DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

UIMQROO

Diciembre 2025

Tabla de contenido

GLOSARIO

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 sijetos 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: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento u 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.

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.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

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. Se consideran sensibles de manera enunciativa más no limitativa, los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas, datos biométricos, preferencia sexual y de género.

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, por 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.

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.

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.

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.

Remisión: A toda comunicación de datos personales realizada exclusivamente entre el responsable y la persona encargada, dentro o fuera del territorio mexicano;

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.

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.

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.

Transferencia: A toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la titular, del responsable o de la persona encargada;

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados de manera enunciativa más no limitativa con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia y en general cualquier uso o disposición de 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.

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.

INTRODUCCIÓN

La Universidad Intercultural Maya de Quintana Roo (UIMQROO), reconoce el Derecho Humano de la protección de datos personales, establecido en la Constitución Política de los Estados Unidos Mexicanos en los artículos 6, apartado A, fracciones II y III y 16, segundo párrafo.

A partir de la reforma constitucional de 2009, la protección de datos personales quedó establecida como un derecho fundamental, el cual reconoce que toda persona tiene derecho a la protección, y al ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales.

El 26 de enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo, la Ley General), que tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de los sujetos obligados.

En fecha 04 de julio de 2017, se publicó la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo reformada el 25 de Noviembre de 2025; de observancia obligatoria en todo el territorio del Estado de Quintana Roo y sus Municipios, que tiene por objeto garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de los Responsables.

El 26 de enero de 2018, se publicó en el Diario Oficial de la Federación los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) cuyo objetivo es desarrollar las disposiciones previstas en la Ley General y, con ello, hacer más comprensible el cumplimiento de los principios, deberes y obligaciones exigidos en materia de protección de datos personales.

En este sentido, la UIMQROO, reconoce la necesidad de observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, responsabilidad; así como los deberes de seguridad y confidencialidad que derivan de las Leyes en materia de datos personales.

Dichos principios y deberes dictan una serie de obligaciones de observancia para los responsables, que tiene como propósito que el tratamiento se realice garantizando la protección de los datos personales de sus titulares.

En relación con el deber de seguridad, los responsables deben elaborar un Documento en el que se establezcan las medidas de seguridad de carácter administrativo, físico y técnico que han de adoptar para el adecuado tratamiento de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción, uso, acceso o

tratamiento no autorizado a través del ciclo de vida de los datos personales; así como garantizar su confidencialidad, integridad y disponibilidad.

OBJETIVO DEL DOCUMENTO DE SEGURIDAD

Garantizar que todo tratamiento de datos personales cuente con las medidas de seguridad necesarias para la protección de los mismos y el cumplimiento de las obligaciones previstas en la Ley de datos.

De conformidad con el artículo 32 de la Ley, establece que el responsable debe realizar las siguientes actividades interrelacionadas:

I. Crear políticas internas para la gestión y tratamiento de los datos personales que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

RESPONSABILIDADES

En apego al artículo 91 de la Ley, establece que el responsable en materia de protección de datos personales, es el Comité de Transparencia.

Es así que cada Sujeto Obligado contará con un Comité, el cual se integrará y funcionará conforme lo establece la Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo y demás normatividad aplicable.

Dicho Órgano, tendrá dentro de sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales. En esa tesitura dicho órgano tiene las funciones siguientes:

I. Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia;

II. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con lo previsto en la presente Ley y demás disposiciones aplicables en la materia;

III. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

IV. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;

V. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la Ley y en aquellas disposiciones que resulten aplicables en la materia;

VI. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;

VII. Dar seguimiento y cumplimiento a las resoluciones emitidas por la Secretaría Anticorrupción y Buen Gobierno de la Administración Pública Federal o las Autoridades Garantes Estatales, según corresponda;

VIII. Establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales, y

IX. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este documento, para lo cual, deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

I. POLITICAS INTERNAS

El Sistema de Gestión de Datos Personales es el medio por el cual la UIMQROO, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus

funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.

II. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

Es un control documentado que permite identificar los procesos en los que las unidades administrativas del Instituto tratan datos personales.

Es a través de esas bases de datos en las que se documenta la información básica de cada tratamiento, con independencia de su forma de almacenamiento.

En la UIMQROO se cuenta con 1 Rectoría y 4 Direcciones que tratan datos personales:

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

Las personas encargadas de llevar a cabo el tratamiento de datos, tienen como funciones y obligaciones las siguientes:

- Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.

- Garantizar la debida protección de los datos personales, conforme a la Ley de datos y las demás disposiciones aplicables en la materia.
- Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.
- Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.
- Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
- Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.

1. Rectoría.

1.1. Toma de Fotografías y usos de imágenes para la difusión Institucional.

2. Dirección de Planeación y Desarrollo Institucional y Mejora Regulatoria.

2.1. Quejas, sugerencias y felicitaciones del Sistema Integral de Gestión de Calidad (SIGC).

2.2. Toma de Fotografías y usos de imágenes para la difusión Institucional.

3. Dirección de Administración y Servicios y de Archivos.

3.1. Expedientes del Personal de Confianza.

4. Dirección Académica.

4.1. Procesos de designación, cambio o declinación del (EN) comité de titulación.

5. Dirección Jurídica y Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

5.1. Elaboración de contratos y convenios.

Con la información recabada a través el inventario de datos personales, se pudo percibir la importancia de analizar cada uno de los principios que señala la Ley; y en consecuencia acorde a cada sistema de tratamiento, se realizaron las actualizaciones de los avisos de privacidad; cabe resaltar que en el art. 19 de la Ley, señala cuando el responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales.

III. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

De conformidad a los artículos 32 Fracción II y 35 Fracción II de la Ley de datos, se describen las funciones y Obligaciones del personal involucrado en el tratamiento de datos personales, en apego a las facultades establecidas en el Decreto por el que se reforma integralmente el decreto por el cual se crea la UIMQROO y demás normativa.

IV. ANÁLISIS DE RIESGOS, ANÁLISIS DE BRECHA Y PLAN DE TRABAJO

En apego al art. 32 fracción IV, el análisis de riesgo debe ser elaborado considerando las amenazas y vulnerabilidades existentes, para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros, identificando los riesgos latentes respecto de cada uno de los tratamientos de datos personales.

Atendiendo lo anterior las unidades administrativas de la UIMQROO que tratan datos personales, realizaron un análisis, acorde a cada sistema enumerado con base a lo siguiente:

Análisis de Riesgos

El análisis de riesgos es un proceso sistemático para conocer y determinar la magnitud de los riesgos a los que se encuentran expuestos los activos de responsable. El análisis de riesgos permite determinar cómo es, cuánto vale y cómo está protegido cada activo (identificando posibles problemas), y anticiparse a las futuras dificultades, lo que nos permitirá tomar mejores decisiones y actuar con oportunidad.

En el análisis de riesgos deben considerarse los siguientes elementos:

- Activos, que se dividen en dos tipos:
  - Activos de información: Datos personales;
  - Activos de apoyo: Elementos físicos e infraestructura que soportan los activos de información;
- Amenazas: Eventos con la capacidad de causar daño a una organización;
- Vulnerabilidades: Debilidades de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Metodología BAA

Se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante:

- Beneficio para el atacante;
- Accesibilidad para el atacante;
- Anonimidad del atacante.

Identificación y clasificación de datos personales

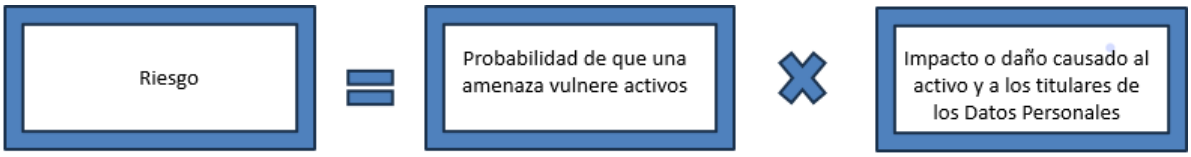
- Clasificación de datos personales;
- Identificación de tipos de datos y de nivel de riesgo inherente.

Análisis de riesgos de datos personales

- Identificación de riesgo por tipo de dato;
- Identificación del nivel de riesgo por tipo de dato;
- Cuestionario de autoevaluación;
- Identificación de nivel de accesibilidad;
- Identificación de nivel de anonimidad;
- Identificación de nivel de riesgo latente.

Identificación de medidas de seguridad

- Tablas de control;
- Procedimiento de selección de medidas de seguridad.



Derivado del análisis, es posible identificar:

Impacto		*Probabilidad*		*Nivel de riesgo*	
Cuantitativo	*Cualitativo*	*Cuantitativo*	*Cualitativo*	*Cuantitativo*	*Cualitativo*
5	**Muy alto**	1	Muy baja	5	Medio
5	**Muy alto**	2	Baja	10	Alto
5	**Muy alto**	3	Media	15	Alto
5	**Muy alto**	4	Alta	20	**Muy alto**
5	**Muy alto**	5	**Muy alta**	25	**Muy alto**
4	Alto	1	Muy baja	4	Bajo
4	Alto	2	Baja	8	Medio
4	Alto	3	Media	12	Alto
4	Alto	4	Alta	16	Alto
4	Alto	5	**Muy alta**	20	**Muy alto**
3	Medio	1	Muy baja	3	Bajo
3	Medio	2	Baja	6	Medio
3	Medio	3	Media	9	Medio
3	Medio	4	Alta	12	Alto
3	Medio	5	**Muy alta**	15	Alto
2	Bajo	1	Muy baja	2	Muy bajo
2	Bajo	2	Baja	4	Bajo
2	Bajo	3	Media	6	Medio
2	Bajo	4	Alta	8	Medio
2	Bajo	5	**Muy alta**	10	Alto
1	Muy bajo	1	Muy baja	1	Muy bajo
1	Muy bajo	2	Baja	2	Muy bajo
1	Muy bajo	3	Media	3	Bajo
1	Muy bajo	4	Alta	4	Bajo
1	Muy bajo	5	**Muy alta**	5	Medio

La combinación de los tres factores analizados permitió definir el nivel de riesgo latente por tratamiento, lo cual contribuirá a identificar el nivel de medidas de seguridad que deban implementarse en cada caso.

Análisis de Brecha

Consistente en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados, cuya información da sustento a las políticas y mecanismos institucionales en materia de protección de datos personales que se deban aprobar. Lo anterior con el objetivo de atenderlas de manera escalonada y en coordinación con cada una de las áreas.

Derivado del análisis fue posible identificar como vulneraciones comunes:

1. Robo de información, modificación-destrucción no autorizada de la información, acceso no autorizado a los sistemas.
2. Daños estructurales, fuego, inundación.
3. Fenómenos climáticos y sísmicos.

V. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Cuando hablamos de los mecanismos de monitoreo y revisión de las medidas de seguridad en protección de datos personales, nos referimos a todas las acciones, actividades, instrumentos, herramientas, controles o mecanismos administrativos, técnicos y físicos que permitan protegerlos contra daño, pérdida, alteración, destrucción, uso o acceso no autorizado, garantizando con ello la confidencialidad, integridad y disponibilidad de los datos personales.

Con la finalidad de identificar las medidas de seguridad de manera enunciativa se describen las medidas comunes.

1. Medidas de seguridad administrativas: Acciones y mecanismos implementados en el tratamiento de datos personales a nivel organizacional, como lo son las políticas y procedimientos para la gestión y revisión de la seguridad de la

información, identificación, clasificación y borrado seguro de la información, así como sensibilización y capacitación del personal, en materia de protección de datos personales.

2. Medidas de seguridad físicas: Acciones y mecanismos para proteger el entorno físico, instalaciones, equipos, soportes o sistemas e datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor.

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

3. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología y los recursos involucrados en su tratamiento.

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

VI. EL PROGRAMA GENERAL DE CAPACITACIÓN

El programa concentra los retos en materia de seguridad de datos personales que afrontan las instancias, es así que el personal de la UIMQROO deberá capacitarse

cuando menos una vez al año, con la intención de que todos los servidores públicos puedan participar.

La importancia de implementar un Sistema de Gestión de Seguridad de Datos Personales en el sector público radica en la protección de los datos personales, los cuales deben ser tratados atendiendo los principios y deberes establecidos por la Ley de datos, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de los titulares.

La correcta implementación del Sistema y constante actualización, ayuda a mitigar los efectos de una vulneración de datos personales, evita sanciones a servidores de los titulares hacia el responsable del tratamiento, permite una constante mejora.

VII. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

Dentro de los mecanismos se cuenta con el propósito de tener una mejora continua, actuar, planificar, verificar y hacer.

Es así que el presente documento de seguridad se actualizará cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad, e
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad; y
V. Cuando surjan documentos, formatos, recomendaciones, etc. por parte de la Autoridad Garante Local para la mejora del documento de seguridad.

Ser en el mundo, Ser nosotros