SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES DE LA UNIVERSIDAD INTERCULTURAL MAYA DEL ESTADO DE QUINTANA ROO

V.I-2025

INTRODUCCIÓN

La protección de los datos personales constituye un derecho humano fundamental consagrado en el artículo 6º y 16º, de la Constitución Política de los Estados Unidos Mexicanos, así como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). En cumplimiento de este mandato constitucional y legal, la Universidad Intercultural Maya de Quintana Roo (UIMQROO) adopta un enfoque institucional y sistemático para garantizar el debido tratamiento de los Datos Personales que se encuentran bajo su Administración.

Como institución pública de educación superior, la UIMQROO reconoce su responsabilidad en la protección de los Datos Personales que recaba, utiliza, transmite, conserva o elimina en el ejercicio de sus funciones sustantivas y administrativas.

La confianza de los titulares (comunidad estudiantil, docentes, personal administrativo, aspirantes, proveedores, visitantes y sociedad en general) es un activo fundamental que debe ser preservado mediante la implementación de políticas claras, medidas de seguridad robustas y una cultura organizacional de respeto a la privacidad y Protección de Datos Personales.

En este contexto, el presente Sistema de Gestión de Protección de Datos Personales (SGPDP) tiene como propósito establecer un marco integral para la administración responsable de los datos personales, orientado a:

- Proteger la confidencialidad, integridad y disponibilidad de los datos personales;
- Prevenir vulneraciones o tratamientos indebidos;
- Promover el respeto a los principios y deberes establecidos por la LGPDPPSO;
- Facilitar el ejercicio efectivo de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición);
- Cumplir con las obligaciones normativas de transparencia, rendición de cuentas y legalidad en el tratamiento de datos personales.

El presente documento constituye el inicio formal de un esfuerzo institucional orientado a consolidar una política de privacidad sólida, transversal y alineada con los principios de legalidad, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

A través del SGPDP, la Universidad se compromete a garantizar el respeto y la protección de los datos personales como parte esencial de su quehacer educativo, científico y comunitario.

Marco Normativo.

El Sistema de Gestión de Protección de Datos Personales (SGPDP) de la UIMQROO se fundamenta en el cumplimiento de un conjunto de disposiciones jurídicas de observancia obligatoria para los sujetos obligados del ámbito público en México, y específicamente para las instituciones de educación superior de carácter público.

Estas normas establecen las bases, principios, derechos y obligaciones en materia de protección de datos personales, así como los mecanismos para garantizar su debida gestión y resguardo:

1. Tratados Internacionales en Materia de Derechos Humanos.

El marco normativo también se sustenta en tratados internacionales de los que el Estado mexicano es parte, como la Declaración Universal de los Derechos Humanos en su Artículo 12.

2. Constitución Política de los Estados Unidos Mexicanos.

Artículo 6º y 16º, reconocen el derecho de toda persona a la protección de sus datos personales, el acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición respecto al tratamiento.

3. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Norma reglamentaria de los artículos 6º y 16 constitucionales, tiene por objeto establecer las bases, principios, deberes y procedimientos para el tratamiento legítimo, controlado e informado de los datos personales en posesión de los sujetos obligados.

4. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo.

Estas dos últimas obliga a los sujetos obligados a adoptar medidas de seguridad físicas, técnicas y administrativas, así como a garantizar el ejercicio de los derechos por parte de los titulares.

5. Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

Establece la obligación de los sujetos obligados de documentar sus actos y garantizar tanto el acceso a la información como la protección de los datos personales cuando estos formen parte de expedientes o documentos públicos.

6. Normativa Universitaria y Reglamentación Interna.

El SGPDP se desarrollará en concordancia con la normatividad institucional vigente, incluyendo el Decreto por el que se reforma integralmente el decreto por el cual se crea la UIMQROO y demás instrumentos normativos aplicables. Asimismo, se deberá armonizar con las políticas de gestión documental, archivo institucional y demás sistemas de gestión aplicables.

Definiciones.

Activo: Es cualquier elemento que representa un valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones.

Los activos deben entenderse como los datos personales y sistemas de tratamiento que representan un derecho intrínseco de las personas titulares, y también como los elementos que representan valor para el sujeto obligado, en tanto que con ellos opera la propia entidad.

Amenaza: Circunstancia o evento con la capacidad de causar daño a una organización.

Áreas o Unidades Administrativas: A las instancias de los Sujetos Obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.

Autoridades Garantes Estatales: Al Instituto Quintanarroense de Transparencia para el Pueblo; El Tribunal de Disciplina Judicial del Poder Judicial del Estado de Quintana Roo; El Órgano Interno de Control del Poder Legislativo del Estado de Quintana Roo; y los Órganos Internos de Control de los Órganos Constitucionales Autónomos.

Por cuanto hace a la protección de datos personales en posesión de los partidos políticos será autoridad garante el Instituto Nacional Electoral, de conformidad con lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública y la Ley General de Protección de Datos Personales en posesión de sujetos obligados.

Autoridad Garante Local: Al órgano administrativo desconcentrado denominado Instituto Quintanarroense de Transparencia para el Pueblo, sectorizado a la Secretaría Anticorrupción y Buen Gobierno de Quintana Roo, el cual conocerá de los asuntos en materia de transparencia y de protección de datos personales en posesión de Sujetos Obligados del poder Ejecutivo del Estado, de sus Municipios, y de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción, aplicando los lineamientos y criterios que establezca el Sistema Nacional conforme a las disposiciones de Ley.

Aviso de Privacidad: Al documento a disposición de la persona titular de la información de forma física, electrónica o en cualquier formato generado por el 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;

Bases de Datos: El conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Bloqueo: A la Identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de 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 que corresponda;

Ciclo de vida: Tiempo que duración y conclusión del tratamiento de los datos personales, para después ser suprimidos, cancelados o destruidos por parte del responsable.

Comité de Transparencia: Al cuerpo colegiado que se integre en cada Sujeto Obligado, en los términos y con las atribuciones que señala el Capítulo IV del Título Segundo de la Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo y la presente Ley.

Comunicar el riesgo: Compartir o intercambiar información entre la alta dirección, custodios y demás involucrados acerca del riesgo.

Cómputo en la Nube: Al Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Consentimiento: A la manifestación de la voluntad libre, específica e informada de la persona titular de los datos personales mediante la cual se efectúa el tratamiento de los mismos.

Custodios: Son aquéllos con responsabilidad funcional sobre los activos, como: los responsables del departamento de datos, administradores de sistemas o responsables de un proceso o de un proyecto en específico, entre otros.

Datos Personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos Personales Sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. 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.

Derechos ARCO: A los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Días: A los días hábiles.

Disociación: Al procedimiento mediante el cual los datos personales no pueden asociarse a la persona titular ni permitir, po r su estructura, contenido o grado de desagregación, la identificación de la misma.

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Evaluación de impacto en la protección de datos personales: Al documento mediante el cual los Sujetos Obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de las personas titulares, así como los deberes de los responsables y las personas encargadas, previstos en las disposiciones jurídicas aplicables.

Finalidad: Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo, de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago

de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones.

Impacto: Una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

Incidente: Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo.

Ley de Transparencia: A la Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo.

Ley General: A la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Medidas compensatorias: A los mecanismos alternos para dar a conocer a las personas titulares el aviso de privacidad, a través de su difusión por medios de comunicación masiva u otros de amplio alcance.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: A las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Al conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Al conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Organización: Grupo de personas y medios organizados con un fin determinado. Puede referirse al sector privado o sector público; para efectos de la presente guía se debe entender como Organización al sujeto obligado.

Persona Encargada: A la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Persona Titular: A la persona a quien corresponden los datos personales.

Plataforma Nacional: A la Plataforma Nacional de Transparencia a que hace referencia el artículo 44 de la Ley General de Transparencia y Acceso a la Información Pública.

Parte interesada: Persona o grupo de personas con intereses específicos sobre una organización. Por ejemplo: inversionistas, clientes, proveedores, autoridades de protección de datos y titulares.

Propietario: Personas que tienen a cargo la ejecución de un proceso que involucra el tratamiento de datos personales.

Responsable: Cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Riesgo de seguridad: Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización.

Riesgo inherente: Riesgo intrínseco al activo, sin considerar las medidas de seguridad implementadas.

Riesgo residual: El riesgo remanente después de tratar el riesgo.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

- Confidencialidad: Propiedad de la información para no estar a disposi- ción o ser revelada a personas, entidades o procesos no autorizados.
- Disponibilidad: Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.
- Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos.

Sistema de datos personales: Conjunto de organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Los sistemas de datos personales se distinguen en:

- Físicos: Conjunto ordenado de datos de carácter personal que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales.
- Automatizados: Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizando una herramienta tecnológica.

Sistema de Gestión de Seguridad: Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley General, los Lineamientos Generales, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Soporte electrónico: Son los medios de almacenamiento inteligibles solo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos, es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros), tarjetas de memoria (USB y SD) y demás medios de almacenamiento masivo no volátil.

Soporte físico: Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados “a mano” o “a máquina”, fotografías, placas radiológicas, carpetas, expedientes, demás análogos.

Sujetos Obligados: A cualquier autoridad, entidad, órgano y organismo de los Poderes Legislativo, Ejecutivo y Judicial, Municipios, Órganos Constitucionales Autónomos, fideicomisos y fondos públicos en el ámbito estatal o municipal que deban cumplir con las obligaciones previstas en la presente Ley.

Supresión: A la baja archivística de los datos personales conforme a las disposiciones jurídicas aplicables en materia de archivos, que resulte en la eliminación, borrado o

destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

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

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

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.

Tratar el riesgo: Procesos que se realizan para modificar el nivel de riesgo.

- Aceptar el riesgo: Decisión informada para coexistir con un nivel de riesgo.
- Compartir el riesgo: Proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.
- Evitar el riesgo: Acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella.
- Reducir el riesgo: Acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.
- Retención del riesgo: Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido.
- Riesgo residual: El riesgo remanente después de tratar el riesgo.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

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

UIMQROO: Se refiere a la Universidad Intercultural Maya de Quintana Roo. Organismo público descentralizado de la Administración Pública Paraestatal del Estado de Quintana Roo.

Unidad de Transparencia: Instancia que auxilia, orienta, gestiona, establece, informa, propone, aplica, asesora, registra y realiza las gestiones necesarias para el manejo, mantenimiento, seguridad, y protección de los sistemas de datos personales en posesión del responsable.

Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

Valorar el riesgo: Proceso para asignar valores a la probabilidad y consecuencias del riesgo.

Vulnerabilidad: Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Vulneración de datos personales: Es la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada.

Alcance y objetivos (Planeación).

Alcance.

El Sistema de Gestión de Protección de Datos Personales (SGPDP) de la Universidad Intercultural Maya de Quintana Roo comprenderá la planeación, implementación, monitoreo y mejora continua de políticas, procedimientos, medidas de seguridad y mecanismos organizacionales para garantizar el debido tratamiento de los datos personales en posesión de la universidad.

Este sistema aplicará a todas las áreas administrativas, desde la Rectoría, unidades académicas, de investigación y extensión universitaria, así como a los procesos que impliquen el tratamiento de datos personales, en formatos físicos o electrónicos, incluyendo:

- Datos de estudiantes, docentes, personal administrativo, egresados, aspirantes, visitantes y proveedores.

- Datos recabados en sistemas de información, plataformas digitales, formularios, investigaciones, bases de datos y archivos institucionales.
- Datos sensibles o especialmente protegidos, conforme al artículo 3º, fracción X de la LGPDPPSO.

De acuerdo a la estructura orgánica de la UIMQROO, el presente documento es aplicable para las siguientes áreas administrativas:

1. Rectoría.
2. Dirección Académica.
3. Dirección de Planeación y Desarrollo Institucional y Mejora Regulatoria.
4. Dirección de Administración y Servicios y de Archivos.
5. Dirección Jurídica y Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Objetivo General (Planeación).

Implementar un modelo institucional integral de gestión de seguridad de protección de los datos personales en posesión de la Universidad Intercultural Maya de Quintana Roo, que garantice el respeto al derecho fundamental a la privacidad, conforme al artículo 6º y 16º de la Constitución Política de los Estados Unidos Mexicanos y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), mediante la articulación de principios y deberes, estrategias organizacionales, prácticas seguras y acciones formativas que promuevan una cultura de Protección de Datos Personales en la Universidad.

Objetivos Específicos

1. Identificar y clasificar los datos personales tratados por la Universidad.
2. Diseñar e implementar avisos de privacidad claros, completos y accesibles.
3. Establecer procedimientos internos para la atención de solicitudes de derechos ARCO.
4. Capacitar al personal universitario sobre protección de datos personales.
5. Realizar análisis de Riesgos y de Brecha a los tratamientos identificados.
6. Integrar la protección de datos personales en el desarrollo de políticas, sistemas informáticos, bases de datos, investigaciones y servicios universitarios.
7. Documentar y mantener actualizado el documento de seguridad institucional.

Disposiciones Generales.

A. Principios en materia de protección de datos personales.

La UIMQROO deberá observar los principios:

Licitud. El tratamiento de datos personales deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Finalidad. Todo tratamiento de datos personales que se efectúe bajo responsabilidad de la UIMQROO deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiera.

Lealtad. La UIMQROO no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses de la persona titular y la expectativa razonable de su privacidad.

Consentimiento. Cuando no se actualicen algunas de las causales de excepción previstas en la Ley General, se deberá contar con el consentimiento previo de la persona titular para el tratamiento de los datos personales.

Calidad. Se deberán adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión, a fin de que no se altere su veracidad.

Proporcionalidad. Sólo se deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Información. A través del Aviso de Privacidad, se deberá informar a la persona titular, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Responsabilidad. Se deberán adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la LGPDPPSO.

B. Deberes en materia de protección de datos personales.

La UIMQROO deberá observar los deberes:

Deber de Seguridad. Establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Deber de Confidencialidad. Definir e implementar controles y mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden sigilo respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con la UIMQROO.

Ejercicio de los Derechos Arco y la Portabilidad de los Datos Personales.

A. Ejercicio de los Derecho ARCO

De conformidad con los artículos 42 al 50, 79, fracción II, y 80 de la LGPDPPSO, los titulares cuentan con los derechos siguientes:

Derecho de Acceso: Acceder a sus datos personales, así como a conocer la información relacionada con las condiciones y generalidades de su tratamiento.

Derecho de Rectificación: El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

Derecho de Cancelación: El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Derecho de Oposición: El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular.

B. Portabilidad de los Datos Personales

La portabilidad constituye un derecho de las personas titulares que tiene por objeto la reutilización de sus datos personales.

A través del ejercicio de la portabilidad, las personas titulares pueden recibir los datos personales que han proporcionado a un responsable y transmitirlos a otro responsable, siempre y cuando los datos personales se encuentren en un formato estructurado, de uso común y lectura mecánica.

Política de Gestión de Datos Personales (Planeación).

La implementación de una política institucional de gestión Protección de Datos Personales en la UIMQROO constituye un elemento esencial para garantizar la protección efectiva de la información personal que se encuentra bajo el control de sus distintas unidades administrativas. Esta política debe enmarcarse en el cumplimiento de lo establecido en el Artículo 56 de los Lineamientos Generales en la materia, el cual señala que los responsables deberán adoptar políticas internas que definan mecanismos, criterios y procedimientos que aseguren la confidencialidad, integridad y disponibilidad de los datos personales durante todo su ciclo de vida.

Desde esta perspectiva, la política de gestión de datos personales:

Define qué se debe proteger, especificando que los activos de información incluyen los datos personales generados o tratados por la institución, ya sea en funciones académicas, administrativas, de investigación o vinculación social. Esta información representa un recurso estratégico y sensible, cuya protección es indispensable para mantener la confianza de la comunidad universitaria.

Determina quién es responsable, al establecer una cadena clara de rendición de cuentas entre los responsables, encargados y custodios del tratamiento de datos, en cada unidad administrativa. Este principio de responsabilidad proactiva refuerza el cumplimiento de la normatividad vigente y la prevención de vulneraciones a los derechos de los titulares.

Justifica por qué se protege, alineando cada tratamiento de datos a finalidades legítimas, claras y explícitas, conforme al principio de finalidad previsto en la Ley

General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Define cómo se protege, mediante acciones concretas, procedimientos internos y medidas de seguridad físicas, técnicas y administrativas que permitan mitigar riesgos y prevenir incidentes que comprometan la información personal.

Establece cuándo y por cuánto tiempo se protege, considerando el ciclo de vida de los datos personales, desde su recolección hasta su supresión o resguardo archivístico conforme a las disposiciones aplicables en materia de transparencia, archivos y protección de datos personales.

En el contexto de la UIMQROO, cada unidad administrativa deberá implementar esta política en sus procesos operativos, académicos y administrativos, asegurando que el tratamiento de datos personales se realice bajo estándares de legalidad, proporcionalidad y responsabilidad. Esta acción no solo contribuye al cumplimiento normativo, sino que fortalece la gobernanza institucional, promueve la cultura de privacidad y reduce el riesgo de sanciones legales o afectaciones a los derechos de las personas.

Funciones y Obligaciones del Personal que trata Datos Personales (Planeación).

La correcta identificación de las funciones y obligaciones del personal que interviene en el tratamiento de datos personales es un componente clave del Sistema de Gestión de Seguridad de la Información de la Universidad. El Artículo 57 de los Lineamientos Generales de Protección de Datos Personales establece que los responsables deberán definir y asignar funciones específicas al personal involucrado en el tratamiento de datos, con el fin de garantizar su seguridad durante todo el ciclo de vida del Dato Personal.

En este sentido, las unidades administrativas de la UIMQROO, en concordancia con sus atribuciones, deben:

- Identificar al personal que realiza tratamiento de datos personales, ya sea en actividades de recolección, uso, almacenamiento, transferencia o supresión de la información.

- Identificar el tipo de tratamiento que cada unidad efectúa, en función de las actividades operativas y administrativas que desarrollan.
- Detectar los perfiles y privilegios adecuados de acceso, según el nivel de responsabilidad y la naturaleza de los datos tratados, a fin de limitar los riesgos y reforzar el principio de “mínimo privilegio”.
- Definir claramente las responsabilidades en caso de incidentes de seguridad, asegurando mecanismos efectivos de rendición de cuentas y respuesta ante vulneraciones.

Al delimitar con precisión estas funciones y obligaciones, la UIMQROO no solo fortalece su capacidad operativa para proteger los datos personales en posesión de cada unidad administrativa, sino que también avanza hacia una cultura institucional de privacidad, cumplimiento normativo y mejora continua.

Identificar y establecer la cadena de rendición de cuentas dentro del tratamiento de datos personales es fundamental para asegurar la trazabilidad de responsabilidades y la vigilancia efectiva del cumplimiento normativo en cada unidad administrativa de la UIMQROO. Esta cadena permite identificar con claridad quién hace qué, cómo, y bajo qué controles, lo cual es esencial para prevenir, detectar y atender oportunamente cualquier vulneración a la seguridad de los datos. Asimismo, fortalece la responsabilidad institucional al garantizar que todo el personal involucrado actúe con base en principios de legalidad, transparencia y compromiso, fomentando una cultura de protección de datos alineada con los principios de la LGPDPPSO y los Lineamientos Generales en la materia.

Esta etapa es indispensable para garantizar que todas las personas servidoras públicas universitarias que manejan datos personales actúen con conocimiento, responsabilidad y apego a las disposiciones aplicables, en beneficio de los derechos de los titulares y de la integridad institucional.

Inventario de Datos Personales (Planeación).

El inventario de datos personales representa una herramienta esencial para la gestión segura y ordenada de la información en posesión de las unidades administrativas de la Universidad. Conforme al Artículo 58 de los Lineamientos Generales, este inventario permite identificar de forma precisa qué datos personales se recaban, las finalidades de su tratamiento, los medios de obtención, los sistemas o archivos en

que se almacenan, y los responsables de su resguardo. Su elaboración es indispensable para establecer controles efectivos, delimitar riesgos, definir niveles de seguridad adecuados y asegurar el cumplimiento de los principios de licitud, proporcionalidad y calidad.

Además, facilita el cumplimiento de obligaciones institucionales como la emisión de avisos de privacidad, la atención a solicitudes de derechos ARCO, y la realización de evaluaciones de impacto. En el contexto universitario, contar con un inventario actualizado y validado permite a cada unidad administrativa tener una visión clara de los tratamientos que realiza y contribuir activamente a la cultura de protección de datos personales dentro de la UIMQROO.

Ciclo de Vida de los Datos Personales en el Inventario (Planeación).

La gestión adecuada del ciclo de vida de los datos personales es un elemento clave para garantizar su protección integral dentro de la UIMQROO. En concordancia con el Artículo 59 de los Lineamientos Generales, las unidades administrativas deben considerar todas las etapas por las que atraviesan los datos personales (desde su recolección, uso, almacenamiento, conservación, hasta su supresión o resguardo definitivo), con el propósito de aplicar medidas de seguridad apropiadas en cada fase.

Reconocer este ciclo permite a la UIMQROO identificar riesgos específicos en cada momento del tratamiento, establecer responsabilidades claras, y asegurar que los datos sean tratados únicamente por el tiempo necesario y para fines legítimos.

Asimismo, permite cumplir con los principios de finalidad, temporalidad, minimización y responsabilidad, evitando la acumulación innecesaria de información y reduciendo la exposición a incidentes de seguridad. Incluir esta visión en la gestión institucional fortalece el control documental, mejora la administración de archivos y refuerza el compromiso universitario con la protección de los derechos de las personas titulares.

Análisis de Riesgo (Planeación).

El análisis de riesgos es un componente esencial en el marco del Sistema de Gestión de Seguridad de Datos Personales de la UIMQROO, ya que permite identificar,

valorar y priorizar los riesgos que podrían afectar la confidencialidad, integridad o disponibilidad de los datos personales en posesión de las unidades administrativas.

De acuerdo con el Artículo 60 de los Lineamientos Generales, este análisis debe considerar los escenarios de vulnerabilidad en cada fase del tratamiento de datos, así como el impacto potencial ante un incidente de seguridad.

Para la UIMQROO, realizar este ejercicio de manera periódica y documentada permite tomar decisiones informadas sobre la implementación de controles, asignación de recursos y definición de niveles de seguridad proporcionales al nivel de riesgo.

Además, fortalece la cultura de prevención y mejora continua, alineando los procesos institucionales con los principios de responsabilidad proactiva y gestión basada en riesgos.

Por lo tanto, el análisis de riesgos se convierte en una herramienta estratégica para proteger los derechos de los titulares y preservar la integridad institucional de la Universidad.

Bitacora de Riesgos (Planeación).

La identificación y registro sistemático de riesgos mediante una bitácora constituye una práctica fundamental para fortalecer la gestión de seguridad de los datos personales en la UIMQROO.

Esta herramienta permite a las unidades administrativas documentar de manera estructurada los riesgos detectados en sus procesos, así como su nivel de impacto, probabilidad de ocurrencia, causas, consecuencias y controles asociados. La bitácora de riesgos no solo facilita el seguimiento y actualización continua del análisis de riesgos previsto en el artículo 60 de los Lineamientos Generales, sino que también promueve una cultura de prevención, permite anticiparse a incidentes, y genera evidencia documental del cumplimiento institucional del principio de responsabilidad proactiva.

Además, contribuye a la toma de decisiones estratégicas para mitigar riesgos, asignar recursos y definir prioridades en materia de protección de datos personales,

garantizando un entorno más seguro para la comunidad universitaria y los titulares de la información.

Análisis de Brecha (Planeación).

El análisis de brecha es una herramienta clave para evaluar el grado de cumplimiento de las obligaciones en materia de protección de datos personales dentro de la UIMQROO. De acuerdo con el Artículo 62 de los Lineamientos Generales, permite identificar las diferencias entre la situación actual de las medidas, políticas y procedimientos implementados, y el marco normativo aplicable.

Para la UIMQROO, realizar un análisis de brecha en cada unidad administrativa permite detectar omisiones, deficiencias o áreas de oportunidad en la gestión de seguridad de los datos personales, así como establecer un plan de acción claro y medible para subsanarlas.

Esta práctica fortalece la capacidad institucional de autocorrección, fomenta una cultura de mejora continua y asegura que la universidad avance de forma progresiva y documentada hacia el cumplimiento total de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En consecuencia, el análisis de brecha se convierte en una herramienta estratégica para alinear los procesos universitarios con los principios de responsabilidad, transparencia y legalidad.

Plan de Trabajo (Implementar y operar).

El establecimiento de un plan de trabajo institucional en materia de protección de datos personales es indispensable para dirigir de forma ordenada, estratégica y verificable las acciones de cumplimiento normativo al interior de la UIMQROO. De acuerdo con el Artículo 62 de los Lineamientos Generales, las unidades administrativas deben definir un conjunto de acciones específicas que permitan corregir deficiencias, consolidar procesos y avanzar hacia una gestión integral de seguridad.

Este plan de trabajo debe estar alineado con los principios de responsabilidad y mejora continua, y ser coherentes con los elementos estructurales del sistema de

gestión, tales como: el alcance y objetivos institucionales, la política de datos personales, la definición de funciones y obligaciones, el inventario y ciclo de vida de los datos, el análisis de riesgos, la bitácora de riesgos y el propio análisis de brecha.

Propuesta de tres acciones prioritarias para el año 2026:

1. Formalización y difusión de la Política Institucional de Protección de Datos Personales en toda la UIMQROO, con su adopción obligatoria por parte de todas las unidades administrativas, y capacitación inicial para su aplicación práctica.
2. Desarrollo del primer Diagnóstico Institucional de Riesgos y Análisis de Brecha, acompañado de la creación y actualización de la bitácora de riesgos, que permita definir prioridades de intervención, asignar responsables y generar evidencia documental de cumplimiento.
3. Elaboración de Inventarios de Datos Personales en cada unidad administrativa, como base para definir medidas de seguridad adecuadas.

Este plan de trabajo será el punto de partida para estructurar una hoja de ruta institucional que articule los esfuerzos de cada unidad administrativa y consolide un sistema de gestión de protección de datos personales sólido, progresivo y conforme a la normatividad vigente.

Monitoreo y supervisión periódica de las medidas de seguridad implementadas.

El establecimiento en la UIMQROO de un plan de monitoreo y supervisión en materia de protección de datos personales es fundamental para garantizar el funcionamiento continuo, efectivo y conforme a la ley.

Según lo dispuesto en el Artículo 63 de los Lineamientos Generales, este plan permitirá verificar periódicamente el cumplimiento de las medidas de seguridad, identificar desviaciones, y tomar decisiones oportunas ante riesgos o incidentes. En el contexto universitario, las unidades administrativas deben asumir un papel activo y sistemático en la vigilancia de sus prácticas relacionadas con el tratamiento de datos personales, priorizando la revisión de factores de riesgo y la detección de posibles vulneraciones a la seguridad, como accesos indebidos, fugas de información, pérdidas de datos o incumplimientos de obligaciones normativas.

El plan de monitoreo y supervisión no solo fortalece la transparencia interna y la rendición de cuentas, sino que también permite documentar evidencia de cumplimiento, generar alertas tempranas, y retroalimentar las políticas, procedimientos y controles establecidos. Esta práctica es clave para mantener actualizadas las acciones preventivas y correctivas, conforme a un enfoque de mejora continua y gestión basada en riesgos.

Propuesta de tres acciones prioritarias para el año 2026:

1. Implementación de revisiones semestrales de cumplimiento en cada unidad administrativa, enfocadas en verificar la aplicación de medidas de seguridad físicas, técnicas y administrativas, con base en el inventario de datos personales y el ciclo de vida identificado.
2. Establecimiento de un protocolo de seguimiento de incidentes y vulneraciones, que incluya la identificación de factores de riesgo recurrentes, la clasificación del impacto, el registro en la bitácora de riesgos, y la activación de medidas de respuesta inmediata.
3. Desarrollo de auditorías internas semestrales sobre el análisis de brecha y el plan de trabajo, para evaluar avances, detectar omisiones, validar controles implementados y ajustar los objetivos del sistema de gestión de acuerdo con los hallazgos.

Estas acciones permitirá a la UIMQROO consolidar un sistema robusto de supervisión, reducir la exposición institucional a riesgos legales o reputacionales, y fortalecer la confianza de la comunidad universitaria en el tratamiento responsable de sus datos personales.

Plan de Mejora Continua, Capacitación .y Cultura de la Protección de Datos Personales

El plan de mejora continua constituye la fase estratégica del Sistema de Gestión de Seguridad de Datos Personales, mediante la cual la UIMQROO evalúa, actualiza y fortalece de forma sistemática las políticas, medidas y prácticas implementadas en materia de protección de datos personales.

Esta etapa, prevista en la LGPDPPSO y desarrollada en el Artículo 64 de los Lineamientos Generales, no solo implica corregir deficiencias o mitigar riesgos, sino

también consolidar una cultura institucional orientada al cumplimiento, la prevención y la excelencia operativa.

En este marco, la capacitación del personal adquiere un papel fundamental. El propio artículo 64 menciona, los responsables deben diseñar e implementar programas de formación continua que aseguren que todas las personas involucradas en el tratamiento de datos personales comprendan sus funciones, obligaciones y las implicaciones legales de sus acciones. En una institución como la UIMQROO, conformada por diversas unidades administrativas con funciones académicas, administrativas, tecnológicas y comunitarias, la formación continua es esencial para lograr una aplicación transversal, coherente y efectiva de los principios de protección de datos personales.

El plan de mejora continua permite que los aprendizajes derivados de ejercicios como el análisis de brecha, el monitoreo, la bitácora de riesgos o el ciclo de vida de los datos, se traduzcan en acciones concretas de capacitación, actualización normativa, rediseño de procesos y fortalecimiento institucional.

Propuesta de tres acciones prioritarias para el año 2026:

1. Diseño e implementación de un programa anual de capacitación por perfiles, dirigido a personal directivo, administrativo, operativo y académico, con módulos diferenciados según sus funciones en el tratamiento de datos personales y con énfasis en la responsabilidad institucional.
2. Incorporación de resultados del análisis de brecha y monitoreo de riesgos en los contenidos del programa de formación, con el objetivo de que la capacitación responda a los hallazgos reales detectados en las unidades administrativas.
3. Evaluación semestral del nivel de cumplimiento y madurez del sistema de gestión, a través de indicadores de desempeño institucional y encuestas de autoevaluación por unidad, para ajustar procesos, reforzar controles y retroalimentar las políticas institucionales.

Con estas acciones, la UIMQROO consolida un enfoque dinámico, reflexivo y orientado a resultados en la protección de datos personales, alineado con el marco jurídico vigente y con su compromiso de promover una administración pública universitaria transparente, legal y respetuosa de los derechos humanos.