

REGLAMENTO PARA LA PROTECCIÓN DE DATOS PERSONALES¹

Entrada en vigor: 05 de octubre de 2026

¹ Su estructura, redacción, formato y contenido responden a los criterios establecidos por la Abogacía General de la Universidad Iberoamericana Ciudad de México.

ÍNDICE:

TÍTULO I

DISPOSICIONES GENERALES

CAPÍTULO ÚNICO

DISPOSICIONES GENERALES

TÍTULO II

PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I

PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO II

REMISIÓN Y TRANSFERENCIA DE DATOS PERSONALES

CAPÍTULO III

EJERCICIO DE DERECHOS ARCO

TÍTULO III

MEDIDAS DE PREVENCIÓN

CAPÍTULO I

DISPOSICIONES GENERALES APLICABLES A LAS MEDIDAS DE PREVENCIÓN

CAPÍTULO II

DE LAS MEDIDAS DE PREVENCIÓN GENERALES Y ESPECÍFICAS

TÍTULO IV

PROCESOS QUE IMPLIQUEN TRATAMIENTO DE DATOS PERSONALES

CAPÍTULO ÚNICO

PROCESOS QUE IMPLIQUEN TRATAMIENTO DE DATOS PERSONALES

TÍTULO V

VULNERACIÓN

CAPÍTULO ÚNICO

VULNERACIÓN

TÍTULO VI

RESPONSABILIDADES, SANCIONES Y CUMPLIMIENTO

CAPÍTULO ÚNICO
RESPONSABILIDADES, SANCIONES Y CUMPLIMIENTO

TRANSITORIOS

REGLAMENTO PARA LA PROTECCIÓN DE DATOS PERSONALES DEL TECNOLÓGICO UNIVERSITARIO DEL VALLE DE CHALCO

TÍTULO I

DISPOSICIONES GENERALES

CAPÍTULO ÚNICO

DISPOSICIONES GENERALES

Artículo 1. Objeto.

El presente Reglamento tiene por objeto establecer las disposiciones en la materia de protección de Datos personales que garanticen, a toda persona física que proporcione sus Datos personales al Tecnológico Universitario del Valle de Chalco (en adelante Tecnológico Universitario o TUVCH), en cualquier espacio físico o virtual autorizado, que en el Tratamiento de éstos, se respetarán sus derechos, y se realizará conforme a lo establecido en las disposiciones oficiales en materia de protección de Datos personales aplicables al TUVCH, incluyendo:

- I. Las Medidas de prevención, generales y específicas, así como las Autoridades universitarias responsables de su aplicación;
- II. Los principios para la protección de los Datos personales;
- III. Las reglas sobre la Transferencia de los Datos personales;
- IV. Las pautas para el ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO);
- V. Los procedimientos institucionales que impliquen el Tratamiento de Datos personales; y
- VI. Las responsabilidades, sanciones y la vigilancia del cumplimiento de este instrumento.

Artículo 2. Ámbito de Validez.

El presente Reglamento es de observancia obligatoria para las Autoridades universitarias, el personal del TUVCH y las y los prestadores de servicios profesionales, que recaben, obtengan, procesen, utilicen, almacenen, divulguen o estén en contacto con Datos personales en posesión de la Universidad, así como para las personas Titulares de los mismos.

Artículo 3. Definiciones.

Para efectos del presente Reglamento, y con independencia de las definiciones establecidas en las disposiciones oficiales en materia de protección de datos personales en posesión de los particulares, con el uso de mayúsculas o minúsculas indistintamente, se entenderá por:

- I. **Abogacía General:** El área de la Universidad Iberoamericana Ciudad de México, responsable para atender las solicitudes de ejercicio de Derechos ARCO, las solicitudes de revocación del Consentimiento de las personas Titulares, y solicitudes para limitar el uso o divulgación de los Datos personales;
- II. **Auditoría Interna:** Es el área adscrita a la Universidad Iberoamericana Ciudad de México, responsable de vigilar y revisar el debido cumplimiento del presente Reglamento;
- III. **Autoridad universitaria:** Cualquier autoridad unipersonal o colegiada prevista en la normatividad del TUVCH o en su organigrama.

Para los efectos de este instrumento, se considerarán también como Autoridades universitarias a aquellas que, en el desempeño de su encargo, ejerzan funciones de autoridad frente al personal o estudiantado del TUVCH, o que sean responsables de la relación profesional o contractual de cualquier otra índole, establecida con personas físicas o morales.

Estas autoridades tienen a su cargo la implementación y, en su caso, el diseño de las medidas de prevención generales y específicas;

- IV. **Aviso de Privacidad:** Documento a disposición de la persona titular de la información de forma física, electrónica o en cualquier formato generado por el Sujeto Regulado y/o responsable, a partir del momento en el cual se recaben sus

datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

- V. **Buzón de datos personales:** Medio electrónico y físico habilitado por el TUVCH para atender las solicitudes de ejercicio de Derechos ARCO;
- VI. **Comunidad universitaria:** La integrada por las autoridades universitarias académicas y administrativas, el personal académico, administrativo, estudiantes, personas egresadas y personas prestadoras de servicios profesionales docentes;
- VII. **Consentimiento expreso:** Se deberá entender que el consentimiento es expreso cuando la voluntad de la persona titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología;
- VIII. **Consentimiento tácito:** Cuando habiéndose puesto a disposición de la persona titular el aviso de privacidad, esta no manifieste su voluntad en sentido contrario;
- IX. **Datos personales:** Cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;
- X. **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 ésta. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;
- XI. **DPCI:** Dirección de Promoción y Comunicación Institucional;

- XII. Derechos ARCO:** Son los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de los Datos personales;
- IX. Docentes:** Al profesorado que presta sus servicios profesionales sea por un contrato civil o por una relación laboral;
- XII. Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los Datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado;
- XIII. Persona Encargada:** La persona física o jurídica, que sola o conjuntamente con otras, trate Datos personales por cuenta del Sujeto Regulado y/o Responsable, como consecuencia de la existencia de una relación jurídica que le vincula con ésta y delimita el ámbito de su actuación para la prestación de un servicio;
- XIV. Oficina Jurídica:** Área enlace del TUVCH, responsable de las gestiones necesarias para brindar el apoyo a la Abogacía General en cuanto a la atención de las solicitudes de derechos ARCO, las solicitudes de revocación del Consentimiento de las personas Titulares, y las solicitudes para limitar el uso o divulgación de los Datos personales;
- XV. Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y/o sujeto regulado y la persona encargada, dentro o fuera del territorio mexicano;
- XVI. Sujeto regulado y/o Responsable:** Personas físicas o morales de carácter privado que llevan a cabo el tratamiento de datos personales;
- XVII. Supresión:** Se refiere a la eliminación de los Datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones legales aplicables;
- XVIII. Titular:** Persona física a quien corresponden los Datos personales;

XIX. Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la titular, del Sujeto Regulado y/o responsable y de la persona encargada del tratamiento;

XX. Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales;

XIV. TUVCH: Tecnológico Universitario del Valle de Chalco; y

XXI. Vulneración: Cuando intencionada o no intencionadamente, se liberan Datos Personales en un ambiente no confiable, en cualquier fase del tratamiento, lo cual podría afectar los derechos patrimoniales o morales de sus titulares.

Los supuestos de la vulneración son:

- a) Pérdida o destrucción no autorizada;
- b) Robo, extravío o copia no autorizada;
- c) Uso, acceso o tratamiento no autorizado; o
- d) Daño, alteración o modificación no autorizada.

TÍTULO II

PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I

PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

Artículo 4. Licitud.

El TUVCH, en carácter de Sujeto Regulado y/o Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, estará obligado a obtener los datos y utilizarlos de manera lícita, conforme a lo dispuesto por la legislación mexicana y el

derecho internacional aplicable. En ese sentido, ninguna Autoridad universitaria ni ninguna persona que colabore o participe con la Universidad puede utilizar los Datos personales para actividades ilícitas, ni de forma tal que contravenga lo dispuesto por las disposiciones oficiales vigentes y aplicables en nuestro país, incluyendo los convenios o acuerdos internacionales de los cuales México sea parte.

Artículo 5. Lealtad.

El TUVCH, en carácter de Sujeto Regulado y/o Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, a través de sus Autoridades, colaboradores/as y participantes, estará obligado a respetar la confianza que depositan los y las Titulares al proporcionar su información, en el sentido de que ésta será tratada conforme a lo que acordaron y lo establecido en el Aviso de Privacidad, observando la expectativa razonable de privacidad a que se refieren las disposiciones oficiales en la materia.

Se entiende como expectativa razonable de privacidad, la confianza que deposita cualquier persona en el TUVCH, respecto de que los Datos Personales proporcionados, serán tratados conforme a lo acordado, en los términos establecidos por las leyes.

Por otra parte, ninguna Autoridad universitaria ni ninguna persona que colabore o participe con el TUVCH debe obtener Datos personales a través de medios engañosos o fraudulentos, privilegiando en todo momento la expectativa razonable de privacidad.

Lo anterior significa que no se recaben Datos personales con dolo, mala fe o negligencia y se informen todas las finalidades del Tratamiento en el Aviso de Privacidad.

Artículo 6. Información.

El TUVCH, en carácter de Sujeto Regulado y/o Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, a través de sus Autoridades universitarias, colaboradores/as y participantes, estará obligado a poner a disposición de los y las Titulares su Aviso de Privacidad -ya sea de manera física, electrónica, visual, sonoro o por cualquier medio o tecnología permitida por la ley-, a través del cual se deberán informar las características más importantes del Tratamiento al que serán

sometidos los Datos personales, antes de que sean recabados a fin de que pueda tomar decisiones informadas al respecto.

Las personas aspirantes, Comunidad universitaria y de terceras personas en general, tendrán derecho a conocer el Aviso de Privacidad correspondiente antes de proporcionar su información personal.

Artículo 7. Consentimiento.

Una vez que los y las Titulares hayan conocido el Aviso de Privacidad del TUVCH, de no oponerse al mismo, se entenderá que brindan su Consentimiento tácito, para la obtención y uso de los Datos personales; excepto en el caso de los Datos personales sensibles, financieros y patrimoniales, en el que las Autoridades universitarias deberán recabar el consentimiento expreso y por escrito, de conformidad con que establecen las disposiciones oficiales vigentes.

En cualquier momento del Tratamiento se podrá revocar el Consentimiento que se haya otorgado, siempre y cuando no exista alguna disposición normativa que obligue a continuar con éste.

No se requerirá del Consentimiento para el tratamiento de los Datos personales de los y las Titulares en los siguientes casos:

- I. Esté previsto en una ley;
- II. Los datos figuren en fuentes de acceso público;
- III. Los Datos personales se sometan a un procedimiento previo de disociación;
- IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre la persona Titular y el Sujeto Regulado y/o Responsable.

En caso de que sea necesaria la transferencia de Datos personales a terceros para el propósito al que se refiere la presente fracción, los terceros no podrán utilizar los Datos personales para propósitos distintos a aquellos para los cuales se les hubieren transmitido;

- V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
- VI. Cuando sean necesarios por razones estadísticas, científicas o de interés general, previo procedimiento por el cual no puedan asociarse los Datos personales con la persona Titular a la que se refieran;
- VII. Cuando exista una orden de autoridad competente que funde y motive la necesidad de recabarlos; y
- VIII. En los demás casos que se establezcan en la normatividad oficial vigente.

Artículo 8. Calidad.

El TUVCH, en carácter de Sujeto Regulado y/o Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, a través de sus Autoridades, colaboradores/as y participantes, estará obligado a tomar las medidas necesarias para que los datos sean exactos, completos, correctos y actualizados para los fines para los cuales se obtuvieron.

De igual forma, asume la obligación de borrar los Datos personales, cuando éstos hayan dejado de ser necesarios para el cumplimiento de las finalidades para las cuales se hayan obtenido.

Artículo 9. Finalidad.

Todos los Datos personales que sean objeto de Tratamiento por las Autoridades universitarias o por las y los colaboradores del TUVCH, así como las personas que participen con éste, se limitarán al cumplimiento de las finalidades (usos o propósitos) que fueron informadas en el Aviso de Privacidad.

Cuando se pretenda utilizar los Datos personales para un fin distinto, que no sea compatible o similar a aquéllos establecidos en el Aviso de Privacidad, se deberá obtener el Consentimiento expreso.

Artículo 10. Proporcionalidad.

Todos los Datos personales que sean objeto de Tratamiento por las Autoridades universitarias o por las y los colaboradores del TUVCH, así como por las personas que

participen con éste, deberán resultar necesarios, adecuados y relevantes para cumplir con las finalidades para las cuales se obtuvieron y, además deberán procurar solicitar a las y los Titulares el menor número posible de Datos personales.

El TUVCH, en carácter de Sujeto Regulado y/o Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, mediante sus Autoridades universitarias, colaboradores/as y participantes, estará obligado a tener especial cuidado con los Datos personales sensibles y sólo solicitarlos cuando éstos sean necesarios para la finalidad de que se trate, limitando el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

Artículo 11. Responsabilidad.

El TUVCH, en carácter de Sujeto Regulado y/o Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, por conducto de sus Autoridades universitarias, colaboradores/as y participantes, aplicará todas las medidas, las mejores prácticas y estándares en la protección de Datos personales y para la rendición de cuentas con relación al uso y cuidado de la información personal que esté en su posesión, así como de aquella que haya transmitido a terceros, garantizando que el aviso de privacidad sea respetado en todo momento.

Artículo 12. Seguridad.

El TUVCH, a través de sus Autoridades universitarias, colaboradores/as y participantes, resguardará los Datos personales bajo Medidas de seguridad adecuadas, físicas, administrativas y/o técnicas, que eviten su pérdida, alteración, destrucción, daño, uso, acceso o Tratamiento no autorizado.

Artículo 13. Confidencialidad de la información.

Todos los Datos personales tratados por las Autoridades universitarias o por las y los colaboradores o participantes del TUVCH, se mantendrán bajo estricta confidencialidad y no se difundirán ni compartirán con terceros, salvo que exista Consentimiento para ello o alguna obligación normativa requiera su difusión.

Cuando se contrate el servicio de una persona Encargada para el manejo de los Datos personales, el contrato respectivo contendrá cláusulas de confidencialidad y establecerá las obligaciones y responsabilidades de ésta, con relación al uso de los Datos personales.

Cuando sea necesaria la transferencia de Datos personales, previa a la formalización de un contrato, se deberá suscribir un convenio de confidencialidad. Este deber de confidencialidad subsistirá aún después de finalizar la relación con el titular de los datos o, en su caso, con el Sujeto Regulado y/o Responsable.

CAPÍTULO II

REMISIÓN Y TRANSFERENCIA DE DATOS PERSONALES

Artículo 14. Remisión.

Las remisiones nacionales e internacionales de Datos personales entre el Sujeto Regulado y/o Responsable y una persona encargada no requerirán ser informadas al Titular ni contar con su consentimiento.

La persona Encargada, será considerado responsable con las obligaciones propias de éste, cuando:

- I. Destine o utilice los Datos personales con una finalidad distinta a la autorizada por el Sujeto Regulado y/o Responsable; o
- II. Efectúe una transferencia, incumpliendo las instrucciones del Sujeto Regulado y/o Responsable.

La persona Encargada no incurrirá en responsabilidad cuando, previa indicación expresa del Sujeto Regulado y/o Responsable, remita los Datos personales a otro Encargado designado por este último, al que hubiera encomendado la prestación de un servicio o Transfiera los Datos personales a otro Responsable conforme a lo previsto en las disposiciones oficiales.

Artículo 15. Condiciones para la Transferencia.

La Transferencia de Datos personales, sea ésta nacional o internacional, se encontrará sujeta al Consentimiento de su Titular, salvo las excepciones previstas en las disposiciones oficiales en la materia y deberá ser informada a este último mediante el Aviso de Privacidad y limitarse a la finalidad que la justifique.

Asimismo, el tratamiento de los datos se hará conforme a lo convenido en el Aviso de Privacidad, el cual contendrá una cláusula en la que se indique si la persona Titular acepta o no la transferencia de sus datos.

Cuando se realice una Transferencia nacional, el área responsable deberá formalizarla mediante algún instrumento jurídico que cuente con las cláusulas contractuales correspondientes, que permita demostrar que el TUVCH comunicó al tercero receptor las condiciones en las que la o el Titular consintió el Tratamiento de sus Datos personales, en términos del Aviso de Privacidad, asimismo, dicho tercero asumirá las mismas obligaciones que el Sujeto Regulado y/o responsable.

Cuando se realice una Transferencia internacional, el área responsable deberá acordar o celebrar con el tercero receptor cláusulas contractuales u otros instrumentos jurídicos, en los que se prevean al menos, las mismas obligaciones a las que se encuentra obligado el Sujeto Regulado y/o responsable que transfiere los Datos personales, así como las condiciones en las que la o el Titular consintió el Tratamiento de sus Datos personales.

Artículo 16. Excepciones aplicables a las Transferencias del TUVCH.

No se requerirá consentimiento de las personas Titulares, cuando los Datos Personales:

- I. Se transfieran o compartan entre diferentes áreas del TUVCH, entidades académicas, sociedades que formen parte del sistema universitario jesuita, asociaciones civiles, sociedades e instituciones que obren enunciadas en el Aviso de Privacidad, para su tratamiento en el ámbito de su competencia;
- II. Cuando sea necesario para la prevención o el diagnóstico médico, prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
- III. La transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés de la persona Titular, por el Sujeto regulado y/o responsable y un tercero:

- IV. Para la salvaguarda de un interés público, o para la procuración o administración de justicia, ejercicio o defensa de un derecho en un proceso judicial, o
- V. La transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el Sujeto regulado y/o responsable y la persona Titular.

Siempre que se cumplan con las provisiones contenidas en los principios del presente Reglamento y los ordenamientos oficiales.

La excepción prevista en el inciso a), no será aplicable a las Autoridades universitarias, colaboradores/as y participantes del TUVCH, tratándose de la solicitud de información a los órganos disciplinarios internos sobre los procedimientos, resoluciones y personas que intervengan, cuando no sean parte en los referidos procedimientos.

Artículo 17. Obligaciones del TUVCH cuando funge como receptor de Datos personales.

Cuando el TUVCH sea receptor de Datos personales, por conducto de sus Autoridades, colaboradores/as y participantes, deberá tratarlos de conformidad con lo señalado en el Aviso de Privacidad, limitando el Tratamiento de los datos que son transferidos a las finalidades que justificaron las Transferencias.

De igual forma, asumirá las obligaciones que corresponden a la Responsable y/o el Sujeto Regulado que transfirió los datos previstos en el Aviso de Privacidad, incluyendo el deber de confidencialidad.

CAPÍTULO III

EJERCICIO DE DERECHOS ARCO

Artículo 18. Obligaciones generales.

La Oficina Jurídica en coordinación con la Abogacía General, en el ámbito de sus respectivas competencias, será la responsable de dar trámite a las solicitudes de las y los Titulares en el ejercicio de los Derechos ARCO y de la revocación del

Consentimiento, en los plazos establecidos por las normas oficiales en la materia, y tanto ésta, como las Autoridades universitarias, así como las personas colaboradoras y participantes, en el ámbito de sus atribuciones, atenderán las siguientes reglas:

- I. No se podrá condicionar el ejercicio de alguno de los Derechos ARCO a que se ejerza previamente otro derecho, ni impedir que se ejerza un derecho por el hecho que previamente se ejerció otro;
- II. La o el Titular, en el ejercicio del derecho de oposición, en la medida de lo posible, deberá justificar la situación específica por la que solicita el cese del tratamiento de sus datos personales ya sea, para evitar que su persistencia le cause un daño o perjuicio o, bien, si sus datos personales son objeto de un tratamiento automatizado que produzca una afectación significativa a sus intereses, derechos o libertades de la o el Titular;
- III. El ejercicio del derecho de cancelación no podrá limitarse porque la o el Titular haya ejercido el derecho de acceso con anterioridad;
- IV. Las Autoridades universitarias y las personas colaboradoras y participantes del TUVCH deberán resguardar los Datos personales de tal manera que se permita el ejercicio eficiente de los Derechos ARCO, así como el acceso a los Datos personales cuando proceda;
- V. En el caso de que se haya ejercido el derecho de acceso, el periodo en el cual la o el Titular podrá acceder a sus Datos personales en el sitio donde se encuentre la información, no podrá ser menor al establecido por la ley;
- VI. La Oficina Jurídica del TUVCH dará aviso de la rectificación o cancelación solicitada por el o la Titular a los terceros a los que se hayan transferido Datos personales, a fin de que realicen lo conducente;
- VII. Las Autoridades universitarias y las personas colaboradoras y participantes del TUVCH deberán rectificar los Datos personales cuando proceda su ejercicio, en los términos que indique la Abogacía General en coordinación con la Oficina Jurídica del TUVCH;

- VIII.** Cuando proceda la cancelación de Datos personales, se deberá establecer el periodo de bloqueo y notificarlo al o a la Titular, establecer Medidas de seguridad adecuadas para el periodo de bloqueo, llevar a cabo el bloqueo en el plazo que se indique en las disposiciones oficiales en la materia y transcurrido el periodo de bloqueo, suprimir los Datos personales;
- IX.** No procederá la cancelación de Datos personales en los casos en que así lo señalen las disposiciones oficiales;
- X.** Se deberán bloquear los Datos personales, previa supresión, y no tratarlos en ese periodo, salvo con fines de almacenamiento, legales y de responsabilidad;
- XI.** Las Autoridades universitarias y las personas colaboradoras y participantes del TUVCH no deberán tratar los Datos personales para las finalidades correspondientes, cuando proceda el ejercicio de oposición;
- XII.** En todos los casos de negativa de ejercicio de los Derechos ARCO o revocación del Consentimiento, se deberá justificar con las consideraciones legales adecuadas, y se deberá informar a la persona Titular el derecho que le asiste para solicitar a la autoridad oficial el inicio del procedimiento de protección de derechos; y
- XIII.** Las Autoridades universitarias y las personas colaboradoras y participantes del TUVCH deberán participar en la gestión de listados de exclusión para llevar un control sobre el ejercicio del derecho de oposición.

Se entenderá por listado de exclusión la base de datos que tiene por objeto registrar de manera gratuita la negativa de la persona Titular al tratamiento de sus Datos personales.

Artículo 19. Medios para el ejercicio de los Derechos ARCO.

El o la Titular, para el ejercicio de los Derechos ARCO, podrá presentar, por sí mismo o a través de su representante, la solicitud de ejercicio de estos derechos, por medio del Buzón de datos personales, cumpliendo con los requisitos señalados en el Aviso de Privacidad.

El TUVCH podrá establecer formularios, sistemas y otros métodos simplificados para facilitar al o a la Titular el ejercicio de los Derechos ARCO.

Tratándose del ejercicio de Derechos ARCO de personas fallecidas, la solicitud podrá presentarse por aquellos que acrediten su interés legítimo, en los términos establecidos en las disposiciones oficiales.

En el Tratamiento de Datos personales en los que la o el Titular sea menor de edad, o de personas con discapacidad o que se encuentren en estado de interdicción, se tomarán las medidas necesarias para otorgar su máxima protección y se dará cuenta al padre, a la madre o a quien ejerza su tutela, así como a las autoridades gubernamentales competentes conforme a las disposiciones oficiales.

TÍTULO III

MEDIDAS DE PREVENCIÓN

CAPÍTULO I

DISPOSICIONES GENERALES APLICABLES A LAS MEDIDAS DE PREVENCIÓN

Artículo 20. Medidas de Prevención.

Las medidas de prevención tienen como objetivo establecer las acciones de seguridad, administrativas, técnicas, físicas y digitales que el TUVCH implementará para garantizar la protección de los Datos personales de las y los integrantes de la Comunidad universitaria, así como de cualquier persona de la que se traten dichos datos, dentro y fuera de las instalaciones.

Las medidas de prevención deberán permitir el ejercicio de los Derechos ARCO en los términos establecidos en las disposiciones oficiales en materia de protección de Datos personales en posesión de los particulares.

CAPÍTULO II

DE LAS MEDIDAS DE PREVENCIÓN GENERALES Y ESPECÍFICAS

Artículo 21. Medidas de Prevención Generales.

Todo el personal y las Autoridades universitarias del TUVCH, según el ámbito de sus atribuciones, son responsables de la prevención y deberán ejecutar las siguientes medidas generales:

- I. Promover y divulgar el presente Reglamento con el personal a su cargo;
- II. Antes de recabar Datos personales, poner a disposición de las y los Titulares el Aviso de Privacidad integral;
- III. Definir, implementar y operar sus objetivos, lineamientos, procesos, procedimientos, controles y mecanismos indicadores que permitan la medición de las vulneraciones a la seguridad, en las actividades que involucran el Tratamiento de Datos personales, tanto en los ambientes físicos como en los digitales, en apego a lo establecido en el presente Reglamento y en el resto de la normatividad universitaria, lo cual deberá contemplar, por lo menos:
 - a) La vigilancia del entorno de trabajo físico, dentro de las instalaciones de la universidad;
 - b) Establecer las Medidas de seguridad para el trabajo a distancia extraordinario; y
 - c) Prevenir el robo de información, tanto físico como digital.
- IV. Establecer los criterios mínimos para el tratamiento de Datos biométricos, en el ámbito de su competencia, previa autorización de la Oficina Jurídica, en coordinación con la Abogacía General, y considerando la guía, criterios o documento orientador sobre el Tratamiento de datos biométricos vigente, emitida por las autoridades oficiales, nacionales o internacionales de las que México forme parte, en la materia;
- V. Cumplir con todas las Medidas de seguridad, especialmente con aquellas en materia de seguridad de la información establecidas en la normatividad universitaria vigente, procurando la autenticación de los usuarios en los

sistemas de Tratamiento de Datos personales, y su control de acceso, así como vigilar su cumplimiento, en el ámbito de su competencia;

- VI.** Implementar, dentro de sus áreas, las Medidas de seguridad establecidas en la *Guía de borrado seguro* (**Anexo Único** de este Reglamento), cuyo cumplimiento es de observancia obligatoria.

Las Medidas de seguridad deberán ser implementadas previo a la recolección de Datos personales y durante todo su Tratamiento, en caso contrario, la Autoridad universitaria correspondiente asumirá el riesgo ante una vulneración de los Datos personales tratados por medios físicos o electrónicos;

- VII.** Eliminar los Datos personales que ya no sean necesarios para realizar las finalidades previstas en el Aviso de Privacidad correspondiente, de conformidad con el Plazo de conservación establecido de acuerdo con la legislación en materia de archivos y con la *Guía de borrado seguro*; y notificar a la Oficina Jurídica y a la Auditoría Interna, previo a que se realice el borrado, supresión o cancelación de Datos personales;

- VIII.** Reportar a la Dirección de Administración y Finanzas, por conducto de la Coordinación de Informática, todos aquellos sistemas o bases de datos electrónicos que contengan Datos personales tratados en el ejercicio de las atribuciones del área a su cargo y que hayan sido generados sin conocimiento ni asistencia de dicha Coordinación;

- IX.** Participar en todas las capacitaciones en materia de protección de Datos personales que se promuevan al interior del TUVCH y promover la participación de su personal en éstas;

- X.** Cumplir con las Medidas de seguridad aplicables a las Transferencias y Remisiones de Datos personales y sobre la recolección de éstos a través de una persona Encargada o un tercero, establecidas en las disposiciones oficiales en materia de protección de Datos personales en posesión de los particulares;

- XI.** Cumplir con las Medidas de seguridad basadas en la aplicación de procesos de anonimización, minimización y disociación para el uso de Datos personales.

Para efectos de lo anterior, se entenderá por:

- a) **Anonimización:** Consiste en eliminar o reducir al mínimo los riesgos de re-identificación de los Datos personales;
- b) **Minimización:** Se refiere a que el Sujeto Regulado y/o Responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento; y
- c) **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.

XII. Cuando se requiera recabar Datos personales por medio de sistemas electrónicos, emplear exclusivamente los institucionales que cuenten con la debida licencia o, de manera excepcional y justificada, solicitar la autorización de la Coordinación de Informática para utilizar sistemas no institucionales;

XIII. Para el tratamiento de imágenes y/o voz de las y los Titulares de Datos personales con fines publicitarios, se requerirá su consentimiento previo y por escrito, el cual deberá manifestarse a través de los documentos que para tal fin sean facilitados por la Oficina Jurídica;

XIV. Vigilar que su Aviso de Privacidad integral se mantenga actualizado en todos los medios, tanto físicos como digitales;

XV. Notificar a la Oficina Jurídica la necesidad de realizar cambios en el Aviso de Privacidad integral, sobre todo cuando requieran modificaciones en las finalidades primarias, Transferencias o en el tipo de Datos personales o Datos personales sensibles que recaban;

XVI. Notificar de inmediato a la Coordinación de Informática, cualquier vulneración a los Datos personales por un medio o canal digital, o a la Secretaría Ejecutiva si se trata de una vulneración por medios físicos, a fin de que notifiquen a la Dirección General y a la Oficina Jurídica, para que cada una

de estas áreas efectúe las acciones necesarias para solventar la problemática, en el ámbito de su competencia;

- XVII.** Notificar a la Coordinación de Informática cuando algún sistema y/o aplicación que usen o pretendan utilizar procese o almacene Datos personales;
- XVIII.** Para realizar el borrado seguro de los Datos personales en el caso de trabajo extraordinario a distancia, los soportes que contengan dichos datos deberán ser trasladados a la Universidad, para garantizar que sean destruidos o eliminados de forma adecuada, de conformidad con lo establecido en el **Anexo Único “Guía de Borrado Seguro”** del presente Reglamento;
- XIX.** Notificar a la Auditoría Interna y a la Coordinación de Recursos Humanos los casos de incumplimiento de lo establecido en el presente Reglamento por parte del personal a su cargo; y
- XX.** En caso de incumplimiento de lo establecido en el presente Reglamento por parte del personal a su cargo, participar con la Coordinación de Recursos Humanos para que ésta determine y aplique las sanciones correspondientes, de acuerdo con lo establecido en la normatividad universitaria, en el contrato correspondiente y en su caso, en el Reglamento Interior de Trabajo.

Artículo 22. Medidas de Prevención Específicas de las áreas que realizan investigación académica.

Cualquier área del TUVCH que realice investigación académica será responsable de ejecutar las siguientes medidas de prevención específicas:

- I.** El Tratamiento de Datos personales en función de la finalidad investigadora y su divulgación, deberá llevarse a cabo procurando emplear procesos de anonimización, minimización y disociación, evitando en todo momento la comunicación de Datos personales a terceros ajenos al TUVCH sin contar con el Consentimiento de las personas Titulares;
- II.** En las encuestas relacionadas con proyectos de investigación en las que se recaben Datos personales, deberá insertarse un enlace con el Aviso de Privacidad integral y, tratándose de Datos personales sensibles, será necesario

recabar el Consentimiento por escrito y de manera expresa, de las personas Titulares de dichos datos; y

- III. El tratamiento de Datos personales que se lleve a cabo con motivo de investigaciones que se realicen con la participación de terceras personas o instituciones, y dichos datos sean recabados o usados por éstas, deberá informarse de dicha situación a las personas Titulares, poniendo a su disposición el Aviso de Privacidad integral.

Artículo 23. Medidas de Prevención Específicas de las instancias universitarias que atienden y resuelven procedimientos relacionados con la disciplina y el orden al interior de la Comunidad universitaria.

Las instancias universitarias que atienden y resuelven procedimientos relacionados con la disciplina y el orden al interior de la Comunidad universitaria serán responsables de ejecutar las siguientes medidas de prevención específicas:

- I. Poner a disposición de las personas de las que se requiera recabar Datos personales con motivo de la investigación de los casos que les competa conocer, el Aviso de Privacidad correspondiente, previo a su obtención;
- II. Resguardar y tomar las Medidas de seguridad que se estimen pertinentes para la protección de los Datos personales que se recaben con motivo de la investigación de los casos que les competa conocer, particularmente respecto de las resoluciones o dictámenes que se emitan, y
- III. Transferir los Datos personales que traten, sólo cuando se fundamente esta necesidad en las disposiciones institucionales u oficiales vigentes.

Artículo 24. Medidas de Prevención Específicas de la Abogacía General.

La Abogacía General será responsable de ejecutar las siguientes medidas de prevención específicas:

- I. Aprobar el procedimiento de atención a las solicitudes que se reciben en el Buzón de Datos personales del TUVCH;
- II. Aprobar el Aviso de Privacidad Integral del TUVCH;

- III. Atender, gestionar y dar curso a las solicitudes de Derechos ARCO que se reciban en el Buzón de Datos personales de TUVCH;
- IV. Autorizar el procedimiento a seguir para diseñar, establecer y difundir la actualización o cambios en el Aviso de Privacidad integral que soliciten las diferentes áreas del TUVCH;
- V. Apoyar a la Oficina Jurídica para brindar asesoría a las diferentes áreas del TUVCH, en materia de protección de Datos personales, así como para elaborar materiales de difusión dirigidos a la Comunidad universitaria;
- VI. Coadyuvar con la Oficina Jurídica en la revisión de los contenidos de las capacitaciones en materia de protección de Datos personales y, en su caso, apoyar en su impartición;
- VII. Determinar la procedencia de notificar alguna vulneración de Datos personales a las personas Titulares afectadas, así como, en coadyuvancia con la Oficina Jurídica, de dar aviso y/o denunciar el hecho ante las autoridades correspondientes cuando se trate de la vulneración de datos previstas en los artículos 39 y 40 del presente Reglamento, y
- VIII. Atender y dar seguimiento a los procedimientos administrativos o judiciales que se generen ante la autoridad oficial en la materia.

Artículo 25. Medidas de Prevención Específicas de la Oficina Jurídica.

La Oficina Jurídica será responsable de ejecutar las siguientes medidas de prevención específicas:

- I. Proponer a la Abogacía General la difusión del procedimiento de atención a las solicitudes que se reciben en el Buzón de Datos personales y, en su caso, proponer los ajustes a que haya;
- II. Presentar a la Abogacía General el proyecto de Aviso de Privacidad integral del TUVCH así como sus actualizaciones y coordinarse con la Dirección de

Promoción y Comunicación Institucional para su implementación, una vez aprobado;

- III. Coadyuvar con la Abogacía General en la atención y gestión de las solicitudes de Derechos ARCO que se reciban en el Buzón de Datos personales;
- IV. Brindar asesoría a las diferentes áreas del TUVCH en materia de protección de Datos personales, en coordinación con la Abogacía General;
- V. Apoyar a la Coordinación de Recursos Humanos en la revisión de los contenidos de las capacitaciones en materia de protección de Datos personales, en coordinación con la Abogacía General, y
- VI. Coadyuvar con la Abogacía General en los procedimientos administrativos o judiciales que se generen ante la autoridad oficial en la materia.

Artículo 26. Medidas de Prevención Específicas de la Auditoría Interna.

La Auditoría Interna será responsable de ejecutar las siguientes medidas de prevención específicas:

- I. Diseñar, establecer y difundir el procedimiento a seguir para supervisar el cumplimiento de las obligaciones establecidas en el presente Reglamento y la atención a las consultas que puedan surgir por parte de las áreas universitarias con respecto al tema de protección de Datos personales;
- II. Supervisar el cumplimiento de las obligaciones en materia de la protección de Datos personales, que se señalan en el presente Reglamento;
- III. Dar seguimiento a los compromisos o acuerdos que se establezcan con las Autoridades universitarias, derivados de la supervisión enunciada en el presente artículo;
- IV. Emitir recomendaciones a las Autoridades universitarias, sobre las áreas de oportunidad que resulten de la supervisión a que se refiere el presente artículo o por algún hallazgo propio de la de Auditoría Interna, y

- V. En los casos de incumplimiento del presente Reglamento por parte del personal, realizar la investigación correspondiente y emitir un informe al respecto, dirigido a la Autoridad universitaria que tiene a su cargo el personal que, en su caso, realizó el incumplimiento y a la Coordinación de Recursos Humanos.

Artículo 27. Medidas de Prevención Específicas de la Dirección de Administración y Finanzas.

La Dirección de Administración y Finanzas será responsable de ejecutar las siguientes medidas de prevención específicas:

- I. Vigilar que se mantenga actualizado el Aviso de Privacidad sonoro, que aparece en el conmutador del TUVCH, así como asegurarse de que aparezca al inicio de la grabación;
- II. Mantener actualizado y visible el Aviso de Privacidad sobre las cámaras de seguridad, así como asegurarse que esté ubicado en todos los accesos a las instalaciones del TUVCH;
- III. Atender las solicitudes de las Autoridades universitarias sobre la señalética que contenga Avisos de Privacidad;
- IV. En coordinación con la Autoridad Universitaria que tenga a su cargo al personal que se vea involucrado en el incumplimiento del presente reglamento, deberá determinar y aplicar las sanciones correspondientes, de acuerdo con lo establecido en la normativa universitaria, el contrato correspondiente y, en su caso, el Reglamento Interior de Trabajo, y
- V. Velar por el adecuado Tratamiento de los Datos personales contenidos en los registros de personas que visitan el TUVCH.

Artículo 28. Medidas de Prevención Específicas de la Dirección de Promoción y Comunicación Institucional.

La Dirección de Promoción y Comunicación Institucional será responsable de ejecutar las siguientes medidas de prevención específicas:

- I. Mantener actualizada la liga y la página electrónica institucional, en que se encuentre alojado el Aviso de Privacidad Integral, así como alojar la versión vigente de éste, al momento en que lo solicite la Oficina Jurídica, y
- II. Difundir las campañas de cultura para la protección de Datos personales, que le solicite la Oficina Jurídica.

Artículo 29. Medidas de Prevención Específicas de la Dirección de Desarrollo y Fomento Institucional.

La Dirección de Desarrollo y Fomento Institucional será responsable de ejecutar las medidas de prevención específicas, consistentes en solicitar, resguardar y eliminar la información generada:

- I. Con motivo de la vinculación que realicen las áreas que dependen de esta, con instituciones públicas y privadas u organizaciones civiles nacionales e internacionales;
- II. De personas egresadas y externas del TUVCH que acudan a alguna actividad de educación continua o idiomas, y
- III. De los y las menores de edad que realicen prácticas, servicio social o prácticas profesionales en el TUVCH.

Lo anterior, de acuerdo con lo especificado en el presente Reglamento.

Artículo 30. Medidas de Prevención Específicas de la Dirección Académica

La Dirección Académica será responsable de ejecutar las medidas de prevención específicas, consistentes en:

- I. Mantener en resguardo los expedientes del estudiantado y no proporcionar información ni documentación a personas que no estén autorizadas por estos, y
- II. Solo compartir la información del estudiantado a otras áreas del TUVCH, cuando justifiquen su aplicación en las actividades correspondientes a su cargo.

Artículo 31. Medidas de Prevención Específicas de la Dirección del Medio Universitario

La Dirección del Medio Universitario será responsable de ejecutar las medidas de prevención específicas, consistente en:

- I. Cuidar el manejo de los Datos personales en las transmisiones que se realicen desde TUVCH Radio, y
- II. Resguardar la información y documentación que se recabe derivado de los programas de cultura, deporte y bienestar, y del Área de Reflexión Universitaria.

Artículo 32. Medidas de Prevención Específicas de la Coordinación de Informática.

La Coordinación de Informática será responsable de ejecutar las siguientes medidas de prevención específicas:

- I. Coadyuvar con las Autoridades universitarias, en la implementación de sistemas de gestión de seguridad de Datos personales, en el ámbito de sus respectivas competencias, que abarquen todos los sistemas de la Universidad;
- II. Establecer y aplicar los criterios mínimos para la contratación de servicios de cómputo en la nube, a nivel institucional, en los casos en que ello implique el Tratamiento de Datos personales, considerando las recomendaciones, guías, documentos o disposiciones expedidas por la autoridad oficial en la materia;
- III. Aplicar metodologías de análisis de riesgo, considerando los estándares previstos en las guías, recomendaciones y en las Normas Mexicanas en la materia, emitidas por las autoridades oficiales;
- IV. Diseñar, implementar y difundir un plan de Manejo de Incidentes de Seguridad de Datos personales, considerando las recomendaciones, guías, documentos o disposiciones expedidas por la autoridad oficial en la materia;
- V. Apoyar a la Dirección de Promoción y Comunicación Institucional, en los aspectos técnicos, para que ésta pueda atender las solicitudes de sustitución o

implementación del Aviso de Privacidad integral, que requieran las diferentes áreas, una vez que haya sido autorizado por la Oficina Jurídica a las mismas;

- VI. Asegurarse que el Aviso de Privacidad integral, que aparece en los diferentes sistemas del TUVCH, se muestre antes de que se recolecten los Datos personales;
- VII. Realizar, paulatinamente y de acuerdo a la disponibilidad técnica y presupuestal, las adecuaciones necesarias en todos los sistemas institucionales, incluyendo los existentes, aquellos por desarrollarse y los desarrollados por externos, a fin de apoyar al área que tenga a su cargo el Buzón de Datos personales, para que pueda brindar pronta atención a las solicitudes de Derechos ARCO, en cuanto al acceso, rectificación, exclusión, bloqueo, cancelación, oposición y borrado de los datos personales en los sistemas, considerando los ejercicios de derechos ARCO que resultaren procedentes;
- VIII. Dar atención a todos los requerimientos de los activos informáticos que impliquen el Tratamiento de Datos personales de cada área del TUVCH;
- IX. Emitir y difundir los criterios necesarios para la protección de los Datos personales en todos los sistemas electrónicos empleados por el TUVCH;
- X. Establecer las medidas de seguridad de la información que se encuentre en medios electrónicos, para un apropiado tratamiento de los riesgos a los cuales se hallan expuestos los Datos personales en posesión del TUVCH, considerando las recomendaciones, guías, documentos o disposiciones expedidas por la autoridad oficial en la materia, y
- XI. Colaborar en la concientización de la Comunidad universitaria, en materia de seguridad de la información en medios electrónicos.

Artículo 33. Medidas de Prevención Específicas de la Coordinación de Recursos Humanos.

La Coordinación de Recursos Humanos será responsable de ejecutar las siguientes medidas de prevención específicas:

- I. Diseñar e impartir, en conjunto con la Oficina Jurídica y por lo menos 2 veces al año, capacitación en materia de protección de Datos personales a las y los colaboradores del TUVCH;
- II. Asegurar que todos los contratos del personal del TUVCH, así como de las personas prestadoras de servicios profesionales, contengan la cláusula de confidencialidad respecto de los Datos personales que traten;
- III. En coordinación con la Autoridad universitaria que tenga a su cargo al personal que se vea involucrado en el incumplimiento del presente Reglamento, deberá determinar y aplicar las sanciones correspondientes, de acuerdo con lo establecido en la normatividad universitaria, el contrato correspondiente y, en su caso, el Reglamento Interior de Trabajo;
- IV. Establecer los criterios y estándares mínimos de protección para el tratamiento de Datos personales biométricos en el ámbito laboral, con base en lo establecido en las disposiciones emitidas por las autoridades oficiales, cuyo cumplimiento será de observancia obligatoria;
- V. Por conducto del servicio médico:
 - a) Observar las disposiciones oficiales en materia de salud, así como las Normas Oficiales Mexicanas en la materia, relacionadas con la protección de Datos personales;
 - b) Reconocer que la titularidad de los Datos personales y Datos personales sensibles le pertenece a las personas de las cuales son inherentes, procediendo de conformidad con lo establecido en el artículo 7 del presente Reglamento, contenidos en los expedientes del servicio médico del TUVCH;
 - c) Abstenerse de solicitar Datos personales o Datos personales sensibles que sean innecesarios para el servicio que prestan;
 - d) Cumplir estrictamente con lo previsto en la fracción VII del artículo 21 de este Reglamento, y

- e) Asegurarse o gestionar, en su caso, los convenios con terceras personas para prestar servicios de laboratorio médico u otro que implique tratamiento de Datos personales sensibles del personal o del estudiantado, y que dichas terceras personas pongan a disposición el Aviso de privacidad correspondiente para su firma autógrafa.

TÍTULO IV

PROCESOS QUE IMPLIQUEN TRATAMIENTO DE DATOS PERSONALES

CAPÍTULO ÚNICO

PROCESOS QUE IMPLIQUEN TRATAMIENTO DE DATOS PERSONALES

Artículo 34. Inventario

La Coordinación de Informática llevará un inventario de los sistemas y bases de datos electrónicos, institucionales o no institucionales, que contengan Datos personales, que obren en el TUVCH y deberá mantenerlo actualizado.

Las diversas Áreas del TUVCH deberán colaborar con la Coordinación de Informática en la construcción y actualización de este inventario, en el ámbito de sus competencias.

Artículo 35. Nuevos procesos.

Cualquier nuevo programa, mecanismo, política o procedimiento por medio del cual se realice el Tratamiento de Datos personales, solo podrá llevarse a cabo cuando se cuente con el previo visto bueno de la Oficina Jurídica, en coordinación con la Abogacía General.

Artículo 36. Servicios en la nube.

Para el Tratamiento de Datos personales en servicios, aplicaciones e infraestructura, así como en el denominado cómputo en la nube, solo se podrán utilizar aquellos servicios que cuenten con los requisitos que marcan las disposiciones oficiales aplicables y, además, hayan sido aprobados por la Oficina Jurídica del TUVCH y por la Coordinación de Informática.

Los proveedores de este tipo de servicios deberán contar con las Medidas de seguridad o, en su defecto, establecer las adoptadas por el TUVCH, en atención a los riesgos del Tratamiento y naturaleza de los Datos personales.

El TUVCH no podrá adherirse a servicios que no garanticen, mediante el contrato correspondiente, la debida protección de los Datos personales.

Artículo 37. Uso de Inteligencia artificial.

Todo Tratamiento de Datos personales que implique el uso de inteligencia artificial deberá apegarse a las disposiciones oficiales aplicables y emplearse únicamente los servicios y licencias aprobados y proporcionados por la Coordinación de Informática.

La Coordinación de Informática deberá asegurarse de que los proveedores de este tipo de servicios cuenten con las Medidas de seguridad necesarias para evitar riesgos en el tratamiento de Datos personales.

Artículo 38. Subcontratación.

Toda subcontratación de servicios por parte del TUVCH, que implique el Tratamiento de Datos personales, deberá ser autorizada por la Oficina Jurídica y por la Coordinación de Informática, asimismo, deberá ser formalizada con la entidad Encargada mediante algún instrumento jurídico que cuente con las cláusulas contractuales correspondientes.

La entidad Encargada deberá realizar el Tratamiento de Datos personales de conformidad con lo establecido en el Aviso de privacidad integral, el instrumento contractual celebrado con el TUVCH y las disposiciones institucionales y oficiales vigentes.

Sólo se permitirá la transmisión de los Datos personales en posesión del TUVCH a terceros cuando obre autorizada la subcontratación y la transferencia de dichos datos por la Oficina Jurídica y por la Coordinación de Informática, en los casos en que se trate de cuestiones tecnológicas, incluso aquellas con fines de conservación, y siempre en apego a lo señalado en el presente Reglamento y a las buenas prácticas emitidas por las autoridades oficiales.

TÍTULO V

VULNERACIÓN

CAPÍTULO ÚNICO

VULNERACIÓN

Artículo 39. Vulneración de Datos personales.

Toda vulneración de seguridad de Datos personales ocurrida en cualquier fase del Tratamiento deberá ser informada de inmediato a la Secretaría Ejecutiva quien dará aviso a la Dirección General, a la Oficina Jurídica y a la Coordinación de Informática, así como a cualquier otra Autoridad universitaria que considere pertinente, a fin de que se tomen las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación con el objeto de analizar sus causas e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes.

De confirmarse una afectación significativa de los derechos patrimoniales o morales de las y los Titulares de los Datos personales, la Abogacía General determinará la procedencia de notificar a las personas Titulares afectadas y, en coadyuvancia con la Oficina Jurídica, de dar aviso y/o denunciar el hecho ante las autoridades correspondientes.

Las Autoridades universitarias señaladas en el primer párrafo de este artículo analizarán sus causas e implementarán las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes a efecto de evitar que la vulneración se repita.

Todas las áreas del TUVCH deberán reportar a la Auditoría Interna cualquier vulneración que ocurra por medios físicos o electrónicos en cualquier espacio de la Universidad, y ésta registrará el incidente en una bitácora de vulneraciones, la cual deberá contener: descripción de la vulneración, en qué consistió la vulneración, la fecha, el motivo o la causa y las acciones correctivas.

Artículo 40. Catálogo de vulneración.

Se entenderá como vulneración el incidente de seguridad que afecta los Datos personales en cualquier fase de su tratamiento, de manera enunciativa más no limitativa:

- I. La pérdida o destrucción no autorizada;
- II. El robo, extravío o copia no autorizada;
- III. El uso, acceso o Tratamiento no autorizado, incluyendo la imagen o voz de las personas integrantes de la Comunidad universitaria;
- IV. El daño, la alteración o modificación no autorizada, y
- V. La revelación o exposición de información a través de internet o medios masivos de comunicación.

TÍTULO VI

RESPONSABILIDADES, SANCIONES Y CUMPLIMIENTO

CAPÍTULO ÚNICO

RESPONSABILIDADES, SANCIONES Y CUMPLIMIENTO

Artículo 41. De las Causas de Responsabilidad.

Serán causas de responsabilidad de las Autoridades universitarias y de las personas colaboradoras y participantes del TUVCH, las siguientes:

- I. Tratar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente documentos que contengan Datos personales, de manera indebida, incluyendo la imagen de la o del Titular, que se encuentren bajo su custodia, a los cuales tengan acceso o conocimiento con motivo de su contrato, empleo, cargo o comisión;
- II. Tratar Datos personales sin haber puesto a disposición de la persona Titular el Aviso de Privacidad correspondiente o sin recabar su Consentimiento por escrito, en los casos en que las disposiciones oficiales lo requieran;

- III. Actuar con negligencia, dolo o mala fe en la substanciación de las solicitudes de Derechos ARCO;
- IV. Entregar información clasificada como reservada o confidencial a terceros ajenos, sin previa autorización de su superior jerárquico o contraviniendo lo establecido en el presente Reglamento;
- V. Entregar de manera incompleta información requerida en una solicitud de acceso;
- VI. No proporcionar información o Datos personales, o bien, no rectificar, cesar en el Tratamiento o cancelar estos últimos como resultado de un ejercicio de Derechos ARCO, que fuere procedente;
- VII. Declarar dolosamente la inexistencia de información o de Datos personales, cuando ésta exista total o parcialmente en los archivos del TUVCH;
- VIII. Omitir reiteradamente dar respuesta a las solicitudes de Derechos ARCO, dentro de los plazos indicados por la Abogacía General en coordinación con la Oficina Jurídica y los previstos en las disposiciones oficiales;
- IX. No proporcionar a la Oficina Jurídica del TUVCH los documentos e información que deban recibir o sean requeridos para la atención de los ejercicios de Derechos ARCO, dentro de los plazos indicados por la Oficina Jurídica en coordinación con la Abogacía General y los establecidos en las disposiciones oficiales;
- X. Obstruir el ejercicio de vigilancia y revisión al cumplimiento que la Auditoría Interna realice;
- XI. Usar ilícitamente los Datos personales, de conformidad con lo establecido en las disposiciones oficiales vigentes;
- XII. No acatar, por dolo o negligencia, las indicaciones emitidas por la Abogacía General o por la Oficina Jurídica, como resultado de un ejercicio de Derechos ARCO;

- XIII.** Abstenerse de informar a la Coordinación de Informática sobre los sistemas o bases de datos electrónicos que contengan Datos personales y que hayan sido generados sin conocimiento ni asistencia de aquella;
- XIV.** No acatar las Medidas de seguridad y/o disposiciones institucionales vigentes en materia de seguridad de la información, establecidas en la normatividad universitaria vigente, y
- XV.** No observar cualquier otra cuestión prevista en el presente Reglamento, en la normatividad universitaria vigente o en las disposiciones oficiales aplicables.

Artículo 42. Sanciones.

Las Autoridades universitarias, así como las personas colaboradoras y participantes del TUVCH que incurran en una conducta de responsabilidad, de las señaladas en el artículo anterior, serán sancionadas de conformidad con lo establecido en la normatividad universitaria y en el contrato respectivo, sin perjuicio de la participación que corresponda a la Auditoría Interna.

La reincidencia será considerada como grave para efectos de la sanción que se imponga.

Artículo 43. Verificación de Cumplimiento del Reglamento.

La Auditoría Interna, con el objeto de supervisar el cumplimiento del presente Reglamento, podrá iniciar las acciones necesarias para ello, en las que podrá requerir a las Autoridades universitarias acreditar evidencias de las obligaciones aquí consignadas, así como efectuar revisiones en sus expedientes y bases de datos.

Si en virtud de la verificación hecha por la Auditoría Interna se detecta el ocultamiento de información o incumplimientos a alguna de las disposiciones del presente Reglamento y/o de las disposiciones oficiales, se sancionará a la persona responsable de conformidad con lo señalado en el artículo anterior.

TRANSITORIOS

PRIMERO. El presente Reglamento entrará en vigor a partir del día hábil siguiente a su publicación en el Comunicado Oficial del TUVCH.

SEGUNDO. La dirección de correo electrónico que fungirá como Buzón de datos personales del TUVCH, en tanto no se modifique, será: datospersonales@tuvch.mx

En caso de no poder contactar con el Buzón de datos personales de manera electrónica, se podrá acudir de forma presencial ante la Oficina Jurídica, en un horario de 9:00 a 13:00 horas, de lunes a viernes, en la siguiente dirección:

Av. Tezozómoc s/n, esquina Popocatepetl, Colonia Alfredo Baranda, Cp. 56610, Valle de Chalco, Solidaridad, Estado de México, dentro de la Dirección General.

TERCERO. La implementación de las medidas tecnológicas previstas en los artículos 21, fracciones III, IV y VIII, 32 fracciones I, III, VII, IX y X y 34 del presente Reglamento se hará de manera paulatina en atención a las capacidades técnicas, económicas y de personal del TUVCH.

CUARTO. La implementación del plan de Manejo de Incidentes de Seguridad de Datos personales prevista en el artículo 32 fracción IV, deberá efectuarse dentro de un plazo de 6 meses contados a partir de la entrada en vigor del presente Reglamento.

QUINTO. En tanto no se cuente con personal de auditoría interna del TUVCH, las funciones de dicho ámbito las ejercerá la Auditoría Interna de la Universidad Iberoamericana Ciudad de México.

La Secretaría Ejecutiva del TUVCH fungirá como enlace entre las áreas internas con la Auditoría Interna de la Universidad Iberoamericana Ciudad de México.

SEXTO. La Norma Oficial Mexicana en materia de salud, a la que se refiere el artículo 33, fracción V, inciso a) del presente Reglamento, es la NOM-004-SSA3-2012, en tanto no se modifique.

ANEXO ÚNICO

GUÍA PARA EL BORRADO SEGURO DE DATOS PERSONALES EN EL TECNOLÓGICO UNIVERSITARIO DEL VALLE DE CHALCO

La destrucción y borrado de información es un tema de vital importancia para proteger la confidencialidad, integridad y disponibilidad de la información, y en particular de los Datos personales, por esta razón, se deben analizar los medios más eficaces para evitar que se pueda recuperar la información que ya no se requiere.

Las técnicas de borrado seguro buscan que no sea posible recuperar la información, tanto física como electrónica, cuando haya dejado de ser necesaria para el cumplimiento de las finalidades previstas en el Aviso de Privacidad y las disposiciones legales aplicables; y evitan que personas no autorizadas puedan tener acceso a esos datos.

GENERALIDADES

1.- Glosario

Para los efectos del presente Anexo, además de las definiciones establecidas en el Reglamento, se entenderá por:

- I. **Borrado seguro:** Medida de seguridad por la cual se establecen métodos y técnicas para la eliminación definitiva de los Datos personales, de modo que la probabilidad de recuperarlos sea mínima;
- II. **Medio electrónico:** Todo recurso de almacenamiento al que se puede acceder sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido, para examinar, modificar o almacenar los Datos personales, incluidos los *microfilms*. Podemos considerar entre estos medios, por ejemplo, a los discos duros (tanto los propios del equipo de cómputo como los portátiles), memorias extraíbles como *USB* o *SD*, *CDs*, videocasetes, *DvDs*, *Blue-rays*, entre otros, incluyendo el uso de servicios de almacenamiento en línea;

- III. **Medio físico:** Todo recurso de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o resguardar los Datos personales. Por ejemplo: archiveros, gavetas, cajones, carpetas, documentos, etc., y
- IV. **Sobreescritura:** Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de *software*.

2.- Responsabilidades de las áreas del TUVCH

Con base en la *Guía para el Borrado seguro de Datos Personales*, emitida por el entonces Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ², todas las áreas del TUVCH, a través de sus titulares, que realicen Borrado seguro deberán:

- I. Documentar los procesos y procedimientos para el Borrado seguro de Datos personales a seguir al interior de estas, de conformidad con lo establecido en el presente Anexo;
- II. Establecer los plazos de conservación de los Datos personales y de los medios de almacenamiento que les contengan, tanto físicos como electrónicos, con base en los siguientes 4 aspectos:
 - a) La naturaleza de los Datos personales contenidos;
 - b) Tiempo requerido para llevar a cabo las finalidades del tratamiento;
 - c) Plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables; y

² Consultable en: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_Borrado_Seguro_DP.pdf

- d) Periodo de bloqueo. El cual se efectúa sólo a solicitud de la Abogacía General, en coordinación con la Oficina Jurídica, a consecuencia de la recepción de una solicitud de ejercicio de derechos ARCO.

Se entiende por periodo de bloqueo a la identificación y conservación de los 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 éstas.

Durante dicho periodo, los Datos personales no podrán ser objeto de tratamiento y, transcurrido éste, se procederá a su cancelación en la base de datos o el sistema que corresponda;

- III. Identificar las responsabilidades legales y definir las contractuales, sobre el resguardo y eliminación de los Datos personales;
- IV. Identificar los medios en los que almacenan Datos personales, para implementar técnicas de Borrado seguro, considerando si los Datos personales se almacenan en un Medio físico o electrónico, incluyendo en la nube;
- V. Implementar las medidas de seguridad y buenas prácticas, señaladas en la tabla única de la presente Guía, que permitan minimizar el riesgo de recuperación de información que haya sido borrada de cualquier Medio físico o electrónico, incluyendo en la nube;
- VI. Realizar y documentar las operaciones de Borrado seguro, observando lo siguiente:
 - a) Al seleccionar una herramienta de Borrado, de las establecidas en la presente guía, apegarse al procedimiento institucional, para identificar claramente que el proceso de Borrado se ha llevado a cabo, detallando cuándo y cómo ha sido realizado; y
 - b) En caso de que la destrucción lógica o electrónica (la efectuada en medios digitales), no se realice correctamente por fallo del dispositivo, este hecho debe

documentarse claramente en el Acta de Destrucción y consultar a la Coordinación de Informática sobre el método de Borrado seguro que se podría utilizar.

- VII. Asegurar, en el ámbito de sus atribuciones, que la disposición de los residuos derivados de la destrucción física se realice en apego a la gestión ambiental del campus y de conformidad con el principio jesuita del cuidado de la casa común;
- VIII. Determinar, de acuerdo con el volumen de información que se va a destruir y a su nivel de riesgo, si la destrucción se realizará por personal del TUVCH o se contratará a un tercero, y
- IX. Para la destrucción de documentos que contengan Datos personales, en soporte físico o electrónico, considerar la categoría de la información de acuerdo con la tabla siguiente:

**Tabla única para la clasificación de los Datos personales
y forma de proceder para el Borrado seguro.**

Categoría	Descripción	Medios físicos	Medios electrónicos
Estándar	Contiene información de identificación, contacto, datos laborales o académicos de una persona física identificada o identificable, tal como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico,	Cuando contenga máximo 2 Datos personales (no sensibles) por cada página: Deberá destruir el documento en un equipo de trituración de documentos o materiales que pueda reducirlos a fragmentos de	Si la información se encuentra en dispositivos regrabables (CD-RW, Casetes, Videocasetes, DVD-RW, Blue-Ray, etc.): • Destrucción física. Si la información se encuentra en equipos de cómputo:

	lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.	cuando menos 6 milímetros o, en caso de que se decida utilizar como papelería de reúso, se deberán testar las secciones que contienen Datos personales y sólo utilizarlo de manera interna, en la propia área, no en áreas ajenas ni con externos. Cuando contenga 3 o más Datos personales (no sensibles) en la misma página: Deberá destruir el documento en un equipo de trituración de documentos o materiales, que pueda reducirlos a fragmentos de cuando menos 6 milímetros. En este caso, el documento no se podrá reutilizar.	• Sobreescritura, previa autorización de la Coordinación de Informática. Si la información se aloja virtualizada en la infraestructura del TUVCH: • Sobreescritura, previa autorización de la Coordinación de Informática.
--	---	--	---

		En ambos supuestos no es necesario elaborar listado alguno ni notificar a la Oficina Jurídica, ni a la Auditoría Interna sobre la destrucción.	
Sensible	Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física e información relativa al tránsito de las personas dentro y fuera del país. También son datos de nivel sensible aquéllos que permitan inferir el patrimonio de una persona, que incluye, entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, estatus en el buró de	Con independencia del número de Datos personales sensibles que contenga (incluso 1): Deberá notificarse vía correo electrónico a la Oficina Jurídica para su conocimiento, y a la Auditoría Interna para su atención, así como elaborar un listado de los documentos a destruir y triturarlos en partículas de 2X15 mm, y firmar el Acta de Destrucción, de	Según en el medio en el que se encuentre almacenada la información, se deberá consultar a la Coordinación de Informática, para que ésta determine cualquiera de las siguientes formas de borrado, en concordancia con los estándares internacionales de eliminación segura de medios: • Sobreescritura • Desmagnetización • Destrucción física

	crédito, seguros, afores, fianzas y números de tarjetas bancarias de crédito y/o débito. Son considerados también los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica y cualquier otro que permita autenticar a una persona. Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en	conformidad con lo establecido en el apartado correspondiente de la presente Guía. La destrucción de estos documentos deberá realizarse en presencia de la Auditoría Interna.	
--	---	---	--

	materia laboral, civil, penal o administrativa. Finalmente, se contemplan los Datos personales sensibles de acuerdo con la ley, es decir, aquéllos que afecten a la esfera más íntima de su titular. Por ejemplo, se consideran los que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave a la integridad del titular. Los documentos institucionales que comúnmente contienen Datos personales sensibles son, por ejemplo:		
--	---	--	--

	expedientes escolares, clínicos, migratorios, jurídicos, de becas, laborales, disciplinarios, entre otros.		
Especial	Esta categoría corresponde a los datos cuya naturaleza única, o bien debido a un cambio excepcional en el contexto de las operaciones usuales de la organización, pueden causar daño directo a las y los titulares, por ejemplo, la Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito, mencionado anteriormente, en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo, fecha de vencimiento, códigos de seguridad, datos de banda	En el caso de documentos físicos tratados por entes externos, el método de eliminación se tendrá que definir en el contrato de prestación de servicios, previa consulta a la Auditoría Interna, en coordinación con la Oficina Jurídica y, en su caso, con la Abogacía General. Además, se deberán determinar las evidencias a generar, que demuestren que el Borrado seguro se llevó a cabo adecuadamente.	En el caso de documentos electrónicos tratados por entes externos, el método de eliminación se tendrá que definir en el contrato de prestación de servicios, previa consulta a la Auditoría Interna, a la Oficina Jurídica y a la Coordinación de Informática, en el ámbito de su competencia. Además, se deberá determinar las evidencias a generar, que demuestren que el Borrado seguro se llevó a cabo adecuadamente. Cualquier otro documento, incluidos los tratados de manera interna, que corresponda a esta categoría deberá ser consultado a la Auditoría Interna y a la

	magnética o número de identificación personal (PIN). En esta categoría se deben clasificar los documentos que provengan de entes externos con los que se relaciona el TUVCH en su labor de incidencia social.	Cualquier otro documento, incluidos los tratados de manera interna, que corresponda a esta categoría deberá ser consultado a la Auditoría Interna, y a la Oficina Jurídica, coadyuvada, en su caso, por la Abogacía General, para determinar en conjunto con dichas áreas el destino de este.	Oficina Jurídica, coadyuvada, en su caso, por la Abogacía General, para determinar en conjunto con dichas áreas el destino de este.
--	---	--	--

Cuando se utilice el equipo para la tritución de documentos físicos, el área del TUVCH que lo necesite tendrá que requerir el préstamo a la Oficina Jurídica del TUVCH, para que establezca la fecha y la hora para llevar a cabo la actividad.

La operación del equipo deberá ser autorizada por la persona titular de la dirección de área correspondiente, y estará a cargo de la persona que esta designe.

DESTRUCCIÓN A TRAVÉS DE UN TERCERO

Cuando se contrata un proveedor para destruir la información, el área deberá:

- i. Suscribir un contrato, en donde se defina de forma detallada el servicio que prestará el tercero, así como las responsabilidades de ambas partes y las medidas para el resguardo, registro y vigilancia de los medios de almacenamiento;

- II. Verificar si el proveedor cuenta con credenciales, certificaciones o cualquier prueba de que el Borrado seguro se realiza en un ambiente controlado, y
- III. Solicitar al prestador de servicio un certificado o acta del proceso de borrado realizado.

DESTRUCCIÓN EN LA NUBE

Si la información se resguarda en la *nube*, el área deberá:

- I. Suscribir un contrato en el que se establezcan cláusulas de Borrado seguro;
- II. Revisar las políticas del proveedor respecto a las copias de seguridad y respaldos que realiza de la información;
- III. Verificar que el proveedor garantice que el borrado se aplique en todos los dispositivos sincronizados, en los que se haya replicado la información, y
- IV. Solicitar al proveedor evidencia del proceso de Borrado seguro que realizará.

Se entiende como almacenamiento en la nube, el servicio al cual se accede a través de Internet, para almacenar en espacios virtualizados, archivos con contenido como imágenes, documentos, videos, bases de datos, entre otros. Este servicio normalmente es proporcionado por un proveedor de servicios.

ACTA DE DESTRUCCIÓN

El formato “**Acta de Destrucción**”, deberá integrar la siguiente información:

- I. Lugar, fecha y hora de inicio y de cierre del proceso de destrucción de la información;
- II. Listado de documentos o archivos que serán destruidos;

- III. Motivo de la destrucción;
- IV. Nombre y firma de la persona titular del área que autoriza;
- V. Nombre y firma de la persona responsable de realizar la destrucción de los documentos o archivos; y
- VI. Nombre y firma de la persona integrante de la Auditoría Interna que presencie la destrucción.

La destrucción física y digital de la información, deberá realizarse en presencia de Auditoría Interna.

MÉTODOS DE BORRADO NO PERMITIDOS

Por no ser métodos de Borrado seguro, no se deberán emplear los siguientes:

- I. Para Medios físicos:
 - a) Destrucción manual;
 - b) Desechar documentos de forma íntegra a los contenedores de basura;
 - c) Incineración, o
 - d) Destrucción química.
- II. Para Medios electrónicos:
 - a) Toda aquella acción que no conlleve la eliminación definitiva, tanto de la información de la “lista de archivos” como del contenido de la misma;
 - b) Los comandos de borrado por defecto de los sistemas operativos;
 - c) Formateo;
 - d) Incineración, o
 - e) Destrucción química.

TRANSITORIOS

PRIMERO. Para todo lo relacionado con la presente Guía, las áreas del TUVCH deberán ponerse en contacto con la Secretaría Ejecutiva.

SEGUNDO. En tanto no se cuente con personal de Auditoría Interna, las actividades de borrado seguro se coordinarán desde la Secretaría Ejecutiva del TUVCH con la Auditoría Interna de la Universidad Iberoamericana Ciudad de México.