UNAM

RED·TIC

Red de Responsables TIC

U N A M

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

Segunda versión

Noviembre de 2022

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 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 del servicio.

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.

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. Es la 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. 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).

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 mantenerla actualizada y validada a partir de 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, y que 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 éstos 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 describen 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.

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.

Portabilidad de datos. Capacidad para transferir fácilmente datos de un sistema a otro sin tener que volver a ingresarlos.

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.

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 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)/ TLS (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" (Odín, 2011).

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

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 la protección de datos personales.

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

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.

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

- Participar de manera proactiva en actividades de compartición de información de acuerdo con estos lineamientos, en cumplimiento de sus funciones de gestión y operación de las TIC; así como coordinar efectivamente la realización de estas actividades al interior de su entidad o dependencia, 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.
- Documentar y dar seguimiento a los procedimientos establecidos y de mejora en el marco de aplicación de las presentes políticas.
- Identificar los activos de información administrados por su área universitaria que sean útiles para optimizar procesos en la Universidad, a fin de promover su intercambio a través de servicios que puedan consumirse por otros sistemas de información.
- 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.

c) Del personal de las TIC y personal universitario que hace uso de 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 de TIC, sus propuestas de mejora respecto al almacenamiento de datos y las oportunidades para mejorar la gestión y aprovechamiento de la información, de acuerdo a su clasificación jurídica (pública, confidencial y/o sensible).

Capítulo I. Lineamientos. Disposiciones generales

a) Sobre la información

- Toda información publicada por la UNAM debe cumplir con los siguientes 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.
- La información, como activo de la universidad, debe estar disponible en el momento en que sea necesario, respetando las medidas de seguridad y confidencialidad correspondientes a 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 adecuadamente de acuerdo con sus atribuciones.
    - 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.
    - Cuidar la calidad de los datos que generan o recopilan.
    - Cerciorarse del almacenamiento confiable y seguro de los datos.
    - 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.
- 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 a su clasificación y a la normatividad universitaria y federal.
- Toda información almacenada digitalmente, transmitida por correo o por medios electrónicos debe protegerse de acuerdo con 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 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*, 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.
- 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 garantizar la soberanía de la Universidad sobre dichos activos, sin perjuicio de su integridad y acceso a su contenido.

c) Sobre la neutralidad tecnológica y la interoperabilidad

- En el diseño de soluciones tecnológicas debe buscarse 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 origen seleccionada.
- Los estándares seleccionados deben ser abiertos, ser referentes internacionales, estar vigentes y contar con soporte amplio de una organización o comunidad.
- Deben privilegiarse plataformas tecnológicas que, en cuanto a sistemas operativos, bases de datos y arquitecturas orientadas a servicios (como por ejemplo, interfaces de programación de aplicaciones APIs), faciliten la compartición y almacenamiento seguro de la información entre las áreas universitarias.
- Debe privilegiarse el almacenamiento e intercambio de información en protocolos y formatos basados en estándares abiertos.

d) Sobre las fuentes de información

- Los sistemas universitarios deben privilegiar la obtención de información por medio de fuentes de datos autoritativas, por ejemplo, obtener los datos como el nombre de los trabajadores y su área de adscripción de la Dirección General de Personal.
- La información o datos almacenados de forma electrónica en la universidad deben provenir de fuentes confiables, es decir, de aquellas que cuenten con mecanismos que aseguren que la información que será transmitida y almacenada en las áreas universitarias es válida.
- Las áreas universitarias deben considerar 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.

e) Sobre la calidad de los datos universitarios

- Las áreas universitarias deben identificar los datos que puedan ser objeto de análisis para la toma de decisiones en la universidad y determinar las 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.
- Las áreas universitarias deben establecer controles y programar revisiones de los datos que ayuden a evitar problemas en la calidad de datos 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.
- Los Responsables TIC deben contemplar la calidad de los datos desde el diseño de la base

de datos 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.

- Las áreas universitarias deben corroborar que los sistemas bajo su responsabilidad cuentan con los controles y mecanismos necesarios para la validación de los datos que se almacenan.
- Cada área universitaria es responsable de analizar la calidad de sus datos y definir su proceso de limpieza de datos, identificando los que pueden ser limpiados, los que no pueden serlo y los que deben ser eliminados.
- Las áreas universitarias deben observar respecto a la calidad de datos, aspectos como:
    - Cumplir con la normatividad universitaria de transparencia,
    - Mantener la confidencialidad de los datos de accesos no autorizados,
    - Establecer medidas que permitan que los datos almacenados cumplan con aspectos como que no deban ser modificados no puedan ser borrados o alterados,
    - Que la integridad de los datos almacenados o compartidos pueda ser verificada,
    - Que los datos almacenados sean conservados durante los periodos legales estipulados, entre otros.

f) Sobre los sistemas de información

- 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.
- Los usuarios que tengan acceso de forma individual a sistemas y aplicaciones son responsables de usar adecuadamente las credenciales de acceso que les son 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. 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 son responsables de que los datos o información contenidos en sus sistemas o aplicaciones dirigidos a la prestación de servicios digitales, permanezcan completos e inalterados o que en su caso sólo sean modificados por los usuarios y mecanismos autorizados.
- Las áreas universitarias únicamente deben solicitar a los usuarios la información absolutamente necesaria para obtener un determinado servicio.
- Las áreas universitarias deberán buscar, en la medida de lo posible, que los usuarios sólo tengan que aportar 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.

- Las áreas universitarias son responsables de que los datos e información que manejan y almacenan 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.

g) Sobre la integración de las bases de datos

- Las áreas universitarias deben definir los procesos necesarios para promover 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.
- Se deberán identificar los datos relevantes de los procesos universitarios que realmente aportan valor y documentar los datos describiéndolos a nivel metadato. De no existir esta documentación se deberá crearla y obtener su aprobación por parte los responsables de las áreas involucradas y titulares.
- Dentro de las áreas universitarias se deberá promover la eliminación o disminución de silos de datos, con la intención de:
    - Buscar que los usuarios tengan acceso a datos de valor en menor tiempo.
    - Facilitar las tareas de conexión a los datos.
    - Entender el flujo de información y contribuir a la mejora de los procesos de consulta, intercambio y uso de datos.
    - Eliminar o disminuir la duplicidad de trabajo en el registro de datos, en diferentes sistemas y procesos.
    - Maximizar el valor de los datos, aprovechar la variedad de datos existentes y, como resultado, contribuir a la mejora de la toma de decisiones.
    - Permitir la compartición de información entre sistemas.
- Se debe fomentar que en las bases de datos se sigan reglas de semántica y sintaxis que permitan generar una vista unificada y contribuyan a la compartición entre diferentes fuentes de datos, para la gestión de los procesos y servicios universitarios. Considerando prácticas como:
    - Identificar, entender, documentar, catalogar y, en su caso, reclasificar los datos de interés (los datos relevantes para el área universitaria y la UNAM) almacenados en las bases de datos.
    - Establecer criterios de calidad de los datos, de acuerdo a su interés u objetivo.
    - Establecer prácticas para la compartición de datos, que incluyan la limpieza de datos dispares almacenados en diferentes bases de datos y combinarlos.
    - Establecer una vista de datos unificada que permita publicar los datos y poderlos presentar de forma consistente con el fin de facilitar su consumo por parte de los usuarios finales.
    - Planear los procesos de unificación que considere la formación de una base sólida de datos que sea útil a corto, mediano y largo plazo, para el área universitaria y la UNAM.
    - Si es el caso, utilizar catálogos institucionales, nacionales o internacionales para normalizar datos.

h) Sobre los servicios en nube pública y privada

- Debe privilegiarse el alojamiento de información en instalaciones de la universidad y en territorio nacional.
- Verificar si la normatividad vigente permite el uso de nube pública para el fin deseado, pues en algunos casos no es posible utilizar un modelo de despliegue de nube pública debido a las restricciones que refieren las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en posesión de la universidad, en el artículo 21 se establece que "para los sistemas que realicen el tratamiento automatizado de datos personales sólo está permitido el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información" (UNAM, 2020).
- Antes de contratar servicios en nube, las áreas universitarias deben analizar si sus aplicaciones y datos son susceptibles de migrar y adaptarse a este tipo de servicios, en términos de costos, beneficios, tecnologías, tiempos y cumplimiento normativo.
- Los servicios en nube de un proveedor deben permitir la interoperabilidad con otros servicios públicos o privados de manera segura, así como el intercambio de información entre las interfaces o APIs (por sus siglas en inglés, Interfaz de Programación de Aplicaciones) en cualquier extremo.
- Los servicios en nube de un proveedor deben tener capacidad para la migración de aplicaciones y datos del área universitaria a otros servicios en nube o de manera local.
- Respecto a los datos que se utilizarán en un servicio en 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 sea acordes a las necesidades y a la normatividad universitaria y federal.
- El proveedor de los servicios en nube deberá implementar la funcionalidad apropiada para el servicio de almacenamiento de cómputo en la nube 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 almacenados en la nube en sus productos.
- Para utilizar servicios en la nube pública, las áreas universitarias deben considerar las siguientes medidas:
    - 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 datos como en su almacenamiento.
    - El proveedor debe presentar evidencia de que cumple con el marco normativo nacional y universitario respecto al tratamiento de datos personales y a los aspectos que la misma establezca independientemente de la localización de los servidores.
    - Las áreas universitarias deben tener el control sobre el acceso y gestión de los datos, procesos y servicios.
    - El contrato del servicio debe establecer 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.
- Preferentemente 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.
- Establecer por escrito un acuerdo de nivel de servicio (SLA, por sus siglas en inglés) sobre las características y el rendimiento del servicio en la nube que el proveedor se compromete a cumplir, estableciendo métricas y herramientas que permitan la verificación del cumplimiento, por parte del área universitaria.

i) Sobre la seguridad de la información

- Las áreas universitarias deben 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 de recuperación en caso de desastres, considerando sus necesidades de almacenamiento y compartición de información.
- 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.
- De igual forma deben establecer los mecanismos de seguridad necesarios para proteger los datos personales, sensibles y de alto valor cuando se transmitan entre sistemas de información y durante su almacenamiento.
- 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.
  - Procedimientos para la remoción de información intercambiada en caso de que esta constituya una violación a la normatividad o legislación vigente.
  - 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.
- 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 notificar y reportar la divulgación no autorizada y las brechas de seguridad ocurridas, así como el derecho de auditar y 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 cuyas características la definan como delicada, privada o de tratamiento especial, necesita ser apoyada a través de una solicitud formal por oficio o un acuerdo por escrito entre las áreas universitarias, así como de una carta de confidencialidad tratándose de información sensible o confidencial. 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.
- La información en acceso abierto objeto de intercambio entre áreas internas o externas a la Universidad deberá compartirse siguiendo la normatividad vigente, respetando los derechos de autor y de propiedad intelectual, estableciendo licencias de uso y utilizando protocolos y estándares abiertos.

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 que resulten útiles para dar respuesta a la solución. Las áreas universitarias autoritativas deben establecer 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 debe 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 debe supervisar que las medidas técnicas establecidas, como el uso de firewall, copias se seguridad, uso de cifrado, sistemas actualizados y contraseñas seguras, se realicen y puedan ser verificadas.
- El área responsable de la información es la encargada 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.

- El área responsable de la información es 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 debe 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, la utilización 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.
- Entre las áreas universitarias que intercambian información, se debe establecer el correcto ciclo de los datos que se reciben, si estos 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 sensible, crítica o confidencial

- A excepción de los datos abiertos o para la información en acceso abierto las áreas solicitantes deberán observar lo siguiente:
  - 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, conforme a los acuerdos establecidos con el área responsable y 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

- En el contexto de almacenamiento, de acuerdo con la norma ISO/IEC 27040:2015, la disponibilidad de datos se refiere a que tan accesible es un dato cuando se encuentra almacenado en alguna forma, usualmente refiriéndose a almacenes remotos de datos o medios de almacenamiento externos.
- Las dimensiones de confidencialidad, disponibilidad e integridad de la calidad de datos se pueden fortalecer mediante medidas de seguridad que se pueden enfocar en:
  - Protección de la administración del almacenamiento (operaciones e interfaces).
  - Aseguramiento de una adecuada administración de credenciales.
  - Protección de recursos de respaldo de datos y recuperación.

- Protección de los datos en movimiento y almacenados.
- Soporte para la recuperación de desastres y continuidad del negocio.
- Limpieza y desecho adecuados de los datos y medios de almacenamiento.
- Aseguramiento del movimiento de datos autónomo, entre otros (ISO, 2015).

- 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 deben 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 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.

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 ARCOP 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.
- El área responsable de la información debe verificar 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 que no es crítica o confidencial, se aconseja verificar la autenticidad del otro extremo de la comunicación, es decir, corroborar que quien hace 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 mecanismos.
- 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.
- 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.
- 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.
- 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 deben 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

- Para establecer las condiciones de almacenamiento de información, de conformidad con la normatividad universitaria, es indispensable identificar el propósito y fundamento que ésta 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.
  - Cómo se puede acceder a los datos.
  - El formato de la información que será almacenada.
  - El 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 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.
- Dado el valor de la información como activo universitario y propiedad de la institución, deben establecerse procedimientos de operación claros en todas las áreas sustantivas de la actividad de la UNAM, para contar con respaldos periódicos de los datos que sean adecuados y cumplir con los 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 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 sugiere llevar a cabo revisiones semestrales de seguridad, a cargo de personal especializado de la propia área universitaria o de otra.
- Las áreas universitarias deben contribuir a concientizar a sus usuarios respecto a que la información almacenada sea relevante para las actividades de la universidad con el fin de 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* y en el *Catálogo de disposición documental*.
- 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.
- Los sistemas de información para el tratamiento automatizado de datos personales que estén alojados en equipos de la UNAM o en servicios de nube privada, deben 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*
- Los sistemas de información para el tratamiento automatizado de datos personales sólo pueden utilizar servicios de nubes públicas para el resguardo de archivos cifrados que contengan respaldos de la información conforme al artículo 21 de la misma norma (UNAM, 2020).

e) Eliminación de la información y los medios de almacenamiento

- Para la eliminación de información sensible o confidencial deben usarse métodos de borrado seguro en los medios electrónicos que la contengan, que consideren la escritura de valores aleatorios y al menos siete sobreescrituras, para evitar que sean recuperados

por personas no autorizadas.

- En el caso de desecho de equipos de cómputo y medios de almacenamiento por obsolescencia o daño, debe considerarse la destrucción física de soportes no robustos como CD, DVD o papel, para lo cual puede utilizarse una destructora de soportes magnéticos o papel, y para discos duros o cintas puede optarse por el borrado seguro, la desmagnetización o la destrucción física. Se puede recurrir a empresas especializadas en la destrucción certificada de información que entreguen 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*.
- Los responsables TIC deben establecer un procedimiento donde se registre y realicé la verificación del borrado seguro, y quede definida la responsabilidad de quien lo realizó y verificó.

f) Consideraciones generales de seguridad en el almacenamiento

- Las áreas universitarias deben establecer y documentar sus planes de respaldos de seguridad de la información, identificando los datos que necesitan ser resguardados, estableciendo el tipo de respaldo a realizar y su frecuencia, eligiendo los medios de almacenamiento del respaldo y verificando su restauración.
- Las áreas universitarias deben establecer las pautas de almacenamiento en bases de datos y sistemas de archivos, considerando al menos los siguientes aspectos: tipo de información permitida para almacenar, estructura de directorios, niveles de acceso, personas encargadas del respaldo, así como actualización y eliminación.
- Los responsables de los sistemas de almacenamiento e infraestructura asociada deben considerar 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 de configuración maliciosos o accidentales, ataques de malware, así como de tratamiento o borrado inadecuado después de su uso.
- 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 y revisar regularmente las excepciones, fallas y eventos de seguridad de la información de los sistemas y dispositivos de almacenamiento a su cargo.
- Deben establecerse controles para proteger los sistemas y dispositivos de almacenamiento de cambios no autorizados, borrado o desactivación de registros de eventos.
- 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, mal uso, alteración, eliminación o destrucción.
- Las áreas universitarias establecerán las reglas para el almacenamiento local de la información en sus equipos de escritorio y portátiles, que utilizan los trabajadores universitarios adscritos a ellas, considerando al menos los siguientes aspectos:
    - 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.
- Restricciones en la instalación de software y descarga de archivos que pudieran afectar a la información almacenada.

g) Sobre el uso de Bóvedas Digitales

- Con el fin de preservar digitalmente a largo plazo objetos digitales pueden emplearse servicios como el de bóveda digital, los cuales deben garantizar que los documentos almacenados conserven sus las características y atributos, así como la autenticidad, fiabilidad, integridad, disponibilidad, custodia y cumplimiento normativo. En el caso de la universidad, la DGTIC prestará el servicio de Bóveda Digital UNAM a las áreas universitarias que así lo requieran.
- Las áreas universitarias son responsables de determinar el tipo de información que guardarán en este tipo de servicio, conforme a la normatividad aplicable, y definir los metadatos para su organización e indexación, que permitan la recuperación de los documentos incorporados.
- Los responsables TIC deben dimensionar la capacidad de almacenamiento que requieren y definir qué usuarios tendrán acceso al servicio de Bóveda Digital UNAM.
- Las áreas universitarias que soliciten utilizar la Bóveda Digital UNAM deben considerar que el motivo de la solicitud esté alineado con el propósito de preservación a largo plazo y fuera de línea con el que fue creada la bóveda.
- La solicitud deberá cumplir con los parámetros necesarios para solicitar el servicio, contribuir al cumplimiento de los objetivos de la UNAM, así como del área solicitante tomado en cuenta los aspectos siguientes:
  - Los datos almacenados en Bóveda Digital UNAM deben ser propiedad de la universidad y deben ser considerados críticos por el área universitaria, con un nivel de riesgo tal que su merma, pérdida o alteración tuvieran efectos negativos en la operación del área universitaria, de los proyectos de docencia, investigación y servicios centrales, por lo que se excluyen los datos propiedad de miembros de la comunidad universitaria y terceros.
  - Los datos almacenados en Bóveda Digital UNAM no deben ser transaccionales, por lo que quedan excluidas 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 inferior a un año.
  - Quedarán excluidos los respaldos de equipos de escritorio, portátiles y datos de cuentas de correo (buzón, contactos, documentos adjuntos), entre otros.
- 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 recursos humanos en la gestión de la información

a) Reforzamiento de las capacidades y habilidades del personal involucrado

- Las áreas universitarias deben capacitar al personal que captura información en los sistemas institucionales, respecto a su uso y al registro de datos; además deben comunicarle claramente sus responsabilidades en la gestión de la información.
- Debe capacitarse 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.

b) Difusión de buenas prácticas entre el personal

- Deben promoverse prácticas que contribuyan a fortalecer la calidad de la información, los sistemas y la seguridad para la compartición de información entre áreas universitarias.
- Deben darse a conocer entre el personal de las áreas universitarias, buenas prácticas relacionadas con el almacenamiento de información, tales como: buenas prácticas de seguridad, uso, conservación y destrucción de información almacenada, medios de almacenamiento, así como prácticas que cada área universitaria considere relevantes.

Capítulo V. Transitorios

- Cualquier asunto no contemplado en los presentes lineamientos y políticas 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: 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 datos personales**. Recuperado: 31 de agosto de 2022. URL: https://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: 31 de agosto 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: 31 de agosto 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**. Recuperado: 31 de agosto de 2022. URL: https://home.inai.org.mx/wp-content/uploads/AmenazasDP.pdf

[1] El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

- 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
- Instituto Nacional de Ciberseguridad (2016). **Guía de almacenamiento seguro de la información**. Recuperado: 31 de agosto de 2022. URL: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad.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)**.
- 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

- 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 (2021). **Glosario de términos de TIC**. Red-TIC, UNAM. Recuperado: 31 de agosto 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: 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 nivel de servicio de la Bóveda Digital UNAM**. Red-TIC, UNAM. Recuperado: 31 de agosto de 2022. URL: https://www.red-tic.unam.mx/content/politica-acuerdo-nivel-servicio-boveda-digital

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
Ana Pérez Arteaga, IIMAS
Alberto González Guízar, DGTIC

Revisión

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