Universidad Veracruzana

LA INFORMACIÓN

Clasificación, cifrado y metadatos

metared

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

www.incibe.es

ÍNDICE

ÍNDICE DE FIGURAS

1. CLASIFICACIÓN DE LA INFORMACIÓN

Bases de datos, hojas de cálculo, facturas, datos personales de estudiantes, etc., son muchos los datos que gestiona una universidad y no todos tienen la misma criticidad. Una de las partes más importantes a la hora de proteger la información **[Ref. - 1]** de una universidad es clasificarla correctamente antes de tomar ninguna acción. El proceso de clasificación **[Ref. - 2]** se puede dividir en 4 pasos.

1.1. Inventariado de los activos

Etapa fundamental en la que **se deben tener en cuenta todos los recursos con los que cuenta la universidad, tanto en formato físico, como en formato digital.** Además, es conveniente catalogar otras características de los activos como su tamaño, ubicación o departamentos que intervienen en su gestión.

1.2. Criterios de clasificación

La universidad debe escoger los criterios que mejor se adapten a sus circunstancias. Estos pueden ser las necesidades o requisitos de confidencialidad, integridad y disponibilidad de cada activo para las actividades principales de la misma. Un ejemplo orientativo sobre cómo clasificarla en base a la confidencialidad de la misma sería:

confidencial
información de gran relevancia para el futuro de la universidad;

restringida
accesible, únicamente, para determinado personal de la universidad y sin la cual no pueden desempeñar su trabajo;

uso interno
accesible, exclusivamente, para el personal de la universidad;

pública
información de dominio público como, por ejemplo, la publicada en la página web.

1.3. Clasificar cada activo

El siguiente paso consiste en **etiquetar cada activo** de forma adecuada, un ejemplo sería añadiendo etiquetas al comienzo del nombre del archivo.

[confidencial]Proyectos_2020.docx

[restringido]nóminas_2018.xlsx

[interno]Cuadrantes_mes.xlsx

[publico]Historico_mensajes_Redes_Sociales.xlsx

También podrían utilizarse marcas de agua o códigos de color.

1.4. Tratamiento de la información

El siguiente paso consiste en elaborar un **listado con los controles de seguridad que se llevarán cabo para proteger cada activo.** Un ejemplo del tratamiento que recibirá cada tipo de información, en función de su confidencialidad, será:

LIMITAR EL ACCESO

CIFRADO

COPIAS DE SEGURIDAD

CONTROLES ESPECÍFICOS

ACUERDOS DE CONFIDENCIALIDAD

- Limitar el acceso de personas o grupos. Se deberá llevar un control de accesos para que la información sea accesible, únicamente, por el personal que la necesite para su trabajo, según los roles o perfiles. Por ejemplo, los datos de estudiantes no son necesarios para el personal de RRHH. No toda la Comunidad Universitaria debe tener acceso a todos los recursos.
- Cifrado.
- Copias de seguridad.
- Medidas específicas como las indicadas en el recurso formativo anterior relativas al cumplimiento de la LOPDGDD u otra normativa que aplique a la universidad.
- Medidas específicas para la información sujeta a acuerdos de confidencialidad.

2. CIFRADO DE LA INFORMACIÓN

A la hora de proteger la información en formato electrónico, una de las medidas más eficaces es el cifrado de la información **[Ref. - 3].** Mediante esta técnica podemos **ofuscar cualquier fichero y hacerlo inaccesible a otras personas que no sepan la clave de descifrado.**

El cifrado es una de las mejores medidas de seguridad para el almacenamiento y transmisión de **información sensible, especialmente a través de soportes y dispositivos móviles o servicios de almacenamiento en la nube.**

Para que la información cifrada sea lo más confidencial posible se han de seguir una serie de recomendaciones:

- la clave elegida para el cifrado debe ser lo más robusta posible;
- se ha de escoger un algoritmo criptográfico fuerte, preferiblemente de dominio público, como AES-256, evitando el uso de aquellos que ya ha sido comprometida su robustez;
- cada cierto tiempo se debe comprobar que el método criptográfico elegido no es vulnerable;
- la perdida de la clave de descifrado imposibilitará el acceso a la información. Se debe almacenar en un lugar seguro y del que se pueda recuperar;
- la herramienta de cifrado, como sucede con todo el software, debe estar actualizada a la última versión.

Aunque existen múltiples herramientas para el cifrado de información, muchas aplicaciones de compresión de ficheros y ofimática disponen de la posibilidad de comprimir con contraseña, lo que puede ser suficiente, en la mayoría de los casos, si la contraseña utilizada es lo más robusta posible.

3. METADATOS, RIESGOS Y CÓMO ELIMINARLOS

Un «metadato» es aquella información que incluye ficheros digitales pero que no forma parte del contenido. Algunos ejemplos de metadatos son la fecha de creación, la fecha de modificación o el autor del fichero.

Tenemos que tener en cuenta que cada tipo de fichero tiene sus propios metadatos. Por ejemplo, mientras que un fichero ofimático como un Word puede contener el autor del documento, una imagen puede incluir además sus dimensiones, información de dónde se tomó la foto o incluso el modelo de cámara utilizado.

Aunque pueden ser muy útiles, **en algunos casos pueden proporcionar información valiosa sobre nosotros a los ciberdelincuentes** como nombres de usuario, fechas de creación o modificación de los documentos, ubicación de las fotografías, aplicación utilizada, etc.

Por ello, debemos **eliminar los metadatos antes de enviar el fichero a otra persona, o subirlos a la página web de la universidad o a un servicio de almacenamiento en la nube.**

La mayoría de programas de ofimática más utilizados incorporan funcionalidades para eliminar esta información. También se puede hacer desde el propio sistema operativo como es el caso de Windows mediante la opción de botón derecho -> Propiedades -> Detalles. A continuación, se selecciona «Quitar propiedades e información personal» y se abrirá una nueva ventana. Se selecciona la opción «Quitar las siguientes propiedades de este archivo» y posteriormente «Seleccionar todo». Por último, clic en «Aceptar» y el proceso de borrado de metadatos ha terminado.

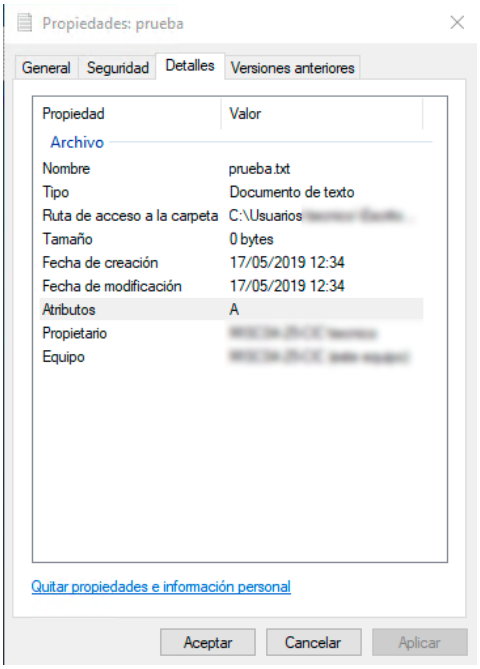

Ilustración 1. Los tres pilares de la seguridad de la información

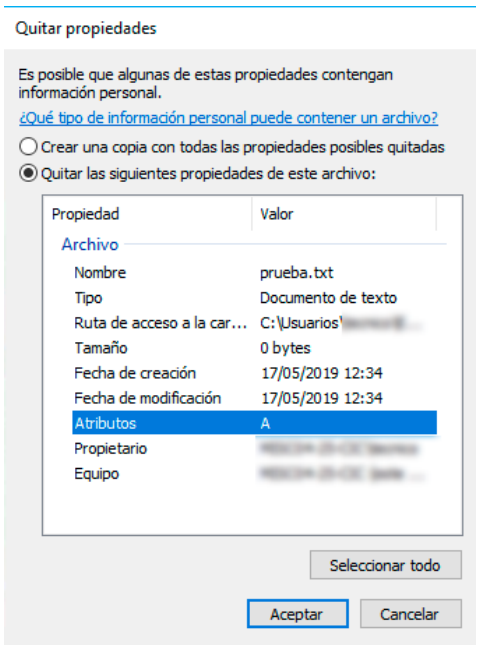

Ilustración 2. Pasos para borrar los metadatos mediante Windows 2

4. REFERENCIAS

1. INCIBE - Protege tu Empresa - ¿Qué te interesa? - Protección de la información - https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

2. INCIBE - Protege tu Empresa – Blog - Primeros pasos para clasificar la información de tu organización - https://www.incibe.es/protege-tu-empresa/blog/primeros-pasos-clasificar-informacion-tu-organizacion

3. INCIBE - Protege tu Empresa – Herramientas – Políticas - Uso de técnicas criptográficas - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

3. INCIBE - Protege tu Empresa - Herramientas - Políticas - Uso de técnicas criptográficas - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

4. INCIBE-CERT – Traffic Light Protocol (TLP) - https://www.incibe-cert.es/tlp