Anáhuac México

Política de Privacidad

Documento aprobado el 04 de abril de 2022

Comisión de Protección de Datos Personales

<< Volver al inicio

CONTENIDO

<< Volver al inicio

PROPÓSITO

Garantizar el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales que deberán operar e implementar las diversas áreas de la Universidad Anáhuac México, que en el ejercicio de sus funciones realicen algún tratamiento de datos personales.

NORMATIVIDAD APLICABLE

- Convenio No. 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Estrasburgo, 28.I.1981)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (*D.O.F.,* 5 de julio de 2010)
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (*D.O.F.,* 21 de diciembre de 2012)
- Guía para implementar un sistema de gestión de seguridad de datos personales (junio de 2015)
- Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (junio de 2016)
- Recomendaciones para el manejo de incidentes de seguridad de datos (junio de 2018)
- Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo (abril de 2021)

NORMATIVIDAD ORIENTADORA

- Directrices para la armonización de la protección de datos en la comunidad iberoamericana
- Dictamen 15/2011 sobre la definición de consentimiento
- Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas)

<< Volver al inicio

CAPÍTULO I. DISPOSICIONES GENERALES

Artículo 1. Objeto

Esta política de privacidad tiene por objeto garantizar y proteger, en lo que concierte al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, dignidad humana, y privacidad personal y familiar.

Artículo 2. Ámbito de aplicación

La presente política es de observancia general y obligada para todo el personal de la Universidad Anáhuac México involucrada en cualquier tipo de tratamiento de datos personales con independencia de la forma o modalidad de su recolección, procesamiento, almacenamiento y organización, así como establecer las medidas de seguridad para evitar cualquier daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado de los datos personales registrados tanto en soportes físicos como electrónicos.

Artículo 3. Definiciones

Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales.

Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de estas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento, y transcurrido este periodo se procederá a su cancelación en la base de datos que corresponde.

Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Ciberseguridad: Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

<< Volver al inicio

Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Derechos ARCO: Son los derechos de acceso, rectificación, cancelación y oposición.

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Encargado: La persona física o jurídica que sola, o conjuntamente con otras, trate datos personales por cuenta del responsable.

Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos.

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

Listado de exclusión: Base de datos que tiene por objeto registrar de manera gratuita la negativa del titular al tratamiento de sus datos personales.

Medidas de seguridad administrativas: Conjunto de acciones y mecanismos para establecer la gestión, el soporte y la revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados a a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la Universidad, equipo e información; b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones; c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad; y d) Garantizar la eliminación de datos de forma segura.

Medidas de seguridad técnicas: Conjunto de actividades, controles o mecanismos con resultado medible que se valen de la tecnología para asegurar: a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados; b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Se incluyan acciones para la adquisición¸ operación, desarrollo y mantenimiento de sistemas seguros; y d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

Política: La política de privacidad de la Universidad Anáhuac México.

Reglamento: El reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Remisión: La comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano.

Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Supresión: Actividad consistente en eliminar, borrar o destruir el o los datos personales una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas por el responsable.

Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

Titular: La persona física a quien corresponden los datos personales.

Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

Universidad: Universidad Anáhuac México.

Artículo 4. Cómputo de plazos

En los supuestos en que esta Política señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 5. Del Departamento de Datos Personales

El Departamento de Protección de Datos Personales asesorará a las diversas áreas de la Universidad en materia de protección de datos personales conforme a los principios, deberes y obligaciones establecidos en la Ley Federal, su Reglamento, la presente Política y demás normatividades aplicables.

<< Volver al inicio

Artículo 6. De los enlaces de protección de datos personales

Para las actividades señaladas en la presente Política será necesario contar con la designación de personal que actúe como enlace en materia de datos personales.

Las personas titulares de las diversas áreas de la Universidad designarán al personal como enlace en materia de protección de datos personales para establecer un canal de comunicación efectivo entre el Departamento de Protección de Datos Personales y las áreas de la Universidad.

Artículo 7. De la Comisión de Protección de Datos Personales

La Comisión de Protección podrá sugerir a las diversas áreas de la Universidad que realicen o dejen de hacer ciertas acciones con el fin de prevenir algún incumplimiento a las disposiciones en materia de protección de daros personales.

Cuando este advierta un hecho que pueda constituir una falta disciplinaria en materia de protección de datos personales en términos de la normatividad aplicable, dará vista a la autoridad correspondiente conforme al artículo 17 del Reglamento de Sana Convivencia y Disciplina para el inicio de las medidas preventivas y correctivas que estas indiquen o que prudentemente resulten pertinentes.

CAPÍTULO II. PRINCIPIOS DE PROTECCIÓN Y DERECHOS DE LAS PERSONAS

Artículo 8. Finalidad de los datos

Los datos personales solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y proporcionales en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Dichos datos serán tratados de forma leal y lícita. Los datos personales objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recolectados. No se considera incompatible el tratamiento posterior de estos con fines históricos, estadísticos o científicos.

Artículo 9. Mecanismos para acreditar el cumplimiento del principio de finalidad

Para acreditar el debido cumplimiento a este principio se deberá observar lo siguiente:

- Establecer mediante un inventario las finalidades de cada tratamiento que realice cada área de la Universidad. En dicho documento se verificará que estas finalidades sean específicas, determinadas y acordes con las atribuciones de la Universidad. Además, se determinará cuáles de ellas son primarias y cuáles secundarias.
- Verificar que en los avisos de privacidad se informen todas las finalidades para la cuales se tratan los datos personales y que se encuentren descritas de manera clara, así como que se cuente con un mecanismo para que el titular pueda manifestar su negativa para el tratamiento de datos personales para finalidades secundarias.
- Vigilar que el personal de la Universidad únicamente trate datos en términos de las finalidades informadas en el aviso de privacidad correspondiente.

Artículo 10. Proporcionalidad de los datos

Para el objeto de tratamiento de los datos personales únicamente se harán de aquellos que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

Artículo 11. Calidad de los datos

1. Los datos personales serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del titular. Si los datos fueran recogidos directamente del titular, se considerarán exactos los facilitados por este.
2. Si los datos personales registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviera conocimiento de la inexactitud.
3. Cuando los datos hubieran sido comunicados a un tercero, la Universidad notificará a este, en el plazo de diez días, la rectificación o cancelación efectuada.

En el plazo de diez días desde la recepción de la notificación, el tercero que mantuviera el tratamiento de los datos deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos personales no requerirá comunicación alguna con el titular, sin perjuicio del ejercicio de los derechos ARCO reconocidos en la Ley Federal y su Reglamento.

Artículo 12. Cancelación de los datos

Los datos personales serán suprimidos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el titular. Una vez cumplido el periodo, los datos solo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo previsto en el artículo 25 de la Ley Federal.

Los datos personales serán tratados de forma que permitan el ejercicio de derecho de acceso, en tanto no procesa su cancelación.

Artículo 13. Mecanismos para acreditar el cumplimiento del principio de calidad

Para acreditar el debido cumplimiento a este principio se deberá observar lo siguiente:

- Documentar las actualizaciones y supresiones realizadas de datos personales.
- Documentar el informe a los encargados a los que se haya comunicado datos personales sobre las correcciones o actualizaciones de los datos personales que tengan lugar, a fin de que realicen lo conducente en la base de datos que manejen.
- Contar con los procedimientos para la conservación, bloqueo y supresión de los datos personales.
- Verificar que dichas obligaciones del principio de calidad se encuentren previstas en las cláusulas contractuales u otros instrumentos jurídicos que se firmen con terceros.

Artículo 14. Información en la recolección de los datos

1. Los titulares a los que se soliciten datos personales deberán ser previamente informados de manera expresa, precisa e inequívoca:
    - La identidad y domicilio del responsable;
    - Las finalidades del tratamiento de datos personales;
    - Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso divulgación de los datos;

- Los medios para ejercer los derechos ARCO, de conformidad con lo dispuesto en esta Ley.
- Las transferencias de datos que se efectúen, y
- El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad.
- En el caso de la recolecta de datos personales sensibles, se deberá señalar expresamente que se trata de este tipo de datos.

2. Con el fin de llevar el principio de información a su máxima expresión, la Universidad hará de conocimiento la existencia de esta Política cuando recoja datos personales a través de formularios, indicando su ubicación en la página web de la Universidad, para su consulta.
3. Cuando los datos personales no hayan sido recabados del titular, este deberá ser informado de forma expresa, precisa e inequívoca por la Universidad dentro de los tres meses siguientes al momento de registro de los datos, salvo que ya hubiera sido informado con anterioridad del contenido del tratamiento, de la procedencia de los datos, de la posibilidad de ejercitar los derechos ARCO, y de la identidad y dirección del responsable del tratamiento.

Artículo 15. Mecanismos para acreditar el cumplimiento del principio de información

Para acreditar el debido cumplimiento a este principio se deberá observar lo siguiente:

- Contar con los avisos de privacidad integral y simplificado por cada proceso de tratamiento de datos personales que se lleve a cabo.
- Documentar la forma en que se obtienen los datos personales en cada actividad, tratamiento o procedimientos.
- Capacitar al personal que recaba los datos personales, a fin de que conozca los momentos de la puesta a disposición del aviso de privacidad.

Artículo 16. Consentimiento del titular

1. El tratamiento de los datos personales requerirá el consentimiento inequívoco del titular, salvo las excepciones de Ley.

2. El consentimiento podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
3. En los casos en los que no sea necesario el consentimiento del titular para el tratamiento de los datos, y siempre que una ley no disponga lo contrario, este podrá oponerse a su tratamiento en cualquier momento. En tal supuesto, la Universidad excluirá del tratamiento los datos relativos al titular.
4. Respecto a los datos personales relativos a la salud, estos solo podrán ser recabados y tratados cuando por razones de interés general así lo disponga una Ley o el titular consienta expresamente.
5. Solo con el consentimiento expreso y por escrito del titular podrán ser objeto de tratamiento los datos personales que revelen la ideología, afiliación sindical, opiniones políticas, preferencia sexual, creencias religiosas, filosóficas y morales. Cuando en relación con estos proceda a recabar el consentimiento, se advertirá al titular de su derecho a no prestarlo.

Artículo 17. Mecanismos para acreditar el cumplimiento del principio de consentimiento

Para acreditar el debido cumplimiento a este principio se deberá observar lo siguiente:

- Mantener bajo resguardo una copia del documento en el cual se haya manifestado el consentimiento del titular para el tratamiento de sus datos, cuando este proceda.
- Documentar la puesta a disposición del aviso de privacidad al titular en aquellos casos en los cuales sea válidos el consentimiento tácito.
- Identificar en el aviso de privacidad, aquellos datos personales y finalidades que requieren del consentimiento de su titular para su tratamiento.

Artículo 18. Licitud y lealtad de los datos

Los datos personales únicamente serán tratados por el responsable de manera lícita y leal, lo que supone que tiene que actuar con apego a las leyes en general y en lo particular a la normatividad sobre protección de datos personales.

<< Volver al inicio

Artículo 19. Responsabilidad de los datos

Conforme a este principio se velará por el cumplimiento del resto de los principios, se adoptarán medidas necesarias como estándares y mejores prácticas para su aplicación y se demostrará ante el Órgano garante que se cumplen con sus obligaciones en torno a sus obligaciones a la protección de datos personales.

Artículo 20. Deber de confidencialidad

1. Toda persona que intervenga en cualquier fase del tratamiento de los datos personales está obligado a guardar secreto respecto de los mismos y el deber resguardarlos. La obligación de confidencialidad subsistirá aun después de finalizar sus relaciones con la Universidad.
2. El incumplimiento del deber de confidencialidad será sancionado de conformidad con lo previsto en la legislación vigente.

Artículo 21. Deber de seguridad

El personal de la Universidad deberá observar y garantizar que las medidas físicas, técnicas y administrativas que el responsable implemente para proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, se desarrollen en sus términos.

Artículo 22. Factores para determinar las medidas de seguridad

1. La Universidad determinará las medias de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:
    - El riesgo inherente por tipo de dato personal;
    - La sensibilidad de los datos personales tratados;
    - El desarrollo tecnológico, y
    - Las posibles consecuencias de una vulneración para los titulares.
2. De manera adicional al apartado 1 del presente artículo, se procurará tomar en cuenta los siguientes elementos:
    - El número de titulares;
    - Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;

- El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y
- Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

3. Para la seguridad de los datos personales, la Universidad adoptará un Sistema de Gestión de Seguridad de Datos Personales (SGSDP) basado en el ciclo PHVA (Planear-HacerVerificar-Actuar).

Artículo 23. Medidas de seguridad físicas

Las diversas áreas de la Universidad que traten datos personales deberán tomar las siguientes medidas de manera enunciativa más no limitativa:

- Protección de instalaciones, equipos, soportes o bases de datos personales;
- Utilización de candados, cerrojos, cerraduras, tarjetas de identificación, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de puertas, gavetas, cajones, archiveros;
- Implementación de sistemas de vigilancia, alarmas, y de prevención y protección contra siniestros tales como incendios, señalamiento de áreas de acceso restringido;
- Aparatos de identificación por medio de la voz, iris, huella, ADN y demás datos biométricos;
- Resguardo de datos personales a través de infraestructura que garantice las condiciones adecuadas de humedad, polvo, iluminación solar y temperatura, y evite el deterioro por plagas, consumo de alimentos y otros factores presentes en el entorno.

Artículo 24. Medidas de seguridad administrativas

Las diversas áreas de la Universidad que traten datos personales deberán tomar las siguientes medidas de manera enunciativa más no limitativa:

- Identificación y autentificación de la persona autorizada para el tratamiento de datos personales;
- Implementación de contraseñas, claves y protocolos de seguridad;
- Identificación de roles y perfiles;
- Realización de inventario de datos personales, análisis de riesgo y de brecha;
- Elaboración de planes de trabajo para la futura implementación de medidas faltantes y necesarias;

- Monitoreo y revisión periódica de las medidas;
- Capacitación de personal;
- Elaboración de bitácoras de registro y seguimiento de las actividades que se realizan con la base de datos personales;
- Elaboración de procedimientos para dar aviso al personal custodio de los datos personales sobre la presencia y el acceso de personas no autorizadas;
- Emisión de reglas sobre la introducción de equipos de cómputo, accesorios y gadgets, o de conexión inalámbrica en áreas restringidas de tratamiento de datos personales;
- Emisión de reglamentación interna que contemple infracciones y sanciones en relación con el indebido tratamiento de datos personales;
- Emisión de reglas para la baja documental en soportes físicos y electrónicos;
- Emisión de medidas para la prevención y notificación de intrusiones e incidentes;
- Emisión de reglas de uso sobre dispositivos de almacenamiento externo;
- Elaboración de manuales de operaciones; instauración de protocolos para casos de emergencia; realización de pruebas y simulacros;
- Inclusión de cláusulas o contratos de confidencialidad para el personal laboral;
- Procedimientos de disociación de datos personales.

Artículo 25. Medidas técnicas de seguridad

Las diversas áreas de la Universidad que traten datos personales deberán tomar las siguientes medidas de manera enunciativa más no limitativa:

- Encriptación y cifrado de los datos;
- Realización de copias de seguridad, resguardos o backups;
- Almacenamiento en dos ubicaciones diferentes;
- Atención de fallas de equipo electrónico y de cómputo;
- Indicación de software autorizado;
- Deshabilitación o cancelación de dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.);

- Realización de labores de mantenimiento, preventivo y correctivo de equipos electrónicos y de cómputo;
- Instalación de firewalls, antivirus, watchdogs, mecanismos para evitar la pérdida y filtración de datos (data loss prevention);
- Segregación de funciones mediante perfiles de acceso;
- Mecanismos de control de acceso;
- Monitorización del uso de datos personales;
- Implementación de técnicas de disociación.

CAPÍTULO III. DE LAS REMISIONES Y TRANSFERENCIAS DE LOS DATOS PERSONALES

Artículo 26. Comunicación de datos personales

1. Los datos personales objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legitimas del remisor y del receptor con el previo consentimiento del titular.
2. El consentimiento exigido en el apartado anterior no será preciso, sin perjuicio de lo dispuesto en el artículo 36 de la Ley, en los siguientes supuestos:
    I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
    II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
    III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
    IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
    V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público o para la procuración o administración de justicia;

VI. Cuando la transferencia sea precisa para el reconocimiento, el ejercicio o la defensa de un derecho en un proceso judicial, y

VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

3. Será nulo el consentimiento para la comunicación de los datos personales a un tercero cuando la información que se facilite al titular no le permita conocer la finalidad a que destinará los dato cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretende comunicar.
4. El consentimiento para la comunicación de los datos personales tiene también carácter de revocable.
5. Aquel a quien se comuniquen los datos personales se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la Ley, su Reglamento y demás normatividad aplicable.
6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 27. Comunicación de datos con fines de investigación

La comunicación de datos o su uso interno con fines de investigación solo se producirá si está autorizada en la Ley o se ha utilizado un procedimiento de disociación.

Artículo 28. Acceso a los datos por cuenta de terceros para la prestación de servicios a la Universidad

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio a la Universidad.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones de la Universidad, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato ni los comunicará, ni siquiera para su conservación, a otras personas. En caso de incumplimiento de las estipulaciones establecidas, el encargado del tratamiento será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

En el contrato se estipularán, asimismo, las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

3. Si el encargado de tratamiento necesita para la prestación de un servicio a la Universidad subcontratar con un tercero parte del tratamiento, deberá contar con autorización previa escrita de la Universidad. Esta autorización puede estar contemplada en el contrato del servicio con el encargado de tratamiento o ser formalizada posteriormente para siempre antes de realizar la subcontratación. En cualquier caso, el subcontratista tendrá las obligaciones de encargado de tratamiento y seguirá las instrucciones de la Universidad para ese tratamiento, así como el cumplimiento de las disposiciones legales correspondientes.
4. Una vez cumplida la prestación contractual, los datos personales deberán ser destruidos o devueltos a la Universidad, al igual que cualquier soporte o documentos en que conste algún dato personal objeto del tratamiento. No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos.
5. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Artículo 29. La Universidad Anáhuac México como encargada de tratamiento de datos personales

En la manipulación de datos de otras instituciones, la Universidad aplicará las presentes políticas de privacidad en su tratamiento interno, así como las medidas de seguridad acordadas con dicha institución.

Artículo 30. Transferencias internacionales de datos

1. La Universidad podrá realizar transferencias internacionales de datos personales cuando el receptor de los datos personales asuma las mismas obligaciones en materia de datos personales a las que esta se encuentra sujeta.
2. Cuando la Universidad transfiera los datos personales podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones a las que se encuentra sujeta, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.

3. La Universidad, en caso de considerarlo necesario, podrá solicitar la opinión del Instituto respecto a si las transferencias internacionales que realicen cumplen con lo dispuesto por la Ley y su Reglamento.

CAPÍTULO IV. EJERCICIO DE LOS DERECHOS ARCO

Artículo 31. Derecho de Acceso

1. El titular tendrá derecho a solicitar y obtener gratuitamente información de sus datos personales sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización en pantalla, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, fotocopia, certificada o no, correo electrónico o sistema de comunicación electrónica, o cualquier otro sistema que sea adecuado a la configuración o implantación material de la base de datos o la naturaleza del tratamiento, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
3. Las áreas de la Universidad resolverán sobre la solicitud de acceso en un plazo no mayor a diez días contados desde la recepción de la misma cuando esta:
    - Cuente con la información y procede la entrega de la misma;
    - Cuente con la información y contiene datos personales de terceros y/o información confidencial de la Universidad o de terceros;
    - La información resulta ser inexistente en los archivos del área.

    En el caso de que la Universidad no disponga de datos personales del titular se le comunicará igualmente en el mismo plazo.
4. Podrá negarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando estas impidan revelar a los titulares el tratamiento de los datos a los que se refiera el acceso.

<< Volver al inicio

Artículo 32. Derecho de rectificación y cancelación

1. Las áreas de la Universidad resolverán sobre la solicitud de rectificación o cancelación en un plazo no mayor a diez días contados desde la recepción de la misma.

   En el caso de que la Universidad no disponga de datos personales de los titulares se lo comunicará igualmente en el mismo plazo.
2. Serán rectificados los datos personales cuyo tratamiento no se ajuste a los dispuesto en la Ley y su Reglamento, y en particular, cuando tales datos resulten inexactos o incompletos.
3. Serán cancelados los datos personales cuyo tratamiento no se ajuste a los dispuesto en la Ley y su Reglamento, y en particular, cuando tales datos resulten inadecuados o excesivos.

   La cancelación procederá respecto de la totalidad de los datos personales del titular contenidos en una base de datos, o solo parte de ellos, según lo hayan solicitado.

   La cancelación dará lugar al bloqueo de los datos personales, conservándose únicamente para los plazos de prescripción que en su caso la norma contemple para la observación de una obligación legal. Cumplido el citado plazo, deberá procederse a la supresión.
4. Podrán denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando estas impidan revelar a los titulares el tratamiento de los datos a los que se refiera el acceso.
5. Si los datos rectificados o cancelados hubieran sido comunicados previamente, deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.
6. Los datos personales deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la Universidad y el titular.

Artículo 33. Derecho de oposición

1. El titular tendrá derecho a que no se lleve a cabo el tratamiento de sus datos personales o se cese en el mismo en los siguientes supuestos:

a. Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal que lo justifique, siempre que una Ley no disponga lo contrario.
b. Cuando se trate de base de datos que tengan por finalidad la realización de actividades de publicidad y prospección comercial.
c. Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al titular y basada únicamente en un tratamiento automatizado de sus datos personales.

2. El derecho de oposición se ejercerá según el procedimiento descrito en el artículo 34 de esta Política. Cuando la oposición se realice con base en la letra a) del numeral 1 del presente artículo, en la solicitud deberán hacerse constar los motivos fundados y legítimos relativos a una concreta situación personal del titular, que justifican el ejercicio de este derecho.
3. La Universidad resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. En el caso de que la Universidad no disponga de datos personales de los titulares se lo comunicará igualmente en el mismo plazo.
4. Se excluirán del tratamiento los datos relativos al titular que ejercite su derecho de oposición o se denegará motivadamente la solicitud del mismo.

Artículo 34. Procedimiento de derechos ARCO

1. Los derechos de acceso, rectificación, oposición o cancelación de datos se ejercerán siempre ante la Universidad y de forma complementaria a lo indicado en este artículo. La Universidad podrá articular tantos procedimientos específicos se consideren necesarios para agilizar el ejercicio de estos derechos.
2. Con objeto de facilitar el ejercicio de ARCO a los miembros de la Comunidad Universitaria se habilitará un sistema que contenga un formulario simplificado que facilite a los titulares la presentación de sus peticiones. En especial, se potenciará el derecho de acceso con la consulta inmediata a los datos almacenados en las bases de datos de la Universidad.
3. De forma complementaria a lo indicado en el apartado 2 de este artículo, cualquier petición de oposición, acceso, rectificación o cancelación sobre datos personales se podrá realizar mediante escrito libre presentado directamente ante el oficial de Datos Personales de la Universidad Anáhuac México,

en Campus Norte, enviarlas a través de servicios de mensajería o a la siguiente dirección electrónica: privacidad.norte@anahuac.mx o privacidad.sur@anahuac.mx

4. Los derechos ARCO son derechos personalísimos y serán ejercidos por el titular, o en su caso su representante legal. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro.
5. La entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos. Dicho derecho se ejercerá por el titular en forma gratuita, previa acreditación de su identidad ante el responsable. No obstante, si la misma persona reitera su solicitud en un periodo menor a doce meses, los costos no serán mayores a tres días de Salario Mínimo General Vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas.
6. Los padres o tutores no tendrán acceso al expediente académico o cualquier otro dato personal de sus hijos salvo que los mismos hayan expresamente consentido la transmisión de la información. Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente Capítulo, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto.
7. El titular podrá presentar una solicitud de protección de datos cuando considere que su derecho a la protección de sus datos personales ha sido vulnerado, por lo que podrá acudir ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

CAPÍTULO V. CIBERSEGURIDAD

Artículo 35. Mejores prácticas en ciberseguridad

La Universidad se encuentra obligada a monitorear, identificar, analizar y, en su caso, implementar las mejores prácticas nacionales e internacionales en materia de ciberseguridad que coadyuven en la protección de la privacidad y datos personales.

<< Volver al inicio

Artículo 36. Obligaciones en materia de ciberseguridad

1. La Dirección de Operación Tecnológica deberá documentar y configurar los controles en materia de TIC y de ciberseguridad, de tal manera que permitan generar evidencia de acciones u omisiones que, de manera directa o indirecta, dañen, perturben, vulneren, comprometan o pongan en riesgo los datos personales.
2. Las diversas áreas de la Universidad deberán compartir información entre sí y con la Dirección de Operación Tecnológica sobre vulnerabilidades, amenazas cibernéticas y ataques, a efecto de prevenirlos, mitigarlos o eliminar sus efectos.

CAPÍTULO VI. GESTIÓN DE RIESGO DE PRIVACIDAD

Artículo 37. Riesgo de privacidad

El riesgo de privacidad surge del incumplimiento de las leyes, regulaciones, normas y expectativas regulatorias aplicables de privacidad. Para mitigar dicho riesgo la Universidad deberá observar e implementar: 1) Evaluaciones de controles y riesgos de privacidad; 2) Identificación y gestión del riesgo de privacidad; 3) Monitoreo y pruebas del riesgo de privacidad; 4) Reporte del riesgo de privacidad, y 5) Comunicación y capacitación.

Artículo 38. Evaluaciones de control y riesgos de privacidad

1. La mitigación del riesgo de privacidad exige evaluaciones efectivas de controles y riesgos. La Universidad es responsable de establecer, implementar y efectuar las evaluaciones aplicables de controles y riesgos como vía para garantizar que el personal pueda identificar y evaluar de forma periódica a) Sus riesgos de privacidad más significativos con base en el impacto potencial del riesgo: y b) La eficacia de los controles relacionados.

Artículo 39. Identificación y gestión del riesgo de privacidad

1. Los problemas y riesgos específicos relacionados con la privacidad serán manejados, de forma proactiva, a través del proceso de evaluación del impacto a la privacidad (EIP) y, de forma reactiva, a través de la gestión de los eventos de privacidad y de las solicitudes de derechos ARCO de los titulares.

2. En términos del apartado anterior, se llevará a cabo la elaboración de una valuación de impacto conforme a las directrices EIPD emitidas por el Instituto cuando:
    a. El tratamiento conlleve la elaboración de perfiles, especialmente de aspectos relacionados con el rendimiento laboral, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos de los titulares.
    b. El tratamiento se vea destinado a tomar decisiones sobre los titulares que produce efectos jurídicos para las personas o que les afectan significativamente de modo similar.
    c. El tratamiento sea usado para observar, supervisar y controlar a los titulares, incluidos los datos obtenidos a través de redes o de la observación sistemática de una zona de acceso público.
    d. El tratamiento involucre datos personales de categorías especiales, como los datos personales sensibles que puedan afectar a la esfera más íntima de su titular, o cuya utilización pueda dar origen a discriminación o conlleve un riesgo grave para este.
    e. El tratamiento se realice a datos de gran escala.
    f. Los datos deriven de dos o más operaciones de tratamiento de datos realizadas para distintos fines o por responsables distintos, de manera que exceda las expectativas razonables del titular.
    g. El tratamiento conlleve el uso de una nueva tecnología, toda vez que este nuevo uso puede implicar nuevas formas de recolección y utilización de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas, por lo que las consecuencias personales y sociales del empleo de una nueva tecnología pueden ser desconocidas.
    h. El tratamiento de datos de titulares vulnerables represente el aumento del desequilibrio de poder entre los titulares y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos o de ejercer sus derechos. Entre los titulares vulnerables pueden incluirse a niños, empleados, segmentos más vulnerables de la población que necesitan una especial protección o cualquier otro caso en el que se identifique este supuesto
    i. El tratamiento impida a los titulares ejercer un derecho o utilizar un servicio o ejecutar un contrato.

<< Volver al inicio

Artículo 40. Monitoreo y pruebas del riesgo de privacidad

El Departamento de Datos Personales y los enlaces de protección de datos personales realizarán actividades de monitoreo continuas en sus respectivas jurisdicciones con el fin de estar al tanto de lo que ocurre dentro o fuera de la Universidad, monitorear su posible impacto en las evaluaciones de riesgo y asegurarse de que se efectúan los escalamientos necesarios.

Artículo 41. Comunicación y capacitación

Una sólida cultura del riesgo requiere un entorno que promueva los buenos comportamientos y valores, y permite la identificación y mitigación de los riesgos de privacidad. La comunicación y la capacitación eficaces que reflejen los valores de la Universidad y la conducta ética esperada es parte importante de mantener una sólida cultura del riesgo, por lo que la Universidad emprenderá las siguientes acciones:

- Comunicaciones o capacitación (incluyendo los programas obligatorios de vinculación y capacitación anual) para apoyar la concientización necesaria que promueva de manera uniforme y sólida el apego a los valores de la Universidad y prácticas esperadas en materia de privacidad; y
- Capacitación específica para riesgos mayores identificados en materia de privacidad, incluyendo la capacitación relacionada con las evaluaciones del impacto a la privacidad y la gestión de incidentes y violaciones.

TRANSITORIOS

Primero. Las disposiciones de la presente política podrán modificarse mediante acuerdo de dos tercios de los integrantes de la Comisión, cuando así lo consideren conveniente.

Segundo. La presente Política entrará en vigor a partir de su aprobación por la Comisión de Protección de Datos Personales.

Tercero. Notifíquese la presente política a las personas titulares de las diversas áreas de la Universidad y difúndase al interior de la misma.

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

Departamento de Datos Personales
Tel.: 55 56 27 02 10 ext. 8675
privacidad.norte@anahuac.mx
privacidad.sur@anahuac.mx

anahuac.mx/mexico