UNAM

RED·TIC
Red de Responsables TIC
U N A M

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

Noviembre de 2021, 1ª versión

Índice

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

Objetivo

Proporcionar elementos de referencia para la aplicación de buenas prácticas para 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 a: 1) el personal universitario que interviene en el proceso de almacenamiento, compartición, transformación, uso y explotación de la información y/o 2) aquellos 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

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

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).

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.

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. La acción realizada por medio de la cual un sistema proporciona datos a otro de acuerdo con los criterios y mecanismos que se hayan establecido para ello, con la finalidad de dar cumplimiento a un objetivo institucional.

Confiabilidad. Nivel de certeza de que un proceso, 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).

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, y que puede ser pública, reservada o confidencial.

Integridad. Propiedad de la información relativa a su exactitud y completitud, es decir, los datos han permanecido completos e inalterados y, en su caso, sólo han sido modificados por la fuente de confianza y mecanismos autorizados (Glosario ISO 27001:2013).

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.

Portabilidad. Conjunto de características que permiten el uso de algún elemento o componente en una plataforma distinta de la que fue generado, sin requerir alguna modificación o inversión considerable.

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

Resiliencia. Capacidad de proteger un activo de información con el fin de que los sistemas e infraestructura tengan la capacidad de mantener su funcionamiento, recuperarse de un fallo y conservar la confiabilidad.

Servicios de nube privada. En el contexto UNAM, es el modelo de servicio de tecnología de información proporcionado bajo demanda a las Áreas Universitarias, en infraestructura propiedad de la Universidad y que brinda 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 bajo demanda a terceros, operada en infraestructura ajena a la Universidad.

SSL (Secure Sockets Layer)/ TSL (Transport Layer Security). 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.

Tecnologías de Información y Comunicación (TIC). Son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de la información.

Túnel punto a punto. Es una técnica para crear un túnel entre dos puntos de una red, para transmitir información de forma cifrada y segura.

Marco legal aplicable

Los reglamentos, normas y leyes que aplican en el tratamiento de los datos y de la 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 la protección de datos personales.

A continuación se indican aquellas normas que se considera 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

Responsabilidades en relación a estos lineamientos

a) De los titulares de las entidades o dependencias universitarias

- Comunicar, difundir y concientizar al respecto de la aplicación de los presentes lineamientos 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.

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

- Participar de manera proactiva en la aplicación de las actividades de compartición de información de acuerdo con estos lineamientos en cumplimiento de sus funciones de gestión y operación de las TIC. Así como lograr una coordinación efectiva para la realización de estas actividades al interior de su entidad o dependencia y en colaboración con otras áreas universitarias.
- Identificar los activos de información del área universitaria, categorizarlos adecuadamente y establecer los mecanismos para su correcto almacenamiento con fines de resguardo, disponibilidad, integridad, recuperación y confiabilidad.
- Complementariamente, documentar y dar seguimiento a los procedimientos establecidos y de mejora en el marco de aplicación de las presentes políticas.

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

- Contribuir a la aplicación de estos lineamientos en las actividades que le sean asignadas en sus áreas universitarias.
- Comunicar a los responsables de las TIC, las propuestas de mejora que se identifiquen al respecto del almacenamiento de los datos y de las oportunidades para una mejor gestión y aprovechamiento de la información, considerando su respectiva clasificación jurídica (pública, confidencial y/o sensible).

Capítulo I. Lineamientos. Disposiciones generales

a) Sobre la información

- Toda la información publicada deberá cumplir con atributos de calidad como la 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.
- La información es un activo de la Universidad, que debe estar disponible en el momento en que se necesite, guardando las medidas de seguridad y confidencialidad de acuerdo con su clasificación.
- Dentro del manejo relevante, ético y seguro de la información que posee y gestiona la UNAM, las áreas universitarias deberán observar lo siguiente:
    - Cumplir con los objetivos universitarios y con los servicios que prestan, utilizando los datos de manera adecuada y de acuerdo con sus atribuciones.
    - 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.
    - Cuidar la calidad de los datos que generan o recopilan.
    - Cerciorarse del almacenamiento confiable y seguro de los datos.
- La interoperabilidad de los sistemas informáticos al interior de la UNAM deberá 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.
- Las áreas universitarias sensibilizarán y orientarán al personal universitario en el correcto resguardo de la información reservada y confidencial, asegurando que no se divulgue y tenga el tratamiento correcto de acuerdo con su clasificación y con la normatividad universitaria y federal.
- Toda información almacenada digitalmente, transmitida por correo o por medios electrónicos debe protegerse acorde a la normatividad sin importar la forma que tome o los medios por los que se comparta o almacene.

b) Sobre las responsabilidades acerca de la información

- Las áreas universitarias serán 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*, la normatividad vigente aplicable y los presentes lineamientos.
- Las áreas universitarias deben garantizar, en términos de las disposiciones jurídicas aplicables, la no divulgación de datos o información a terceros o a sistemas no autorizados.

c) Sobre la neutralidad tecnológica y la interoperabilidad

- En el diseño de soluciones tecnológicas se deberá buscar la neutralidad tecnológica y el aprovechamiento de estándares abiertos, fomentando que la información sea generada, almacenada o transmitida electrónicamente pueda ser consultada y utilizada en un marco de portabilidad, independientemente de la tecnología origen seleccionada.
- Algunas características que deben tener los estándares abiertos seleccionados son: que se encuentren vigentes, que sean referentes internacionales, que sean abiertos, con amplio soporte por una comunidad u organización.
- Se deberán privilegiar aquellas plataformas tecnológicas en cuanto a sistemas operativos, bases de datos y arquitecturas orientadas a servicios (como por ejemplo, interfaces de programación de aplicaciones APIs) que faciliten la compartición y almacenamiento seguro de la información entre las áreas universitarias.
- Se deberá privilegiar el almacenamiento e intercambio de información en formatos basados en estándares abiertos.

d) Sobre los sistemas de información

- 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.
- Las áreas universitarias serán responsables de que los datos o información contenidos en sus sistemas o aplicaciones para la prestación de servicios digitales, hayan permanecido completos e inalterados y, en su caso, que sólo hayan sido modificados por aquellos usuarios y mecanismos autorizados.
- Las áreas universitarias únicamente solicitarán a los usuarios que proporcionen la información absolutamente necesaria para obtener un determinado servicio.
- Las áreas universitarias deberán buscar, en la medida de lo posible, que los usuarios puedan aportar sus datos una sola vez, estando en condiciones de almacenarlos, recuperarlos y compartirlos en las fuentes autoritativas que la Universidad establezca.
- Las áreas universitarias serán responsables de que la información o datos manejados y almacenados por sus sistemas o aplicaciones para la prestación de servicios digitales cuenten y cumplan con un nivel de servicio comprometido entre ellas y, en su caso, con los usuarios.
- Los portales web y sistemas de información en línea que manejen información confidencial o sensible o que den un servicio crítico, deberán 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.

- Los usuarios que de forma individual tengan acceso a los sistemas y aplicaciones serán responsables de hacer un uso adecuado de las credenciales de acceso que les sean otorgadas.
- Se recomienda realizar pruebas de revisión de vulnerabilidades de sistemas y aplicaciones web cada 6 meses. En caso de algún proceso mayor de actualización o cambio de tecnología, es recomendable realizar de manera planificada las pruebas aplicables (funcionalidad, regresión, carga, entre otras) en ambientes de desarrollo habilitados para ello antes de efectuarla actualización o sustitución a un ambiente de producción.

e) Sobre los servicios en nube pública

- Se deberá privilegiar el alojamiento de la información en instalaciones de la Universidad y en territorio nacional.
- El proveedor debe indicar en el contrato de prestación de servicios que cuenta con mecanismos implementados y auditados para garantizar la disponibilidad, integridad y seguridad de la información, así como presentar evidencia de que cumple con el marco normativo nacional y universitario respecto al tratamiento de datos personales y a los aspectos que la normatividad mexicana aplicable establezca independientemente de la localización de los servidores.
- En el caso de utilizar servicios en la nube pública, las áreas universitarias deben considerar las siguientes medidas:
    - Que el proveedor manifieste que cuenta con medidas para proteger la disponibilidad, integridad y confidencialidad de la información de las áreas universitarias, tanto almacenada como en tránsito.
    - Tener el control sobre el acceso y gestión de los datos, procesos o servicios.
    - Establecer dentro del contrato que la propiedad de la información proporcionada por las áreas universitarias es propiedad de la UNAM y que no podrá utilizarse para cualquier fin distinto del convenido.
    - Solicitar medidas para aislar la información de las áreas universitarias, respecto a la de otros clientes con los que se comparten elementos de cómputo en común.
    - Seleccionar proveedores que de preferencia demuestren estar sujetos a revisiones o auditorías por terceros de reconocido prestigio, así como en cumplimiento de estándares de seguridad de la información certificados.

f) Sobre la seguridad de la información

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

- Las áreas universitarias establecerán sus planes de continuidad y recuperación de desastres considerando sus necesidades de almacenamiento y compartición de información.
- Se recomienda implementar registros detallados (bitácoras) que les permitan identificar y analizar situaciones, generales o específicas, dentro de la información manejada por los servicios digitales que proporcionan.
- Para acceder a datos personales, información sensible o confidencial desde otros lugares a través de Internet o redes públicas, se recomienda usar una conexión segura a través de una Red Privada Virtual (VPN por sus siglas en inglés) para que la información se transmita cifrada en bloques de 128 bits como mínimo y llaves de 2048 bits.
- 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.
- El acceso a la información almacenada y su compartición sólo podrán hacerlo las personas que hayan sido autorizadas por el responsable del resguardo de la información. Para ello, se sugiere establecer elementos de trazabilidad de las actividades realizadas.
- Para el intercambio seguro de la información confidencial o sensible entre las áreas universitarias y en su caso con terceros, debe existir la firma de acuerdos que consideren:
    - Responsabilidades de gestión para controlar y notificar la transmisión, el envío y recepción.
    - Niveles de control de acceso que se tendrán acorde a la clasificación de la información.
    - Procedimientos para asegurar la trazabilidad y no repudio.
    - Normas técnicas mínimas para el empaquetado y transmisión, uso de controles criptográficos y canales seguros de comunicación.
    - Mecanismos e interfaces para compartir o intercambiar información.
    - Suscribir acuerdos de confidencialidad y no divulgación, en los cuales se especifique la información a proteger y los usos permitidos de la misma, así como también las responsabilidades, los procesos para notificar y reportar la divulgación no autorizada o brechas de seguridad ocurridas, el derecho de auditar y de supervisar actividades que involucran información confidencial.
    - Responsabilidades y compromisos en caso de incidentes de seguridad, tales como pérdida de datos.

Capítulo II. Políticas para la compartición de información

a) Generales

- La información objeto de intercambio entre las áreas universitarias de la UNAM necesita ser apoyada a través de una solicitud formal por oficio o un acuerdo por escrito, así como de una carta de confidencialidad tratándose de información sensible o confidencial, entre las áreas universitarias.

- 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.
- Los acuerdos para el intercambio de información 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 para tal fin.

b) De las áreas responsables de información

- Se debe privilegiar que los mecanismos de compartición de información se realicen directamente con el área autoritativa o fuente primaria de los datos, siguiendo los mecanismos de compartición vigentes establecidos que resulten útiles para dar respuesta a la solución. Las áreas universitarias autoritativas establecerán las reglas y procedimientos para el acceso e intercambio de información que tengan bajo su resguardo.
- El responsable del tratamiento de la información del área universitaria deberá establecer medidas técnicas y organizativas que garanticen la seguridad de la información, sobre todo aquella considerada sensible o confidencial.
- El área responsable de la información supervisará que las medidas técnicas establecidas se realicen y puedan ser verificadas, por ejemplo: uso de *firewall*, copias se seguridad, uso de cifrado, sistemas actualizados, contraseñas seguras, entre otros.
- El área responsable de la información será la encargada de dar la autorización de las solicitudes para compartir información que cumplan con los requisitos establecidos y que generen beneficios justificados en el marco de los objetivos institucionales.
- El área responsable de la información será la encargada de identificar, evaluar y gestionar los riesgos de la información a su cargo e implementar los controles de seguridad necesarios para su tratamiento y protección.
- El área responsable de la información acordará en conjunto con el área solicitante los aspectos del intercambio de la información entre los cuales se encuentran: el formato a utilizar, mecanismos de seguridad y transmisión, cómo será utilizada la información, criterios de intercambio de información (técnicos, semánticos, jurídicos, organizativos, entre otros), formalización operativa y administrativa.
- Dentro del marco que rige el intercambio entre las áreas universitarias, se deberá establecer el correcto ciclo de los datos que se reciben, si éstos serán almacenados o no, bajo qué tipo de mecanismos se protegen en reposo y en tránsito, así como en su caso, el correcto procedimiento de eliminación o sanitización de los mismos.

c) De las áreas solicitantes de información

- El área solicitante deberá pedir por escrito la información que requiere le sea compartida y considerando responder a las siguientes preguntas:
    - ¿Quién está solicitando la información?
    - ¿Qué información se necesita?

- ¿Cuál será el uso que tendrá la información compartida, qué tratamiento se le dará y cuál es la justificación de la necesidad para compartirla?
- ¿Quién será responsable de su protección y resguardo dentro del área solicitante?
- ¿Cuál es la frecuencia que se está solicitando?

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

d) De la calidad de la información

- Las áreas universitarias deberán identificar aquellos datos que deben ser objeto de análisis para apoyar la toma de decisiones y así determinar las métricas que consideren adecuadas para las características de calidad de los datos (disponibilidad, portabilidad, recuperabilidad, accesibilidad, conformidad, confidencialidad, eficiencia, precisión, trazabilidad, exactitud, completitud, consistencia, credibilidad, vigencia, entendibilidad, es decir, el grado en el cual el dato tiene atributos que le permiten ser leído e interpretado por usuarios) o un subconjunto de ellas de acuerdo con las que consideren como más prioritarias.
- Se deberá evitar en la medida de lo posible la redundancia en los datos y proteger la integridad de los mismos.
- Es indispensable disminuir problemas de actualización de los datos en las tablas, por ejemplo, asegurando que los datos se actualicen en una sola tabla al no existir datos duplicados. Si se establecen restricciones de integridad referencial, esto contribuye a que no se generen inconsistencias en los datos al no permitir que se elimine o altere de forma indebida un dato que mantiene relación con otros.
- Las áreas universitarias deberán establecer los mecanismos que consideren adecuados para fortalecer la calidad de la información, entre los cuales se encuentran: validaciones de la captura de datos en los sistemas informáticos, capacitación en los procesos de captura de información, cambios en el diseño de la base de datos, mejora en los procesos de manejo de información, entre otros.
- Los datos tienen un ciclo de vida, por lo que es fundamental identificar hasta qué punto es veraz y vigente la información después de haber pasado un cierto tiempo, por lo que las áreas universitarias establecerán los tiempos y procedimientos para su actualización; o en su caso, de acuerdo con la naturaleza de los datos, determinar si el mecanismo de consulta en tiempo real resulta más conveniente.

e) De los mecanismos de compartición de información

- Las áreas universitarias, principalmente las autoritativas, deben buscar diseñar y mantener 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 que faciliten el intercambio de manera independiente a plataformas o lenguajes de programación.

- Se deberá firmar una carta de confidencialidad por parte del personal que recibirá la información relacionada a datos personales que mantenga la custodia y preserve los derechos ARCO del titular de la información.
- Los mecanismos de transferencia que sean usados deben proteger los intercambios de información de datos sensibles o confidenciales entre áreas universitarias a través de:
  - la identificación y registro del remitente y el receptor,
  - el uso del cifrado en los datos intercambiados,
  - 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.
- La entidad o dependencia responsable de la información verificará que el mecanismo utilizado para la transferencia se encuentre habilitado únicamente para las personas o áreas universitarias explícitamente autorizadas para ello, con el soporte de firmas y certificados digitales correspondientes.

f) De la transmisión de la información

- Todas las transferencias de información sensible o confidencial deberán considerar utilizar un canal de comunicación cifrado entre el cliente y el servidor.
- Para la transmisión de información no crítica o confidencial, se aconseja verificar la autenticidad del otro extremo de la comunicación, es decir, corroborar que quien hizo la solicitud sea quien dice ser, antes de proceder al intercambio de información. Además de realizar verificaciones sobre su integridad y confiabilidad al ser transmitida.
- 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*, *SSL/TLS*, Red Privada Virtual (VPN por sus siglas en inglés), túneles punto a punto, llaves públicas o privadas, entre otros.
- Todas las transacciones programadas deberán estar bajo el control exclusivo del área responsable de la información asegurando que únicamente los datos autorizados para cada operación específica podrán ser transferidos.
- En caso de que se comprometan las contraseñas de las cuentas para intercambio es aconsejable bloquearlas y cambiarlas, realizando un análisis de la causa que originó la brecha de seguridad.

g) Consideraciones de seguridad para la compartición de información

- 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*.
- Las medidas de seguridad que se implementen deben respaldar la confidencialidad, integridad y disponibilidad de la información.

- Las medidas de seguridad considerarán la resiliencia permanente de la verificación y evaluación de la eficacia de las medidas, la capacidad de restaurar los datos y el tratamiento en caso de incidente físico o técnico.
- Fuera de lo dispuesto en el marco de la transparencia universitaria y proactiva, las áreas universitarias deberán implementar las medidas de seguridad para evitar el uso de información personal identificable cuando se publique o divulgue información de manera abierta tanto en forma escrita como digital.
- 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.
- Las áreas universitarias deberán mantener 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 información

a) Generales

- Es fundamental identificar el propósito y fundamento que tendrá la información que se recabe para establecer las condiciones de almacenamiento que deben considerarse para cumplir con la normatividad universitaria. 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).
- Las áreas universitarias deberán sensibilizar a su personal en la protección de la información almacenada en sus equipos de cómputo, en las bases de datos y dispositivos, teniendo en cuenta la normatividad aplicable.
- Dado el valor de la información como activo universitario y propiedad de la institución, se deben establecer procedimientos de operación claros al interior de todas las áreas sustantivas de las actividades de la UNAM, para que existan respaldos periódicos de la datos de acuerdo con sus características para cumplir con principios de resguardo,

recuperación, continuidad y acceso determinados por la naturaleza, criticidad y variabilidad de la información.

b) Medios de almacenamiento

- Para la elección del medio de almacenamiento las áreas universitarias deberán considerar al menos lo siguiente:
  - 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.
  - 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.
- 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*.
- Las áreas universitarias contribuirán a concientizar a sus usuarios acerca de que la información almacenada sea relevante para las actividades de la Universidad para aprovechar mejor los recursos.

c) Conservación de la información

- La información almacenada en las áreas universitarias necesita conservarse durante los plazos estipulados en la normatividad vigente antes de poder ser eliminada, como pueden ser bajo la consideración del ciclo vital de los documentos señalado en los *Lineamientos generales para la organización, administración y conservación de los archivos de la UNAM*.
- 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.

d) Uso de servicios en la nube

- Las áreas universitarias que realicen almacenamiento en la nube deberán realizar acuerdos con el proveedor del servicio en la nube considerando que sólo 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.

e) Eliminación de la información y los medios de almacenamiento

- Para la eliminación de información sensible o confidencial se deberán usar métodos de borrado seguro en los medios electrónicos (soportes) que la contengan, que a su vez consideren la escritura de valores aleatorios y al menos 7 sobre-escrituras, para evitar su recuperación por personas no autorizadas.
- En el caso de desecho de equipos de cómputo y medios de almacenamiento por obsolescencia o daño se debe considerar la destrucción física de soportes no robustos como *CD/DVD* o papel, para lo cual se puede utilizar una destructora de papel (o de soportes magnéticos). Para los discos duros o cintas se puede optar por el borrado seguro, la desmagnetización o la destrucción física. De igual forma se puede recurrir a empresas especializadas en la destrucción certificada de información, gestionando la entrega de evidencia de la destrucción.
- Para el procedimiento de borrado seguro de la información de los equipos de cómputo que vayan a ser transferidos o dados de baja se observará lo estipulado en la *Circular DGTIC/003/2017 - Procedimiento para el borrado de información*.

f) Consideraciones generales de seguridad en el almacenamiento

- Las áreas universitarias deberán establecer y documentar sus planes de respaldos de seguridad de la información. En cumplimiento de este punto, se tendrán que identificar los datos que necesitan ser resguardados, establecer la frecuencia y tipo de respaldo a realizar, elegir los medios de almacenamiento del respaldo y verificar su restauración.
- Las áreas universitarias establecerán las pautas acerca del almacenamiento en bases de datos y sistemas de archivos, considerando al menos los aspectos siguientes: tipo de información almacenada permitida, estructura de directorios, niveles de acceso, personas encargadas del respaldo, actualización y eliminación de la misma.
- Las áreas establecerán las pautas para el almacenamiento local de la información en sus equipos de escritorio y portátiles de los trabajadores universitarios adscritos a ellas, considerando al menos los aspectos siguientes:
    - tipo de información permitida,
    - pautas para la generación de estructuras de directorios en los discos duros,
    - tiempo de conservación de los archivos en este medio,
    - mecanismos de protección a emplear, como por ejemplo: uso de antivirus o antimalware, soluciones de protección de datos (cifrado de información, uso de un esquema de RAID, respaldos, entre otros), por mencionar algunos, y
    - restricciones en la instalación de software y descarga de archivos que pudieran afectar a la información almacenada.

Capítulo IV. Transitorios

- Cualquier asunto no contemplado en los presentes lineamientos será analizado y resuelto por el Consejo Asesor de Tecnologías de la Información y Comunicaciones.
- La interpretación de los presentes lineamientos 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: 05 de abril 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: 20 de octubre de 2021. URL: https://www.red-tic.unam.mx/content/circular-dgtic0032017-procedimiento-para-el-borrado-seguro-de-informaci%C3%B3n-de-la-unam
- 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: 05 de abril de 2022. URL: https://dof.gob.mx/nota_detalle.php?codigo=5628885&fecha=06/09/2021
- El cifrado Web (SSL/TSL). **Revista de Seguridad. CERT-UNAM**. Número 31, mayo 2018. URL: https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls
- INAI (2016). **Guía para el borrado seguro de datos personales**. Recuperado: 28 de junio de 2021. URL: http://transparencia.inaes.gob.mx/doctos/pdf/transparencia/Guias/Gu%C3%ADa_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: 05 de abril de 2022. 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: 05 de abril de 2022. 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**. Abril de 2021. https://home.inai.org.mx/wp-content/uploads/AmenazasDP.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
- UNAM (2016). **Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México**. Recuperado: 9 de septiembre de 2021. URL:

  http://www.transparencia.unam.mx/files/documentos/reglamento_transparencia2016.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 (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
- UNAM (2021). **Glosario de términos de TIC**. Red-TIC, UNAM. Recuperado: 05 de abril de 2022. URL: https://www.red- tic.unam.mx/content/glosario-de-terminos-de-tic
- UNAM (2021). **Recomendaciones para el almacenamiento de información**. Red-TIC, UNAM. Recuperado: 05 de abril 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: 05 de abril de 2022. URL: https://www.red-tic.unam.mx/content/recomendaciones-de-comparticion-de- informacion

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

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