PROCEDIMIENTO DE CLASIFICACIÓN DE LA INFORMACIÓN EN LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprobado por Consejo de Gobierno de 6 de junio de 2024

1. Objeto

El objeto del presente procedimiento es la definición de la clasificación de información en los sistemas tecnológicos de la Universitat Politècnica de València dentro del alcance señalado en el Esquema Nacional de Seguridad, aplicando el conjunto de medidas de seguridad que son necesarias para el cumplimiento adecuado, en concreto, las establecidas por los apartados "Protección de la información [mp.info]" y "Protección de los soportes de información [mp.si]".

Los principios u objetivos que han guiado la redacción de esta normativa son los siguientes:

- Determinar unos criterios de clasificación de la información de Universitat Politècnica de València.
- Definir los criterios de marcado y etiquetado de la información.
- Establecer las medidas de seguridad mínimas que deben aplicarse en el tratamiento según el nivel de protección tanto sobre la información como en los soportes.

2. Ámbito de aplicación

Este procedimiento se aplica a todo el ámbito de actuación de la Universitat Politècnica de València, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en la Normativa de Seguridad de la UPV.

El presente documento es de aplicación y de obligado cumplimiento para todo el personal o usuarios que, de manera permanente o eventual, preste sus servicios o trabaje internamente en el Universitat Politècnica de València, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información del Universitat Politècnica de València.

3. Roles y responsables

En el procedimiento de Clasificación de la Información intervienen los siguientes roles:

Responsable de seguridad:

- Coopera y asesora a los Responsables de Información en la clasificación de la información de la organización.
- Propone la implantación de controles para validar el etiquetado, marcado y tratamiento adecuados de la información y detectar desviaciones con respecto a ellos.
- Autoriza la destrucción o borrado de soportes con información sensible.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

Responsables de la información:

- Aprueban la arquitectura y métodos de clasificación de la información que se encuentren bajo su responsabilidad.

Responsables del sistema:

- Asesoran sobre qué medidas de seguridad se pueden llevar a cabo en el sistema.

Administradores del sistema:

- Ejecutan satisfactoriamente la implantación de medidas de seguridad, como la destrucción o el borrado de los soportes que contienen información sensible.

Usuarios:

- Acceden a la información y soportes, y, en consecuencia, deberán estar debidamente autorizados, comprometiéndose a cumplir los requisitos de acceso a la misma.

4. Normativa

4.1. Criterios de Clasificación de la Información

Como estrategia de gestión del riesgo sobre amenazas que pueden comprometer la información, se establecen diferentes niveles de protección que garantizan mayores controles según su importancia para el negocio.

Para esta clasificación no aplica la Ley 9/1968, de 5 de abril, sobre secretos oficiales.

Se ha establecido un criterio de clasificación de la información y se han determinado medidas de seguridad proporcionales al nivel de relevancia del contenido. Las categorías establecidas son mostradas en la tabla siguiente:

Etiquetado	Definición
Información SIN CLASIFICAR o PÚBLICA	Información antigua que todavía no ha sido categorizada atendiendo a los criterios del ENS o que es de dominio público, por lo tanto, de acceso libre a toda persona.
Información de USO OFICIAL	Información a la que puede tener acceso distinto personal de la organización, dependiendo de sus características o responsabilidades con esta. No debería ser accedida por personal que no haya sido autorizado o personal externo a la organización.

4.1.1. Información SIN CLASIFICAR

Se considera información SIN CLASIFICAR aquélla que no tiene asignado ninguno de los otros niveles de clasificación.

Éste será un estado temporal y será asignado a cualquier tipo de información que no esté categorizada en la presente normativa.

Este hecho deberá ser trasladado al Responsable de Seguridad o al Responsable de la Información que corresponda, según el área o contenido, para que asigne un nivel de protección e incluya ese nuevo tipo de información en la preasignación de niveles que establece la presente normativa.

La información que haya sido categorizada como SIN CLASIFICAR se somete a los siguientes criterios:

- Etiquetado: ninguno.
- Marcado: ninguno.
- Tratamiento: La información SIN CLASIFICAR deberá pasar por el proceso de clasificación para que pueda ser marcada conforme el nivel de protección que sea necesaria y sea autorizada y vinculada a un Responsable de Información.

4.1.2. Información PÚBLICA

La Universitat Politècnica de València considera información PUBLICA aquella que es de ámbito público y no está sometida a requisitos legales que requieran preservar su sensibilidad o confidencialidad.

Esto supone que se asume como riesgo aceptable si se produce una filtración, modificación o difusión.

En soporte papel será información pública toda aquella situada en las zonas comunes o accesibles que no se encuentre custodiada por ningún responsable.

La información que haya sido categorizada como PÚBLICA se somete a los siguientes criterios:

- Etiquetado: ninguno.
- Marcado: ninguno.
- Tratamiento: La información que haya sido categorizada como PÚBLICA no está sujeta a ningún tratamiento especial ni gestionada de forma obligatoria.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

4.1.3. Información de USO OFICIAL

La información marcada como USO OFICIAL es aquella que está sometida a requisitos legales que requieren preservar sensibilidad y confidencialidad, tiene valor en las dimensiones de confidencialidad o integridad y supone riesgos ampliamente aceptables o tolerables si se produce una filtración, modificación o difusión.

La Universitat Politècnica de València considera información de USO OFICIAL a aquélla que por su contenido se considere expresamente como tal, siendo este contenido considerado por el Responsable de información.

Para la información de USO OFICIAL se definen condiciones de accesos especiales que afectarán a los archivos físicos en soporte papel y a los archivos en soporte electrónico.

La información de USO OFICIAL solo puede ser conocida por personas concretas en cada área de la entidad y supone riesgos inaceptables si se produce una filtración, modificación o difusión.

La información que haya sido categorizada como de USO OFICIAL se somete a los siguientes criterios:

- Etiquetado: explícito, de forma visible e inteligible, en cualquier tipo de soporte.
- Marcado: explícito, de forma visible e inteligible, en soportes digitales.

- Tratamiento:

Como regla general se emplea el principio de “mínimos privilegios”, es decir, la asignación de acceso se produce en base a la necesidad de conocer y la asigna el responsable de la información.

La regulación de la difusión y la copia de los datos está restringida, salvo al personal que necesite conocer los datos para el correcto desempeño de su labor dentro de la organización.

Se establece la prohibición de transmisión por cualquier medio de soporte, a usuarios internos o externos, que no sea a aquel que haya sido autorizado por el responsable de información.

Almacenamiento en carpetas electrónicas:

- El almacenamiento de la información se podrá realizar en cualquier activo de la organización y nunca en dispositivos externos a esta.
- La información almacenada en los diferentes medios electrónicos como servidor de ficheros o nube, deberá de limitarse definiendo grupos de seguridad para determinar cuáles son los privilegios de acceso a asignar.
- Será el responsable de servicio quién determinará los usuarios que pueden tener acceso a la información, ya sean internos u externos.

Documentación en soporte papel:

- Toda la documentación relevante de cada una de las áreas deberá estar autorizada por el Responsable de la Información y este deberá de velar por garantizar el cumplimiento de las medidas.
- La información estará almacenada en las zonas de trabajo de cada una de las áreas de la entidad.
- Esta información no podrá albergarse en zonas de paso o acceso público al ciudadano, sino que serán espacios de acceso restringido al personal de la entidad.

Los criterios anteriores son definidos y aprobados para este tipo de datos por el Responsable de la Información con el soporte del Responsable de Seguridad; se comunican adecuadamente a las personas que por su trabajo dentro de la organización necesiten tener acceso a este tipo de información.

4.2. Localización de la información

La Universitat Politècnica de València tiene toda la información en soporte electrónico en las carpetas compartidas en los servidores de ficheros corporativos y en las carpetas en la nube corporativa en OneDrive.

En ambos sistemas las medidas de seguridad son las adecuadas para dar soporte al criterio de clasificación de información propuesto.

4.3. Tratamiento de la Información

En cualquiera de los casos descritos, se implementarán las medidas de seguridad contempladas en el Esquema Nacional de Seguridad.

En lo relativo al etiquetado, los activos serán identificados según el criterio de clasificación establecido en el apartado anterior.

En lo relativo a la custodia, se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, mediante las siguientes actuaciones:

- Garantizando el control de acceso con medidas físicas, lógicas o ambas.
- Garantizando que se respetan las exigencias de mantenimiento del fabricante de estos soportes, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

En lo relativo a la digitalización, con carácter general, cuando se escaneen documentos, el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas. Conviene no olvidar retirar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación abandonada en un escáner, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. En caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del Responsable de Seguridad.

En lo relativo al transporte o transmisión, los intercambios de información se realizarán preferentemente en soporte electrónico. Cuando vayan a enviarse documentos de USO OFICIAL, su envío deberá garantizar que solo el receptor legítimo puede conocer dicha información. Para ello se utilizarán técnicas de cifrado de datos o bien del contenido del mensaje (cifrado de archivos) o bien del canal de comunicación (cifrado de las comunicaciones mediante el uso de protocolos seguros).

Cuando el envío se realice mediante servicios de mensajería, deberá asegurarse que el transportista cumple las medidas de seguridad establecidas por el ENS y satisface los requisitos requeridos por el nivel de clasificación de la documentación enviada.

En lo relativo a la limpieza de documentación en soporte electrónico, se retirará de éstos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento. Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

En lo relativo a copias de seguridad, el sistema actualmente implantado permite recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada.

En lo relativo a la destrucción, la medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos. Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido. Se destruirán de forma segura los soportes cuando la naturaleza del soporte no permita un borrado seguro.

5. Definiciones

Información: Es un dato que se trata y que posee un significado para la organización.

Soporte: Es un objeto físico o abstracto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

Como ejemplos de soportes físicos se enumeran: USBs o pendrives, DVD, CD, disquetes, discos duros, cintas DAT, cintas LTO, y en definitiva cualquier dispositivo que almacene datos relevantes.

En este sentido los soportes de almacenamiento se caracterizan por su portabilidad y por no integrarse en el interior de dispositivos de almacenamiento primario como un servidor o un terminal de usuario.

Como ejemplo de soporte abstracto cabe mencionar los sistemas almacenamiento en la nube, como es el caso del sistema corporativo OneDrive.

En relación al tratamiento no automatizado o no informatizado, se entenderá como soporte físico de almacenamiento aquellos archivadores, estanterías, armarios, etc. que almacenen archivos en papel con información clasificada.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen