



Ciberconciencia: un viaje educativo por la seguridad digital de la UNAD



Guía Seguridad de la Información

Universidad Nacional Abierta y a Distancia - UNAD

Rafael Antonio Ramírez Rodríguez

Gerente de Plataformas e Infraestructura Tecnológica
gerencia.plataformas@unad.edu.co

Carlos Andrés Materon

Coordinador Infraestructura Tecnológica
carlos.materon@unad.edu.co

Leonardo Montilla Malaver

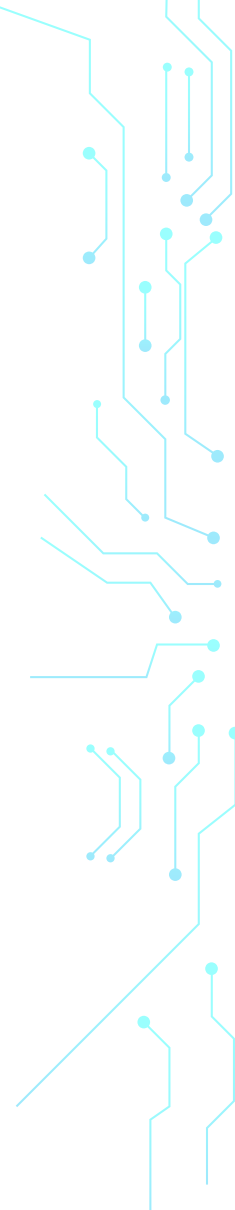
Oficial de la Seguridad de la Información
seguridad.informacion@unad.edu.co

Tatiana Isabel Herazo Usta

Administración Copias de Respaldo
tatiana.herazo@unad.edu.co

Contenido

Seguridad de la información	4
Presentación	4
Objetivos	5
Clasificación de la Información	5
Inventariado de los activos	5
Criterios de clasificación	5
Clasificar cada activo	6
Tratamiento de la información	6
Cifrado de la Información	6
Metadatos, riesgos y como eliminarlos	7
Normatividad institucional	8
Referencias	9



Seguridad de la información

La información institucional que se maneja a través de las redes, equipos y aplicaciones informáticas en general, representan un activo muy valioso para la universidad, el cual puede encontrarse expuesto a diversos riesgos, que de ser explotados causarían un impacto significativo en la continuidad de las funciones normales de la institución.

Por lo anterior es muy importante efectuar acciones que contribuyan en la seguridad de la información de la UNAD, ante lo cual se están desarrollando diversas actividades como la campaña de seguridad de la información, entre otras.

Presentación

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 de una universidad es clasificarla correctamente antes de tomar ninguna acción.



Objetivos

- Apoyar el cumplimiento del Manual de Políticas y Procedimientos Internos para el proceso de Clasificación, cifrado y tratamiento de los metadatos y la información de la Universidad Nacional Abierta y a Distancia UNAD.
- Estandarizar y facilitar la comprensión del procedimiento en las diferentes dependencias que Clasifican y cifran la información de la Universidad.
- Acompañar al personal unadista en el conocimiento gradual de los conceptos, lineamientos, mecanismos y herramientas, para la clasificación, cifrado y tratamiento de los metadatos que puedan comprometer la seguridad del Sistema de Información de la UNAD.



Clasificación de la información

La clasificación de la información es un proceso en el que todas las organizaciones deberían evaluar los datos que poseen y el nivel de protección que cada uno requiere. En la gestión de la seguridad de la información, recordemos que los niveles de acceso están dados por el rol de cada uno de los empleados de una organización, los niveles gerenciales, operativos e incluso los directivos, deben formar parte de este marco de seguridad de dicha clasificación.

Inventariado de los activos

Es la 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.

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.

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, por ejemplo:

- [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.

Tratamiento de la Información

El siguiente paso consiste en elaborar un listado con los controles de seguridad que se llevarán a 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 Ley de protección de datos personales u otra normativa que aplique a la universidad.
- Medidas específicas para la información sujeta a acuerdos de confidencialidad.

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. 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 pérdida 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.



Metadatos, riesgos y como 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. Debemos 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 ciberdelinquentes 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 los 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.

Normatividad Institucional

- Resolución No. 7298 de mayo 10 de 2023: Marco de Referencia del Sistema de Gestión de Seguridad de la Información.
- Resolución No. 367 de enero 17 de 2019: Manual de Políticas y Procedimientos internos para el tratamiento de datos personales.
- Resolución 8547 - de septiembre 8 de 2016: Uso de servicios de tecnologías.
- Acuerdo No. 003 de febrero 27 de 2017.
- Ley Estatutaria 1581 de 2012: Esta ley regula el derecho fundamental a la protección de datos personales en Colombia. Establece los principios fundamentales para el tratamiento de datos personales, incluyendo la confidencialidad y la seguridad de la información. Establece la obligación de contar con políticas de tratamiento de datos y medidas de seguridad para proteger la información.
- Decreto Reglamentario 1377 de 2013: Este decreto reglamenta la Ley 1581 de 2012 y establece las pautas específicas para el manejo de datos personales en Colombia. Define los procedimientos para la inscripción de bases de datos en el Registro Nacional de Bases de Datos.
- Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio (SIC): La SIC emitió esta circular para establecer pautas y recomendaciones específicas sobre la implementación de medidas de seguridad de la información.



- Resolución 2225 de 2007 del Ministerio de Comunicaciones: Esta resolución establece regulaciones para la protección de la información en redes y sistemas de información.
- Ley 1273 de 2009: Conocida como la “Ley de Delitos Informáticos”, esta ley regula los delitos informáticos, incluyendo el acceso ilegal a sistemas y la interceptación de datos.
- Regulación sobre Cifrado: En Colombia, no existe una regulación específica sobre cifrado de datos, pero las organizaciones deben implementar medidas de seguridad adecuadas, incluyendo el cifrado, para proteger la confidencialidad de la información, como lo establece la Ley 1581 de 2012.

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-clasificarinformacion-tu-organizacion>
3. INCIBE - Protege tu Empresa - Herramientas - Políticas - Uso de técnicas criptográficas - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso_tecnicascriptograficas.pdf
4. INCIBE - Protege tu Empresa - Herramientas - Políticas - Uso de técnicas criptográficas - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso_tecnicascriptograficas.pdf
5. INCIBE-CERT-Traffic Light Protocol (TLP)-<https://www.incibe-cert.es/tlp>

