Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo

CURSO/TALLER

Principios y Deberes de la Protección de los Datos Personales

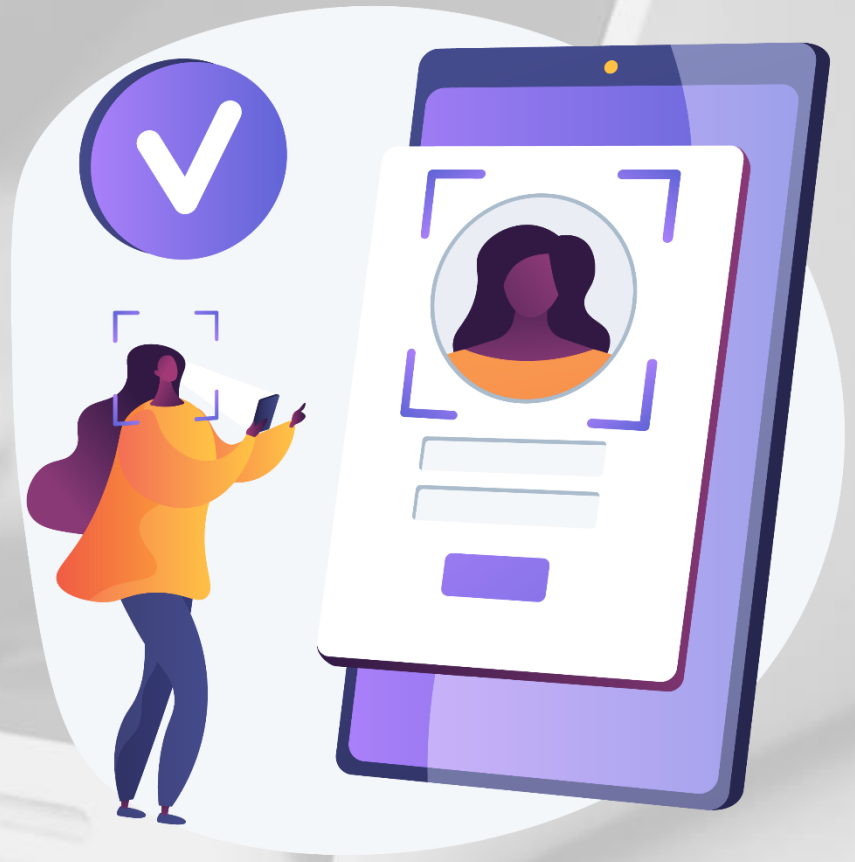
CONTENIDO

1. Los Datos Personales un Derecho Humano reconocido en México
2. Términos y Figuras de la Ley de Protección de Datos Personales
3. Sujetos Obligados de la Ley, responsables del tratamiento de los datos personales
4. 8 Principios rectores de la Ley
5. Deberes: Seguridad y Confidencialidad
6. Medidas de Seguridad
7. Documento de Seguridad
8. Bitácora de Vulnerabilidades
9. Sanciones por incumplimiento a la Ley Local de la materia

Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo

Los Datos Personales como Derecho Humano en México

La protección de datos personales es un derecho humano, reconocido en el **artículo 16** de la Constitución Política de los Estados Unidos Mexicanos, que otorga el poder a **toda persona física** para que sus datos personales sean tratados de manera lícita y leal, a fin de garantizar su privacidad y derecho a la autodeterminación informativa, es decir, a decidir quién puede tratar sus datos personales y para qué fines.



Reforma Constitucional al artículo 16
1 de junio de 2009

"**Nadie** puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento".

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".

Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo

Los Datos Personales como Derecho Humano en México

2007

- Se reforma el artículo 6° constitucional
- Información que se refiere a la vida privada y los datos personales será protegida

2009

- Se reforma el artículo 16, segundo párrafo de la CPEUM
- Se reconoce el derecho a la protección de datos personales como un derecho fundamental

2010

- Se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

26 de Enero 2017

- Se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

4 de Julio de 2017

- Se publica en el P.O.
- La Ley Local de Protección de Datos Personales

Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo

¿Qué es un Dato Personal?

Es cualquier información concerniente a una persona física identificada o identificable, como puede ser el nombre, los apellidos, la dirección postal, el número de teléfono, o cualquier otra información que permita identificar o haga identificable al titular de los datos.

¿Qué se entiende por tratamiento de datos personales?

Tratar datos personales es un concepto amplio, ya que incluye: Obtención, uso, divulgación, almacenamiento. El uso de los datos personales abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de Datos Personales.

¿Qué es un Dato Personal Sensible?

Son datos personales que afectan la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen o conlleve un riesgo grave para éste, como por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro).

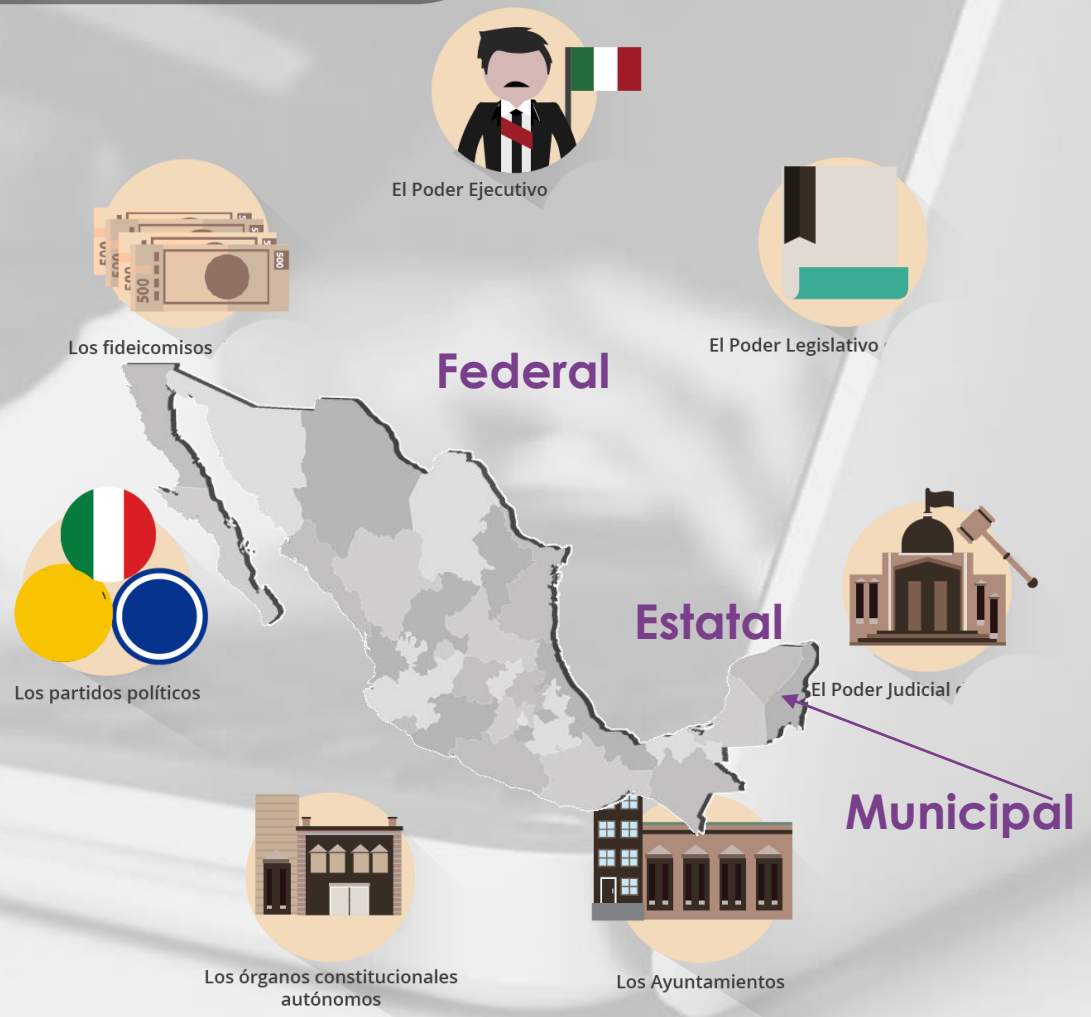
¿Quién es el titular de los datos personales?

Es la persona física a quien refieren y pertenecen los datos personales que son objeto de tratamiento. Por tanto, es el dueño de los datos personales, aunque éstos estén en posesión de un tercero para su tratamiento.

¿Quién es el responsable del tratamiento?

Los Sujetos Obligados a que se refiere el **artículo 2** de la Ley que decidan sobre el tratamiento de datos personales.

Son responsables de los datos personales, en el ámbito estatal y municipal: cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.



Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo

¿Quién es el encargado del tratamiento?

Es la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o adjuntamente con otras trata los datos personales a nombre y por cuenta del responsable. A diferencia de este último, el encargado no decide sobre el tratamiento de los datos personales, sino que lo realiza siguiendo las instrucciones del responsable.

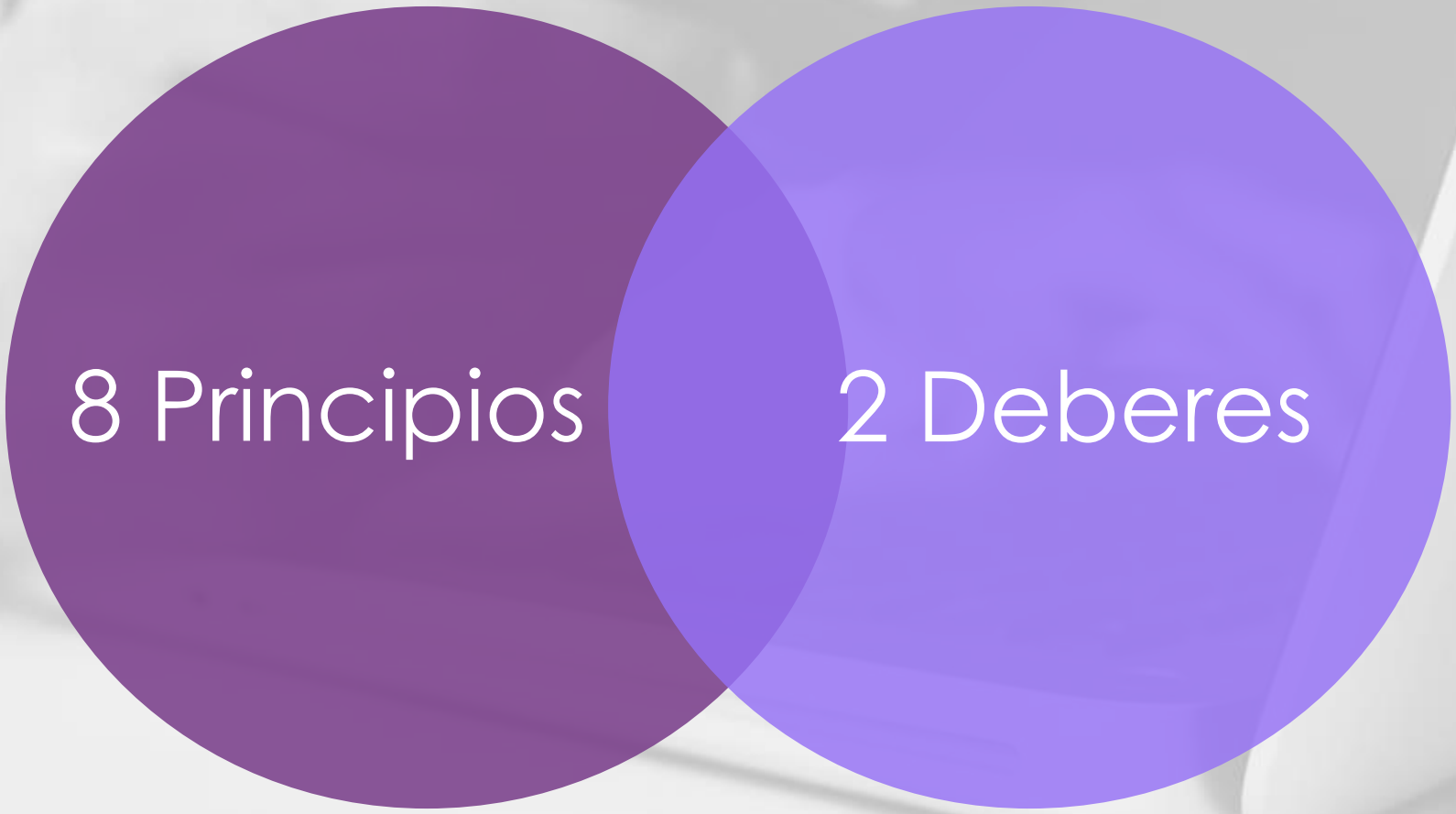
¿Qué es una transferencia de datos personales?

Es toda comunicación de datos personales dentro o fuera de territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Un patrón (responsable del tratamiento) que comunica datos personales de sus trabajadores al Instituto Mexicano del Seguro Social (tercero), para el cálculo de la pensión.

Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo

Principios y Deberes de la Ley de Protección de Datos Personales



LO PRIMERO QUE DEBO HACER PARA CUMPLIR CON MIS OBLIGACIONES

1.CÓMO. Conocer cómo se lleva a cabo el tratamiento de los DP en el Sujeto Obligado. ¿Alguno de estos DP son patrimoniales, financieros o sensibles?

2. DÓNDE: De dónde se obtienen los DP (a través del titular, transferencias, fuentes de acceso público, etc.). De manera Personal, Directa o Indirecta.

3. QUIÉNES: Qué Unidades Administrativas (departamentos) recaban y/o tratan datos personales.

4. PARA QUÉ: Las finalidades del tratamiento. Ej. nómina o expediente de personal.

5. CON QUIÉN y para qué se comparten DP (encargados o terceros). Ej. Call Center.

6. DÓNDE se almacenan los DP (lugar físico: archiveros o electrónico como computadoras, servidores, etc.

7. QUÉ procedimientos y mecanismos y tecnología utilizan en el tratamiento.

8. CUÁNTO tiempo se conservan los Datos Personales.

9.DESTRUCCIÓN: Procedimientos para la destrucción de Datos Personales.

Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo

Principios de la Protección de Datos Personales

Principio de Licitud

- **Artículo 12**: Implica que todo tratamiento de datos personales por parte de los responsables deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Hacer con los datos personales aquello que esté legalmente permitido en observancia a las Leyes de Protección de Datos personales y a la normatividad específica de la materia que se trate y que regule el tratamiento.

Principio de Finalidad

Artículo 13: El principio de Finalidad, implica que todo tratamiento de datos personales que efectué el responsable deberá estar justificado por finalidades **concretas, lícitas, explícitas y legítimas**, en relación con las atribuciones expresas que la normatividad aplicable les confiera.

Para efectos de la presente Ley, se entenderá que las finalidades son:

I. **Concretas**: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que sea posible la existencia de finalidades genéricas que puedan ocasionar confusión en el titular;

II. **Explícitas:** cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad, y

III. **Lícitas y legítimas**: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones expresas del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.

Principio de Lealtad

Artículo El principio de Lealtad, implica que el responsable no deberá obtener y tratar datos personales, **a través de medios engañosos o fraudulentos**, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Se entenderá que el responsable actúa de forma engañosa o fraudulenta cuando:

I. Medie dolo, mala fe o negligencia en el tratamiento de datos personales que lleve a cabo;

II. Realice un tratamiento de datos personales que dé lugar a una discriminación injusta o arbitraria contra el titular, o

III. Vulnere la expectativa razonable de protección de datos personales.

Principio de Consentimiento

Artículo 15. El principio de consentimiento, implica que cuando no se actualice algunas de las causales de excepción previstas en el **Artículo 19**, de la presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

I. **Libre**: sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;

II. **Específica**: referida a **finalidades** concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e

III. **Informada**: que el titular tenga conocimiento del **aviso de privacidad** previo al tratamiento a que serán sometidos sus datos personales.

Principio de Consentimiento

I. Cuando una Ley así lo disponga

II. Transferencias entre responsables

III. Orden Judicial o autoridad competente

IV. Reconocimiento o defensa de derechos del titular ante autoridad Competente.

V. Ejercicio de derechos o cumplimiento de obligaciones derivadas de una relación jurídica.

VI. Cuando exista situación de Emergencia que pueda dañar a un individuo en su persona o bienes

VII. Prevención, diagnóstico o prestación de asistencia sanitaria

VIII. Datos personales en fuentes de Acceso Público

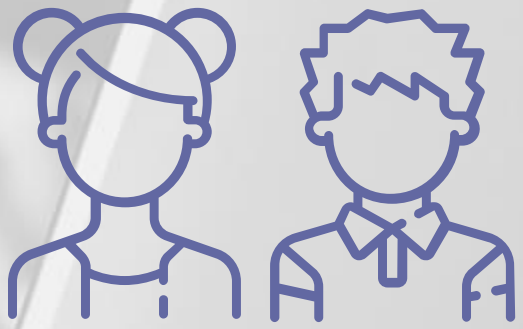
IX. Procedimiento previo de disociación

X. Persona reportada como Desaparecida

Principio de Consentimiento

Consentimiento de Menores de Edad

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a las disposiciones legales aplicables, se estará a lo dispuesto en las reglas de representación previstas en el **Código Civil** para el Estado Libre y Soberano de Quintana Roo y demás normatividad que resulten aplicables.



Principio de Calidad

Artículo 20. El principio de calidad, implica que, el responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos y según se requiera para el cumplimiento de las finalidades concretas, explícitas lícitas y legítimas que motivaron su tratamiento.

Fundamento: Artículos 20, 21 y 22 de la LPDPPSOQROO.

Principio de Proporcionalidad

Artículo 23. El principio de proporcionalidad, implica que el responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y **estrictamente necesarios** para la finalidad concreta, explícita lícita y legítima que justifica su tratamiento.

Principio de Información

Artículo 24. El principio de información, implica que el responsable deberá informar al titular a través del **aviso de privacidad** la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

✓ **Simplificado**

✓ **Integral**

Fundamento: Artículos 24, 25, 26, 27, 28 y 29 de la LPDPPSOQROO.

Principio de Información

- Tendrá por objeto informar al titular sobre los alcances y condiciones generales del tratamiento, a fin de que esté en posibilidad de tomar decisiones informadas sobre el uso de sus datos personales y en consecuencia, mantener el control y disposición sobre ellos.

- El responsable podrá valerse para difundir el aviso de privacidad a través de **medios electrónicos, formatos físicos, medios verbales o cualquier otra tecnología**, siempre y cuando garantice y cumpla con el principio de información.

Fundamento: Artículos, 25 de la LPDPPSOQROO.

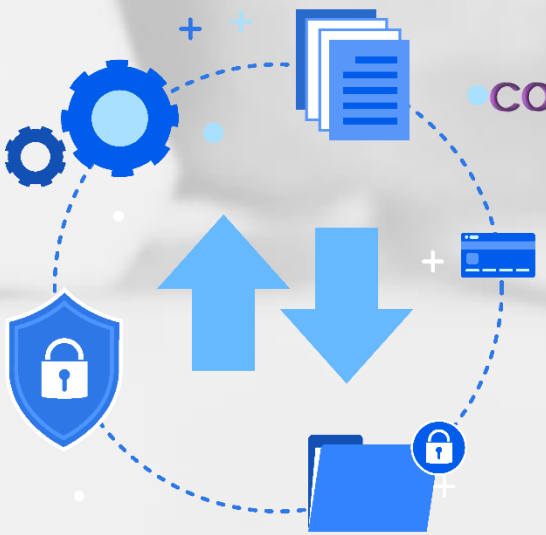
Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo

Aviso de Privacidad Simplificado

I. Denominación del responsable

II. Finalidades del tratamiento

III. Transferencias que requieran consentimiento



IV. Mecanismos para manifestar negativa de tratamiento

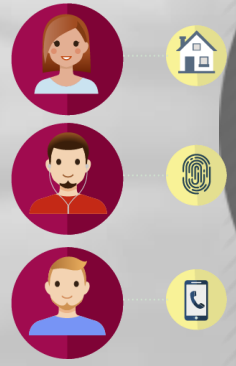
He leído y **NO** acepto los términos

V. Sitio para consultar aviso de privacidad Integral.

Aviso de Privacidad Integral

I. Domicilio del Responsable

II. Datos Personales que se someten al tratamiento



III. Fundamento Legal para Realizar el tratamiento

IV. Finalidades del Tratamiento

V. Mecanismos, medios y Procedimientos para ejercer los Derechos ARCO

VI. Domicilio de la Unidad De Transparencia

VII. Medios en los que el Responsable comunicará cambios del Aviso de Privacidad

Fundamento Art. 28 de la LPDPPSOQROO.

Principio de Responsabilidad

Artículo 30. El principio de responsabilidad, se traduce en que el responsable deberá implementar los mecanismos previstos en el artículo 31 de la presente Ley para **acreditar** el cumplimiento de los **principios, deberes y obligaciones** establecidos en este ordenamiento; y **rendir cuentas** sobre el tratamiento de datos personales en su posesión **al titular y al Instituto**, debiendo observar para tal efecto la legislación aplicable en la materia. Así mismo, podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines, en lo que no se contraponga con la normativa mexicana.

Lo anterior, aplicará aún y cuando los datos personales sean tratados por parte de un **encargado**, así como al momento de realizar **transferencias** de datos personales.

Principio de Responsabilidad

Artículo 31. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

I. Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales;

II. Elaborar **políticas y programas** de protección de datos personales obligatorios y **exigibles al interior** de la organización del Responsable;

III. Poner en práctica un **programa de capacitación** y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;

IV. **Revisar** periódicamente las **políticas y programas** de seguridad de datos personales para determinar las modificaciones que se requieran;

Principio de Responsabilidad

V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;

VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares;

VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y

Principio de Responsabilidad

VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, **aplicaciones electrónicas** o cualquier otra tecnología que implique el tratamiento de datos personales, **cumplan por defecto** con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

El Responsable deberá **revisar las políticas y procedimientos** de control a que se refiere la fracción V del presente artículo, al menos cada dos años y actualizarlas cuando el tratamiento de datos personales sufra modificaciones sustanciales.

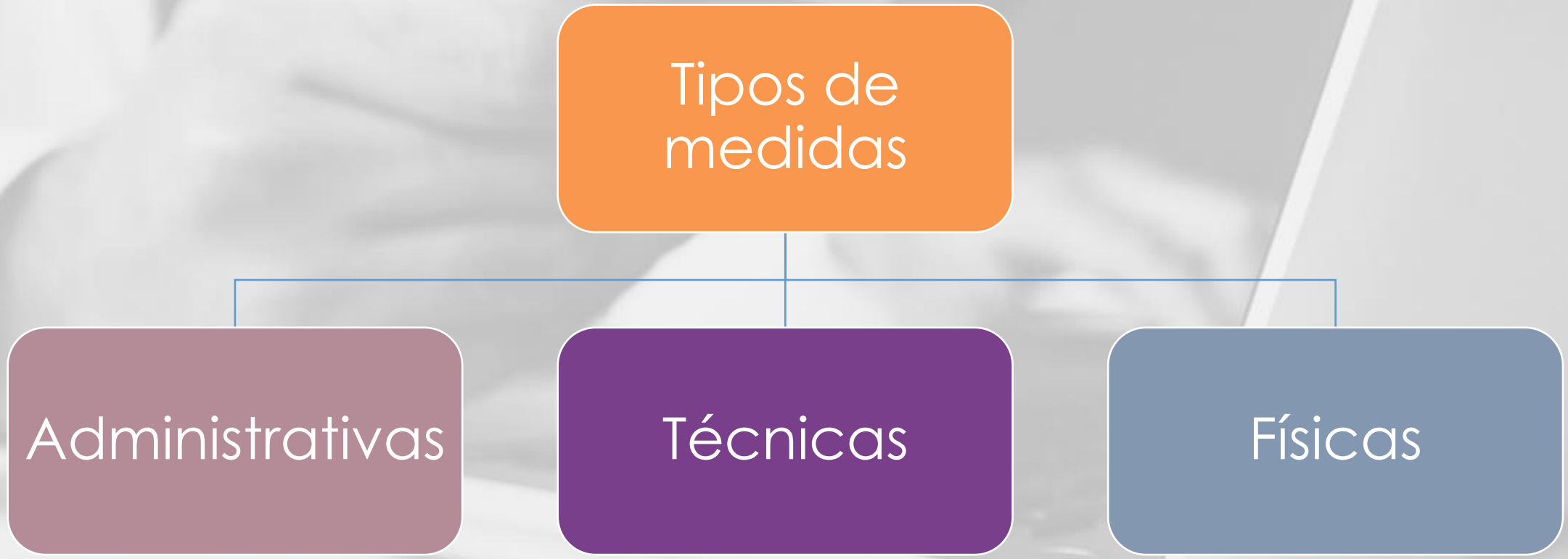
Repaso …

	Principios	Concepto y Características Funcionales
1	Principio de **Licitud**.	Los datos deben recabarse y tratarse de manera lícita, conforme a las leyes en la materia. No obtenerlos de forma engañosa y fraudulenta.
2	Principio de **Consentimiento**.	Todo tratamiento estará sujeto al consentimiento de su titular, salvo excepciones señalas en la Ley. **Expreso**: cuando la voluntad se manifieste verbalmente, por escrito, medios electrónicos o signos inequívocos. **Tácito:** Cuando al haber puesto el Aviso de Privacidad, no manifieste su oposición. *Tratándose de Datos Sensibles: el consentimiento deberá ser expreso y por escrito.
3	Principio de la **Información**.	El responsable tendrá la obligación de informar a los titulares de los datos personales la información que se recaba de ellos y con qué fines, a través de un aviso de privacidad. Conocer quién tiene nuestros datos, para qué los tienen y qué van a hacer con ellos. Si harán transferencias o no a terceros.
4	Principio de la **Calidad**.	Los Datos Personales contenidos en las bases de datos **deberán ser pertinentes, exactos, completos, correctos y actualizados** para los fines para los cuales fueron recabados. *Cancelables cuando las finalidades por las que se recabaron ya han fenecido.
5	Principio de la **Finalidad**.	Limitarse a las finalidades establecidas en el aviso de privacidad. Abstenerse de llevar a cabo tratamientos no compatibles con las finalidades para las que se recabaron. **Deben ser: Legitimas, concretas, específicas.**
6	Principio de **Lealtad y Legalidad**.	El responsable velará por el cumplimiento de los principios de protección establecidos en las leyes en la materia, adoptando medidas necesarias para su aplicación. Se consideran desleales aquellos tratamientos que den pie a una discriminación.
7	Principio de la **Proporcionalidad**.	El tratamiento de los datos personales será el que resulte necesario, adecuado y relevante para las finalidades establecidas en el aviso. **No excesivos necesarios para la finalidad perseguida, correctos, actualizados, etc.**
8	Principio de la **Responsabilidad**	Todo responsable deberá establecer medidas de seguridad Administrativas, Técnicas y Físicas, que permitan proteger los datos, contra daño, alteración o el uso o acceso no autorizado. **Dotarse** de mecanismos para evidenciar el cumplimiento de protección de los datos tanto a los titulares como a las autoridades que supervisen dicho cumplimento.

DEBERES

Artículo 32. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el Responsable **deberá 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**.

Medidas de Seguridad



Medidas de Seguridad

Artículo 33. Las medidas de seguridad adoptadas por el responsable deberán considerar:

I. El riesgo inherente a los datos personales tratados;

II. La sensibilidad de los datos personales tratados;

III. El desarrollo tecnológico;

IV. Las posibles consecuencias de una vulneración para los titulares;

V. Las transferencias de datos personales que se realicen;

VI. El número de titulares;

VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y

VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Medidas de Seguridad

Artículo 34. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, 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 de datos personales;

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;

Medidas de Seguridad

Análisis de Brecha

Medidas de seguridad existentes VS medidas de seguridad

Código	Pregunta o Control	¿Existente?		
		Sí	No	Observaciones
A.	Medidas de seguridad basadas en la cultura del personal			
A.1.	*¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?*			
A.1.1.	Política de escritorio limpio			
A.1.2.	Hábitos de cierre y resguardo			
A.1.3.	Impresoras, escáneres, copiadoras y buzones limpios			
A.1.4.	Gestión de bitácoras, usuarios y acceso			
A.2.	*¿Tienes mecanismos para eliminar de manera segura la información?*			
A.2.1.	Destrucción segura de documentos			
A.2.2.	Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico			
A.2.3.	Fijar periodos de retención y destrucción de información			
A.2.4.	Tomar precauciones con los procedimientos de re-utilización			
A.3.	*¿Has establecido y documentado los compromisos respecto a la protección de datos?*			

Artículo 34.

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.

Documento de Seguridad

I. El inventario de datos personales y de los sistemas de tratamiento;

II. Las funciones y obligaciones de las personas que traten datos personales;

III. El análisis de riesgos;

IV. El análisis de brecha;

V. El plan de trabajo;

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

VII. El programa general de capacitación.

Deber de Confidencialidad

I. Los controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales;

II. Las secciones para restaurar la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;

III.Las medidas correctivas en caso de identificar una vulneración o incidente en los tratamientos de los datos personales;

IV. El proceso para evaluar periódicamente las políticas, procedimientos y planes de seguridad establecidos, a efecto de mantener su eficacia;

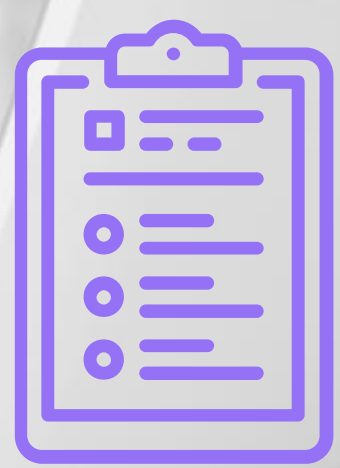
V. Los controles para garantizar que únicamente el personal autorizado podrá tener acceso a los datos personales para las finalidades concretas, lícitas, explicitas y legítimas que originaron su tratamiento, y

VI. Las medidas preventivas para proteger los datos personales contra su destrucción, accidental o ilícita su pérdida o alteración y el almacenamiento, tratamiento, acceso o transferencias no autorizadas o acciones que contravengan las disposiciones de la presente Ley y demás que resulten aplicables.

Bitácoras de Vulnerabilidades

El responsable deberá llevar una bitácora de las vulnerabilidades a la seguridad ocurridas en las que se describa ésta, la fecha en la que ocurrió, el motivo de la misma y las acciones correctivas implementadas de forma inmediata y definitiva.

Ante la vulneración de datos personales, el responsable deberá informar al titular:



I. La naturaleza del incidente
II. Los datos personales comprometidos
III. Las recomendaciones al titular acerca de las medidas que este pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata, y
V. Los medios donde pueden obtener más información al respecto.

Fundamento: Artículo 41,42,43 de la LPDPPSOQROO.

Sanciones

Artículo 171.

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.

II. Incumplir los plazos de atención para responder las solicitudes para el ejercicio de los derechos ARCO.

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales.

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los **principios y deberes.**

V. No contar con el **aviso de privacidad**, omitir en el mismo alguno de los elementos a que se refieren los artículos 26, 27 y 28 de la presente Ley.

VI. Clasificar como confidencial, con dolo o negligencia datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables.

VII. Incumplir el deber de confidencialidad establecido en el artículo 44 de la presente Ley.

Sanciones

VIII. **No establecer las medidas de seguridad en los términos que establecen los artículos 32,33 y 34 de la presente Ley**.

IX. **Presentar vulneraciones** a los datos personales por la falta de **medidas de seguridad**.

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley.

XI. Obstruir los actos de verificación de la autoridad.

XII. Crear bases de datos personales en contravención a lo dispuesto por esta Ley.

XIII. No acatar las resoluciones emitidas por el Instituto.

XIV Aplicar medidas compensatorias en contravención. de los criterios que tales fines establezca el Sistema Nacional.

XV. Declarar dolosamente la inexistencia de datos personales cuando estos existan total o parcialmente en los archivos del responsable.

XVI. No atender las medidas cautelares establecidas por el Instituto.

Sanciones

XVII. Tratar los datos personales de manera que afecte o impida el ejercicio de los derechos fundamentales.

XVIII. No presentar ante el Instituto **la evaluación de impacto** a la protección de datos personales en aquellos casos que resulte obligatoria.

XIX. Realizar actos para intimidar o inhibir a los titulares en el ejercicio de los derechos ARCO.

XX. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 62 fracc. VII de la LTPAIQROO.

XXI. No cumplir con las disposiciones previstas en los artículos de la presente Ley.

GRACIAS

Dirección de Protección de Datos Personales

M.C.C. Hilda Ariadne Cabrera García

- hcabrera@idaipqroo.org.mx

Asesorías Personalizadas vía Zoom