Anáhuac México

Lineamientos para la Gestión de Riesgos de Terceros en Privacidad

Comisión de Protección de Datos Personales

<< Volver al inicio

La Universidad Anáhuac México, inspirada en una genuina conciencia social, tiene un firme compromiso con la privacidad y la protección de datos personales, derechos reconocidos en la Constitución Política de los Estados Unidos Mexicanos.

Por esta razón, la información de índole personal que se le proporciona recibe el debido tratamiento, de conformidad con lo dispuesto en la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, el Reglamento del citado ordenamiento legal y demás normativa aplicable.

En este sentido, la presente regulación institucional abona al cumplimiento de los principios y deberes contenidos en las leyes antes señaladas, así como a las buenas prácticas en materia de protección de datos personales.

Esta regulación es emita por la Comisión de Protección de Datos Personales, órgano colegiado que —instaurado el 17 de agosto de 2020— establece las bases mínimas y condiciones homogéneas respecto a la privacidad y protección de datos personales al interior de la Universidad Anáhuac México.

Este documento fue aprobado el 3 de octubre de 2022.
Última actualización: 3 de octubre de 2022.

<< Volver al inicio

CONTENIDO

<< Volver al inicio

INTRODUCCIÓN

De conformidad con los artículos 6 y 14 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (LFPDPPP), así como por el artículo 47 del Reglamento de la mencionada Ley, el responsable, al asumir el nivel más alto de responsabilidad, debe cumplir y demostrar la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquellos que hayan comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano.

En este contexto, dado que el entorno legislativo es cada vez más profuso y el impacto por el incumplimiento de regulación en materia de protección de datos personales más estricto que nunca, resulta necesario contar, al interior de la Universidad Anáhuac México, con marcos de control que permitan también conocer, elegir, contratar y controlar a los proveedores en materia de privacidad, y ello con carácter previo a la puesta en marcha del correspondiente tratamiento o prestación del servicio.

Es interés del responsable, vigilar y velar por la debida observancia de los principios que rigen el derecho a la protección de los datos personales, referidos en la Ley correspondiente y su Reglamento, así como establecer una serie de reglas mínimas, necesarias y uniformes en torno a la gestión de riesgos de terceros en privacidad.

Considerando lo anterior, se expiden los siguientes: *Lineamientos para la Gestión de Riesgos de Terceros en Privacidad*.

DISPOSICIONES GENERALES

Primero. Los presentes Lineamientos establecen las pautas generales que permitan al responsable concretar e implementar el principio de responsabilidad consagrado en el artículo 47 del Reglamento de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, especialmente a la hora de

elegir a sus proveedores (encargados y/o subencargados), así como en la identificación de cada fase de intervención que se tenga con los mismos: fase precontractual, fase contractual y fase de terminación de la relación contractual.

Segundo. Los presentes Lineamientos son de observancia obligatoria para las áreas de la Universidad Anáhuac México que gestionen, revisen y aprueben la contratación de proveedores.

Tercero. Sin perjuicio de las definiciones previstas en los artículos 3 de la Ley y 2 de su Reglamento, para los efectos de estos Lineamientos se entenderá por:

I. **Acuerdo de encargo:** Es aquel documento que pone al responsable del tratamiento de datos personales en relación con un tercero, con quien le vincula un contrato de prestación de servicios en virtud del cual se produce un acceso a los datos personales contenidos en las bases del responsable del tratamiento.

II. **Candidato:** La persona física o moral que participe en cualquier procedimiento de contratación en la Universidad.

III. **Comisión:** Comisión de Protección de Datos Personales de la Universidad Anáhuac México.

IV. **Ley:** *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*.

V. **Lineamientos:** Lineamientos para la gestión de la privacidad de terceros en privacidad.

VI. **Proveedor:** La persona que celebre contratos de adquisiciones, arrendamientos, colaboraciones académicas nacionales e internacionales o servicios de la Universidad Anáhuac México.

VII. **Reglamento:** Reglamento de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*.

VIII. **Universidad**: Universidad Anáhuac México, nombre comercial de la responsable del tratamiento de datos personales.

Cuarto. Las áreas solicitantes, en el momento previo a la contratación de los servicios, deberán valorar y supervisar si los candidatos electos utilizarán y accederán a datos personales que alberga la Universidad.

Quinto. En caso de que el proveedor requiera usar y acceder a los datos personales que alberga la Universidad, previo a la contratación de los servicios, se deberá realizar una evaluación y selección de proveedores de manera objetiva y evidenciable, en la que se determinará lo siguiente:

1. Que en el uso de la información personal se respetan los principios establecidos en el artículo 6 de la Ley referida.
2. Que el candidato ha previsto y adoptado un conjunto de medidas de seguridad físicas y administrativas para el resguardo de la información.
3. Que dichas medidas de seguridad se verifican y revisan periódicamente.
4. Que el candidato cuenta con políticas internas y procedimiento que permitan cumplir con la privacidad de datos personales desde el diseño.
5. Que el candidato cuenta con un registro de actividades de tratamiento, en los casos que resulte necesario.
6. Que el candidato cuenta con un Oficial de Protección de Datos Personales o Departamento de Datos Personales.
7. Que el candidato ha llevado a cabo los análisis de riesgos y/o evaluaciones de impacto pertinentes.
8. Que el candidato manifieste si realizan o no transferencias internacionales de datos, y su pertinencia.

Determinado lo anterior, las áreas solicitantes deberán elegir únicamente a aquellos candidatos que ofrezcan dichas garantías, de tal manera que el tratamiento de datos que realicen por cuenta del responsable sea conforme con los requisitos establecidos en la normatividad.

Sexto. Electo el proveedor, la responsable formalizará la relación mediante la suscripción de un acuerdo de encargo, en la que se delimitarán las finalidades y los usos de los datos personales que le sean encomendados.

Séptimo. El acuerdo de encargo deberá contener como mínimo:

a) Una descripción suficientemente detallada del mandato al encargado del tratamiento: objeto, duración, naturaleza y finalidad del tratamiento;

b) Una relación de medidas de seguridad físicas y administrativas adoptadas por el encargado del tratamiento;
c) Una descripción suficiente detallada de los datos personales objeto del tratamiento: tipología de datos y categorías de titulares, y
d) Las obligaciones y derechos de las partes.

Octavo. En la práctica se pueden plantear distintas posibilidades de formalización de los acuerdos de encargo:

a) Independientes del contrato de prestación de servicios, obra, entre otros que se suscriba con el proveedor;
b) Formando anexo inseparable de los referidos contratos, y
c) Como acuerdos marcos de tratamiento de datos personales que se firmen entre responsables y encargados.

Noveno. Contratado al proveedor, la responsable implementará una evaluación de desempeño para promover una política de mejora continua y beneficio mutuo entre las partes.

Décimo. La evaluación de desempeño establecerá un proceso de valoración sistemática y documentada sobre los aspectos más significativos de la relación con los encargados del tratamiento de datos. Lo anterior será valorable a través del cuestionario anexo a los presentes Lineamientos.

Décimo primero. En la finalización del contrato con un proveedor que trate datos de carácter personal, el responsable determinará una serie de controles y garantías mínimos:

a) Supresión o devolución a la Universidad de todos los datos personales que el proveedor haya estado tratando. Es importante señalar que la supresión de los datos personales debe hacerse de manera segura, de conformidad con los requisitos que la responsable considere necesario.
b) En la finalización del servicio el proveedor transferirá el conocimiento adquirido o generado durante la prestación del servicio a la Universidad o hacia el proveedor que esta designe, sin que ello repercuta en una pérdida del control o nivel de calidad del servicio.

c) En el caso de los contratos de *cloud computing*, es especialmente relevante la regulación de la portabilidad de los datos a la finalización del contrato.

d) El proveedor deberá traspasar a la Universidad o al proveedor entrante toda la documentación y datos que se hayan generado durante el periodo de prestación del servicio.

e) Es necesario garantizar que el deber de confidencialidad del proveedor se mantiene incluso una vez finalizada la relación contractual.

f) En caso de que el servicio subcontratado se haya llevado a cabo en la sede de la Universidad, se retirará el acceso al proveedor, y si el acceso por parte del proveedor se ha realizado a los sistemas de este, también deberá ser anulado, evitando así que puedan acceder a cualquier recurso interno una vez que el contrato ha finalizado.

Décimo segundo. En el caso de que la finalización del servicio sea no planificada, se deberá considerar una serie de controles adicionales:

a) Se deberán implementar controles temporales durante la finalización del servicio que permitan minimizar el impacto que este tipo de terminaciones pueda llevar asociadas.

b) Se deberá realizar un análisis interno sobre la privacidad para garantizar que los derechos con respecto a la protección de datos de los usuarios afectados por el tratamiento del proveedor "saliente" se siguen manteniendo tanto si el proveedor es sustituido como si no lo es o durante el periodo de transición.

Décimo tercero. En el caso de que se vaya a producir una finalización del servicio no planificada y asociada a un incumplimiento, es importante que, aparte de los controles y garantías mínimos detallados anteriormente, se considere una serie de aspectos adicionales:

a) Identificarse y documentarse específicamente y de manera clara los incumplimientos que se han producido por parte del proveedor y que derivan en la finalización del contrato.

b) Será necesario el aviso por escrito para cualquier tipo de terminación; la notificación debe incluir la razón de poner fin al contrato y una referencia al párrafo del contrato en que se habla de la resolución.

c) Mantener un control sobre el adecuado traspaso del servicio y transferencia del conocimiento para garantizar que no se pierde información en el proceso.

<< Volver al inicio

Décimo cuarto. En el caso de proveedores estratégicos o considerados de riesgo alto, será importante implementar controles y garantías adicionales para garantizar el impacto a la privacidad y protección de datos que esta finalización lleva asociada, así como establecer mecanismos de trazabilidad para dejar constancia del cumplimiento.

A continuación, se detalla una lista de controles adicionales mínimos a tener en cuenta:

a) Garantía de la devolución de los datos o supresión de estos.

b) Garantía del borrado de las copias de seguridad.

c) Análisis de todos los accesos asociados al proveedor.

d) Control del material cedido al proveedor.

Décimo quinto. El incumplimiento de la obligación por la ausencia de control en materia de privacidad en todo el proceso de contratación del proveedor podría dar lugar a la imposición de una sanción y medida disciplinaria conforme a lo establecido por el Reglamento de Sana Convivencia y Disciplina, esto a criterio de la Comisión Consultiva y Disciplinaria de la Universidad Anáhuac México.

Lo anterior no exime al personal de responsabilidades administrativas, civiles, penales o de cualquier otra índole externa de la Universidad.

Décimo sexto. Las situaciones no previstas en los presentes Lineamientos serán resueltas por la Comisión de conformidad con lo previsto en la Ley, su Reglamento, así como demás disposiciones y criterios emitidos por la Universidad.

TRANSITORIOS

Décimo séptimo. Los presentes Lineamientos entrarán en vigor a los tres meses siguientes de su aprobación por la Comisión.

<< Volver al inicio

Décimo octavo. Será atribución de la Comisión la adición, modificación y/o en su caso supresión de las disposiciones aquí contenidas.

ANEXO

	Preguntas de evaluación	Sí	No
1	¿Garantiza el proveedor que cumple con las directrices la *LFPDPPP* y, en consecuencia, que adopta las medidas de seguridad que establece?		
2	¿Cuenta con una política de seguridad de la información y privacidad?		
3	¿Se ha sometido a auditoría de privacidad o protección de datos en los últimos dos años?		
4	¿Realiza los análisis de riesgo y evaluaciones de impacto pertinentes?		
5	¿Tiene un procedimiento para tratar y comunicar las posibles brechas de seguridad?		
6	¿Dispone de un oficial de Protección de Datos Personales o Departamento de Protección de Datos Personales?		
7	¿Dispone de protocolo para tratar todo tipo de incidencias de seguridad?		
8	Si es necesario, ¿cuenta con un registro de actividades de tratamiento?		
9	¿Asume, mediante su firma, las cláusulas de confidencialidad e instruye a sus empleados sobre las mismas, así como a la debida confidencialidad que deben observar con los datos personales que tratan?		
10	¿Aplica medidas para detectar vulnerabilidades tecnológicas y procesos para corregirlas?		
11	¿Subcontrata a terceros para llevar a cabo la prestación de sus servicios?		
12	Si subcontrata con terceros, ¿les comunica las cláusulas de privacidad/exige las medidas de seguridad requeridas?		
13	¿Dispone de un Plan de Continuidad de Negocio?		
14	Indique las principales certificaciones o estándares que posee la compañía en materia de seguridad de la información (ISO 27001, ISO-25999, etc.). _____ (Indique certificación, entidad certificadora y fecha de certificación) _____ _____		

Anáhuac
México

Campus Norte
Av. Universidad Anáhuac núm. 46,
col. Lomas Anáhuac, Huixquilucan,
Estado de México, C.P. 52786
Tel.: 55 56 27 02 10

Campus Sur
Av. de los Tanques núm. 865,
col. Torres de Potrero, Álvaro Obregón,
Ciudad de México, C.P. 01840
Tel.: 55 56 28 88 00

Oficina del Oficial de Protección de Datos Personales
Tel.: 55 56 27 02 10 ext. 8675
privacidad.norte@anahuac.mx
privacidad.sur@anahuac.mx

anahuac.mx/mexico