UNAM

RED·TIC
Red de Responsables TIC
U N A M

RECOMENDACIONES PARA EL ALMACENAMIENTO DE INFORMACIÓN

Noviembre de 2021, 1ª versión

Índice

Recomendaciones para el almacenamiento de información

Introducción

Para el cumplimiento de sus actividades sustantivas, las diversas áreas universitarias que integran a la Universidad Nacional Autónoma de México (UNAM) manejan a diario una gran cantidad y diversidad de datos relativos a docencia, investigación, cultura, gestión administrativa, entre otros.

El manejo relevante, ético y seguro de estos datos para cumplir los objetivos universitarios es fundamental. Bajo este contexto, las áreas universitarias deben:

a) Cumplir los objetivos universitarios y servicios que prestan, utilizando los datos de manera adecuada y de acuerdo con sus atribuciones;
b) Compartir los datos con otras áreas dentro del marco normativo, con la finalidad de coordinar acciones, prestar servicios eficaces y trabajar con información actualizada y confiable;
c) Cuidar la calidad de los datos que generan o recopilan y
d) Garantizar el almacenamiento confiable y seguro de los datos.

Al organizar, clasificar, contextualizar y procesar estos datos, las áreas universitarias generan información que les permiten brindar servicios y trámites, realizar la toma de decisiones a diferentes niveles, dar cumplimiento a los objetivos, metas y proyectos, entre otros fines de acuerdo con sus funciones y alineación con la planeación institucional.

La generación intensa de información, los cambios tecnológicos y las nuevas dinámicas de procesamiento y transmisión de información, impulsan directamente la necesidad de fortalecer los procedimientos de su almacenamiento actual, con la finalidad de que se conserve de forma segura y sea confiable considerando las dimensiones de integridad, seguridad y disponibilidad, cumpliendo con la normatividad vigente.

El presente documento es un marco de referencia para los colaboradores de las entidades académicas y dependencias administrativas universitarias, al respecto de procedimientos, planes y políticas de almacenamiento, conservación, recuperación y borrado de los datos como activo universitario fundamental.

Propósito

Las recomendaciones de almacenamiento incluidas en este documento están dirigidas a orientar las acciones de los involucrados de custodiar la información universitaria durante su ciclo de vida, mediante el fortalecimiento de los procesos y soluciones de almacenamiento. Estas prácticas sugeridas se consideran de valor para el personal con diferentes roles en las áreas universitarias y no se limita su aplicación a perfiles técnicos.

Marco legal o normativo

En México, el derecho a la información se encuentra regulado en la Constitución Política de los Estados Unidos Mexicanos. Para garantizar el ejercicio de este derecho, la Federación y las entidades federativas deben preservar sus documentos en archivos administrativos actualizados y publicarlos a través de los medios electrónicos disponibles.

El marco que regula la compartición de la información está regulado en leyes y códigos federales, así como lineamientos generales y recomendaciones universitarias, los cuales se presentan en la imagen siguiente:

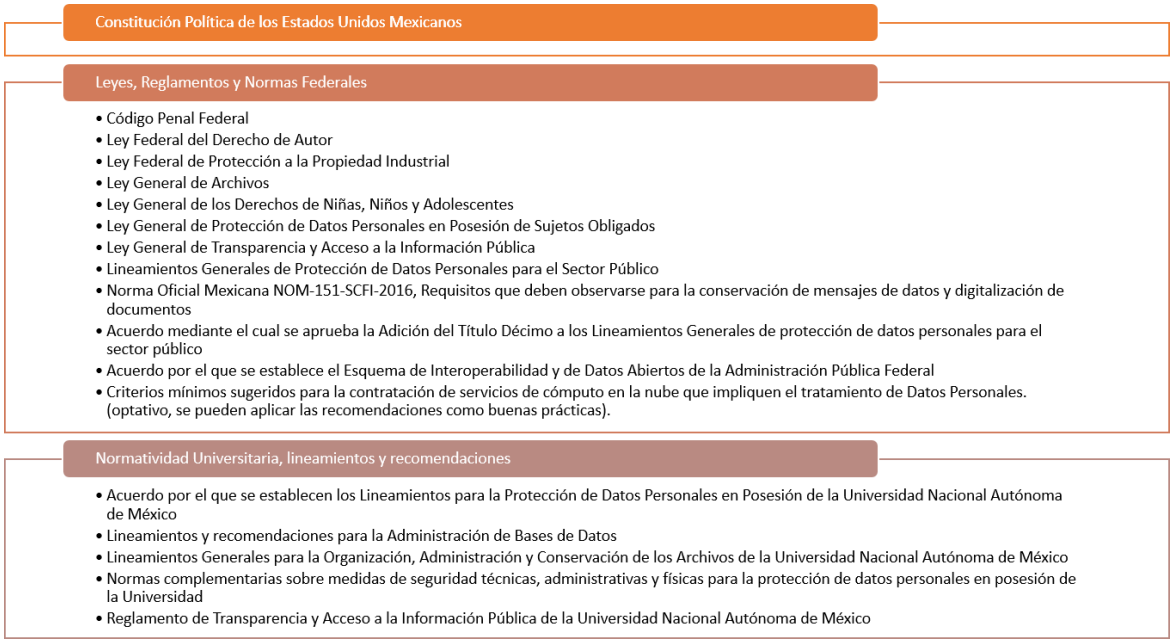

Figura 1. Marco regulatorio

Ciclo de vida de la información

Existen diversos modelos del ciclo de vida de la información. "La gestión del ciclo de vida de la información (ILM) supervisa y conserva los datos desde su creación hasta su destrucción. La gestión contribuye a optimizar el valor de los datos, reducir los costes de mantenimiento y rebajar riesgos de cumplimiento" (Talend, 2020). Para fines de este documento se abordarán las etapas descritas a continuación:

a) **Creación o recepción de la información.** En esta etapa se genera la información por diferentes medios como la captura, generación automatizada de un sistema, recibida por fuentes internas o externas. Se transforma en caso de ser necesario.
b) **Almacenamiento.** La información se guarda en algún medio electrónico para su protección. Aunque se refiere como una etapa independiente, generalmente el almacenamiento persistente ocurre de forma simultánea durante su creación.

c) **Uso y compartición.** La información puede utilizarse y compartirse dentro de una misma área, entre entidades y dependencias universitarias, con externos o de forma abierta a la sociedad. Ello dentro del marco normativo aplicable.
d) **Archivado.** Cuando la información almacenada deja de ser utilizada de forma frecuente, se le debe dar un tratamiento diferente y ubicarse en un medio de almacenamiento con otras características.
e) **Destrucción.** Los datos son eliminados permanentemente cuando la información existente ya no es útil y no es necesario conservarla de acuerdo con los plazos de conservación que estipula la legislación vigente. La imagen siguiente muestra las etapas descritas.

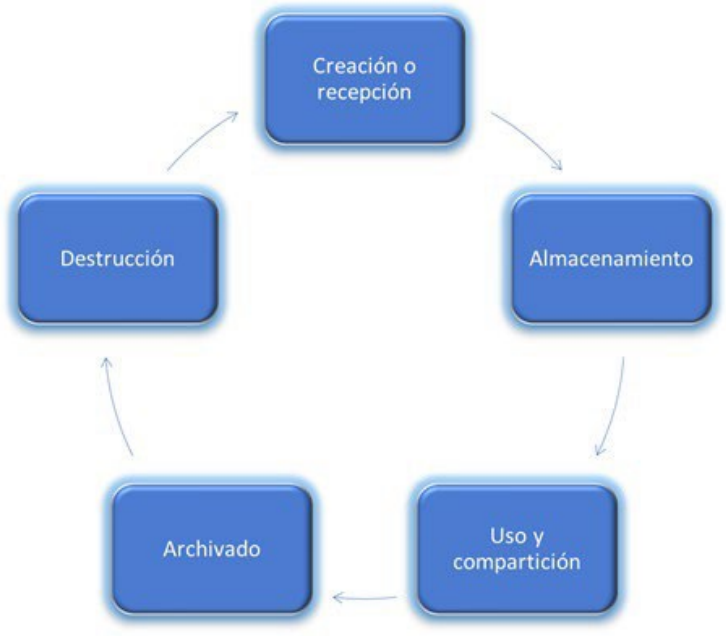

Figura 2. Ciclo de vida de la información

Recomendaciones para el almacenamiento

En la creación o recepción de la información

Consideraciones generales

La creación o recepción de la información es el punto primario dentro del procedimiento donde se obtienen los datos y en el cual es más relevante revisar los controles, mecanismos de verificación y confiabilidad de los mismos, entendiendo que a partir de ello se toman decisiones y se prestan servicios, por ejemplo:

- En la creación de información como pueden ser el registro de equipo de cómputo, la actualización de calificaciones de los alumnos, el registro de préstamo de un libro, entre otros.

- En la recepción de información entre entidades universitarias como lo es en la transferencia de información por medio de archivos de texto plano para validar el estatus de activo o inactivo de los alumnos.

También es fundamental identificar el propósito y fundamento con que se recaban estos datos, para cumplir con un adecuado manejo normativo de los mismos de acuerdo con las atribuciones del área universitaria.

Para diseñar los procedimientos de trabajo y realizar una correcta gestión de la información que se genera o recibe, se recomienda que el personal universitario analice diferentes criterios y escenarios para seleccionar la modalidad y configuración adecuada. Entre los aspectos a evaluar, se encuentran:

- El nivel de confidencialidad de la información.
- El nivel de criticidad de los servicios que utilizan los datos.
- Tipo de información que se desea almacenar.
- La confiabilidad de los datos.
- Frecuencia de uso.
- Volumen esperado de información inicial y estimación del crecimiento.
- Identificar quién accede a los datos y para qué.
- Identificar cómo se puede acceder a ellos.
- Formato de la información que será almacenada.
- Uso de estándares para el nombrado de los archivos, directorios y objetos usados para almacenar la información (por ejemplo, las tablas y tablespaces de las bases de datos).

Por ejemplo:
Denominación del activo de información: Datos personales de alumnos y trabajadores que pueden acceder a los servicios de la biblioteca.

Nivel de confidencialidad de la información	Confidencial (x) Restringida ( ) De uso interno ( ) Público ( )	**Nivel de criticidad**	Alto (x) Medio ( ) Bajo ( )
Confiabilidad de los datos	Alta (x) Media ( ) Baja ( )	**Frecuencia de uso**	Diaria (x) Semanal ( ) Mensual ( ) Semestral ( ) Esporádica ( )
Volumen esperado de información inicial	350,000	**Estimación de crecimiento**	100,000 registros nuevos al año.

Usuario de los datos	Usuario del sistema de préstamo de la biblioteca (alumno, trabajador, administrador del sistema).	**Uso de los datos**	Préstamos y devolución de material bibliotecario, multas y sanciones por retrasos, informes y estadísticas.
Tipo de acceso a los datos	Consulta directa en la base de datos y por medio del sistema de préstamo bibliotecario.	**Formato de la información almacenada**	Base de datos postgreSQL.
Estándares utilizados para el almacenamiento	Lineamientos de bases de datos.		

La relevancia de revisar estos elementos radica en que, por ejemplo:

- el tipo de información que se maneje podría determinar los mecanismos de seguridad a implementar,
- la criticidad podría cambiar los niveles de disponibilidad requeridos,
- la frecuencia podría cambiar la distribución del almacenamiento de los datos o el tipo de dispositivo para el almacenamiento de estos,
- la confiabilidad de los datos podría requerir implementar mecanismos de validación, confirmación o limpieza adicionales,
- el formato de la información cambiaría la configuración física o lógica del almacenamiento, por mencionar algunos casos,
- de acuerdo a las instituciones o uso interno de la información, se puede requerir carta de confidencialidad del personal o instituciones involucradas.

En el almacenamiento

Para almacenar la información se requiere de infraestructura y soluciones confiables y flexibles que permitan fortalecer su uso y protección de acuerdo con las necesidades de la Universidad.

Soluciones de almacenamiento

De acuerdo con las características, naturaleza y uso de los datos es conveniente seleccionar la alternativa más adecuada de almacenamiento. A continuación, se muestran consideraciones y recomendaciones sobre la utilización de los siguientes medios de almacenamiento:

Disco duro de equipo de cómputo (almacenamiento local en equipos de escritorio, equipos portátiles)

Características

La información se encuentra almacenada en los equipos de cómputo que utilizan los trabajadores universitarios para realizar sus actividades profesionales; es de fácil acceso de forma local y la actualización de los archivos es rápida debido a que se encuentran integrados dentro del equipo en el que están trabajando.

Usos recomendados

Es útil para almacenar documentos de trabajo usados por los colaboradores para realizar sus actividades profesionales. Se recomienda que se hagan copias de seguridad en medios de almacenamiento distintos al disco duro local para que, en caso de algún daño, no se pierda la información principal junto con el respaldo.

Recomendaciones

Debido a la variedad de información que se puede almacenar en estos equipos en cumplimiento a las funciones que realiza cada colaborador y área de trabajo en la UNAM, es recomendable establecer políticas que consideren:

- Tipo de información está permitido almacenar, por ejemplo: archivos de documentos de los proyectos en los que participe el trabajador, los archivos que sean necesarios para la realización de las actividades encomendadas al usuario del equipo de cómputo como videos, audios, archivos pdf, entre otros.
- Pautas para la generación de la estructura de directorios en los discos duros, por ejemplo:
  - Los directorios deben estar estructurados por año, dentro de cada año se debe crear un directorio para cada proyecto, por cada proyecto se deben crear subdirectorios de acuerdo a cada etapa del proyecto o fase del proceso, por ejemplo: análisis, diseño, desarrollo y pruebas.
  - Los archivos deben tener un prefijo relativo al proyecto al inicio del nombre, por ejemplo, del grupo de almacenamiento e información compartida, el prefijo podría ser aeic, guion bajo y el nombre del archivo relativo al contenido: aeic_calendario.pdf.
- Tiempo de conservación en estos medios de acuerdo con la naturaleza, utilidad y clasificación de la información, por ejemplo: deben permanecer almacenados durante la ejecución del proyecto.
- Mecanismos de protección a emplear, por ejemplo: uso de antivirus o anti malware, soluciones de protección de datos (cifrado de información, uso de un esquema de RAID, respaldos, entre otros), por mencionar algunos.
- Restricciones en la instalación de software y descarga de archivos que pudieran afectar a la información almacenada, por ejemplo: no se debe descargar software que no se tenga la licencia de uso, juegos, música, entre otros.

Servidores institucionales para almacén de datos

Características

La información se encuentra ubicada en servidores de almacenamiento, principalmente en red y ubicados en centros de datos universitarios. Permiten disponer de un lugar de almacenamiento

común protegido por controles de acceso y facilitan la tarea de compartir información entre los diferentes usuarios.

Usos recomendados

Se recomienda su uso para los siguientes casos:

- Se requiere compartir información entre varios usuarios.
- Como solución para generar un repositorio institucional o una base de conocimiento de la información generada de forma individual o grupal.
- Para que uno o varios colaboradores almacenen información para uso individual o grupal relevante para el trabajo que desempeñan.

Almacenamiento en la nube

Características

Los servicios de almacenamiento en la nube permiten guardar información en espacios virtualizados que pueden estar dentro de las instalaciones universitarias (nube privada) o en las instalaciones de un proveedor externo: Google, Amazon, MS Azure, entre otros (nube pública) o en un esquema combinado de los anteriores (nube híbrida).

Así mismo, ofrecen una solución flexible que pudiera escalarse y modificarse de manera elástica de acuerdo con las necesidades del usuario y las características de almacenamiento más conveniente, considerando la frecuencia de uso y tipo de datos que se manejen.

De acuerdo con el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el cómputo en la nube tiene 5 características esenciales presentadas en la imagen siguiente:

Figura 3. Cómputo en la nube

Usos recomendados

- De los elementos mencionados en la nube, el servicio que se sugiere para solventar la necesidad de almacenamiento de las entidades y dependencias universitarias, es la llamada Simple Service Storage, ya que permite extender la capacidad de almacenamiento de sus centros de datos.
- En el caso de una nube pública, este tipo de servicios contratados también son útiles para optimizar el uso de recursos humanos, evitar la compra de equipo, tercerizar la administración de las líneas de infraestructura del servicio, así como únicamente pagar por los recursos que se usan, lo cual es muy eficiente.

Cumplimiento normativo

Es importante considerar que solo está permitido el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información en sistemas que realicen el tratamiento automatizado. En el caso de los sistemas de información utilizados para el tratamiento automatizado de datos personales ya sea que estén alojados en equipos de la UNAM o en servicios de nube privada, deberán cumplir con lo establecido en los artículos 18 y 19 de las *Normas complementarias sobre medidas de seguridad, técnicas administrativas y físicas para la protección de datos personales en posesión de la Universidad*.

Formatos de Almacenamiento

Como término general se refiere al almacenamiento de datos en diversos volúmenes y que provienen de diferentes usos, los cuales pueden ser un respaldo de base de datos, un respaldo de aplicaciones, metadatos, máquinas virtuales completas, entre muchos otros.

Bases de datos

Esto permite aprovechar las características de los manejadores de bases de datos en el almacenamiento, actualización y uso de la información. La información se puede almacenar en bases de datos relacionales y/o NoSQL (con estructuras más flexibles y escalables), entre otras.

Consideraciones

Diseñar la base de datos de acuerdo con las necesidades determinadas durante el análisis y definir la estructura de almacenamiento (cómo almacenar los datos, en qué formatos) más adecuada.

Los manejadores de bases de datos tienen diferentes características que permiten organizar el almacenamiento de la información de forma física y lógica. Por ello, se recomienda que sean respaldadas mediante procedimientos propios de cada motor de base de datos (backup).

Por ejemplo, cuando se tienen grandes volúmenes de datos se pueden organizar tablas que tienen accesos frecuentes en *tablespaces* y archivos diferentes cuando el manejador de bases de datos lo permita.

Otros factores que se pueden tomar en cuenta en las decisiones de almacenamiento en bases de datos son:

- Frecuencia de modificaciones en los datos almacenados. Por ejemplo: diario.
- Frecuencia de cambios en el espacio de almacenamiento (aumento o disminución del volumen de datos). Por ejemplo: aumento mensual.
- Número de conexiones simultáneas. Por ejemplo: 50 usuarios conectados al mismo tiempo a un sistema.
- Número de transacciones SQL que utilizan espacio de almacenamiento temporal como ordenar, agrupar, entre otras. Por ejemplo: 10 transacciones por minuto.
- Particionado: "algunos mecanismos permiten que diferentes secciones de una misma tabla pueden ser almacenadas en diferentes porciones de disco". Por ejemplo: por año fiscal.
- Tamaño del bloque adecuado para el almacenamiento de los registros. Algunos manejadores de bases de datos permiten especificar el tamaño del bloque para que sea igual o superior al tamaño del bloque del sistema operativo. Por ejemplo: 8 KB para Postgres y Oracle.

Sistema de archivos

La información se puede almacenar en el sistema de archivos del dispositivo de almacenamiento, usando carpetas para organizar la estructura en donde se depositan, consultan, modifican y eliminan los archivos.

Consideraciones

Para seleccionar el tipo de solución de almacenamiento de archivos se sugiere considerar las características siguientes:

- El rendimiento requerido del medio de almacenamiento. Por ejemplo, el tiempo que toma una unidad de disco en responder a una petición completa de lectura/escritura.
- La disponibilidad del servicio de almacenamiento para garantizar el acceso a los datos. Por ejemplo: lunes a viernes de 7 am a 10 pm.
- La seguridad acerca de cómo se protegen los datos contra el acceso no autorizado. Por ejemplo: firewall del equipo de cómputo.
- El método de acceso acerca de cómo los clientes pueden acceder a los datos desde distintas ubicaciones. Por ejemplo: por conexión vía secure shell o sftp.
- Establecer pautas en el área universitaria para la creación de particiones, árbol de directorios, nombrado de archivos para facilitar su búsqueda y control. Por ejemplo: establecer particiones para diferentes rangos de folios para agilizar las búsquedas.
- El ancho de banda y la latencia, en caso de que el medio de almacenamiento se acceda por red. Por ejemplo: El tiempo total que transcurre desde que se envía la información, hasta que la misma llega al receptor.

Respaldo de información

Es un medio de mantener la disponibilidad de la información ante una eventualidad o fallo humano y evitar su pérdida, permitiendo que sea utilizada por los usuarios cuando sea requerida a través de los servicios tecnológicos universitarios.

En este sentido se recomienda realizar las siguientes acciones:

1. **Identificar información a respaldar**. Es importante identificar y clasificar la información que por su nivel de importancia requiera ser respaldada. Por ejemplo: base de datos del sistema de registro de becarios.
2. **Determinar el tipo de respaldo y la frecuencia con que se realizará**. Se recomienda identificar qué tanto cambia la información en un período de tiempo o la cantidad de información que se puede perder con respecto a la fuente original, para realizar un respaldo completo de la misma y definir respaldos parciales (incrementales) o diferenciales en el tiempo que cambie. Por ejemplo: cada mes aumenta el volumen de información en 10,000 registros y se modifica el 10 por ciento de la información actual por lo que se puede hacer un respaldo completo mensualmente y diferencial cada semana.

   Para ello se tiene que determinar:

   - **Punto objetivo de recuperación**. Consiste en definir la pérdida de datos que se puede aceptar, es decir, el intervalo de tiempo entre dos copias de seguridad. Por ejemplo: una semana.
   - **Tiempo objetivo de recuperación**. Consiste en definir cuánto tiempo puede pasar antes de una recuperación completa de los datos, es decir, en cuánto tiempo se recuperará la copia de seguridad de los datos. Por ejemplo: 2 horas.

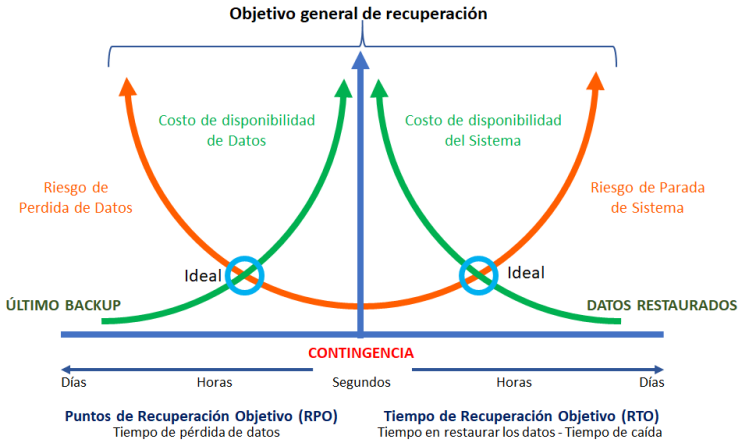

Figura 4. Diagrama de evaluación de Costo/Riesgo en la recuperación de datos.

3. **Seleccionar el medio de almacenamiento**. Se debe tener en cuenta con qué frecuencia es accedida la información o si se requiere tenerla disponible por cuestiones normativas. Por ejemplo: los registros del sistema de préstamos de tabletas se almacenan en la base de datos y las cartas responsivas se almacenan en el sistema de archivos del servidor.
4. **Verificar los respaldos realizados.** Es importante revisar que la información del respaldo puede recuperarse sin problemas. Así mismo, deben verificarse al menos cada 6 meses para validar que los medios y la información resguardada se encuentren en buenas condiciones.

Se sugiere tener más de una única copia de los datos, ya que los medios en los que se encuentren, son susceptibles a daños ambientales y físicos, por lo que se deben mantener alejados de altas temperaturas, polvo, luz solar y humedad.

En este punto es importante contar con una política interna adecuada para que dichos respaldos estén resguardados de manera segura, sin que exista dependencia de una persona única para poder recuperar y, en su caso, restaurar esta información. En este punto, por ejemplo, se pueden sellar sobres de papel con las llaves o claves para acceder a dicho recurso y documentar en qué casos y por cuáles personas se puede abrir este paquete.

Algunas buenas prácticas para el manejo de respaldos son:

- Mantener 3 copias de cualquier archivo importante (1 primario y 2 copias de seguridad).
- Mantener los archivos en 2 tipos de medios o métodos de almacenamiento diferentes para protegerlos contra diferentes tipos de peligros.
- Almacenar 1 copia fuera de sitio.

Una práctica recomendada es realizar un informe diario de las copias de seguridad que se hayan enviado fuera y de las que hayan caducado, destruyendo aquellas que ya no son necesarias.

A continuación, se exponen el tiempo de vida de algunos medios de almacenamiento de información, que bajo condiciones ideales pueden durar:

- Cintas magnéticas alrededor de 25 años, si bien depende del número de reproducciones.
- Discos ópticos según algunos fabricantes, hasta 50 años.
- Discos duros se deterioran antes de 10 años, con un tiempo medio entre fallos de 2 a 9 años.
- Memorias electrónicas alrededor de unos 10 años.

De igual manera, se debe considerar la obsolescencia del formato y del software o del hardware para reproducirlo, dentro de las consideraciones para actualizar los respaldos de la información a nuevos formatos, medios de almacenamiento o aplicaciones.

Por último, aun cuando la tecnología RAID protege contra errores de hardware, no lo hace contra errores de software, por lo que se recomienda hacer copias de seguridad regulares cuando se utiliza un esquema de RAID en los sistemas de almacenamiento. Por ejemplo, aunque se haga uso de RAID 1+0 en bases de datos puede suceder una falla en la controladora o en el software de RAID por lo que es recomendable tener respaldos.

Algunas métricas útiles para la administración de los respaldos de los datos son:

- Frecuencia de las pruebas de los medios de respaldo. Por ejemplo: semanal.
- Tiempo promedio del tiempo de restauración de datos. Por ejemplo: 50 minutos.
- % de restauraciones exitosas. Por ejemplo: 95%.

Por parte de las áreas universitarias, deben existir procedimientos operativos estándar documentados para garantizar que se lleven a cabo estas medidas, a través de un Plan de almacenamiento y protección de respaldos.

Plan de respaldos

Se aconseja contar de manera documentada formal y actualizada con un plan de respaldo de datos en donde se especifique:

- el proceso general de respaldo,
- qué información se respalda. Por ejemplo: base de datos personales de los trabajadores,
- qué tecnologías y recursos de almacenamiento se utilizan. Por ejemplo: MySQL 8.0, sistema de archivos con las fotografías de los trabajadores,
- qué pasos se toman si los datos no se respaldan con éxito. Por ejemplo: Recuperar el respaldo previo y notificar al responsable de la información,
- además de otros elementos como probar los procedimientos de respaldo.

Al terminar de definir el plan de respaldos se debe revisar con las áreas dueñas o responsables de la información, además de buscar la validación y apoyo de la alta dirección de la entidad o dependencia.

En el uso y compartición

Durante el uso y la compartición de la información puede ser necesario enviarla desde su almacenamiento a otra ubicación utilizando medios físicos o lógicos, por lo que, de acuerdo con su naturaleza, es decir, si son datos personales o sensibles, deben de considerarse medidas de protección, a continuación, se mencionan algunas:

Transporte físico

Hay situaciones en las que se requiere transportar información de manera física, por lo que en estos escenarios dependiendo de la cantidad de datos, es necesario considerar algunos estándares para el medio, las cuales pueden ser el Ingress Protection 68 (IP68) o la certificación militar MIL-STD-810G, referentes a la protección contra polvo, humedad y golpes. Además, se debe proteger el dispositivo contra descargas eléctricas donde se va a conectar y de bloquear la escritura.

Transporte lógico

En situaciones donde sea necesario transferir información a través de la red, algunas buenas prácticas incluyen el uso de canales cifrados, los cuales se pueden obtener mediante conexiones SSL (Secure Sockets Layer o capa de conexión segura), HTTPS (HyperText Transfer Protocol Secure, Protocolo de transferencia de hipertexto) o bien haciendo uso de Redes Privadas Virtuales (VPN) y si la información lo amerita, el archivo también debe ir cifrado en caso de ser susceptible de ataques de hombre en medio o fuga de información.

Para el archivado

Una vez que la información ya no necesita ser consultada de manera frecuente o que es considerada histórica, suelen dársele otras consideraciones para su manejo en el almacenamiento, acorde a su tipo, clasificación y la normatividad que aplique. A continuación, se dan algunas recomendaciones para su manejo.

Conservación de la información almacenada

La información almacenada en las entidades y dependencias universitarias necesita conservarse durante los plazos estipulados en la normatividad vigente antes de poder ser destruida. A continuación, se mencionan algunos casos a considerar.

- De acuerdo con el artículo 30 del Código Fiscal de la Federación (CFF), el plazo general es de cinco años respecto a la documentación comprobatoria de los registros o asientos que integran la contabilidad, información que deberá estar disponible en el domicilio fiscal del contribuyente, y en el caso de pérdidas fiscales el plazo podría ampliarse a 15 años o más.
- En el caso de aquellas actividades que se encuentran previstas en el art. 75 del Código de Comercio, tales como: firma de seguros de cualquier especie, expedición o cobro de cheques o letras de cambio, ejecución de operaciones de títulos de crédito, por mencionar algunas, se deberán conservar por un plazo de 10 años, los originales de los documentos que dieron origen al nacimiento de derechos y obligaciones, de conformidad con lo señalado en el art. 49 de la misma ley referida en el presente párrafo.
- En el caso de datos históricos confidenciales se conservan con ese carácter por un plazo de 30 años y, de 70 años en caso de contener datos personales que afecten a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este.
- En el caso de la información generada por las entidades y dependencias universitarias, los plazos de conservación estarán definidos por el periodo de guarda de la documentación en los archivos de trámite, de concentración e histórico, según sea el caso, es decir, consistirá en la combinación de la vigencia documental, el término precautorio, así como el periodo de reserva, de acuerdo con lo señalado en el documento "*Instrumentos de Control y Consulta Archivística de la Universidad Nacional Autónoma de México 2021*"[1].

Los elementos clave en relación con la conservación de los soportes son la accesibilidad, la legibilidad, la perdurabilidad y la preservación de la autenticidad. Se debe almacenar la información en un soporte normalizado y perdurable, el que sea más adecuado a las necesidades de conservación a corto, mediano o largo plazo.

Destrucción

Cuando la información ya no es necesaria o el medio de almacenamiento se daña o se vuelve obsoleto, es necesario tomar una decisión respecto a lo que se va a hacer, que en su caso puede

[1] http://www.transparencia.unam.mx/documentos_transparencia/Instrumentos_Archivisticos_2021.pdf.

ser eliminar la información o reemplazar el medio. Para lo cual se debe seguir considerando la naturaleza de la información y las disposiciones normativas que sigan aplicando a la misma.

Borrado seguro

Es importante indicar que, para la eliminación de datos personales, los sistemas de información que den tratamiento automatizado aplicarán el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos, de acuerdo con lo señalado en el artículo 20 relativo de las *Normas complementarias sobre medidas de seguridad, técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.*

Todo equipo de cómputo (computadoras, servidores, sistemas de almacenamiento) que contenga medios de almacenamiento debería revisarse para asegurar que todos los datos sensibles o confidenciales, se hayan removido o se haya sobrescrito con seguridad para evitar que sea recuperada y pueda caer en manos de terceros.

Los dispositivos de almacenamiento dañados que contengan datos sensibles pueden requerir una evaluación de riesgo para determinar si estos deberían destruirse físicamente, antes que ser enviados para su desecho. La información puede verse comprometida si la reutilización o eliminación de los equipos se realiza de manera descuidada.

Para la información sensible o confidencial que ya no se requiere tener almacenada, es importante escoger un procedimiento que garantice que no podrá ser recuperada por otra persona, para ello se utiliza un método de borrado seguro, que consiste en sobrescribir los datos siguiendo un patrón de borrado y realizar diversos ciclos (pasadas) de escritura que no permita su recuperación de modo alguno. Para ello se puede hacer uso de herramientas de borrado seguro.

Algunas herramientas de borrado seguro son:

Windows

- SDelete
- Hddguru (Wipe My Disks)

Linux

- srm
- wipe

MacOS

- Permanent eraser
- Disk Utility

Consideraciones generales de seguridad en el almacenamiento

Un aspecto importante para definir la seguridad de la información dentro de un área universitaria es que conozca qué archivos, bases de datos y columnas se consideran suficientemente confidenciales por las unidades de negocio y saber dónde se encuentran los datos.

Para identificar los datos que requieren ser protegidos se pueden analizar aquellos cuya pérdida afectaría a la continuidad de servicios institucionales o que son la razón de ser del área universitaria.

De igual forma, para determinar la protección necesaria de la información se recomienda analizar las siguientes preguntas:

- Capa física— ¿Cómo y dónde se almacena físicamente la información? Por ejemplo: la información se encuentra en el servidor servidor_beta.
- Capa empírica— ¿Cuáles son los canales de acceso a la información? Por ejemplo: acceso local en el servidor y acceso por VPN.
- Capa sintáctica— ¿Cuáles son los requisitos de retención? ¿La información es histórica u operacional? Por ejemplo: La información es operacional.

Algunos riesgos comunes en el manejo de datos son:

- Corrupción o alteración de datos, ya sea de forma accidental o maliciosa.
- Pérdida o robo de una parte o la totalidad de los datos.
- Falta de acuerdos de confidencialidad y la poca o nula aplicación de las leyes de protección de datos.
- Liberación prematura de datos.

Es por ello que se deben evaluar los riesgos a los que puede estar sometidos los datos a cargo de un área universitaria, por lo que tienen que definirse e implementarse algunas medidas y controles para la protección de la información almacenada, como pueden ser:

- Mantener la completitud, exactitud, validez y accesibilidad de los datos almacenados.
- Monitorear actividades clave de la administración de datos como son: respaldos, recuperación y eliminación.
- Realizar el almacenamiento seguro de la información que se deba conservar y de los registros de actividad como garantía del cumplimiento legal o normativo que aplique.
- Cifrar información crítica en tránsito o en almacenamiento.
- Destruir de manera segura la información una vez terminada su vida útil.
- Asegurar que los sistemas de almacenamiento pueden resistir y recuperarse de fallas originadas por un error, ataque deliberado o desastre (Plan de continuidad).
- Realizar copias de seguridad definiendo la vigencia de la misma y planes de recuperación.
- Almacenar las copias en sitios cerrados seguros, en una ubicación distinta del original para poder restaurar la información en caso de desastre.
- Restringir el acceso a las ubicaciones donde se encuentran las copias de seguridad exclusivamente a las personas autorizadas.

- Controlar la obsolescencia de los dispositivos de almacenamiento sobre todo para información histórica o que por normatividad se tenga que mantener durante un largo período.
- Controlar el uso de almacenamiento y servicios en la nube, evaluando los acuerdos periódicamente, al menos una vez por año, respecto a la seguridad y al cumplimiento normativo.
- Hacer uso de antivirus, antimalware y otro software de protección en los equipos que almacenan la información o bien los equipos donde se monta o accede a la información.

Anexos

Anexo I. Términos y definiciones

Almacenar información. Para efectos de este documento, entenderemos almacenar información como el acto de guardar información de forma ordenada, para poder disponer de ella cuando se requiera. Bajo este contexto, cualquier información que la Universidad resguarde para ser usada o compartida entre los sistemas universitarios.

Almacenamiento de información en formato electrónico. Cuando se encuentra en archivos electrónicos, bases de datos o almacenes de datos.

CD (Compact Disc). "soporte digital óptico de almacenamiento de información con una capacidad de 80 minutos de audio o 700 MB de datos" (Chicano, 2013:22).

Cinta magnética: soporte de almacenamiento de datos prácticamente obsoleto que se utiliza en la actualidad como respaldo de archivos" (Chicano, 2013:22).

Disco duro (hard disc -HD). "periférico no volátil encargado de almacenar la información de modo permanente en un ordenador. Utiliza un sistema de grabación magnético para almacenar datos digitales, y está compuesto por uno o varios discos rígidos unidos por un eje que gira a gran velocidad dentro de una carcasa. Sobre cada uno de los discos se encuentra un cabezal encargado de la lectura/escritura de los impulsos magnéticos" (Chicano, 2013:22)"

Disco duro removible. "disco duro que se conecta al ordenador mediante un puerto USB.

DVD (Disco Versátil Digital, Digital Versatile Disc). "surge en 1995 y se utiliza en un principio como reemplazo de la cinta de vídeo VHS. Hay distintas versiones según su capacidad de almacenamiento y funcionalidades: DVD-ROM (para solo lectura), DVD-R y DVD+R (solo puede escribirse una vez en ellos) y DVD-RW y DVD+RW (permiten grabación y eliminación de datos)" (Chicano, 2013:22).

Pérdida de información. Cuando se altera alguno de sus atributos de integridad, disponibilidad y confidencialidad y, específicamente en el proceso del almacenamiento, la disponibilidad es el atributo más crítico.

Bibliografía y referencias electrónicas

- ADATA (2021). **Explicación de las clasificaciones de protección IP**. Recuperado: 28 de junio de 2021. URL: https://corp.adata.com/mx/support/quiktips/ip- protection-rating-explained
- Amazon (2021). **Almacenamiento de objetos creado para almacenar y recuperar cualquier volumen de datos desde cualquier ubicación**. Recuperado: 28 de junio de 2021. URL: https://aws.amazon.com/es/s3/#:~:text=Almacenamiento%20de%20objetos%20creado%20para,de%20datos%20desde%20cualquier%20ubicaci%C3%B3n&text=Amazon%20Simple%20Storage%20Service%20(Amazon,rendimiento%20l%C3%ADderes%20en%20el%20sector.
- Cámara de Diputados (2015). **Ley General de Transparencia y Acceso a la Información Pública**. Recuperado: 9 de septiembre de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lgtaip.htm
- Cámara de Diputados (2017). **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados** Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lgpdppso.htm
- Cámara de Diputados (2018). **Código de Comercio**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/ccom.htm
- Cámara de Diputados (2018). **Ley General de Archivos**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lga.htm
- Cámara de Diputados (2020). **Ley Federal del Derecho de Autor**. Recuperado: el 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lfda.htm
- Cámara de Diputados (2020). **Ley Federal de Protección a la Propiedad Industrial**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lfppi.htm
- Cámara de Diputados (2021). **Código Fiscal de la Federación**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/cff.htm
- Cámara de Diputados (2021). **Código Penal Federal**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/cpf.htm
- CEPAL (2020). **Gestión de datos de investigación**. Biblioguías – Biblioteca de la CEPAL. Recuperado: 28 de junio de 2021. URL: https://biblioguias.cepal.org/c.php?g=495473&p=4396791
- Conferencia de Archiveros de Universidades Españolas (2007). **La gestión de documentos electrónicos: recomendaciones y buenas prácticas para las Universidades**. Recuperado: 22 de junio de 2021. URL: http://cau.crue.org/wp-content/uploads/recomendacionescau2007_gtdoc.e.pdf
- Chicano, E (2013). **Utilización de las bases de datos relacionales en el sistema de gestión y almacenamiento de datos: UF0348**, IC Editorial, 2013.

- Diario Oficial de la Federación (2016). **Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos**. Recuperado: 28 de junio de 2021. URL: http://www.dof.gob.mx/normasOficiales/6499/seeco11_C/seeco11_C.html
- Diario Oficial de la Federación (2017). **Lineamientos Generales de Protección de Datos Personales para el Sector Público**. Recuperado: 05 de abril de 2022. URL: http://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018
- El español (2019). **Qué es la certificación militar MIL-STD-810G y qué implica para tu móvil**. Recuperado: 28 de junio de 2021. URL: https://www.elespanol.com/elandroidelibre/tutoriales/20190623/certificacion- militar-mil-std-implica-movil/408459877_0.html
- INAI (2018). **Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales**. Recuperado: 05 de abril de 2022. URL: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/ComputoEnLaNube.pdf
- INAI (2020). **Acuerdo mediante el cual se aprueba la Adición del Título Décimo a los Lineamientos Generales de protección de datos personales para el sector público**. Recuperado: 05 de abril de 2022. URL: https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.05.pdf
- Instituto Nacional de Ciberseguridad (2016). **Guía de almacenamiento seguro de la información**. Recuperado: 05 de abril de 2022. URL: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad.pdf
- Oracle (2020). **Más información sobre la migración de datos de aplicación a la nube**. Recuperado: 05 de abril de 2022. URL: https://docs.oracle.com/es/solutions/learn-migrate-app-data-to-cloud/index.html
- Talend (2020). **El impacto del RGPD en la gestión del ciclo de vida de la información**. Recuperado: 25 de junio de 2021. URL: https://www.talend.com/es/resources/gdpr-govern-lifecycle-information/
- UNAM (2016). **Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de Méxic**o. Recuperado: 9 de septiembre de 2021. URL: http://www.transparencia.unam.mx/files/documentos/reglamento_transparencia_2016.pdf
- UNAM (2017). **Lineamientos y recomendaciones para la Administración de Bases de Datos**. Recuperado: 28 de junio de 2021. URL: https://www.red-tic.unam.mx/node/74
- UNAM (2018). **Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México**. Recuperado: 28 de junio de 2021. URL: https://www.red-tic.unam.mx/recursos/LineamientosArchivosUNAM.pdf
- UNAM (2019). **Acuerdo por el que se establecen los Lineamientos para la**

Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México. Recuperado: 9 de septiembre de 2021. URL: https://www.gaceta.unam.mx/index/wp-content/uploads/2019/02/190225-convocatorias.pdf

- UNAM (2020). **Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad**. Recuperado: 28 de junio de 2021. URL: https://www.gaceta.unam.mx/wp-content/uploads/2020/01/200130- convocatorias.pdf
- Wikipedia (2021). **Mecanismos de almacenamiento (MySQL)**. Recuperado: 28 de junio de 2021. URL: https://es.wikipedia.org/wiki/Mecanismos_de_almacenamiento_(MySQL)

Créditos

Rector
Dr. Enrique Luis Graue Wiechers

Secretaria de Desarrollo Institucional
Dra. Patricia Dolores Dávila Aranda

Director General de Cómputo y de Tecnologías de Información y Comunicación
Dr. Héctor Benítez Pérez

Coordinación
MATIE. Alberto González Guízar
Mtra. Irene Sánchez García

Elaboración
José Othoniel Chamú Arias - DGTIC
Susana Laura Corona Correa - DGTIC
José Luis Chávez Sánchez- DGTIC
Alberto González Guízar- DGTIC

Revisión

Fernando Israel González Trejo - FES Acatlán
Miguel Ángel Jiménez Bernal - DGBSDI
Leticia Martínez Calixto - DGTIC
Ana Pérez Arteaga - IIMAS
Hugo Alonso Reyes Herrera - DGTIC

Autorización de publicación en sitio de la RedTIC

Dra. Marcela Peñaloza Báez