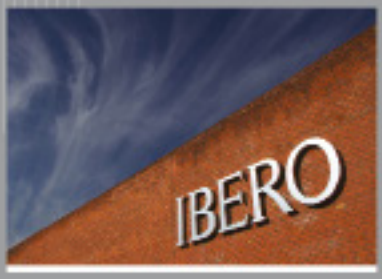
IBERO
CIUDAD DE MÉXICO



Comunicación Oficial

septiembre 2023

611

Fecha publicación: 09 octubre 2023

CONTENIDO

Rectoría

REGLAMENTO PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA UNIVERSIDAD IBEROAMERICANA

ÍNDICE:

REGLAMENTO PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA UNIVERSIDAD IBEROAMERICANA

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 a la Universidad Iberoamericana Ciudad de México (en adelante IBERO), 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 a la IBERO, 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 de la IBERO 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 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 responsable de vigilar y revisar el debido cumplimiento del presente Reglamento;

III. **Autoridad universitaria**: Cualquier autoridad unipersonal o colegiada prevista en la normatividad de la IBERO 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 de la IBERO, 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 físico, electrónico o en cualquier otro formato, a través del cual, la Responsable de la protección y el Tratamiento de los Datos personales informa a la persona Titular de éstos sobre la existencia y características principales del Tratamiento al que serán sometidos sus Datos personales, previo a que ocurra dicho Tratamiento;

V. **Buzón de datos personales**: Medio electrónico y físico habilitado por la IBERO para atender las solicitudes de ejercicio de Derechos ARCO;

VI. Comunidad universitaria: Al conjunto de personas que tienen o tuvieron una relación académica, laboral o civil con la IBERO, de conformidad con su Estatuto Orgánico;

VII. Consentimiento: Manifestación de la voluntad de la persona Titular de los Datos personales, mediante la cual autoriza que se lleve a cabo su Tratamiento;

VIII. Datos personales: Cualquier información concerniente a una persona física, que la identifique o que la haga identificable, expresada en forma numérica, alfabética, gráfica, ortográfica, acústica, biométrica o en cualquier otra;

IX. 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 éste o ésta. 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 y preferencia sexual, entre otros;

X. **DCI**: Dirección de Comunicación Institucional;

XI. **Derechos ARCO**: Son los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de los Datos personales;

XII. **DIT**: Dirección de Informática y Telecomunicaciones;

XIII. **Docentes**: Al profesorado que presta sus servicios profesionales sea por un contrato civil o por una relación laboral;

XIV. **DRH**: Dirección de Recursos Humanos;

XV. **Encargado/a**: La persona física o jurídica, ajena a la Responsable, que sola o conjuntamente con otras, trate Datos personales por cuenta de la 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;

XVI. **IBERO**: Universidad Iberoamericana Cuidad de México;

XVII. 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;

XVIII. Remisión: La comunicación de datos personales entre la responsable y Encargado, dentro o fuera del terri-torio mexicano;

XIX. Responsable: Persona física o jurídica de carácter pri-vado que decide sobre el Tratamiento de Datos perso-nales;

XX. Titular: Persona física a quien pertenecen los Datos personales;

XXI. Transferencia: Toda comunicación de Datos perso-nales realizada a persona distinta de la Responsable o Encargada del Tratamiento;

XXII. Tratamiento: La obtención, uso, divulgación o almacenamiento de Datos personales por cualquier medio.

El uso abarca cualquier acción de obtención, acceso, manejo, aprovechamiento, Transferencia o disposición de Datos personales; y

XXIII. Vulneración: Se refiere a la vulneración a los datos personales que tiene lugar cuando, intencionada o no intencionadamente, se liberan estos 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.

La IBERO, en carácter de Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, estará obligada a obtener los datos y utilizarlos de manera licita, 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.

La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos, privilegiando en todo momento la expectativa razonable de privacidad.

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

Artículo 5. Lealtad.

La IBERO, en carácter de Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, a través de sus Autoridades, colaboradores/as y participantes, estará obligada 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.

Por otra parte, ninguna Autoridad universitaria ni ninguna persona que colabore o participe con la IBERO debe obtener Datos personales a través de medios engañosos o fraudulentos.

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.

La IBERO, en carácter de Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, a través de sus Autoridades, colaboradores/as y participantes, estará obligada a poner a disposición -ya sea física, electrónica o por cualquier medio permitido por la ley- de los y las Titulares su Aviso de Privacidad, 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, de conformidad con la normatividad oficial en la materia.

Será derecho de la Comunidad universitaria 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 de las diferentes áreas de la IBERO, de no oponerse al mismo, se entenderá que brindan su Consentimiento 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, 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 la 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.

La IBERO, en carácter de Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, a través de sus Autoridades, colaboradores/as y participantes, estará obligada 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 de la IBERO, así como las personas que participen con ésta, sólo se utilizarán para 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.

Artículo 10. Proporcionalidad.

Todos los Datos personales que sean objeto de Tratamiento por las Autoridades universitarias o por las y los colaboradores de la IBERO, así como por las personas que participen con ésta, 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.

La IBERO, en carácter de Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, mediante sus Autoridades, colaboradores/as y participantes, estará obligada a tener especial cuidado con el tratamiento de los Datos personales sensibles y sólo solicitarlos cuando éstos sean necesarios para la finalidad de que se trate.

Artículo 11. Responsabilidad.

La IBERO, en carácter de Responsable del Tratamiento de los Datos personales de la Comunidad universitaria, por conducto de sus Autoridades, 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.

Artículo 12. Seguridad.

La IBERO, a través de sus Autoridades, 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 de la IBERO, 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 la Responsable.

CAPÍTULO II

REMISIÓN Y TRANSFERENCIA DE DATOS PERSONALES

Artículo 14. Remisión.

Las remisiones nacionales e internacionales de Datos personales entre la Responsable y un Encargado no requerirán ser informadas al Titular ni contar con su consentimiento.

El Encargado, 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 la Responsable, o

II. Efectúe una transferencia, incumpliendo las instrucciones de la Responsable.

El Encargado no incurrirá en responsabilidad cuando, previa indicación expresa de la 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 encuentra 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 el 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 la IBERO 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, respectivo.

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 sujeta la 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 de la IBERO.

No se requerirá consentimiento de las personas Titulares, cuando los Datos Personales se transfieran o compartan entre diferentes áreas de la IBERO, entidades académicas, sociedades que formen parte del sistema educativo universitario jesuita, asociaciones civiles, sociedades e instituciones que obren enunciadas en el Aviso de Privacidad, para su tratamiento en el ámbito de su competencia, cumpliendo con las previsiones contenidas en los principios del presente Reglamento.

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

Artículo 17. Obligaciones de la IBERO cuando funge como receptora de Datos personales.

Cuando la IBERO sea receptora 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 que transfirió los datos previstas en el Aviso de Privacidad, incluyendo el deber de confidencialidad.

CAPÍTULO III

EJERCICIO DE DERECHOS ARCO

Artículo 18. Obligaciones generales.

La Abogacía General 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. El ejercicio del derecho de cancelación no podrá limitarse porque la o el Titular haya ejercido el derecho de acceso con anterioridad;

III. Las Autoridades universitarias y las personas colaboradoras y participantes de la IBERO 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;

IV. 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;

V. La Abogacía General 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;

VI. Las Autoridades universitarias y las personas colaboradoras y participantes de la IBERO deberán rectificar los Datos personales cuando proceda su ejercicio, en los términos que indique la Abogacía General;

VII. 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;

VIII. No procederá la cancelación de Datos personales en los casos en que así lo señalen las disposiciones oficiales;

IX. Se deberán bloquear los Datos personales, previa supresión, y no tratarlos en ese periodo, salvo con fines de almacenamiento, legales y de responsabilidad;

X. Las Autoridades universitarias y las personas colaboradoras y participantes de la IBERO no deberán tratar los Datos personales para las finalidades correspondientes, cuando proceda el ejercicio de oposición;

XI. En todos los casos de negativa de ejercicio de los Derechos ARCO, 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

XII. Las Autoridades universitarias y las personas colaboradoras y participantes de la IBERO 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.

La IBERO 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 solitud 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 o patria potestad, 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 la IBERO 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 de las instalaciones, como fuera de éstas (teletrabajo).

Se entiende por teletrabajo a la forma de organización laboral subordinada que consiste en el desempeño de actividades remuneradas, en lugares distintos al establecimiento o establecimientos del patrón, por lo que no se requiere la presencia física de la persona trabajadora bajo la modalidad de teletrabajo, en el centro de trabajo, utilizando primordialmente las tecnologías de la información y comunicación, para el contacto y mando entre la persona trabajadora bajo la modalidad de teletrabajo y el patrón.

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 de la IBERO, 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 correspondiente;

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, los documentos fundamentales de la IBERO 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; 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 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, incluyendo 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 en la legislación en materia de archivos y de conformidad con la *Guía de borrado seguro* y notificar a la Abogacía General y a la Auditoría Interna, previo a que se realice el borrado, supresión o cancelación de Datos personales;

VIII. Reportar a la DIT 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 la DIT;

IX. Participar en todas las capacitaciones en materia de protección de Datos personales que se promuevan al interior de la IBERO 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 reidentificación de los Datos personales;

b) **Minimización**: Se refiere a que la 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 DIT 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 Abogacía General;

XIV. Vigilar que su Aviso de Privacidad se mantenga actualizado en todos los medios, tanto físicos como digitales, incluyendo a las otras asociaciones cuya responsabilidad administrativa recaiga en la IBERO;

XV. Notificar a la Abogacía General la necesidad de generar un nuevo Aviso de Privacidad específico, cuando los existentes no respondan fehacientemente al Tratamiento de Datos personales que el área lleva a cabo.

La procedencia de crear cada Aviso de Privacidad se determinará por la Abogacía General en función de su viabilidad y pertinencia;

XVI. Notificar a la Abogacía General la necesidad de realizar cambios en el Aviso de Privacidad que les corresponde, sobre todo cuando requieran modificaciones en las finalidades primarias, Transferencias o en el tipo de Datos personales o Datos personales sensibles que recaban;

XVII. Notificar de inmediato a la DIT y al superior jerárquico cualquier vulneración a los Datos personales, ya sea física, digital o por un tercero, para que a su vez notifiquen al órgano colegiado que la Rectoría constituya en materia de seguridad de la información;

XVIII. Notificar a la DIT cuando algún sistema y/o aplicación que usen o pretendan utilizar procese o almacene Datos personales;

XIX. Para realizar el borrado seguro de los Datos personales en el caso del teletrabajo, 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** del presente Reglamento *Guía de Borrado Seguro*;

XX. Notificar a la Auditoría Interna y a la DRH los casos de incumplimiento de lo establecido en el presente Reglamento por parte del personal a su cargo; y

XXI. En caso de incumplimiento de lo establecido en el presente Reglamento por parte del personal a su cargo, participar con la DRH para que ésta determine y aplique las sanciones correspondientes, de acuerdo a lo establecido en la normatividad universitaria, en el contrato correspondiente y, en su caso, en el Reglamento Interior de Trabajo.

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

Cualquier área de la IBERO 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 a la IBERO 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 que corresponda al área que la lleve a cabo 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 y las políticas correspondientes.

Artículo 23. Medidas Específicas de Prevención de la Dirección de Recursos Humanos.

La DRH será responsable de ejecutar las siguientes medidas de prevención específicas:

I. Diseñar e impartir, por lo menos 2 veces al año, capacitación en materia de protección de Datos personales a las y los colaboradores de la IBERO;

II. Asegurar que todos los contratos del personal de la IBERO, 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; y

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.

Artículo 24. Medidas de Prevención Específicas de la Dirección de Comunicación Institucional.

La DCI será responsable de ejecutar las siguientes medidas de prevención específicas:

I. Mantener actualizada la liga y la página electrónica institucional, en que se encuentren alojados los Avisos de Privacidad, así como alojar las versiones vigentes de éstos, al momento en que lo solicite la Abogacía General; y

II. Difundir las campañas de cultura para la protección de Datos personales, que le soliciten las Autoridades universitarias.

Artículo 25. Medidas de Prevención Específicas de la Dirección de Informática y Telecomunicaciones.

La DIT 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, de acuerdo con lo sugerido por la autoridad colegiada en la materia;

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. Atender las solicitudes de sustitución/implementación de Avisos de Privacidad específicos que soliciten las diferentes áreas, una vez que éstos les hayan sido autorizados por la Abogacía General a las mismas;

VI. Asegurarse que los Avisos de Privacidad, que aparecen en los diferentes sistemas de la IBERO, se muestren antes de que se recolecten los Datos personales;

VII. Realizar, paulatinamente y de acuerdo a la disponibilidad técnica y presupuestal, las adecuaciones necesarias, en acuerdo con el área correspondiente, en los diferentes sistemas registrados ante la DIT, 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 y de telecomunicaciones contratados por la DIT, que impliquen el Tratamiento de Datos personales de cada área de la IBERO;

IX. Emitir y difundir los criterios necesarios para la protección de los Datos personales en todos los sistemas electrónicos empleados por la IBERO;

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 de la IBERO,

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 26. Medidas de Prevención Específicas de la Abogacía General.

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

I. Diseñar, establecer y difundir el procedimiento de atención a las solicitudes que se reciben en el Buzón de Datos personales;

II. Autorizar los Avisos de Privacidad de la IBERO y coordinarse con las áreas respectivas que tengan a cargo el sitio electrónico, para su sustitución/implementación;

III. Atender, gestionar y dar curso a las solicitudes de Derechos ARCO que se reciban en el Buzón de Datos personales;

IV. Diseñar, establecer y difundir el procedimiento a seguir para las solicitudes de actualización o cambios en los Avisos de Privacidad que soliciten las diferentes áreas de la Universidad;

V. Brindar asesoría a las diferentes áreas de la IBERO, en materia de protección de Datos personales;

VI. Apoyar a la DRH en la revisión de los contenidos de las capacitaciones en materia de protección de Datos personales; y

VII. Atender y dar seguimiento a los procedimientos administrativos o judiciales que se generen ante la autoridad oficial en la materia.

Artículo 27. 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, derivadas de la supervisión enunciada en el presente artículo;

IV. Emitir recomendaciones a las Autoridades universitarias, resultado de las áreas de oportunidad que se deriven de la supervisión a que se refiere el presente artículo o por algún hallazgo propio de la 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 DRH.

Artículo 28. Medidas de Prevención Específicas de la Dirección de Servicios Generales.

La Dirección de Servicios Generales 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 de la IBERO, 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 de la IBERO;

III. Atender las solicitudes de las Autoridades universitarias sobre la señalética que contenga Avisos de Privacidad; y

IV. Velar por el adecuado Tratamiento de los Datos personales contenidos en los registros de personas que visitan la IBERO.

Artículo 29. Medidas de Prevención Específicas de las Clínicas que brindan servicios de salud.

Cualquier persona contratada por la IBERO que trate los Datos personales contenidos en expedientes clínicos será responsable de ejecutar las siguientes medidas de prevención específicas:

I. Observar las disposiciones oficiales en materia de salud, así como las Normas Oficiales Mexicanas en la materia, relacionadas con la protección de Datos personales;

II. Reconocer que la titularidad de los Datos personales y Datos personales sensibles le pertenecen a las personas de las cuales son inherentes, procediendo de conformidad con lo establecido en el artículo **7** del presente Reglamento, respecto de los contenidos en los expedientes de las Clínicas ligadas a la IBERO;

III. Abstenerse de solicitar Datos personales o Datos personales sensibles que sean innecesarios para el servicio que prestan; y

IV. Cumplir estrictamente con lo previsto en la fracción VII del artículo **21** de este Reglamento.

Artículo 30. Medidas de Prevención Específicas de las Autoridades universitarias en materia disciplinar.

Las Autoridades universitarias en materia disciplinar 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.

TÍTULO IV

PROCESOS QUE IMPLIQUEN TRATAMIENTO DE DATOS PERSONALES

CAPÍTULO ÚNICO

PROCESOS QUE IMPLIQUEN TRATAMIENTO DE DATOS PERSONALES

Artículo 31. Inventario.

La DIT llevará un inventario de los sistemas y bases de datos electrónicos, institucionales o no institucionales, que contengan Datos personales, que obren en la IBERO y deberá mantenerlo actualizado.

Las diversas Áreas de la IBERO deberán colaborar con la DIT en la construcción y actualización de este inventario, en el ámbito de sus competencias.

Artículo 32. 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 Abogacía General.

Artículo 33. 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 Abogacía General y por la DIT.

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

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

Artículo 34. Subcontratación.

Toda subcontratación de servicios por parte de la Universidad que. implique el Tratamiento de Datos personales, deberá ser autorizada por la Abogacía General y por la DIT, 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 correspondiente, el instrumento contractual celebrado con la IBERO y las disposiciones institucionales y oficiales vigentes.

Sólo se permitirá la transmisión de los Datos personales en posesión de la IBERO a terceros cuando obre autorizada la subcontratación y la trasferencia de dichos datos por la Abogacía General y también por la DIT, en los casos en que se trate de cuestiones tecnológicas, incluso cuando se trate de 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 35. Vulneración de Datos personales.

Cualquier vulneración de seguridad de Datos personales ocurrida en cualquier fase del Tratamiento deberá ser informada

de inmediato al órgano colegiado que la Rectoría constituya en materia de seguridad de la información, para que se tomen las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación para analizar sus causas e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad, así también, el cumplimiento del deber de informar a las y los Titulares, dependiendo del nivel de vulneración y del tipo de Datos personales que, en su caso, se hayan comprometido.

En este caso, la Abogacía General será la Autoridad universitaria responsable de determinar la procedencia de notificar la vulneración a las y los Titulares de los Datos personales afectados, así como de dar aviso y/o denunciar el hecho ante las autoridades correspondientes, con base en las conclusiones del órgano colegiado señalado en el párrafo anterior.

En caso de ocurrir una vulneración a la seguridad, la IBERO analizará sus causas e implementará las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, y la Auditoría Interna lo registrará en una bitácora de vulneraciones, a efecto de evitar que la vulneración se repita.

Todas las áreas de la IBERO deberán reportar a la Auditoría Interna las vulneraciones que se actualicen por medios físicos.

La DIT será la Autoridad universitaria responsable de reportar a la Auditoría Interna las vulneraciones que ocurran a través de medios electrónicos en cualquier espacio de la Universidad.

La bitácora de vulneraciones deberá contener: descripción de la vulneración, en qué consistió la vulneración, la fecha, el motivo o la causa y las acciones correctivas.

Artículo 36. 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;

IV. El daño, la alteración o modificación no autorizada; y

V. La revelación o exposición no autorizada de información personal a través de internet o medios masivos de comunicación.

TÍTULO VI

RESPONSABILIDADES, SANCIONES Y CUMPLIMIENTO

CAPÍTULO ÚNICO

RESPONSABILIDADES, SANCIONES Y CUMPLIMIENTO

Artículo 37. De las Causas de Responsabilidad.

Serán causas de responsabilidad de las Autoridades universitarias y de las personas colaboradoras y participantes de la IBERO, las siguientes:

I. De manera indebida, Tratar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente documentos que contengan Datos personales, 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 de la IBERO;

VIII. Omitir reiteradamente dar respuesta a las solicitudes de Derechos ARCO, dentro de los plazos indicados por la Abogacía General y los previstos en las disposiciones oficiales;

IX. No proporcionar a la Abogacía General 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 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, como resultado de un ejercicio de Derechos ARCO;

XIII. Abstenerse de informar a la DIT 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 38. Sanciones.

Las Autoridades universitarias, así como los personas colaboradoras y participantes de la IBERO 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, 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 39. 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 siguiente a su publicación en la Comunicación Oficial de la IBERO.

SEGUNDO. Se abroga el *Reglamento Para la Protección de Datos Personales de la Universidad Iberoamericana Ciudad de México* publicado en la Comunicación Oficial N. 461, el 31 de mayo de 2012.

TERCERO. Este Reglamento será aplicable para la Universidad Iberoamericana Tijuana, siempre y cuando no contravenga su marco normativo.

En este caso, las Medidas específicas, así como las obligaciones y responsabilidades establecidas para cada una de las Autoridades universitarias de la Ibero Ciudad de México, les serán aplicables por analogía a aquellas de Ibero Tijuana, siempre y cuando sean homólogas a las primeras.

CUARTO. Las Medidas generales y las específicas, así como las obligaciones y responsabilidades establecidas para cada una de las Autoridades universitarias de la Ibero Ciudad de México será extensivas a la atención que éstas realicen a las asociaciones civiles Radio Ibero A.C., Compromiso Social Universidad Iberoamericana A.C. y Educación Media Superior Universidad Iberoamericana A.C.

Las asociaciones civiles enunciadas en este artículo deberán adoptar las Medidas generales dentro su ámbito de competencia.

QUINTO. La dirección de correo electrónico que fungirá como Buzón de datos personales, en tanto no se modifique, será:

Para IBERO CDMX, Prepa Ibero, Centro Ibero Meneses y Radio Ibero:

datospersonales@ibero.mx

En caso de no poder contactar con el Buzón de datos personales de manera electrónica, se podrá acudir de forma presencial ante la Abogacía General de la IBERO, en un horario de 9:00 a 14:00 horas, de lunes a viernes, en la siguiente dirección:

Prolongación Paseo de la Reforma número 880, Colonia Lomas de Santa Fe, Delegación Álvaro Obregón, Código Postal 01219, en la Ciudad de México, edifico T, quinto nivel.

Para IBERO Tijuana:

datospersonales@tijuana.ibero.mx

SEXTO. En el momento en que se expide el presente Reglamento, la Norma Oficial Mexicana en materia de salud, a la que se refiere la fracción I de su artículo **29** es la NOM-004-SSA3-2012.

SÉPTIMO. En tanto se instituye el órgano colegiado en materia de seguridad de la información a que se refiere el artículo **35** del presente Reglamento, cualquier vulneración que se suscite, deberá notificarse a la Rectoría, a la Abogacía General, a la Auditoría Interna y a la DIT, para que estas Autoridades universitarias, procedan de conformidad con lo establecido en el mismo artículo.

ANEXO ÚNICO

GUÍA PARA EL BORRADO SEGURO DE DATOS PERSONALES EN LA UNIVERSIDAD IBEROAMERICANA

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, Blu-rays*, entre otros, incluyendo el uso de servicios de almacenamiento en línea; y

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.

2.- Responsabilidades de las áreas Universitarias.

Con base en la *Guía para el Borrado seguro de Datos Personales*, emitida por el Instituto Nacional de Transparencia, Acceso

a la Información y Protección de Datos Personales (INAI) [1], todas las áreas de la Universidad que realicen Borrado seguro deberán:

I. **Documentar los procesos y procedimientos para el Borrado seguro de Datos personales** a seguir al interior de las mismas, 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

d) Periodo de bloqueo. El cual se efectúa sólo a solicitud de la Abogacía General a consecuencia de la recepción de una solicitud de ejercicio de derechos ARCO.

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

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;

V. **Implementar las medidas de seguridad y buenas prácticas, señaladas en la tabla única de la pre-**

sente Guía, que permitan minimizar el riesgo de recuperación de información que haya sido borrada de cualquier Medio físico o electrónico;

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 DIT 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 la Política Institucional de Sustentabilidad**;

VIII. Determinar, de acuerdo al volumen de información que se va a destruir y a su nivel de riesgo, **si la destrucción se realizará por personal de la Universidad o se contratará a un tercero**, en apego a la normatividad universitaria en materia de gestión y control de contratos y convenios; 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	Forma de proceder para el Borrado seguro	
		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, 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 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 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. En ambos supuestos no es necesario elaborar listado alguno ni notificar a la Abogacía General, ni a la Auditoría Interna sobre la destrucción.	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: • Sobreescritura, previa autorización de la DIT. Si la información se aloja virtualizada en la infraestructura de la IBERO: • Sobreescritura, previa autorización de la DIT.

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 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 materia laboral, civil, penal o administrativa. Finalmente, se contemplan los Datos personales sensibles de acuerdo a 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 universitarios que comúnmente contienen Datos personales sensibles son, por ejemplo, expedientes: escolares, clínicos, migratorios, jurídicos, de becas, laborales, disciplinares, entre otros.	**Con independencia del número de Datos personales sensibles que contenga (incluso 1):** Deberá notificarse vía correo electrónico a la Abogacía General 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 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.	Según en el medio en el que se encuentre almacenada la información, se deberá consultar a la DIT, para que ésta determine cualquiera de las siguientes formas de borrado, en concordancia con los estándares internacionales de eliminación segura de medios: • Sobre-escritura • Desmagnetización • Destrucción física

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 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 la Ibero en su labor de incidencia social.	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 y a la Abogacía General. Además, se deberán determinar las evidencias a generar, que demuestren que el Borrado seguro se llevó a cabo adecuadamente. Cualquier otro documento que corresponda a esta categoría deberá ser consultado a la Auditoría Interna y a la Abogacía General, para determinar en conjunto con dichas áreas el destino del mismo.	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 Abogacía General y a la DIT, 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 que corresponda a esta categoría deberá ser consultado a la Auditoría Interna y a la Abogacía General, para determinar en conjunto con dichas áreas el destino del mismo.

Cuando se utilice el equipo para la trituración de documentos físicos, el área universitaria que lo necesite tendrá que requerir ante la Dirección de Servicios Generales el préstamo de dicho equipo, para que ésta asigne personal capacitado a efecto de que realice la operación, estableciendo la fecha y la hora para llevar a cabo la actividad.

La operación del equipo estará a cargo de la Dirección de Servicios Generales, quién contará con la supervisión y acompañamiento del área que requiera la destrucción.

DESTRUCCIÓN A TRAVÉS DE UN TERCERO

Cuando se realiza la contratación de un proveedor para destruir la información, el área deberá:

I. Suscribir un contrato, de conformidad con los lineamientos universitarios, 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. Atestiguar el borrado y 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, de conformidad con los lineamientos universitarios, 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.

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

UNICO. Para todo lo relacionado con la presente Guía, los correos de contacto serán, en tanto no se modifiquen, los siguientes:

auditoria.interna@ibero.mx. y oj.datospersonales@ibero.mx