RED·TIC
Red de Responsables TIC
U N A M

LINEAMIENTOS GENERALES Y POLÍTICAS SOBRE ALMACENAMIENTO E INFORMACIÓN COMPARTIDA ENTRE LOS SISTEMAS EXISTENTES

Tercera versión

Junio de 2023

Índice

Lineamientos generales y políticas sobre almacenamiento e información compartida entre los sistemas existentes

Objetivo

Proporcionar elementos de referencia para aplicar buenas prácticas que favorezcan el correcto uso y aprovechamiento institucional de la información, así como el almacenamiento confiable de los datos en las áreas universitarias, con la finalidad de coordinar acciones exitosas para ofrecer servicios eficaces que operen con información actualizada, bajo un marco de disponibilidad y calidad de los datos.

Alcance

Los presentes lineamientos están dirigidos al personal universitario que interviene en el proceso de almacenamiento, compartición, transformación, uso y explotación de la información y a quienes están a cargo de sistemas de información, con la finalidad de orientar los procedimientos para compartir e intercambiar información, mediante criterios que apoyen la toma de decisiones y acciones al respecto.

Términos y definiciones

Acuerdo de Nivel de Servicio (Service Level Agreement, SLA). Acuerdo documentado entre el proveedor de servicios y el cliente que identifica los servicios y los objetivos de los mismos.

Almacenar información. Es el acto de guardar información de forma ordenada, mediante el uso de servicios o dispositivos de almacenamiento de confianza, para disponer de ella cuando sea necesario.

Área responsable de la información. Es el área universitaria que tiene bajo su resguardo información obtenida o generada en la Universidad, y que es utilizada en los procesos o sistemas universitarios.

Áreas Universitarias. Las Autoridades Universitarias, Cuerpos Colegiados, Dependencias Administrativas, Entidades Académicas, Tribunal Universitario y Defensoría de los Derechos Universitarios (http://www.transparencia.unam.mx/glosario.html).

Bóveda digital UNAM. Plataforma para el resguardo de información digital, con propósitos de preservación a largo plazo y fuera de línea en el Centro de Datos de la DGTIC, para uso de carácter institucional en cumplimiento de los objetivos de las entidades y dependencias universitarias.

Calidad de datos. Se refiere al grado de cumplimiento de las necesidades de los usuarios respecto a las características de disponibilidad, portabilidad, recuperabilidad, accesibilidad, conformidad, confidencialidad, eficiencia, precisión, trazabilidad, exactitud, completitud, consistencia, credibilidad y vigencia, de acuerdo con la norma ISO/IEC 25012:2008.

Compartir información. Acción mediante la cual un sistema proporciona datos a otro, de acuerdo con los criterios y mecanismos establecidos para ello, con la finalidad de dar cumplimiento a un objetivo institucional.

Confiabilidad. Nivel de certeza de que un proceso o función, entre otros, responde de la forma planeada de acuerdo con una línea base medida.

Confidencialidad. Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados (Glosario ISO 27001:2013).

Dato. Unidad mínima de información (números, letras o símbolos) que representa un objeto, condición o situación y que requiere una interpretación para convertirse en información.

Datos personales. Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier dato. La información académica que existe en los archivos universitarios constituye un dato personal (http://www.transparencia.unam.mx/glosario.html)

Derechos ARCO. Se refiere a aquel derecho que tiene un titular de datos personales para solicitar el acceso, rectificación, cancelación u oposición sobre el tratamiento de sus datos, ante el sujeto obligado que esté en posesión de los mismos.

Disponibilidad de la información. Propiedad de estar accesible y utilizable cuando lo requiera una entidad autorizada (Glosario ISO 27001:2013).

Documentos de archivo. Es aquel que registra un hecho, acto administrativo, legal, fiscal o contable, generado, recibido, obtenido, adquirido, procesado y conservado en el ejercicio de las facultades, funciones o competencias del área universitaria, en cualquier época y con independencia de su soporte.

Filtración de datos. Compromiso de seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal a datos protegidos transmitidos, almacenados o procesados de otra manera.

Fuente primaria de datos autoritativa. Es el área universitaria de la cual se obtiene información confiable para otros usos, como emisión de informes o prestación de servicios universitarios. Es responsable de actualizar y validar la informació a partir de los datos que la misma *área genera o que obtiene e integra a partir de fuentes de datos autónomas*.

Hash. Algoritmo matemático que genera una cadena alfanumérica de resumen seguro de un documento, volumen o dispositivo de almacenamiento, tiene una longitud fija cuyo valor es único.

Información. La contenida en uno o varios documentos físicos o electrónicos que la universidad genere, reciba, obtenga, adquiera, procese o conserve en ejercicio de sus facultades, funciones y competencias. Ésta puede ser pública, reservada o confidencial.

Integridad. Es el principio de seguridad de la información consistente en garantizar la exactitud y la completitud de la información y los sistemas, de manera que estos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

IPSec. Es un estándar y conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet autenticando y/o cifrando cada paquete IP en un flujo de datos.

Metadatos (archivo). El conjunto de datos que describe el contexto, contenido y estructura de los documentos de archivos y su administración, a través del tiempo, y que sirven para identificarlos, facilitar su búsqueda, recuperación, administración y controlar su acceso.

Neutralidad tecnológica. Se refiere a elegir la alternativa tecnológica más adecuada a las necesidades de las dependencias y entidades universitarias, con el propósito de no excluir, restringir, condicionar o favorecer alguna tecnología o modelo de negocio informático en particular.

Portabilidad. Conjunto de características que permite el uso de algún elemento o componente en una plataforma distinta a la cual lo generó, sin requerir alguna modificación o inversión considerable.

Portabilidad de datos. Capacidad para transferir fácilmente datos de un sistema a otro sin necesidad de ingresarlos nuevamente.

Privacidad desde el diseño. Implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso).

Red Privada Virtual (Virtual Private Network, VPN). Es una conexión segura y cifrada entre dos redes o entre un usuario determinado y una red.

Responsable de seguridad de datos personales. Encargado de las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales. Es designado por cada Área Universitaria.

Seguridad en el almacenamiento. Aplicación de controles físicos, técnicos y administrativos para proteger los sistemas e infraestructura de almacenamiento, así como los datos almacenados en ellos.

Servicios de nube privada. En el contexto de la UNAM, es el modelo de servicio de tecnología de información proporcionado bajo demanda a las áreas universitarias, en infraestructura propiedad de esta universidad y que ofrece diversas plataformas para brindar servicios, contar con espacio de almacenamiento o procesamiento, entre otros.

Servicios de nube pública. Modelo de servicio de tecnología de información adquirida a terceros y bajo demanda, operada en una infraestructura ajena a la universidad.

Silo de datos. Colección de información aislada de una entidad o dependencia universitaria e inaccesible para otras áreas de la universidad.

Secure Sockets Layer (SSL) / Transport Layer Security (TLS). "Es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet. Recientemente ha sido sustituido por TLS el cual está basado en SSL y son totalmente compatibles" (Odín, 2011).

Túnel punto a punto. Técnica para crear un camino lógico por los que se transmiten paquetes encapsulados de manera cifrada y segura entre dos puntos de una red.

Marco legal aplicable

Las leyes, reglamentos y normas aplicables al tratamiento de datos e información deben ser identificados y tomados en cuenta para que estas actividades se lleven a cabo dentro de un marco de legalidad. Durante el ciclo de vida de la información se debe observar en cada etapa la normatividad que aplique según el caso. Por ejemplo, en materia de derechos de autor -lo referente a la regulación de los derechos patrimoniales de los programas desarrollados, en materia de transparencia y acceso a la información- y la protección de datos personales, entre otros.

A continuación se indican las normas que es necesario contemplar.

- Leyes, reglamentos y normas federales
  - Código Penal Federal
  - Ley Federal del Derecho de Autor
  - Ley Federal de Protección a la Propiedad Industrial
  - Ley General de Archivos
  - Ley General de los Derechos de Niñas, Niños y Adolescentes
  - Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
  - Ley General de Transparencia y Acceso a la Información Pública
  - Lineamientos Generales de Protección de Datos Personales para el Sector Público
  - Norma Oficial Mexicana NOM-151-SCFI-2016. Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos
  - Acuerdo mediante el cual se aprueba la Adición del Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público
  - Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales
  - Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.
- Normatividad universitaria, lineamientos y recomendaciones
  - Acuerdo por el que se establecen los lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México
  - Lineamientos y recomendaciones para la Administración de Bases de Datos
  - Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México
  - Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México
  - Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad
  - Anexo de las Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad
  - Catálogo de disposición documental
  - Reglamento de Responsabilidades Administrativas de las y los Funcionarios y Empleados de la Universidad Nacional Autónoma de México

Responsabilidades en relación a estos lineamientos

a) De los titulares de las entidades o dependencias universitarias

- Comunicar, difundir y concientizar respecto a la aplicación de estos lineamientos y políticas dentro de su área universitaria.
- Impulsar acuerdos institucionales que favorezcan el aprovechamiento de los datos universitarios para generar más y mejores servicios a la comunidad bajo el marco legal

referido.

- Verificar que en sus áreas universitarias se realice la protección de los datos personales conforme a la normatividad universitaria.
- Designar un responsable de seguridad de datos personales que tenga bajo su custodia la información del área universitaria.
- Impulsar la implementación y mejora en el grado de cumplimiento de las buenas prácticas de seguridad de la información en el área universitaria.
- Verificar que se encuentre establecida la cadena de responsabilidad del personal universitario que interviene en la recepción, almacenamiento, intercambio, difusión, transformación, uso y explotación de la información, para garantizar la seguridad de la información.
- Verificar que se establezca en el área universitaria la clasificación de la información (pública, confidencial, reservada, etc.), de acuerdo con la normatividad aplicable, así como al tipo de información a la que da tratamiento su entidad o dependencia.
- Designar un responsable de seguridad de datos personales que tenga bajo su custodia la información del área universitaria, de conformidad con lo establecido en el artículo quinto transitorio del "Acuerdo por el que se establecen los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México".

b) De los responsables de las Tecnologías de Información y Comunicación (TIC)

- Participar de manera proactiva en actividades de compartición de información en cumplimiento de sus funciones de gestión y operación de las TIC; así como coordinar efectivamente la realización de estas actividades tanto al interior de su entidad o dependencia como en colaboración con otras áreas universitarias.
- Identificar los activos de información de su entidad o dependencia, categorizarlos adecuadamente y establecer los mecanismos para su almacenamiento correcto en términos de resguardo, disponibilidad, integridad, recuperación y confiabilidad.
- Promover el intercambio de información a través de servicios que puedan consumirse por otros sistemas de información.
- Documentar y dar seguimiento a los procedimientos establecidos y de mejora en el marco de aplicación de las presentes políticas.
- Establecer los procedimientos y mecanismos necesarios para coadyuvar o efectuar la preservación digital de aquellos activos de información que su área universitaria identifique como necesarios a largo plazo, así como los metadatos necesarios para su localización y/o recuperación.
- Verificar periódicamente, en conjunto con el responsable de seguridad de datos personales asignado, el cumplimiento de las buenas prácticas de seguridad de la información e implementar mejoras internas que garanticen la seguridad de la información en el área universitaria.

c) Del personal de las TIC y personal universitario que hace uso de la información universitaria

- Contribuir a la aplicación de estos lineamientos generales y políticas en sus actividades asignadas.
- Observar la normatividad universitaria en materia de protección de datos personales.
- Plantear a los responsables TIC sus propuestas de mejora respecto al almacenamiento de datos y las oportunidades para mejorar la gestión y aprovechamiento de la información, de acuerdo con su clasificación (pública, confidencial y/o sensible).

Capítulo I. Lineamientos. Disposiciones generales

1. Sobre la información

1.1. Fomentar que la información publicada por la UNAM cumpla con los atributos de calidad: accesibilidad, confiabilidad, gratuidad, igualdad, no discriminación, oportunidad, integridad, prontitud, simplicidad, veracidad y verificabilidad. Estas características deben tenerse presentes desde el momento de creación de la información hasta su actualización o disposición final.

1.2. La información, como activo de la universidad, debe estar disponible en el momento que sea necesario, respetando las medidas de seguridad y confidencialidad correspondientes a su clasificación.

1.3. Dentro del manejo ético y seguro de la información que posee y gestiona la UNAM, las áreas universitarias buscarán lo siguiente:

1.3.1. Cumplir con los objetivos universitarios y con los servicios que prestan, utilizando los datos adecuadamente de acuerdo con sus atribuciones.

1.3.2. Compartir los datos con otras áreas dentro del marco normativo con la finalidad de realizar acciones coordinadas, prestar servicios eficaces y trabajar con información actualizada y confiable.

1.3.3. Cuidar la calidad de los datos que generan o recopilan.

1.3.4. Asegurar el almacenamiento confiable y seguro de los datos.

1.3.5. Adoptar las medidas técnicas y tecnológicas que ayuden a garantizar la recuperación y preservación de los documentos de archivo electrónicos que se encuentren en las bases de datos, de acuerdo con la normatividad de archivos.

1.4. Para la interoperabilidad de los sistemas de información al interior de la UNAM se buscará promover políticas, reglas y acuerdos de colaboración claros que garanticen la confiabilidad e integridad de los datos personales durante la compartición y almacenamiento de la información.

1.5. El titular del área universitaria y el responsable de seguridad de datos personales sensibilizarán y orientarán al personal universitario en sus áreas sobre el correcto resguardo de la información reservada y confidencial, con el fin de que no se divulgue y tenga el tratamiento correcto, de acuerdo con su clasificación y la normatividad universitaria y federal vigentes.

1.6. Toda información almacenada digitalmente, transmitida por correo o por medios electrónicos, debe protegerse de acuerdo con la normatividad y sin importar la forma que tome o los medios por los que se comparta o almacene.
1.7. La información clasificada como uno o más documentos de archivo puede constituirse en expedientes electrónicos, los cuales deberán ser almacenados, preservados, custodiados y migrados a medios tecnológicos actualizados, protegidos, incluyendo la digitalización de expedientes en papel en los casos previstos de conformidad con la norma universitaria denominada "Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la UNAM".

2. Sobre las responsabilidades acerca de la información

2.1. Las áreas universitarias son responsables de dar el tratamiento adecuado a la información que almacenen o compartan, de acuerdo con el "*Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México"*, las "*Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad"* y la normatividad aplicable.
2.2. Las áreas universitarias deben asegurar, en términos de las disposiciones jurídicas aplicables, la no divulgación de datos o información a terceros o a sistemas no autorizados.
2.3. Los activos de información son parte del patrimonio universitario, por lo que cualquier medio de almacenamiento, plataforma o software que se utilice para su tratamiento deberá asegurar los derechos de la universidad sobre dichos activos, sin perjuicio de su integridad y acceso a su contenido.
2.4. Las áreas universitarias deben comunicar formalmente a su personal acerca de sus responsabilidades en la gestión de la información y recabar cartas de confidencialidad de cada persona cuando, por sus atribuciones, maneje información confidencial o datos personales.
2.5. El responsable de seguridad de datos personales será el encargado de implementar y mantener el Sistema de Gestión de Seguridad de los Datos Personales (SGSDP) del área universitaria conforme a lo establecido en las "*Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad*".
2.6. Ante a) la pérdida o destrucción no autorizada, el robo, extravío o copia no permitida, b) el uso, acceso o tratamiento no autorizado, o c) el daño, la alteración o modificación no aprobada de datos personales, el responsable de seguridad de datos personales del área universitaria deberá notificar al titular de los datos personales y a la Unidad de Transparencia conforme a lo establecido en el Capítulo III: Medidas de seguridad administrativas para la protección de datos personales de las "*Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad*".
2.7. Las áreas universitarias deben resguardar y preservar la información que deriva del ejercicio de sus facultades, competencias y funciones de conformidad con lo establecido en los Lineamientos Generales para la Organización, Administración y Conservación de

los Archivos de la Universidad Nacional Autónoma de México, así como los Instrumentos de Control y Consulta Archivísticos de la UNAM que cada año emite el Área Coordinadora de Archivos.

3. Sobre la neutralidad tecnológica y la interoperabilidad

3.1. En el diseño de soluciones tecnológicas se sugiere buscar la neutralidad tecnológica y el aprovechamiento de estándares abiertos, fomentando que la información sea generada, almacenada o transmitida electrónicamente, y pueda ser consultada y utilizada en un marco de portabilidad, independientemente de la tecnología seleccionada.

3.2. Se recomienda que los estándares seleccionados sean abiertos, referentes internacionales, vigentes y con un soporte amplio de una organización o comunidad.

3.3. Es recomendable privilegiar las plataformas tecnológicas que faciliten la compartición y almacenamiento seguro de la información entre las áreas universitarias: sistemas operativos, bases de datos y arquitecturas orientadas a servicios (por ejemplo, interfaces de programación de aplicaciones o APIs).

3.4. Se recomienda privilegiar el almacenamiento e intercambio de información a través del uso de protocolos y formatos basados en estándares abiertos. A nivel archivo están disponibles JSON, XML y CSV; a nivel protocolo, SOAP, UDDI, WSDL, WS-Security o JDBC.

3.5. Se recomienda que los sistemas involucrados en el almacenamiento y la transferencia de información utilicen los mismos estándares de codificación en sus bases de datos para evitar problemas de compatibilidad. En su defecto, se aconseja acordar la codificación a emplear antes de realizar cualquier transferencia de datos.

4. Sobre las fuentes de información

4.1. Se recomienda que los sistemas universitarios privilegien la obtención de información por medio de fuentes de datos autoritativas. Por ejemplo, el nombre de los trabajadores y su área de adscripción deben obtenerse de la Dirección General de Personal.

4.2. La información o datos almacenados de forma electrónica en la universidad deben provenir de fuentes confiables, es decir, de aquellas con mecanismos para asegurar que la información transmitida y almacenada es válida.

4.3. Las áreas universitarias considerarán los atributos de seguridad de la fuente de información y de su destino en el intercambio y almacenamiento, estableciendo controles que les permitan cuidar la trazabilidad y responsabilidad sobre los datos.

4.4. Las áreas universitarias que conformen una fuente de información primaria como resultado de sus funciones, considerarán y promoverán que dicha información sea aprovechada para mejorar procesos en otras áreas de la Universidad, observando lo estipulado en los presentes lineamientos y en la normatividad aplicable.

5. Sobre la calidad de los datos universitarios

5.1. Se recomienda que las áreas universitarias identifiquen los datos que puedan ser objeto de análisis para la toma de decisiones en la universidad y consideren métricas de calidad de los datos, en cuanto a las características de disponibilidad, portabilidad, recuperabilidad, accesibilidad, conformidad, confidencialidad, eficiencia, precisión,

trazabilidad, exactitud, completitud, consistencia, credibilidad, vigencia y/o comprensibilidad, que permitan a los usuarios leerlos e interpretarlos.

5.2. Se recomienda a las áreas universitarias establecer controles y programar revisiones de los datos que ayuden a evitar problemas en su calidad, como son: ausencia de valores, valores erróneos o imprecisos, errores ortográficos, violación a las restricciones de unicidad, integridad referencial o verificación, inconsistencia de los datos, duplicidad innecesaria de la información, inconsistencias en las unidades de medida, entre otros.

5.3. Se sugiere a los responsables TIC contemplar la calidad de los datos desde el diseño de la base de datos (normalización) y documentarlo (diagramas entidad-relación y diccionario de datos), conforme a los establecido en los "*Lineamientos y recomendaciones para la administración de bases de datos*" para facilitar la comprensión y proveer de sentido para otras personas.

5.4. Se aconseja a las áreas universitarias corroborar que los sistemas bajo su responsabilidad cuentan con los controles y mecanismos necesarios para la validación de los datos que se almacenan.

5.5. Cada área universitaria es responsable de analizar la calidad de sus datos y definir su proceso de limpieza. Se debe identificar los datos a limpiar, los que no es posible limpiar y los que deben ser eliminados.

5.6. Respecto a la calidad de los datos, las áreas universitarias deben observar lo siguiente:

5.6.1. Cumplir con la normatividad universitaria de transparencia.

5.6.2. Mantener la confidencialidad de los datos de accesos no autorizados.

5.6.3. Establecer medidas para que los datos almacenados no sean modificados, borrados ni alterados.

5.6.4. Asegurar que la integridad de los datos almacenados o compartidos pueda ser verificada.

5.6.5. Garantizar que los datos almacenados sean conservados conforme lo determina la normatividad universitaria en materia de archivos durante los periodos legales establecidos.

6. Sobre los sistemas de información

6.1. Los sistemas considerarán privilegios de roles de usuario partiendo del principio de menor acceso, es decir, solo permitirán el acceso a la información que requiera el usuario para sus funciones.

6.2. Los sistemas considerarán la incorporación de algoritmos de encriptación en la base de datos para los datos confidenciales o sensibles.

6.3. Los portales web y sistemas de información en línea que manejen información confidencial o sensible o que den un servicio crítico, deben observar que las conexiones a ellos se encuentren cifradas con protocolos HTTPS (*Hypertext Transfer Protocol Secure*) y TLS (*Transport Layer Security*) en las versiones estables vigentes.

6.4. Los usuarios con acceso individual a sistemas y aplicaciones son responsables de usar adecuadamente las credenciales de acceso que les otorgan.

6.5. El responsable TIC debe realizar pruebas para revisar vulnerabilidades en sistemas y aplicaciones web cada seis meses. Si se lleva a cabo un proceso mayor de actualización o

cambio de tecnología, es recomendable ejecutar de manera planificada las pruebas aplicables (funcionalidad, regresión, carga, entre otras) en ambientes de desarrollo habilitados para ello antes de efectuar la actualización o sustitución en un ambiente de producción.

6.6. Las áreas universitarias son responsables de conservar y mantener en condiciones adecuadas de operación sus sistemas o aplicaciones para asegurar las actividades de consulta, procesamiento, actualización y correcta utilización de los datos.

6.7. Las áreas universitarias deben incluir en los sistemas de información, o en las páginas donde se recabe información relacionada con datos personales y datos personales sensibles, los Avisos de Privacidad (simplificado e integral) de conformidad con lo establecido en los artículos 17 y 18 del "Acuerdo por el que se establecen los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México".

6.8. Las áreas universitarias son responsables de que los datos o información contenidos en los sistemas o aplicaciones para la prestación de servicios digitales permanezcan completos e inalterados o que, en su caso, sólo sean modificados por los usuarios y mecanismos autorizados.

6.9. Las áreas universitarias únicamente deben solicitar a los usuarios la información absolutamente necesaria para obtener un determinado servicio.

6.10. Las áreas universitarias deben procurar, en la medida de lo posible, que los usuarios aporten sus datos una vez; para ello deben estar en condiciones de almacenar, recuperar y compartir los datos con las fuentes autoritativas que la universidad establezca.

7. Sobre la integración de las bases de datos

7.1. Las áreas universitarias promoverán la integración de las diversas fuentes de información que posean, obteniendo bases de datos limpias y consolidadas que faciliten y mejoren la toma de decisiones.

7.2. Se deberán identificar los datos relevantes de los procesos universitarios que realmente aportan valor y documentar los datos describiéndolos a nivel de metadato. De no existir esta documentación, se deberá crear y obtener su aprobación por parte los responsables de las áreas involucradas y titulares.

7.3. Dentro de las áreas universitarias se deberá promover la eliminación o disminución de silos de datos, con la intención de:

- 7.3.1. Buscar que los usuarios tengan acceso a datos de valor en menor tiempo.
- 7.3.2. Facilitar las tareas de conexión a los datos.
- 7.3.3. Entender el flujo de información y contribuir a la mejora de los procesos de consulta, intercambio y uso de datos.
- 7.3.4. Eliminar o disminuir la duplicidad de trabajo en el registro de datos, en diferentes sistemas y procesos.
- 7.3.5. Maximizar el valor de los datos, aprovechar la variedad de datos existentes y, como resultado, contribuir a la mejora de la toma de decisiones.
- 7.3.6. Permitir la compartición de información entre sistemas.

7.4. En las bases de datos se debe fomentar la aplicación de reglas de semántica y sintaxis para generar una vista unificada y contribuir a la compartición entre diferentes fuentes

de datos para la gestión de los procesos y servicios universitarios. Lo anterior debe considerar prácticas como las que se citan a continuación:

7.4.1. Identificar, entender, documentar, catalogar y, en su caso, reclasificar los datos de interés (relevantes para el área universitaria y la UNAM) almacenados en las bases de datos.
7.4.2. Establecer criterios de calidad de los datos, de acuerdo con su interés u objetivo.
7.4.3. Establecer prácticas para la compartición de datos, que incluyan la limpieza de datos dispares almacenados en diferentes bases de datos y combinarlos.
7.4.4. Establecer una vista de datos unificada que permita publicar los datos y presentarlos de forma consistente para facilitar su consumo por parte de los usuarios finales.
7.4.5. Planear procesos de unificación que consideren la formación de una base sólida de datos útil a corto, mediano y largo plazo para el área universitaria y los fines de la UNAM.
7.4.6. Si es el caso, utilizar catálogos institucionales, nacionales o internacionales para normalizar los datos.

8. Sobre los servicios en nube pública, privada e híbrida

8.1. Las áreas universitarias deben privilegiar el alojamiento de información en instalaciones de la UNAM y en territorio nacional.
8.2. Las áreas universitarias que hagan uso de servicios de nube privada para el despliegue de sistemas para el tratamiento automatizado de datos personales deberán cumplir con lo establecido en los artículos 18, 19 y 20 de las "*Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en posesión de la Universidad*".
8.3. En caso de utilizar una nube pública en sistemas que realicen el tratamiento automatizado de datos personales, se deberá considerar el artículo 21 de las "*Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en posesión de la Universidad*" para el resguardo de archivos cifrados que contengan respaldos de la información.
8.4. El responsable de seguridad de datos personales deberá efectuar un análisis de riesgos y evaluaciones de impacto sobre protección de datos antes de contratar servicios o realizar proyectos de cómputo en la nube.
8.5. Si el área universitaria desea implementar servicios en nube privada, el responsable TIC y el responsable de seguridad de datos personales deberán adoptar medidas para el diseño de la arquitectura tecnológica de los servicios para la protección de los datos personales y/o sensibles que estén bajo su custodia (privacidad desde el diseño).
8.6. Antes de contratar servicios en nube, las áreas universitarias deben analizar si sus aplicaciones y datos son susceptibles de migrar y adaptarse a ellos en términos de costos, beneficios, tecnologías, tiempos y cumplimiento normativo.
8.7. Antes de contratar el servicio de nube, el área universitaria deberá realizar el dimensionamiento de los datos que serán almacenados. Se requiere tanto la estimación del tamaño inicial como del crecimiento esperado por lo menos a un año.
8.8. Los servicios en la nube de un proveedor deben permitir la interoperabilidad con otros

servicios públicos o privados de la universidad de manera segura, así como el intercambio de información entre las interfaces de programación de aplicaciones (APIs, por sus siglas en inglés) en cualquier extremo.

8.9. Los servicios en la nube de un proveedor deben ser capaces de migrar aplicaciones y datos del área universitaria a otros servicios en la nube o locales, sin pérdida de información.

8.10. Respecto a los datos que se utilizarán en un servicio en la nube, el área universitaria debe analizar los riesgos y el nivel de protección requerido para evaluar que los controles y mecanismos del proveedor del servicio sean acordes a las necesidades y a la normatividad universitaria y federal. Se sugiere la consulta de los siguientes documentos elaborados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales: "Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales", "Guía breve para Sujetos Obligados para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales" y "Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales".

8.11. El proveedor de los servicios en la nube deberá implementar la funcionalidad apropiada para brindar el servicio de almacenamiento de cómputo y para la interfaz de gestión de datos en la nube (*Cloud Data Management Interface*, CDMI) respecto del control de acceso, autenticación, cifrado, inicio de sesión y limpieza de los datos.

8.12. Para utilizar servicios en la nube pública e híbrida, las áreas universitarias deben considerar las siguientes medidas:

8.12.1. El proveedor deberá indicar en el contrato de prestación de servicios que cuenta con mecanismos implementados y auditados para garantizar la disponibilidad, integridad y confidencialidad de la información, tanto en el tránsito de los datos como en su almacenamiento.

8.12.2. El proveedor debe presentar evidencia de que cumple con el marco normativo nacional y universitario respecto al tratamiento de los datos personales y a los aspectos que la UNAM establezca, independientemente de la localización de los servidores.

8.12.3. Las áreas universitarias deben tener el control sobre el acceso y gestión de los datos, procesos y servicios.

8.12.4. El contrato del servicio debe establecer que la información proporcionada por las áreas universitarias es propiedad de la UNAM y que no podrá utilizarse para cualquier fin distinto al convenido.

8.12.5. Preferentemente se deben seleccionar proveedores que demuestren estar sujetos a revisiones o auditorías realizadas por terceros de reconocido prestigio, con certificación en el cumplimiento de estándares de seguridad de la información.

8.12.6. Establecer por escrito un acuerdo de nivel de servicio (SLA, *Service Level Agreement*) sobre las características y el rendimiento del servicio en la nube que el proveedor se compromete a ofrecer, estableciendo métricas y herramientas que permitan al área universitaria verificar su cumplimiento.

8.12.7. Debe privilegiarse que el proveedor cuente con mecanismos de alerta y monitoreo al respecto de violaciones de seguridad de los datos. De ocurrir alguna, deberá informar de inmediato y por escrito al responsable TIC del área universitaria.

8.12.8. El proveedor debe contar con mecanismos para garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al área universitaria y que esta última haya podido recuperarlos.

9. Sobre la seguridad de la información

9.1. Las áreas universitarias deben adoptar las medidas técnicas y organizativas identificadas que promuevan la seguridad física y lógica de la red, de los servicios y de los datos confidenciales o sensibles que recogen y procesan, empleando mecanismos y canales de cifrado, por ejemplo.

9.2. Las áreas universitarias establecerán sus planes de continuidad y de recuperación en caso de desastres, considerando sus necesidades de almacenamiento y compartición de información.

9.3. Se recomienda que las áreas universitarias implementen registros detallados (bitácoras) que les permitan identificar y analizar situaciones generales o específicas, dentro de la información manejada por los servicios digitales que proporcionan.

9.4. Las áreas universitarias deberán cumplir con lo establecido en los anexos: IV. Ruta crítica para el cumplimiento de las Medidas de Seguridad Técnicas y V. Formatos para el cumplimiento de las Medidas de Seguridad Técnicas, de acuerdo con las "*Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad*" cuando procesen o transmitan datos personales o sensibles entre sistemas de información y durante su almacenamiento.

9.5. El responsable de seguridad de datos personales, en conjunto con los responsables de los sistemas, debe revisar los riesgos a los que están sometidos los activos de información y los sistemas asociados del área universitaria. También deben actualizar el plan de trabajo con los controles de seguridad a implementar, por lo menos una vez al año o cuando exista un cambio tecnológico u organizacional significativo.

9.6. Para acceder a datos personales, información sensible o confidencial a través de Internet o redes públicas, se recomienda utilizar una conexión segura a través de una Red Privada Virtual (VPN, *Virtual Private Network*) para que la información se transmita cifrada en bloques de 128 bits, como mínimo, y llaves de 2048 bits.

9.7. Para corroborar la integridad de la información sensible o crítica que se transmita o almacene, se deben utilizar funciones hash de 512 bits como mínimo.

9.8. El acceso a la información almacenada y su compartición sólo estará disponible para quienes hayan recibido autorización del responsable de su resguardo. Para ello, se sugiere establecer elementos de trazabilidad de las actividades realizadas.

9.9. Para el intercambio seguro de la información confidencial o sensible entre las áreas universitarias y, en su caso, con terceros, se debe promover la firma de acuerdos que consideren:

9.9.1. Responsabilidades de gestión para controlar y notificar su transmisión, envío y recepción.

9.9.2. Niveles de control de acceso acordes con la clasificación de la información.
9.9.3. Procedimientos para asegurar la trazabilidad y no repudio.
9.9.4. Procedimientos para la remoción de información intercambiada en caso de que ésta constituya una violación a la normatividad vigente.
9.9.5. Normas técnicas mínimas para el empaquetado y transmisión, uso de controles criptográficos y canales seguros de comunicación.
9.9.6. Mecanismos e interfaces para compartir o intercambiar información.
9.9.7. Acuerdos de confidencialidad y no divulgación suscritos, en los cuales se especifique la información a proteger y los usos permitidos de la misma, las responsabilidades y procesos para reportar la divulgación no autorizada y las brechas de seguridad ocurridas, así como el derecho de auditar y supervisar actividades que involucran información confidencial.
9.9.8. Responsabilidades y compromisos en caso de incidentes de seguridad, como la pérdida de datos.

Capítulo II. Políticas para la compartición de información

1. Generales

1.1. La información que sea objeto de intercambio entre las áreas universitarias de la UNAM, y que por sus características se defina como privada, de tratamiento especial y/o incluya datos personales sensibles, para su transferencia deberá apoyarse de una solicitud formal por oficio o un acuerdo por escrito entre las áreas universitarias, de acuerdo con las “Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad”. También será necesaria una carta de confidencialidad cuando se trate de información sensible.
1.2. Los acuerdos para la compartición de información deben considerar el cumplimiento normativo vigente, así como las limitaciones que pudieran existir de acuerdo con el tipo de información solicitada.
1.3. Dichos acuerdos deben definir las responsabilidades de las partes involucradas, el tiempo que durará el intercambio, los procedimientos, los mecanismos, los formatos y los controles de seguridad que se utilizarán.
1.4. La información en acceso abierto, objeto de intercambio entre áreas internas o externas a la Universidad, deberá compartirse siguiendo la normatividad vigente y respetando los derechos de autor y de propiedad intelectual, estableciendo licencias de uso, así como utilizando los protocolos y estándares abiertos.

2. De las áreas responsables de la información

2.1. Son las encargadas de autorizar las solicitudes de compartición de información que cumplan con los requisitos establecidos y generen beneficios justificados en el marco de los objetivos institucionales.
2.2. Identifican, evalúan y gestionan los riesgos de la información a su cargo e implementan los controles de seguridad necesarios para su tratamiento y protección.

2.3. Deberán promover que los mecanismos de compartición de información se realicen directamente desde el área autoritativa o fuente primaria de los datos, siguiendo los mecanismos de compartición vigentes que resulten útiles para dar respuesta a la necesidad.
2.4. Las áreas universitarias autoritativas son las responsables de establecer las reglas y procedimientos para el acceso e intercambio de información bajo su resguardo.
2.5. El responsable del tratamiento de la información del área universitaria debe establecer medidas técnicas y organizativas que garanticen la seguridad de la información, sobre todo aquella considerada sensible.
2.6. Deberá supervisar que las medidas técnicas establecidas, como el uso de firewall, copias de seguridad, cifrado, sistemas actualizados y contraseñas seguras, se realicen y puedan ser verificadas.
2.7. Deberá acordar con el área solicitante los aspectos de la compartición de la información, entre los cuales se encuentran el formato a utilizar, los mecanismos de seguridad y transmisión, el uso que se le dará a la información, los criterios de compartición de información (técnicos, semánticos, jurídicos y organizativos, entre otros), así como la formalización operativa y administrativa.
2.8. Entre las áreas universitarias que intercambia información, se debe establecer el ciclo correcto de los datos que reciben, si serán almacenados o no, bajo qué tipo de mecanismos se protegen en reposo y en tránsito, así como el procedimiento correcto para su eliminación.

3. De las áreas solicitantes de información sensible, crítica o confidencial

3.1. A excepción de los datos abiertos o de la información en acceso abierto, las áreas solicitantes deberán observar lo siguiente:
3.1.1. Pedir por escrito la información que requieren, respondiendo a las siguientes preguntas:
- ¿Quién solicita la información?
- ¿Qué información necesita?
- ¿Cuál será el uso que se le dará a la información compartida?,
- ¿Qué tratamiento se dará a la información?
- ¿Cuál es la justificación de su solicitud?
- ¿Quién será el responsable de proteger y resguardar la información en el área solicitante?
- ¿La información se solicitará por única vez o con alguna frecuencia específica?

3.1.2. El área solicitante será responsable de la información a partir de que tenga acceso a la misma, conforme a los acuerdos establecidos con el área responsable y la normatividad relativa a su protección.
3.1.3. El área solicitante no podrá transmitir estos datos ni hacer uso distinto del convenido con el área responsable de los mismos.

4. De la calidad de la información

4.1. Se debe evitar, en la medida de lo posible, la redundancia en los datos y proteger la integridad de los mismos.

4.2. Es indispensable disminuir problemas de actualización de los datos. Por ejemplo, en el caso de las bases de datos se debe asegurar que los datos se actualicen en una sola tabla; no debe existir duplicidad. Otro ejemplo: establecer restricciones de integridad referencial contribuye a no generar inconsistencias en los datos al no permitir que se elimine o altere de forma indebida un dato que mantiene relación con otros.

4.3. Las áreas universitarias deben establecer los mecanismos que consideren adecuados para fortalecer la calidad de la información: validaciones para la captura de datos en los sistemas informáticos, capacitación en los procesos de captura de la información, mejoras en el diseño de la base de datos y la optimización en los procesos de manejo de información, entre otros.

4.4. Los datos tienen un ciclo de vida. Después de un periodo determinado es fundamental identificar hasta qué punto la información es veraz y se mantiene vigente. Por ello, las áreas universitarias establecerán los tiempos y procedimientos para su actualización o, en su caso, de acuerdo con la naturaleza de los datos, deberán determinar si el mecanismo de consulta en tiempo real resulta más conveniente.

5. De los mecanismos de compartición de la información

5.1. Las áreas universitarias, principalmente las autoritativas, deben procurar el diseño y mantenimiento de mecanismos de compartición de información vigentes y abiertos que aprovechen las ventajas de arquitecturas basadas en servicios, intercambio de mensajes o datos en formatos estándar para facilitar el intercambio de manera independiente a plataformas o lenguajes de programación.

5.2. El personal que reciba la información relacionada con datos personales, y que mantenga la custodia y preserve los derechos ARCOP (Acceso, Rectificación, Cancelación, Oposición y Portabilidad) del titular de la información, deberá firmar una carta de confidencialidad. En caso de no contar con mecanismos para ejercer el derecho a la portabilidad, se recomienda indicarlo en los respectivos avisos de privacidad.

5.3. Los mecanismos de transferencia utilizados deben proteger el intercambio de información y de datos sensibles o confidenciales entre las áreas universitarias, a través de:

5.3.1. La identificación y registro del remitente y del receptor.

5.3.2. El uso del cifrado en los datos intercambiados.

5.3.3. El registro de un sello de tiempo en bitácora que tenga la información sobre la hora de la transferencia y sobre qué datos electrónicos fueron intercambiados.

5.4. El área responsable de la información debe verificar que el mecanismo utilizado para la transferencia esté disponible únicamente para las personas o áreas universitarias explícitamente autorizadas para ello, con el soporte de firmas y certificados digitales correspondientes.

6. De la transmisión de la información

6.1. La transferencia de información sensible o confidencial debe considerar el uso de un canal de comunicación cifrado entre el cliente y el servidor.

6.2. En el caso de la información que no es crítica o confidencial, se aconseja verificar la autenticidad del otro extremo de la comunicación, es decir, corroborar que el solicitante sea quien dice ser, antes de proceder al intercambio de información. También se sugiere realizar verificaciones la integridad y confiabilidad de la información al ser transmitida.

6.3. Cuando se realicen intercambios periódicos de información entre áreas universitarias o terceros (por ejemplo, un proveedor) se deberá privilegiar la transmisión de datos a través de canales seguros, utilizando mecanismos como son: protocolos IPsec, TLS, Red Privada Virtual, túneles punto a punto, llaves públicas o privadas, entre otros mecanismos.

6.4. Todas las transacciones programadas deben estar bajo el control exclusivo del área responsable de la información, teniendo la certeza de que sólo podrán ser transferidos los datos autorizados para cada operación específica.

6.5. En caso de que se comprometan las contraseñas de las cuentas utilizadas para el intercambio de información, se aconseja bloquearlas y cambiarlas. Posteriormente se debe realizar un análisis de la causa que originó la brecha de seguridad.

7. Consideraciones de seguridad para la compartición de información

7.1. Las medidas de seguridad establecidas en las áreas responsables de la información deben contemplar las "*Normas complementarias sobre medidas de seguridad, técnicas administrativas y físicas para la protección de datos personales en posesión de la Universidad*".

7.2. Las áreas universitarias involucradas deben tomar las medidas necesarias para que la información compartida esté segura en todo momento, lo que implica el uso de métodos de autenticación y autorización que limiten el acceso a la información sólo a los usuarios autorizados, dejando evidencia documental de la trazabilidad de los datos.

7.3. Las medidas de seguridad que se implementen deben garantizar la confidencialidad, integridad y disponibilidad de la información.

7.4. Las medidas de seguridad considerarán la verificación y evaluación de la eficacia de los controles y procedimientos para restaurar los datos y el tratamiento en caso de incidente físico o técnico.

7.5. Las áreas universitarias implementarán las medidas de confidencialidad para evitar el uso de información personal identificable cuando se publique o divulgue información de manera abierta tanto en forma escrita como digital, salvo la información que por cumplimiento de transparencia deba ser publicada de forma abierta.

7.6. Las reglas de acceso o intercambio de información contemplan: perfiles de acceso, permisos exclusivos para el desarrollo de la actividad, procedimientos para realizar distintas tareas, canales de comunicación permitidos, redes y/o equipos de cómputo que podrán interactuar, entre otros, de manera que se garantice su protección acorde a la naturaleza de la información y en estricta observancia de la normatividad.

7.7. Se recomienda que las áreas universitarias mantengan un proceso de autorización y un

registro de todos los privilegios asignados a los sistemas de información, bases de datos y carpetas compartidas, controlando los derechos de acceso de los usuarios, por ejemplo, de lectura, escritura, borrado y ejecución a nivel objeto o registro.

Capítulo III. Políticas para el almacenamiento de la información

1. Generales

1.1. Para establecer las condiciones de almacenamiento de la información, de conformidad con la normatividad universitaria, es indispensable identificar el propósito y fundamento que tendrá, así como:
- El nivel de confidencialidad de la información.
- El nivel de criticidad de los servicios que utilizan los datos.
- El tipo de información que se desea almacenar.
- La confiabilidad de los datos.
- La frecuencia de uso.
- El volumen esperado de información inicial y estimación del crecimiento.
- Quién accede a los datos y para qué fines.
- Cómo se puede acceder a los datos.
- El formato de la información que será almacenada.
- El uso de estándares para nombrar archivos, directorios y objetos usados para almacenar la información. Por ejemplo, las tablas y *tablespaces* de las bases de datos).

1.2. Las áreas universitarias deben cumplir con los plazos de conservación establecidos en los Instrumentos de Control y Consulta Archivísticos de la UNAM que emite cada año el Área Coordinadora de Archivos.

1.3. Las áreas universitarias deben sensibilizar a su personal sobre la protección de la información almacenada en bases de datos, equipos de cómputo y otros dispositivos que utilizan, de acuerdo con la normatividad aplicable.

1.4. Se recomienda que los sistemas universitarios utilicen formatos estandarizados y abiertos para el almacenamiento de la información y con ello facilitar que pueda ser compartida y leída por todos los sistemas involucrados.

1.5. Las áreas universitarias buscarán la disponibilidad de los datos que se encuentren almacenados de forma remota o en medios de almacenamiento externos, de acuerdo con la norma ISO/IEC 27040:2015 “Seguridad de almacenamiento”.

1.6. Se sugiere establecer procedimientos de operación claros en todas las áreas sustantivas de la UNAM para contar con respaldos periódicos y verificados de los datos.

1.7. Se debe cumplir con los principios de resguardo, recuperación, continuidad y acceso a la información, determinados por su naturaleza, criticidad y variabilidad. Para ello es importante validar que la información es propiedad de la institución; en caso de que pertenezca a terceros, se deberá contar con los permisos necesarios de los respectivos titulares de la información.

2. Medios de almacenamiento

2.1. Para la elección del medio de almacenamiento, las áreas universitarias considerarán al menos lo siguiente:

2.1.1. Las necesidades que le permitan cumplir con sus funciones, considerando elementos como el nivel de confidencialidad, criticidad de la información, volumen de datos, frecuencia de uso, recursos disponibles, seguridad, rendimiento requerido, entre otros.

2.1.2. Las características de las tecnologías de los medios de almacenamiento: el tiempo de vida indicado por el fabricante, el número de sobreescrituras que acepta sin degradarse o dañarse, capacidad de almacenamiento, costo, condiciones ambientales (humedad, temperatura, aislamiento, entre otros) y los cuidados que el medio requiere.

2.2. La forma de organización, conservación y control de los medios de almacenamiento empleados será establecida dentro de cada entidad o dependencia considerando la clasificación de la información, la trazabilidad y lo establecido en las "*Normas complementarias sobre medidas de seguridad, técnicas administrativas y físicas para la protección de datos personales en posesión de la Universidad*".

2.3. Las áreas universitarias son responsables de utilizar herramientas e implementar procesos para la gestión de la infraestructura que contribuya a garantizar la adecuada disponibilidad y rendimiento de todos los elementos de almacenamiento, la protección y seguridad de los datos, y el cumplimiento de los requisitos normativos. Se recomienda llevar a cabo revisiones semestrales de seguridad, que deben estar a cargo de personal especializado del área y/o con apoyo de otra universitaria.

2.4. Las áreas universitarias establecerán controles sobre cualquier operación realizada en los medios de almacenamiento que contengan datos personales y/o sensibles: mantenimiento, reparación, sustitución, entre otros.

2.5. Las áreas universitarias deben concientizar a sus usuarios respecto a almacenar información relevante para las actividades de la Universidad con el fin de aprovechar mejor los recursos.

2.6. En el traslado de medios de almacenamiento a instalaciones externas al área universitaria, se sugiere asegurar que se cumple la cadena de custodia de los mismos y que se consideren mecanismos de cifrado para evitar la pérdida o fuga de información.

3. Conservación de la información

3.1. La información almacenada en las áreas universitarias debe conservarse durante los plazos estipulados en la normatividad vigente antes de ser eliminada, bajo la consideración del ciclo vital de los documentos, de acuerdo con los "*Lineamientos generales para la organización, administración y conservación de los archivos de la UNAM"* y el *"Catálogo de disposición documental"*.

3.2. Los elementos a considerar en relación con la conservación de los soportes de almacenamiento son la accesibilidad, la legibilidad, la perdurabilidad y la preservación de la autenticidad durante el tiempo de resguardo.

4. Eliminación de la información y los medios de almacenamiento

4.1. Para la eliminación de información sensible o confidencial es recomendable usar métodos de borrado seguro en los medios electrónicos que la contengan. Estos métodos deben considerar la escritura de valores aleatorios y, al menos, siete sobreescrituras para evitar que la información sea recuperada por personas no autorizadas.

4.2. Cuando se desechan equipos de cómputo y medios de almacenamiento por obsolescencia o daño, se sugiere considerar la destrucción física de soportes no robustos: CD, DVD o papel. En este proceso puede utilizarse una destructora de soportes magnéticos o de papel; en el caso de los discos duros o cintas puede optarse por el borrado seguro, la desmagnetización o la destrucción física. También se puede recurrir a empresas especializadas en la destrucción certificada de información, las cuales deben entregar evidencia de la destrucción.

4.3. El procedimiento de borrado seguro de la información, en equipos de cómputo que serán transferidos o dados de baja, requiere la aplicación de lo estipulado en la "*Circular DGTIC/003/2017 - Procedimiento para el borrado de información*".

4.4. Los responsables TIC deben establecer un procedimiento para registrar y verificar el borrado seguro. Es necesario definir la responsabilidad de quien lo lleva a cabo y de quien verifica su ejecución; adicionalmente se sugiere considerar la aplicación del procedimiento definido en la "sección H De la Baja documental de los Lineamientos generales para la organización, administración y conservación de los archivos de la UNAM".

5. Consideraciones generales de seguridad en el almacenamiento

5.1. Las dimensiones de confidencialidad, disponibilidad e integridad de la calidad de datos en el almacenamiento se pueden fortalecer con medidas de seguridad encaminadas a:

5.1.1. Proteger la administración del almacenamiento (operaciones e interfaces).

5.1.2. Asegurar una adecuada administración de las credenciales.

5.1.3. Proteger los recursos de respaldo de datos y recuperación.

5.1.4. Proteger los datos en movimiento y almacenados.

5.1.5. Soportar la recuperación de desastres y continuidad del negocio.

5.1.6. Eliminar adecuadamente los datos y medios de almacenamiento.

5.2. Las áreas universitarias establecerán y documentarán sus planes de respaldo en materia de seguridad de la información. Deben identificar los datos que necesitan ser resguardados, establecer el tipo de respaldo a realizar y su frecuencia, seleccionar los medios de almacenamiento del respaldo y verificar su restauración.

5.3. En el plan de respaldo, las áreas universitarias describirán las acciones que permitan llevar a cabo los respaldos y la recuperación de los datos que deban ser protegidos para garantizar que la información sea recuperada en caso de fallas o errores en el almacenamiento o transferencia.

5.4. Las áreas universitarias establecerán las pautas de almacenamiento en bases de datos y sistemas de archivos de acuerdo con los "*Lineamientos y recomendaciones de administración de bases de datos*", considerando al menos los siguientes aspectos: tipo de información que se permite almacenar, estructura de directorios, niveles de acceso,

personas encargadas del respaldo, así como actualización y eliminación.

5.5. Los responsables de los sistemas de almacenamiento e infraestructura asociada considerarán los controles, mecanismos y/o procedimientos necesarios para reducir riesgos de acceso y uso no autorizado, denegación de servicio, corrupción, modificación o eliminación de datos, fuga o filtración de datos, daño, robo o pérdida accidental de medios o elementos de almacenamiento, cambios maliciosos de configuración o accidentales, ataques de malware, así como de tratamiento o borrado inadecuado después de su uso.

5.6. Los responsables de los sistemas de almacenamiento e infraestructura asociada deben mantener los registros de eventos de la actividad de los usuarios al menos durante un año. También es necesario que revisen regularmente las excepciones, fallas y eventos de seguridad de la información de los sistemas y dispositivos de almacenamiento a su cargo.

5.7. Se recomienda establecer controles para proteger los sistemas y dispositivos de almacenamiento de cambios no autorizados, borrado o desactivación de registros de eventos.

5.8. El cifrado de los respaldos que se almacenen en la nube pública no deberá ser de menor capacidad al equivalente a AES (*Advanced Encryption Standard*) de 128 bits.

5.9. Los responsables TIC deben definir e implementar políticas, procedimientos y controles para la gestión de medios extraíbles, con el fin proteger datos confidenciales o sensibles: evitar la divulgación no autorizada, el mal uso, su alteración, eliminación o destrucción.

5.10. Las áreas universitarias establecerán las reglas para el almacenamiento local de la información en los equipos de escritorio y portátiles que utilizan los trabajadores universitarios adscritos a ellas, considerando al menos los siguientes aspectos:

5.10.1. Tipo de información permitida.

5.10.2. Pautas para la generación de estructuras de directorios en los discos duros.

5.10.3. Tiempo de conservación de los archivos en este medio.

5.10.4. Mecanismos de protección a emplear, por ejemplo: uso de antivirus o antimalware o soluciones de protección de datos (cifrado de información, respaldos, replicación de datos, entre otros), por mencionar algunos.

5.10.5. Restricciones en la instalación de software y descarga de archivos que pudieran afectar la información almacenada.

6. Sobre el uso de bóvedas digitales

6.1. Con el fin de preservar objetos digitales a largo plazo, se pueden emplear servicios como el de una bóveda digital. Éste debe garantizar que los documentos almacenados conserven sus características y atributos, así como su autenticidad, fiabilidad, integridad, disponibilidad y custodia; siempre en apego a la normatividad. En el caso de la universidad, la DGTIC presta el servicio Bóveda Digital UNAM a las áreas universitarias que lo requieran.

6.2. Las áreas universitarias son responsables de determinar el tipo de información que guardarán, conforme a la normatividad aplicable, y de definir los metadatos para su organización e indexación con la intención de permitir la recuperación de los documentos.

6.3. Los responsables TIC dimensionarán la capacidad de almacenamiento que requieren y definirán a los usuarios que deben tener acceso al servicio de Bóveda Digital UNAM.
6.4. Las áreas universitarias que soliciten utilizar la Bóveda Digital deben considerar que su solicitud esté alineada con el propósito de preservación a largo plazo y fuera de línea.
6.5. La solicitud del área universitaria deberá tomar en cuenta los aspectos siguientes:
6.5.1. Los datos almacenados en Bóveda Digital UNAM deben ser propiedad de la universidad y considerados críticos por el área universitaria, con un nivel de riesgo tal que su merma, pérdida o alteración podrían tener efectos negativos en la operación del área universitaria, de los proyectos de docencia, investigación y servicios centrales, por lo que se excluyen los datos que sean propiedad de miembros de la comunidad universitaria o de terceros.
6.5.2. Los datos almacenados en Bóveda Digital UNAM no deben ser transaccionales, por lo cual se deben excluir las bases de datos vigentes y en producción, acervos o repositorios en desarrollo o cualquier otro tipo de información que cambie su estructura, dimensiones o contenido en un período menor a un año.
6.5.3. Quedarán excluidos los respaldos de información procedentes de computadoras de escritorio y portátiles; así como los datos de las cuentas de correo electrónico (buzón, contactos, documentos adjuntos), entre otros.
6.6. Las áreas universitarias que hagan uso de la Bóveda Digital UNAM deberán atender lo establecido en la "*Política de Uso y Acuerdo del Nivel de Servicio de la Bóveda Digital UNAM*".

Capítulo IV. Sobre los recursos humanos en la gestión de la información

1. Reforzamiento de las capacidades y habilidades del personal involucrado

1.1. Las áreas universitarias capacitarán al personal que captura información en los sistemas institucionales, respecto a su uso y registro, con la finalidad de prevenir errores y malas prácticas que puedan comprometer la calidad de los datos, la seguridad y privacidad de la información.
1.2. Capacitar al personal técnico en el dominio de los procesos y reglas de negocio necesarios para la operación y soporte de los servicios y medios de almacenamiento y compartición de información.
1.3. Con el fin de tener una gestión de información efectiva y eficiente, los recursos humanos responsables de diseñar, desarrollar y administrar los sistemas de información necesitan conocer las políticas y procedimientos de gestión de información, así como las regulaciones y estándares institucionales en materia de seguridad de la información.

2. Difusión de buenas prácticas entre el personal

2.1. Las áreas universitarias promoverán buenas prácticas que contribuyan a fortalecer la calidad de la información, los sistemas y la seguridad para la compartición de información entre las áreas universitarias.

2.2. Difundir entre el personal de las áreas universitarias buenas prácticas sobre el almacenamiento de información, relacionadas con seguridad, uso, conservación y destrucción de la información resguardada y medios de almacenamiento; además de otras que cada área universitaria considere relevantes.

Capítulo V. Transitorios

1. Cualquier asunto no contemplado en los **Lineamientos generales y Políticas sobre almacenamiento e información compartida entre los sistemas existentes** será analizado y resuelto por el Consejo Asesor de Tecnologías de la Información y Comunicaciones.
2. La interpretación de los presentes lineamientos y políticas para efectos jurídicos, corresponde a la Oficina de la Abogacía General de la UNAM.

Bibliografía y referencias electrónicas

- Avast (2021). **Guía básica sobre una VPN. Qué son y cómo funcionan**. Recuperado: 31 de agosto de 2022. URL: https://blog.avast.com/es/guia-basica-sobre-vpn-que-son-y-como-funcionan
- DGTIC (2017). **Circular DGTIC/003/2017 procedimiento para el borrado seguro de información de la UNAM almacenada en medios digitales**. Recuperado: 31 de agosto de 2022. URL: https://www.red-tic.unam.mx/recursos/2017/2017_Circular_DGTIC_003_2017.pdf
- Diario Oficial de la Federación (2021). **Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal**. Recuperado: 31 de agosto de 2022. URL: https://dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021
- Diario Oficial de la Federación (2016). **Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos para la Organización y Conservación de los Archivos**. Recuperado: 28 de septiembre de 2022: URL: https://dof.gob.mx/nota_detalle.php?codigo=5436056&fecha=04/05/2016#gsc.tab=0
- INAI[1] (2016). **Guía para el borrado seguro de datospersonales**. Recuperado: 3 de marzo de 2023. URL: http://transparencia.inaes.gob.mx/doctos/pdf/transparencia/Guias/Gu%EDa_Borrado_Seguro_DatosPersonales.pdf
- INAI (2018). **Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales**. Recuperado: 9 de marzo de 2023. URL: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/ComputoEnLaNube.pdf
- INAI (2021). **Guía breve para sujetos obligados para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales**. Recuperado: 9 de marzo de 2023. URL: https://home.inai.org.mx/wp-content/uploads/Guia_SO_CC.pdf
- INAI (2021 b). **Recomendaciones para reconocer las principales amenazas a los datos personales, a partir de la valoración respecto al riesgo**. Recuperado: 31 de agosto de 2022. URL: https://home.inai.org.mx/wp-content/uploads/AmenazasDP.pdf
- INAI (2018). **Recomendaciones para el manejo de incidentes de seguridad de datos personales**. Recuperado: 28 de septiembre de 2022. URL: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/Recomendaciones_Manejo_IS_DP.pdf

- INAI (2018). **Guía para el tratamiento de datos biométricos**. Recuperado: 28 de septiembre de 2022. URL: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf
- INAI (2021). **Conformidad de contratos de adhesión de servicios de cómputo en la nube vs los criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales**. Recuperado: 28 de septiembre de 2022. URL: https://home.inai.org.mx/wp- content/uploads/ContratosASCN_CN.pdf
- Idaip (2018). **Guía medidas de seguridad para la protección de datos personales**. Recuperado: 03 de marzo de 2023. URL: https://www.idaip.org.mx/archivos/formatos/Promocion_Vinculacion/Gu%C3%ADa%20medidas%20de%20seguridad.pdf
- Itaipue (2019). **Privacidad por diseño y privacidad por defecto**. Recuperado: 04 de marzo de 2023. URL: https://itaipue.org.mx/portal/documentos/datosPersonales/PrivacidadDisenioDefecto.pdf
- Instituto Nacional de Ciberseguridad (2016). **Guía de almacenamiento seguro de la información**. Recuperado: 3 de mayo de 2023. URL: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf
- Agencia Española de Protección de Datos (2019). Guía de Privacidad desde el Diseño. Recuperado: 3 de marzo de 2023. URL: https://www.aepd.es/es/documento/guia-privacidad-desde-diseno.pdf
- Odín, Dante. et. al. (2011). El cifrado Web (SSL/TLS). **Revista de Seguridad. CERT- UNAM**. Número 10, mayo 2011. Recuperado: 31 de agosto de 2022. URL: https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls
- Organización Internacional de Normalización (2015). **Information technology - Security techniques - Storage security (ISO/IEC 27040:2015)**.
- Organización Internacional de Normalización (2021). **Information security — Encryption algorithms — Part 1: General (ISO/IEC 18033-1:2021).**
- National Institute of Standards and Technology (2017). **Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (NIST SP 800-67)**.
- Organización Internacional de Normalización (2017). **Information technology - Cloud computing - Interoperability and portability (ISO/IEC 19941)**.
- Organización Internacional de Normalización (2018). **Cloud computing - Service level agreement (SLA) framework - Part 2: Metric model (ISO/IEC 19086- 2)**.
- Organización Internacional de Normalización (2015). **Sistemas de transferencia de datos e información espacial. Sistema abierto de información de archivo (OAIS). Modelo de referencia (UNE-ISO 14721:2015)**.
- Organización Internacional de Normalización (2020). **ISO 30300:2020. Information and documentation - Records management - Core concepts and vocabulary.**
- Organización Internacional de Normalización (2016). **ISO 15489-1:2016. Information and documentation - Records management - Part 1: Concepts and principles.**
- Organización Internacional de Normalización (2018). **ISO 15489-2:2018. Information**

and documentation - Records management - Part 2: Guidelines.

- NIST (2020). **Security Guidelines for Storage Infrastructure**. Recuperado: 16 de mayo de 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf
- NIST (2010). **Contingency Planning Guide for Federal Information Systems**. Recuperado: 16 de mayo de 2023. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf
- UNAM (2016). **Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México**. Recuperado: 2 de septiembre de 2022. URL: http://www.transparencia.unam.mx/documentos_transparencia/manual-de- normas_2021.pdf
- Voutssás, A. B. A. D. (2017). **Un marco de referencia para la preservación digital.** Serie: Temas fundamentales de preservación digital. Cuadernos digitales de archivística 1. Archivo General de la Nación. México. https://www.gob.mx/cms/uploads/attachment/file/228996/InterPARES_1_020617.pdf
- Voutssás, A. B. A. D. (2017). ***Desarrollo de políticas y procedimientos para la preservación digital.*** *Serie: Temas fundamentales de preservación digital. Cuadernos digitales de archivística 2*. Archivo General de la Nación. México. https://www.gob.mx/cms/uploads/attachment/file/228990/InterPARES_2_020617.pdf
- UNAM (2017). **Lineamientos y recomendaciones para la administración de bases de datos**. Recuperado: 31 de agosto de 2022. 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: 31 de agosto de 2022. URL: https://www.red-tic.unam.mx/recursos/LineamientosArchivosUNAM.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: 14 de septiembre de 2022. https://www.red-tic.unam.mx/recursos/2020/2020_Norma_ComiteTransparencia_01.pdf
- UNAM (2022). **Catálogo de disposición documental**. Recuperado: 31 de agosto de 2022. URL: https://www.repositoriotransparencia.unam.mx/DocumentosDigitales/descargar/JOHE_1650676046
- UNAM (2022). **Glosario de términos de TIC**. Red-TIC, UNAM. Recuperado: 25 de mayo de 2023. URL: https://www.red-tic.unam.mx/recursos/2022/2022_Glosario_RedTIC_01.pdf
- UNAM (2023). **Manual de Datos Abiertos de Colecciones Universitarias Digitales**. DGRU, UNAM. Recuperado: 16 de mayo de 2023. URL. https://dgru.unam.mx/wp-content/uploads/2019/10/D.MA_.CCUD_CG_001_20171012_Manual_Datos_Abiertos_interactivo.pdf

- UNAM (2021). **Recomendaciones para el almacenamiento de información**. Red-TIC, UNAM. Recuperado: 31 de agosto de 2022. URL: https://www.red-tic.unam.mx/content/recomendaciones-para-el-almacenamiento-de-informacion
- UNAM (2021). **Recomendaciones para la compartición de información**. Red-TIC, UNAM. Recuperado: 31 de agosto de 2022. URL: https://www.red-tic.unam.mx/content/recomendaciones-de-comparticion-de-informacion
- UNAM (2022). **Política de uso y Acuerdo del de servicio de la Bóveda Digital UNAM**. Red-TIC, UNAM. Recuperado: 3 de marzo de 2023. URL: https://www.red-tic.unam.mx/content/politica-acuerdo-nivel-servicio-boveda-digital
- UNAM (2022). **Política de uso y Acuerdo de Nivel de Servicio - Infraestructura como Servicio (IaaS).** Red-TIC, UNAM. Recuperado: 3 de marzo de 2023. URL: https://www.red-tic.unam.mx/content/politica-de-acuerdo-nivel-de-servicio-infraestructura-como-servicio-iaas
- Open Web Application Security Project (2023). **OWASP Top Ten**. Recuperado: 25 de mayo de 2023. URL: https://owasp.org/www-project-top-ten/

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

Logística
Mtra. Irene Sánchez García

Red de responsables TIC
Elaboración
Ana Pérez Arteaga, IIMAS-UNAM
Pedro Bautista Fernández, DGTIC-UNAM
Susana Laura Corona Correa, DGTIC-UNAM
Alberto González Guízar, DGTIC-UNAM
Fernando Zaragoza Hernández, DGAE-UNAM

Revisión
Antonio Baruch Cuevas Ortiz, DGOAE-UNAM
José Othoniel Chamú Arias, DGTIC-UNAM
José Luis Chávez Sánchez, DGTIC-UNAM
Fernando Israel González Trejo, FES Acatlán-UNAM
Miguel Ángel Jiménez Bernal, DGBSDI-UNAM
Leticia Martínez Calixto, DGTIC-UNAM
Angel Martínez Hernández, DGTIC-UNAM
Damián Morales, DTI-Universidad de El Salvador
José Luis Olín Martínez, DGTIC-UNAM
Leonard Pulido Cauzard, DGAE-UNAM
Belén Ramírez Martínez, DGPe-UNAM
Elizabeth Rangel Gutiérrez, DGTIC-UNAM
Hugo Alonso Reyes Herrera, DGTIC-UNAM
Raúl Rodríguez Martínez, DGTIC-UNAM
Rubén Sáenz González, DGRU-UNAM

Eprin Varas Gabrelian, DGTIC-UNAM
Armando Vega Alvarado, DGAE-UNAM

Autorización de publicación en sitio de la RedTIC

Dra. Ana Yuri Ramírez Molina

Créditos históricos (2022)

Red de responsables TIC Elaboración. Susana Laura Corona Correa, DGTIC; José Luis Chávez Sánchez, DGTIC; Alberto González Guízar, DGTIC; Ana Pérez Arteaga, IIMAS

Revisión. Fernando Israel González Trejo, FES Acatlán; Miguel Ángel Jiménez Bernal, DGBSDI; Armando Vega Alvarado, DGAE; Fernando Zaragoza Hernández, DGAE; Leonard Pulido Cauzard, DGAE; Rubén Sáenz González, DGRU; Pedro Bautista Fernández, DGTIC; Leticia Martínez Calixto, DGTIC; Hugo Alonso Reyes Herrera, DGTIC; José Othoniel Chamú Arias, DGTIC; Francisco Javier Romero Murillo, DGTIC

Autorización de publicación en sitio de la RedTIC. Dra. Ana Yuri Ramírez Molina

Créditos históricos (2021)

Red de responsables TIC Elaboración. Susana Laura Corona Correa, DGTIC; José Luis Chávez Sánchez, DGTIC; Alberto González Guízar, DGTIC; Ana Pérez Arteaga, IIMAS

Revisión. José Othoniel Chamú Arias, DGTIC; Fernando Israel González Trejo, FES Acatlán; Miguel Ángel Jiménez Bernal, DGBSDI; Leticia Martínez Calixto, DGTIC; Hugo Alonso Reyes Herrera, DGTIC; Armando Vega Alvarado, DGAE **Autorización de publicación en sitio de la RedTIC.** Dra. Marcela Peñaloza Báez