

POLÍTICA PARA LA CLASIFICACIÓN Y ALMACENAMIENTO DE LA INFORMACIÓN FÍSICA Y DIGITAL

Contenido

1. Propósito de la Política.....	2
2. Alcance	2
3. Definiciones.....	2
4. Clasificación de la información.....	2
4.1 Información pública	2
4.2 Información de uso interno.....	3
4.3 Información confidencial.....	3
4.4 Información secreta.	3
5. Almacenamiento de la información digital	5
6. Definición de permisos en el espacio de almacenamiento en los servidores UNAB	5
7. Tiempo de permanencia de la información en los servidores UNAB.....	5
8. Almacenamiento de información documental confidencial y de uso interno.....	6
9. Almacenamiento de información documental secreta.....	6

1. Propósito de la Política

Esta política está orientada a proporcionar a los encargados del tratamiento de la información los lineamientos necesarios para realizar un proceso efectivo de almacenamiento, clasificación y protección de los activos de información de la UNAB

2. Alcance

El presente documento aplica a todas las personas que mantienen un vínculo laboral o contractual con la UNAB, los asociados de negocios o personas pertenecientes a las universidades en convenio. Cubre la información compuesta por todos los datos personales de estudiantes, empleados, proveedores (personas naturales) o cualquier otro tipo de información utilizada en las actividades del día a día de la organización y que se encuentra en forma física o digital.

3. Definiciones

- **Información digital.** Es la información que es almacenada, transmitida o procesada a través de dispositivos electrónicos como discos duros, memorias USB, CD, DVD etc. o a través de sistemas de información.
- **Información física.** Es la información documental que la UNAB utiliza como soporte a las actividades diarias y que se encuentra almacenada en las diferentes dependencias.
- **Cifrado.** Método matemático que permite aumentar la seguridad de un mensaje o de un archivo mediante la transformación del mismo con la ayuda de una clave de tal manera que solo puede ser leído por la persona que conoce dicha clave.
- **Nube pública.** Infraestructura disponible en Internet que permite el almacenamiento de la información de manera libre y con autenticación previa.

4. Clasificación de la información

Los encargados del tratamiento de la información deben clasificar los activos de información que tienen bajo su responsabilidad en una de las siguientes cuatro categorías (ver Tabla 1).

4.1 Información pública. Esta información en su forma digital o en su forma física, podrá ser divulgada y diseminada sin restricciones en el contenido o la audiencia (por ejemplo, Detalles de los programas, folletos y otros materiales de las carreras y de mercadeo). Sin embargo, la divulgación o difusión de la información no debe violar las leyes o regulaciones aplicables (ej. derechos de autor) y la modificación debe estar restringida a las personas autorizadas expresamente para dicha tarea. Esta información en su forma digital puede ser almacenada en el PC o en repositorios designados por la organización para tal fin, si esta en forma física en los escritorios o archivadores auxiliares.

4.2 Información de uso interno. Esta información puede ser revelada o difundida únicamente a personas que cuenten con vínculos laborales, contractuales, asociados de negocios y/o vínculos educativos con la UNAB y a otras personas autorizadas por la alta dirección, sin ningún tipo de restricciones en el contenido. Si dicha información está en forma digital puede ser almacenada en el PC o en repositorios internos designados por la organización para tal fin, si esta en forma física puede ser almacenada en los escritorios o en archivadores auxiliares.

4.3 Información confidencial. Esta información debe estar sujeta a restricciones de acceso y debe estar disponible solo para las personas que cuenten con la debida autorización. En esta categoría se ubican los datos personales de naturaleza semiprivada, privada y sensible que la UNAB ha recibido en custodia y la información crítica de la Universidad. Si dicha información está en forma digital, debe ser ubicada en el área de almacenamiento en los servidores de la UNAB. Si esta en forma física debe ser almacenada bajo llave en el escritorio o en los archivadores auxiliares de las dependencias. No se debe realizar divulgación o difusión de esta información.

Se prohíbe el almacenamiento de datos de esta categoría en los equipos de cómputo o medios de almacenamiento removibles pertenecientes al funcionario, en nubes públicas como Google Drive o Dropbox o cualquiera que haga sus funciones. No se deben retirar de la UNAB documentos de esta categoría sin la autorización del responsable de los mismos.

4.4 Información secreta. Esta información tiene un importante valor empresarial para la UNAB y la revelación o divulgación no autorizada puede causar un perjuicio grave a la Institución. Toda la información que no esté clasificado de forma explícita como pública, de uso interno o confidencial se considerará secreto. La información secreta digital debe ser cifrada cuando se almacena o cuando se trasmite. Los documentos de esta categoría deben ser almacenados bajo fuertes medidas de seguridad física (ej: caja fuerte)

Se prohíbe el almacenamiento de datos de esta categoría en nubes públicas como Google Drive o Dropbox o cualquiera que haga sus funciones. Los documentos con información secretan tendrán manejo restringido únicamente por sus directos responsables, se prohíbe su copiado o su inspección sin la autorización del responsable de los mismos. Se debe realizar la destrucción segura de dichos documentos, cuando hayan perdido su utilidad más no su calidad de secretos.

Clasificación	Ejemplo de información	Cantidad Típica	Costos de Seguridad	Ejemplos de medidas de seguridad digital	Ejemplos de medidas de seguridad física
Pública	Folletos de programas, comunicaciones de prensa, revistas, informes, entre otros	Muchos documentos	Mínimos	Copiado a discos de solo lectura, copias en disco duros, nubes públicas	Consulta libre de la información
Uso Interno	Políticas de la compañía, información de procesos, Guías de Catedra, memorandos, entre otros.	Muchos documentos	Medio	Copias en discos duros, Accesos controlados por usuarios Windows o Mac	Uso restringido al entorno de trabajo UNAB. Destrucción segura de documentos.
Confidencial	Proyectos, datos personales de los estudiantes, empleados o proveedores, Información de salarios, historias clínicas, planes estratégicos, entre otros	Documentos seleccionados	Alta	Copia en áreas de almacenamiento protegidas por sistemas de respaldo y autenticación de usuarios.	Uso restringido, acceso monitoreado, control de impresión y de copiado, destrucción segura de documentos
Secreto	Contraseñas de los usuarios.	Documentos seleccionados	Muy alta	Accesos seguros, ciframiento. Almacenamiento en servidores. Copias de Backup Diarias	Uso restringido a los responsables de la información, destrucción segura de documentos, Almacenamiento bajo llave, caja fuerte.

Tabla 1. Listado de Clasificaciones

5. Almacenamiento de la información digital

- a) Todas las dependencias tienen derecho a un espacio de almacenamiento en los servidores UNAB para resguardar allí cualquier documento de trabajo de copia única e importante para la dependencia.
- b) El espacio de almacenamiento será definido por Tecnologías de Información y comunicaciones UNAB y será esta dependencia la encargada de la administración técnica del mismo, incluyendo dentro de sus tareas sin limitarse a: La realización de copias de seguridad, el monitoreo del crecimiento del almacenamiento y la disponibilidad del servicio.
- c) El espacio de almacenamiento le permitirá al usuario recuperar su información en caso de una falla en su PC de escritorio o portátil que le haya sido asignado por la UNAB. Por tal motivo los integrantes de cada dependencia serán los responsables del manejo de la información y de ubicarla en el área de almacenamiento siempre que se le haga algún cambio o modificación.
- d) La información archivada en el espacio de almacenamiento de los servidores UNAB, será copiada a los medios de respaldo diariamente con una contención de un mes, es decir se guardan las versiones de los últimos 30 días.
- e) Los documentos archivados en el área de almacenamiento podrán ser borrados por el usuario que cuente con los permisos para realizar dicha función, el mismo será designado por el responsable de cada dependencia.
- f) Si el personal autorizado para el ingreso a la información detecta cualquier violación de las normas de seguridad o de vulnerabilidad de los sistemas de información, debe notificarlo a la oficina de Seguridad de la Información; en ningún caso se puede revelar a terceros.

6. Definición de permisos en el espacio de almacenamiento en los servidores UNAB

- a) El jefe de cada dependencia tiene la función de establecer la estructura de permisos de sus usuarios para acceder al espacio de almacenamiento de su dependencia en los servidores UNAB.
- b) El jefe de cada dependencia será el responsable de informar a la oficina de Tecnología de Información y Comunicaciones, la activación o el bloqueo de acceso a la información de las personas pertenecientes a su dependencia.

7. Tiempo de permanencia de la información en los servidores UNAB

- a) Los documentos de consulta constante pueden permanecer en forma indefinida en el área de almacenamiento.

- b) Los documentos almacenados en los servidores UNAB y que no hayan sido accedidos por espacio de 12 meses se considerarán documentos finales y estos documentos serán enviados al repositorio de almacenamiento definido por Tecnologías de Información y Comunicaciones para tal fin.

8. Almacenamiento de información documental confidencial y de uso interno

- a) La información documental clasificada como confidencial se debe mantener bajo inventario, debe ser almacenada bajo llave y su acceso debe ser monitoreado por el responsable de la misma.
- b) La información documental confidencial debe ser accedida únicamente por las personas que la requieren para el desarrollo de sus funciones laborales. El custodio de la información debe mantener un registro de las personas que acceden a la información confidencial almacenada en las bases de datos documentales.
- c) El proveedor que realice un proceso de microfilmación, restauración o encuadernación etc. de bases de datos documentales con información confidencial o de uso interno, debe firmar el documento de compromiso de confidencialidad que la UNAB tenga establecido.
- d) Si el personal custodio de la información detecta cualquier violación de las normas de seguridad, debe notificarlo a la oficina de Seguridad de la Información; en ningún caso se puede revelar esta información a terceros.

9. Almacenamiento de información documental secreta

La información documental secreta debe almacenarse bajo fuertes medidas de seguridad física (cajas fuertes etc.), su acceso será controlado por el responsable de la misma. Se debe realizar la destrucción segura de los documentos desactualizados o que han perdido su utilidad, pero no su calidad de secreto.

Declaración Final

Esta política fue creada por la Oficina de Seguridad de la Información y revisada por el Comité de Tecnología UNAB. Cada año o en el momento en que se requiera, se verificará la legislación y normas que apliquen en el entorno en el que se desenvuelve la organización para mantenerla actualizada