia con que se realice.
  - La restauración suele ser más rápida que la incremental, ya que basta con recuperar una copia completa y una copia diferencial.

7.4. Verificación y comprobación de las copias

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

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

7.5. Retención de las copias

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

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

8. Responsabilidades

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

Apéndice: Lenguaje de género

Esta normativa ha sido redactada con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.

ANEXO: Acrónimos y glosario de términos

Backup

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

ENS

Esquema Nacional de Seguridad. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por el RD 951/2015 de 23 de Octubre.

Offsite

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

SI

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

SIC

Servicio de Informática y Comunicaciones. Servicio cuyo objetivo es atender las necesidades de apoyo informático a las tareas de estudio, docencia, investigación y gestión en la Universidad de Sevilla.