METODOLOGÍA PARA EL ANÁLISIS DE RIESGO DE DATOS PERSONALES
Unidad de Transparencia

1. Presentación

El presente documento de referencia se elaboró por la Unidad de Transparencia del Centro de Investigación en Matemáticas, A.C. (CIMAT) y tiene como finalidad dotar de herramientas necesarias a las áreas responsables para determinar el análisis de riesgo en el tratamiento de datos personales a su responsabilidad.

Para lo anterior, se ofrecen algunas aproximaciones al tema de medidas de seguridad en materia de protección de datos personales, cuya referencia son los estándares reconocidos en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO).

En principio y a través del análisis de los conceptos básicos que inciden alrededor del tema, se explica la importancia de las medidas de seguridad en los sujetos obligados y el papel que juegan en la protección de las bases de datos personales. Posteriormente se profundiza en los tipos de medidas de seguridad, categorización de datos y análisis de riesgo.

A partir de este documento orientador, la Unidad de Transparencia desarrolla y aproxima elementos objetivos para continuar con la implementación de las disposiciones legales en la materia, particularmente para la recopilación de los insumos necesarios para la actualización del Documento de Seguridad de este Centro de Investigación, bajo los parámetros del artículo 35 de la Ley.

Además, los trabajos en este rubro ayudarán a sensibilizar a las personas involucradas con el tratamiento de los datos personales sobre los parámetros de seguridad y uso adecuado de los mismos, garantizando la confidencialidad y los derechos de protección de los datos personales de los titulares, y las áreas podrán reconocer el estatus que guardan sus tratamientos de datos personales en relación con el estándar idóneo de medidas de seguridad que deberían adoptar.

---

1 VIDE. INAI, Metodología de Análisis de Riesgo BAA, 2015

2. Principios y deberes

Los deberes legales en materia de datos personales deben entenderse a partir de los principios que son la guía para su tratamiento, el cual debe sujetarse a los siguientes estándares:

- Licitud: sujetarse a las facultades y atribuciones que la normatividad aplicable le confiera al sujeto obligado.
- Finalidad: estar justificado.
- Lealtad: los datos personales deben recabarse de manera legítima, garantizando su protección y privacidad.
- Consentimiento: se deberá contar con el consentimiento del titular de los datos personales en caso de que éste sea necesario recabarse.
- Calidad: los datos personales deben ser exactos, correctos, completos y actualizados, a fin de que no se altere la veracidad de éstos.
- Proporcionalidad: solo debe ser de aquellos datos personales adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.
- Información: se deberá informar al titular que sus datos personales serán tratados y explicar la finalidad de éste.
- Responsabilidad: los responsables del tratamiento de los datos personales adoptarán las medidas necesarias para garantizar su protección.

Así, los deberes legales apuntalan la protección de los datos personales a través de la implementación de medidas de seguridad y la garantía de confidencialidad de los mismos. De conformidad con la garantía de confidencialidad, los responsables del tratamiento de datos personales tienen el deber de no divulgar, no poner a disposición de terceros, ni emplear datos personales para otros propósitos que no sean aquellos para los cuales se obtuvieron.

3. Medidas de seguridad, categorización de datos y riesgo latente.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales y deben conjugarse con el nivel de protección que requieren las bases de datos. Por ejemplo, el nivel de protección será mayor cuando se trate de bases de datos que resguarden datos personales sensibles y/o almacenen información de una gran cantidad de titulares.

La finalidad de las medidas de seguridad es garantizar, con mecanismos tangibles, la protección de los datos personales en todas las áreas donde se tratan.

3.1. Las medidas de seguridad administrativas.

Son las políticas y procedimientos para la gestión, soporte, 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.

3.2. Medidas de seguridad físicas.

Se refieren a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor. Se deben considerar, entre otras, las siguientes actividades:

- 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.

3.3. Medidas de seguridad técnicas

Son el 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:

- 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.

3.4. Categorización de datos.

Uno de los métodos para determinar el nivel de medidas de seguridad que deben adoptarse en cada base de datos, es conocer la categoría de los datos personales que albergan cada uno de éstas. A continuación, se detallan algunos parámetros de clasificación aceptados:

- **Datos de identificación:** El nombre completo, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, demás análogos;
- **Datos electrónicos:** Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas;
- **Datos laborales:** Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, demás análogos;
- **Datos patrimoniales:** Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales, demás análogos;
- **Datos sobre procedimientos administrativos:** La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio, demás análogos;
- **Datos académicos:** Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados, cartas de recomendación, listados de calificaciones y reconocimientos, demás análogos;
- **Datos de tránsito y movimientos migratorios**: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria, y demás análogos;
- **Datos sobre la salud:** El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona, y demás análogos;
- **Datos biométricos:** Huellas dactilares, ADN, fotografías, geometría de la mano, características de iris y retina, demás análogos; y,
- **Datos especialmente protegidos (sensibles):** En algunos casos los datos biométricos arriba señalados, origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual; así como los datos de niños y niñas y demás análogos.

Es necesario advertir que algunos tipos de datos arriba mencionados son susceptibles de hacerse públicos, cuando por ley exista una obligación de difundirlos y/o se trate de servidores públicos, tal es el caso de algunos datos identificativos, patrimoniales, laborales, académicos, etcétera.

4. Niveles de riesgo.

Las medidas de seguridad que deberán adoptarse por el responsable de la Unidad Administrativa deben tomar como referencia el nivel de riesgo que presenta cada tratamiento de datos personales. Para ello, es necesario calcular los factores de riesgo por tipo de dato, por tipo de acceso y por entorno desde el cual se realizan los tratamientos de los datos personales.

4.1. A partir del tipo de dato.

Es posible reconocer el factor de riesgo inherente, como se muestra a continuación:

Tipo de dato	Riesgo inherente	Nivel de riesgo
Datos de identificación	Bajo	1
Datos electrónicos; laborales; patrimoniales; procedimientos administrativos	Medio	2
Datos de tránsito y movimientos migratorios; Sobre la salud; biométricos	Alto	3
Datos especialmente protegidos (sensibles)	Muy alto	4 -5

Al riesgo inherente, es necesario sumarle el volumen de titulares contenidos en la base de datos, por ejemplo:

- Menos de 100 titulares (>100).
- Menos de 1000 titulares (>1000).
- Menos de 10,000 (>10,000)
- Más de 10,000 (<10,000).

El riesgo inherente más el volumen de titulares, da como resultado el nivel de riesgo por tipo de dato:

Nivel de riesgo por tipo de dato				
Tipo de dato / Número de titulares	>100	>1000	>10,000	>100,000
Datos especialmente protegidos (sensibles)	4	4	5	5
Datos de tránsito y movimientos migratorios	1	2	3	3

Nivel de riesgo por tipo de dato				
Tipo de dato / Número de titulares	>100	>1000	>10,000	>100,000
Sobre la salud; biométricos				
Datos electrónicos; laborales; patrimoniales; procedimientos administrativos	1	1	2	2
Datos	1	1	1	1

El nivel de riesgo por tipo de dato servirá para determinar los controles que se deben considerar para su protección.

4.2. A partir del tipo de acceso.

Se mide determinando la cantidad de accesos potenciales a los datos personales que se pretenden proteger en un intervalo de tiempo, por ejemplo, durante una semana. Para este parámetro entre mayor sea la accesibilidad, mayor riesgo existe para la información.

ACCESIBILIDAD (CANTIDAD DE ACCESOS)	Nivel de Riesgo
>10	1
>20	2
>30	3
>40	4-5

4.3. Riesgo por tipo de entorno.

Representa el nivel de anonimidad para acceder o hacer uso de los datos personales que se tratan. Entre mayor anonimidad ofrezca el entorno, mayor riesgo existe de que se vulnere la seguridad.

En caso de que se accedan por más de un entorno a los datos personales, se debe considerar el entorno de mayor riesgo.

ENTORNO	Nivel de Riesgo
Físico	1
Equipo de cómputo	2
Nube	3
Internet	4-5

La combinación de los tres factores analizados da como resultado el nivel de riesgo latente de cada tratamiento de datos personales, lo cual contribuye a identificar el nivel de medidas de seguridad que deben implementarse en cada caso.

Una vez que se calcula el nivel de riesgo latente por cada tratamiento de datos personales, es posible realizar estrategias para identificar los modelos de medidas de seguridad que deben aplicarse a cada uno de ellos.

Realizar un análisis de riesgos por cada tratamiento ayudará a identificar el nivel de medidas de seguridad que deben ser implementadas para la protección de los datos personales.

Una vez identificado el ideal de medidas de seguridad que deberían implementarse, se realiza un comparativo con aquellas que son implementadas por las áreas, obteniendo con ello un análisis de brecha, a través del cual se han construido los planes de trabajo, mecanismos de monitoreo y revisión de medidas de seguridad y programas de capacitación, elementos que conforman el Documento de Seguridad de este Centro de Investigación.

ANÁLISIS DE RIESGO
SISTEMAS DE TRATAMIENTO
CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS, A.C.

Guanajuato, Gto., a 29 de marzo de 2024

ANALISIS DE RIESGO						
Sistema de Tratamiento	**NIVELES DE RIESGO**				**Riesgo del Sistema**	
	Tipo de dato	**Volumen de Titulares**	**Tipo de acceso**	**Tipo de entorno**		
Ejercicio de derechos ARCO	1	1	1	2	1	Bajo
Solicitudes de acceso a la información	1	1	1	2	1	Bajo
Reclutamiento de Personal	5	4	1	2	3	Alto
Expediente de Personal	5	4	1	2	3	Alto
Enfermería Institucional	5	4	1	2	3	Alto
Apoyo Académico	3	1	1	2	1	Bajo
Eventos académicos	1	1	1	4	1	Bajo
Eventos académicos (menores de edad)	5	2	1	4	3	Alto
Registro servicio de hospedaje CIMATEL	1	1	1	1	1	Bajo
Registro hospedaje CIMATEL (menores)	5	2	1	4	3	Alto
Contratos y convenios derivados de las actividades de vinculación	1	1	1	2	1	Bajo
Admisión a posgrados	2	1	1	2	1	Bajo
Postulación de Becarios	2	1	1	2	1	Bajo
Visita de grupos al CIMAT	1	1	1	1	1	Bajo
Inscripciones de nuevo ingreso	2	1	1	2	1	Bajo
Sistema de Egresados del CIMAT	2	1	1	2	1	Bajo
Registro de Usuarios de Biblioteca	1	1	1	2	1	Bajo
Repositorio de Tesis	1	1	1	2	1	Bajo
Control de Parque Vehicular	5	4	1	1	2	Medio
Monitoreo y videovigilancia	1	1	1	1	1	Bajo
Visitas de escuelas	1	1	1	1	1	Bajo

	ANALISIS DE BRECHA						
Sistema de Tratamiento	**Nivel de riesgo**	**Medidas de seguridad aplicadas**				**Nivel de riesgo**	**Prioridad acciones**
		Admvas.	**Físicas**	**Técnicas**	**Suma**		
Ejercicio de derechos ARCO	Bajo	1	1	1	3	Bajo	Moderado
Solicitudes de acceso a la información	Bajo	1	1	1	3	Bajo	Moderado
Reclutamiento de Personal	Alto	1	1	1	3	Alto	Crítico
Expediente de Personal	Alto	1	1	1	3	Alto	Crítico
Enfermería Institucional	Alto	1	1	1	3	Alto	Crítico
Apoyo Académico	Bajo	1	1	1	3	Bajo	Moderado
Eventos académicos	Bajo	1	1	1	3	Bajo	Moderado
Eventos académicos (menores de edad)	Alto	1	1	1	3	Alto	Crítico
Registro servicio de hospedaje CIMATEL	Bajo	1	1	1	3	Bajo	Moderado
Registro hospedaje CIMATEL (menores)	Alto	1	1	1	3	Alto	Crítico
Contratos y convenios derivados de las actividades de vinculación	Bajo	1	1	1	3	Bajo	Moderado
Admisión a posgrados	Bajo	1	1	1	3	Bajo	Moderado
Postulación de Becarios	Bajo	1	1	1	3	Bajo	Moderado
Visita de grupos al CIMAT	Bajo	1	1	1	3	Bajo	Moderado
Inscripciones de nuevo ingreso	Bajo	1	1	1	3	Bajo	Moderado
Sistema de Egresados del CIMAT	Bajo	1	1	1	3	Bajo	Moderado
Registro de Usuarios de Biblioteca	Bajo	1	1	1	3	Bajo	Moderado
Repositorio de Tesis	Bajo	1	1	1	3	Bajo	Moderado
Control de Parque Vehicular	Medio	1	1	1	3	Medio	Moderado
Monitoreo y videovigilancia	Bajo	1	1	1	3	Bajo	Moderado
Visitas de escuelas	Bajo	1	1	1	3	Bajo	Moderado