UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL
Dirección General de Cómputo y de
Tecnologías de Información y Comunicación

DGTIC

Asunto: Servicios de almacenamiento en nube pública
y la protección de datos personales

Titulares de las Secretarías, Coordinaciones, Direcciones de Escuelas, Facultades, Institutos, Centros, Programas y Direcciones Generales

Los servicios de almacenamiento en nube pública están ampliamente extendidos en varios ámbitos del quehacer universitario, estos se ofrecen y gestionan por terceros que también son responsables de la seguridad y protección de la información, en contraste con los servicios de almacenamiento en nube privada, como los proporcionados por el Centro de Datos de la UNAM, que utiliza recursos institucionales, lo que permite un control técnico y el cumplimiento de políticas internas.

El uso de los servicios de almacenamiento en nube pública conlleva riesgos potenciales tales como brechas de seguridad, términos y condiciones insuficientes o incompatibles con la normatividad universitaria, acceso no autorizado a información institucional, delimitación de responsabilidades insuficientes, acuerdos de servicio con vacíos en cuanto a continuidad, fallas o tiempos, datos personales alojados en infraestructura fuera del país, controles de autenticación no ideales, complicaciones en la recuperación de credenciales de acceso, inexistencia de métodos de cifrado o métodos incompletos, controles de acceso de baja complejidad, infraestructura paralela a la institucional no reportada, incumplimiento del modelo de seguridad compartida, potencial pérdida de control en recursos compartidos, riesgo de sustracción de información y robo de datos por acceso no autorizado.

Por lo anteriormente expuesto se establecen recomendaciones para reducir riesgos en este tipo de servicios, como son el cifrado de datos personales, que su uso sea para el resguardo de respaldos, accesos verificados por mas de un responsable, no almacenar o ejecutar elementos que puedan identificarse como dato personal o dato personal sensible, preponderantemente buscar la utilización de servicios similares provistos por el Centro de Datos de la UNAM y finalmente observar las medidas y recomendaciones adicionales para la protección de datos personales aplicables a los servicios provistos por el propio Centro de Datos de la UNAM.

Para contar con mayores elementos al respecto, se anexa al presente la **CIRCULAR 03/2022**

Atentamente
"Por Mi Raza Hablará el Espíritu"
Ciudad Universitaria, CdMx, 24 de febrero de 2022.
Director General

Dr. Héctor Benítez Pérez

c.c.p. Dr. Enrique Graue Wiechers, Rector de la UNAM.
Dr. Leonardo Lomelí Vanegas, Secretario General de la UNAM.
Dra. Patricia Dávila Aranda, Secretaria de Desarrollo Institucional de la UNAM
Dr. Alfredo Sánchez Castañeda, Abogado General y Presidente del Comité de Transparencia de la UNAM.
Dr. José Meljem Moctezuma, Titular de la Unidad de Transparencia de la UNAM.
Responsables de Seguridad de Datos Personales de cada área universitaria de la UNAM.
Responsables de TIC de cada área universitaria de la UNAM.

Circular: 03/2022

Asunto: Servicios de almacenamiento en nube pública y la protección de datos personales

A los Titulares de las Secretarías, Coordinaciones, Direcciones de Escuelas, Facultades, Institutos, Centros, Programas y Direcciones Generales

Los servicios de almacenamiento en nube pública se han extendido a varios ámbitos del quehacer universitario, por lo que reviste particular importancia identificar los potenciales riesgos que su uso conlleva, así como conocer las medidas recomendadas que se deben implementar, en especial cuando se resguardan en esos servicios datos personales en posesión de la UNAM.

Cabe mencionar que los servicios de almacenamiento en la nube pública son ofrecidos por terceros a través de infraestructura y recursos cuya propiedad es del proveedor, quién también es responsable de la seguridad y protección de la información. En contraste, los servicios de almacenamiento en nube privada como es el caso de los proporcionados por el Centro de Datos de la UNAM en DGTIC - utilizan recursos institucionales, lo que permite un mayor control técnico y el cumplimiento de políticas internas.

Algunos de los riesgos y vulnerabilidades relacionados con la protección de datos personales y que se deben atender cuando se utiliza almacenamiento en servicios de nube pública son:

I. Brechas de seguridad por desconocimiento de las opciones de configuración en el servicio.

II. Términos y condiciones del servicio que resulten insuficientes o incompatibles con la normatividad universitaria.

III. Potencial acceso a información institucional bajo el argumento de "mejora en el servicio".

IV. Delimitación insuficiente de las responsabilidades tanto para el cliente (persona titular del área universitaria o responsable de TIC) como para el proveedor de servicios.

V. Contratos de acuerdos de servicio (Service Level Agreement o SLA) que no aseguren la calidad y continuidad del almacenamiento, la recuperación ante fallas o el tiempo de respuesta en caso de incidentes.

VI. Resguardo de los datos personales en infraestructura informática alojada fuera del país.

VII. Controles de autenticación simples o no acordes a estándares y mejores prácticas.

VIII. Robo de sesiones o credenciales de acceso. Acciones complicadas para su recuperación que retrasen la operación o el correcto funcionamiento de sistemas institucionales.

IX. Métodos ausentes o incompletos para el cifrado en tiempo real de la información o en procesos por lotes.

X. Controles de acceso de baja complejidad que facilitan el robo de identidad del cliente con acceso a la cuenta de servicios de almacenamiento en la nube pública.

XI. Aparición de tecnología de información invisible (infraestructura paralela a la institucional que no es reportada a las áreas de control o gobernanza de TIC).

XII. Incumplimiento del modelo de seguridad compartida, siendo generalmente el proveedor del servicio el responsable de la seguridad de la nube y la institución de los datos y aplicaciones.

XIII. Dependencia de un solo recurso para el almacenamiento de la información y potencial pérdida de control en recursos compartidos.

XIV. Información sustraída por haber sido publicada "en plano", esto es: sin ningún tipo de protección por contraseña, clave o cifrado.

XV. Robo de datos por acceso no autorizado de personas malintencionadas (hackers).

Lo antes expuesto no representa una prohibición para la contratación de servicios de almacenamiento en nube pública con proveedores externos. Sin embargo, es fundamental conocer los potenciales riesgos en la seguridad de la información que en ellos se almacena. Las principales recomendaciones para reducir esas vulnerabilidades son:

I. Ningún dato personal podrá estar en infraestructura de nube pública de forma no cifrada.

II. Solo se permite el uso de servicios de almacenamiento en la nube pública para el resguardo de respaldos integrales o incrementales de información que contenga datos personales y que estén cifrados.

III. El área universitaria deberá llevar a cabo las medidas pertinentes para que más de un responsable, plenamente identificado, tenga el acceso verificado al respaldo cifrado.

IV. No almacenar o ejecutar en infraestructura de cómputo en la nube de proveedores externos los sistemas de información, de archivos, bases de datos y todo tipo de contenido digital (textos, imágenes, audios, videos, datos biométricos, registros, aplicaciones, programas, etc.) que puedan identificarse como dato personal o dato personal sensible.

V. En el caso de que el área universitaria requiera capacidad de almacenamiento y/o procesamiento de información asociada al tratamiento de datos personales, la DGTIC podrá proporcionar los servicios similares a los de los proveedores de nube pública, por medio de la infraestructura del Centro de Datos que sustenta la operación de la Nube UNAM con los siguientes servicios:

   a. Infraestructura como servicio. Dotación de servidores virtuales para ejecución de sistemas de información que den tratamiento a datos personales.
   b. Respaldos como servicio. Capacidad de resguardo, en equipos propiedad de la UNAM, de todo conjunto de datos personales a los que el área dé tratamiento con sus sistemas e infraestructura local o la que le haya sido asignada por la DGTIC como parte del servicio de Nube UNAM.
   c. Bóveda digital. Resguardo de datos a largo plazo (5 o más años) que no requiere consulta o cambios constantes, pero que por sus características es relevante para el área universitaria su preservación por un periodo considerable de tiempo.

VI. La utilización de los servicios descritos de Nube UNAM, así como el uso de cualquier infraestructura local del área universitaria, requieren de las siguientes medidas y recomendaciones adicionales para la protección de datos personales a los que dé tratamiento la institución:

   a. Protección contra vulnerabilidades. El área universitaria deberá asegurar la información que tenga en su infraestructura o en el Centro de Datos de la UNAM en DGTIC, por medio de un análisis de potenciales vulnerabilidades, al cual podrá apoyarle la Coordinación de Seguridad de la Información UNAM CERT de la DGTIC.
   b. Respaldos. Deberán programarse respaldos periódicos de los sistemas y acervos, ya sea en infraestructura local o con el apoyo de los Respaldos como Servicio en el Centro de Datos.
   c. Acceso y control. Es fundamental que el área universitaria tenga plenamente identificados los usuarios, roles y niveles de permisos de acceso en sus sistemas de información.

d. Actualizaciones. Todo sistema o acervo que contenga o dé tratamiento a datos personales, deberá actualizarse periódicamente, en función de las necesidades del área universitaria y para garantizar el continuo cumplimiento de lo estipulado en los lineamentos y normas para la protección de datos personales.
e. Supervisión. El área universitaria debe designar a un responsable de seguridad de datos personales para verificar su correcta implementación y configuración.
f. Análisis de riesgos. Como parte del cumplimiento de las normas complementarias, el área universitaria deberá realizar un análisis continuo de las amenazas y riesgos a los que estén sujetos sus sistemas de información, y deberá establecer los procesos para mitigar esos riesgos a partir del análisis de brecha respectivo; y
g. Protocolos. El área universitaria deberá establecer y aplicar el procedimiento en caso que se presente la vulneración de datos personales, ya sea que los datos estén en su infraestructura o en el Centro de Datos de la UNAM en DGTIC.

Finalmente, en caso de que desee utilizar los servicios de nube privada que ofrece la DGTIC-UNAM, podrán ser solicitados por el responsable de TIC del área universitaria a través del Sistema de Gestión de ServiciosTIC (www.gtic.unam.mx) o vía correo electrónico a la cuenta sistemas.tic@unam.mx

Ciudad Universitaria, CdMx, 24 de febrero de 2022