Protección de Datos Personales en el sector de Turismo

Dra. Isabel Davara F. de Marcos

7 de Junio de 2022

QUINTANA ROO
SECRETARÍA DE TURISMO
Asociación de Internet MX.
idaip Quintana Roo
Por tu derecho a saber

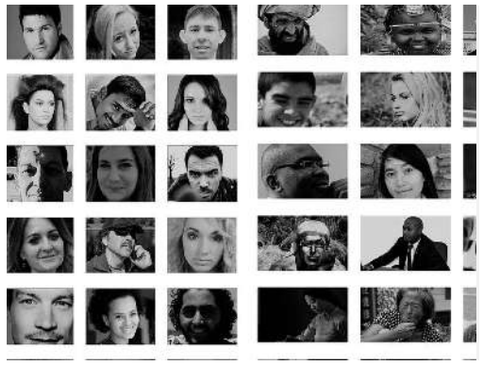
CONTENIDO

1. Conceptos fundamentales

¿QUÉ ES LA PROTECCIÓN DE DATOS PERSONALES?

Un derecho fundamental y un derecho del titular de los datos reconocido en el artículo 16 de la Constitución Mexicana

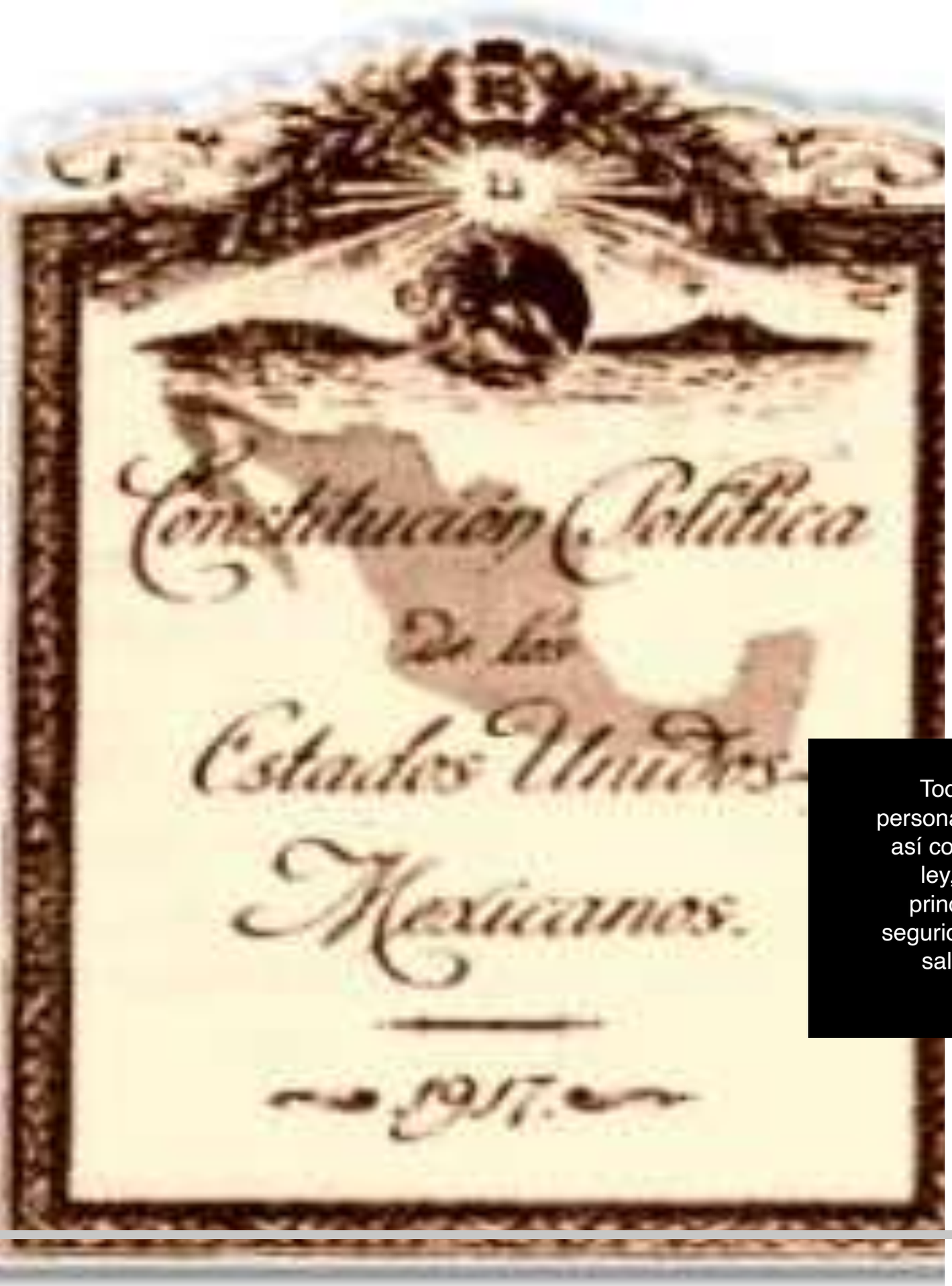
Una obligación del responsable del tratamiento y un compromiso con el titular de los datos



- **Objeto**: datos personales referidos al titular de los datos (persona física)
- **Finalidad**: garantizar su privacidad y el derecho a la autodeterminación informativa de las personas

Derecho a la **autodeterminación informativa**:

- Conocer y decidir quién, cómo y de qué manera recaba y utiliza sus datos personales
- Libertad para elegir qué desea comunicar, cuándo y a quién, manteniendo el control
- Derecho autónomo y fundamental, directamente conectado con la dignidad y la libertad de la persona



RECONOCIMIENTO CONSTITUCIONAL

En el 2007 se publicó la reforma al artículo 6 de la Constitución y, el 1 de junio de 2009 se publicó una reforma al artículo 16 de la Constitución que incorpora un párrafo específicamente destinado a la protección de datos personales. Finalmente, el 30 de abril de 2009 se reformó el 73 de la Constitución atribuyendo al Congreso Federal el poder para legislar en materia de datos personales en posesión de particulares.

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.

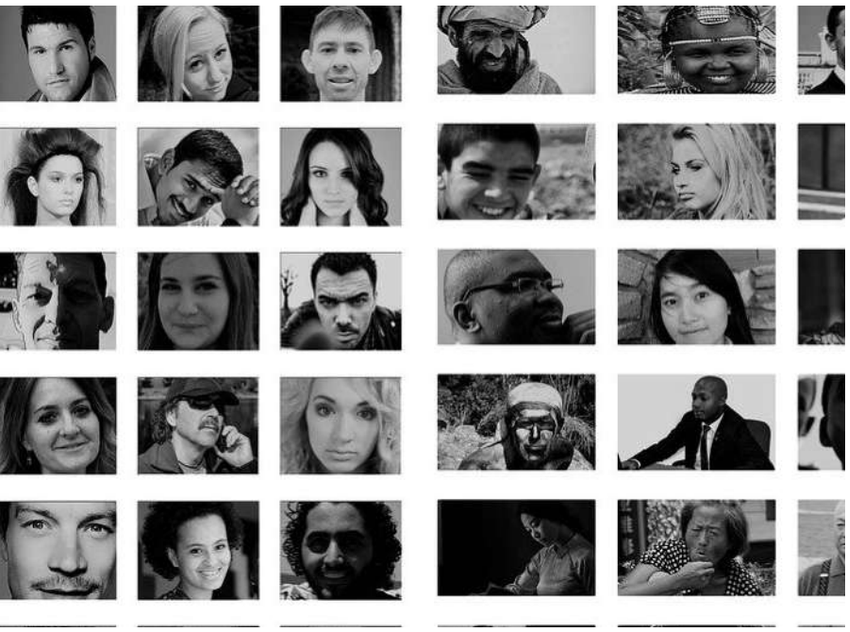
NORMATIVIDAD

SECTOR PRIVADO

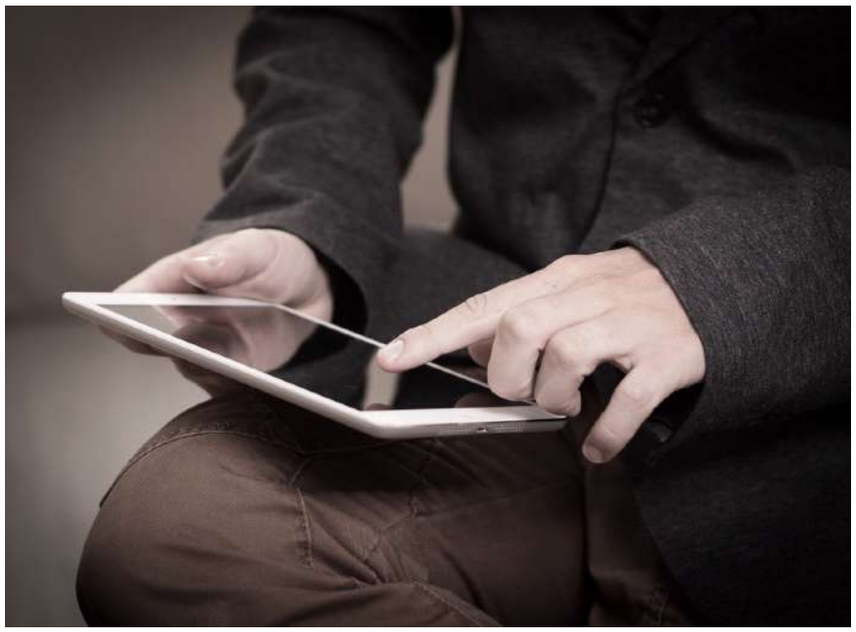
- El artículo 6, párrafo segundo, fracción II, el artículo 16, párrafo segundo, y el artículo 73 inciso XXIX-O de la Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares (“LFPDPPP”).
- Reglamento de la LFPDPPP.
- Lineamientos para el Aviso de Privacidad.
- Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
- Criterios Generales para la Instrumentación de Medidas Compensatorias sin la Autorización Expresa del Instituto Federal de Acceso a la Información y Protección
- Parámetros para el correcto desarrollo de los esquemas de autorregulación
- Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante.
- Recomendaciones en materia de Seguridad de Datos Personales
- Lineamientos para difusión de avisos de privacidad en hiperenlaces o hipervínculos.
- Las Reglas de uso del logotipo del Registro de Esquemas de Autorregulación Vinculante REA INAI y condiciones para su autorización.

SECTOR PÚBLICO

- El artículo 6, párrafo segundo, fracción II, el artículo 16, párrafo segundo, y el artículo 73 inciso XXIX-O de la Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley General de Transparencia y Acceso a la Información Pública.
- Lineamientos para la elaboración, ejecución y evaluación del Programa Nacional de Protección de Datos Personales (Consejo Nacional del SNT)
- Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
- Lineamientos Generales para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ejerza la facultad de atracción
- Lineamientos para la recepción, sustanciación y resolución de los recursos de revisión en materia de datos personales, interpuestos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
- Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales.
- Criterios generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público
- Acuerdo mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales.
- Lineamientos que Establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales.

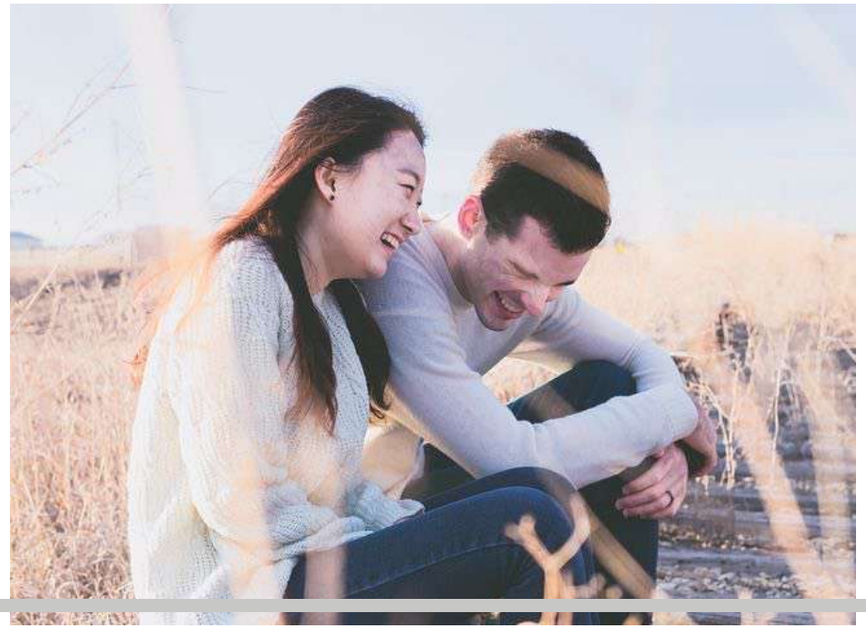


La reputación empresarial no es un activo restaurable, por lo que es muy importante adoptar las acciones necesarias para protegerla y evitar que pueda verse afectada.



El incumplimiento a la normatividad puede afectar seriamente la imagen corporativa y la confianza de los clientes, usuarios e inversionistas en la empresa.

Incumplir con las obligaciones previstas en la LFPDPPP puede dar lugar a la imposición de MULTAS de 100 a 320 mil veces el equivalente al valor diario de la UMA.



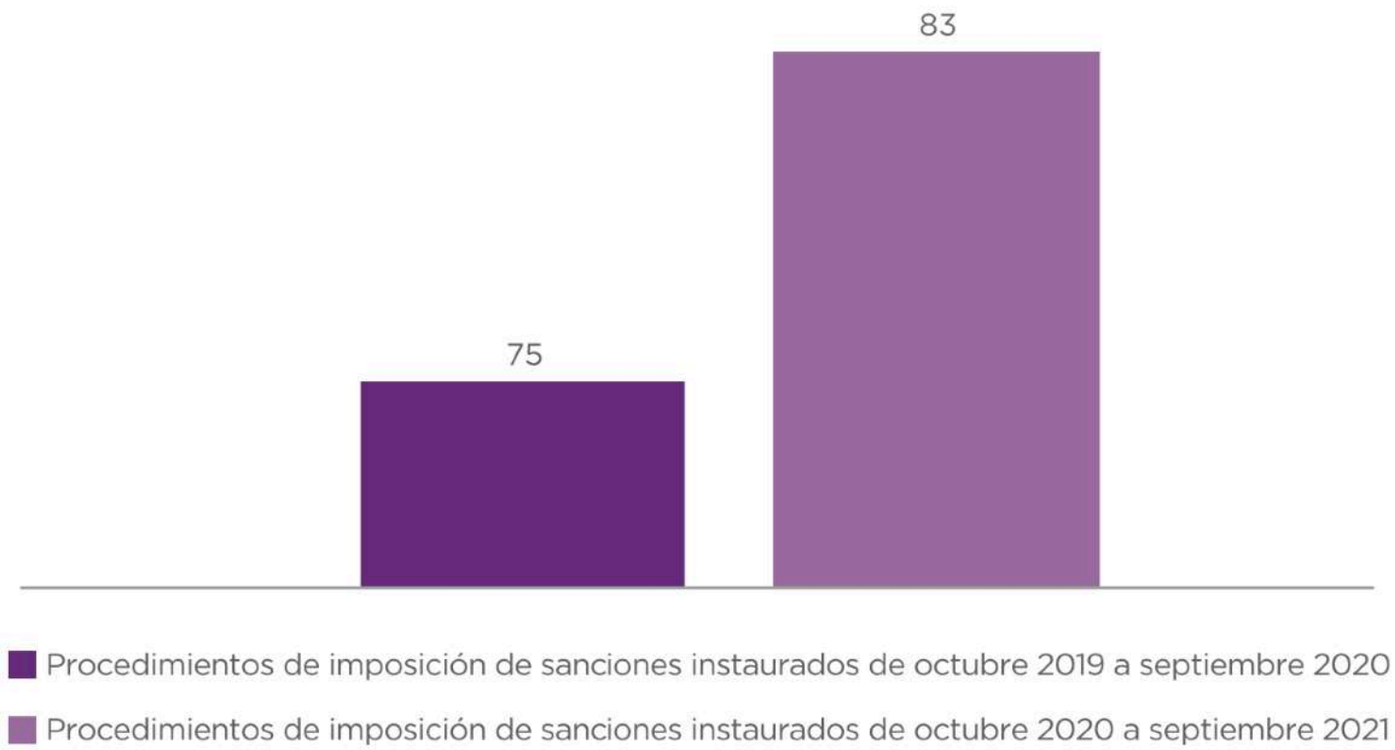
INFORME DE LABORES DEL INAI, 2021

En materia de protección de datos personales en posesión de los particulares, el INAI recibió 307 solicitudes de protección de derechos, con el fin de revisar la legalidad de la actuación de los responsables del tratamiento de los datos a una solicitud de ejercicio de derechos ARCO. Cifra que implica un incremento del 35.2% comparado con el periodo anterior.

En materia de verificación, en el sector privado, el INAI inició 104 procedimientos de verificación, de los cuales concluyó 49 y quedaron 55 en trámite.

También se instauraron 83 procedimientos de imposición de sanciones

GRÁFICA 7.5 Procedimientos instaurados

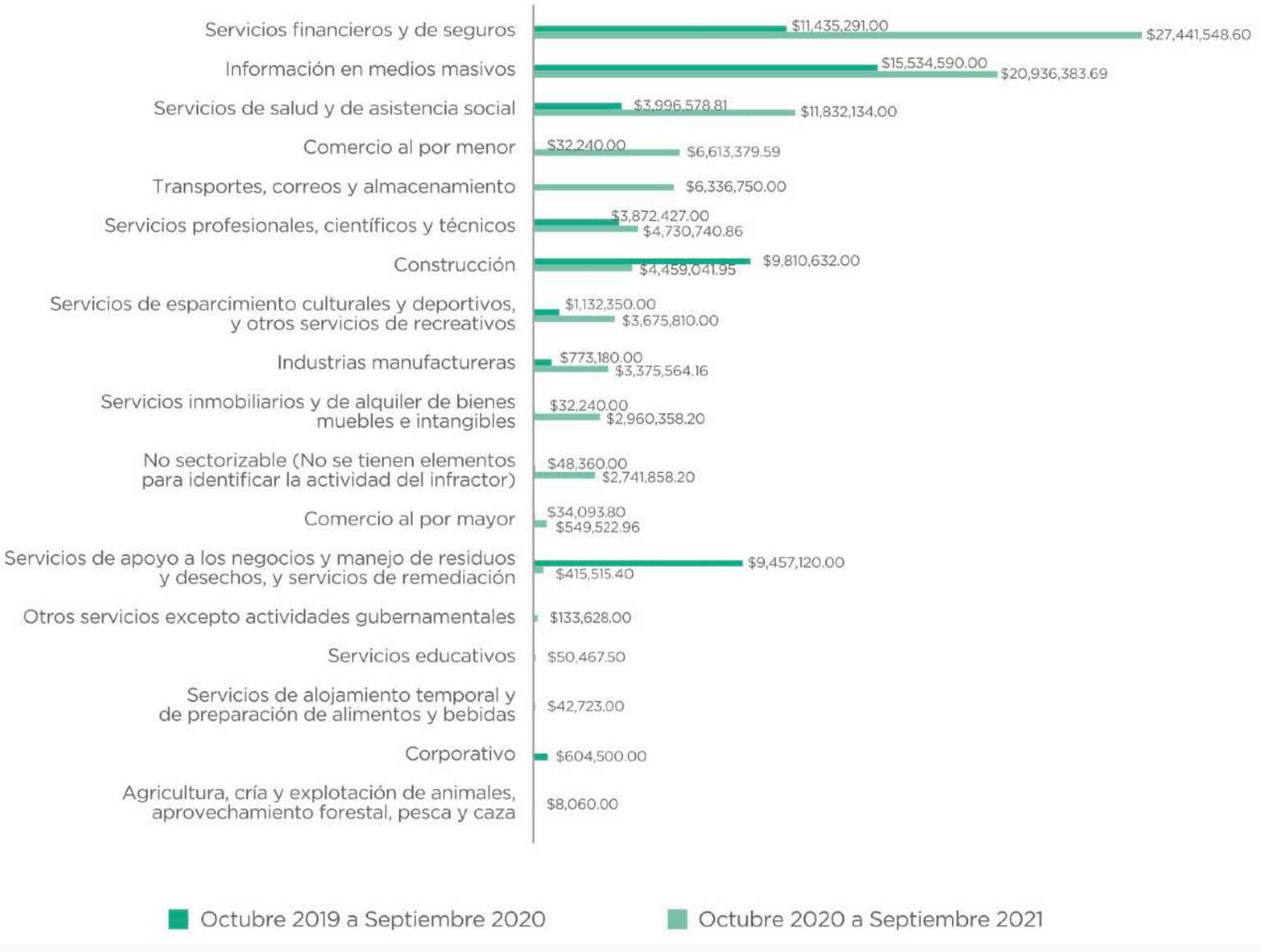


FUENTE: Secretaría de Protección de Datos Personales, 2021. Dirección de Protección de Derechos y Sanción.

INFORME DE LABORES DEL INAI, 2021

El INAI impuso multas por **96 millones 295 mil pesos.** Cifra que es 69.6% mayor a la reportada en el periodo anterior. Los tres sectores donde más se concentraron estas sanciones fueron los de "Servicios financieros y de seguros", con 28.5%; "Información en medios masivos", con 21.7%; y "Servicios de salud y de asistencia social", con el 12.3%.

GRÁFICA 7.6 Importe de multas por sector productivo



MULTA MÁS ALTA

Actualmente la multa más alta que ha impuesto el INAI asciende a **32 millones de pesos** y fue impuesta a una entidad bancaria que dio tratamiento a datos sensibles de terceros sin consentimiento (cónyuge del titular), mismos que no se justificaban para la finalidad de autorización de un crédito automotriz.

DATO PERSONAL- DEFINICIÓN

En la normativa mexicana sólo tiene sentido la protección de datos sobre los datos de las personas físicas.

Persona identificable es toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador.

Acerca de la información sobre personas morales hablaríamos de otras protecciones jurídicas, pero no de aplicación de la normativa en protección de datos personales.

> ***"cualquier información concerniente a una persona física identificada o identificable" (art. 3.V. LFPDPPP)***

La información de personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o de prestación de servicios, tampoco le será aplicable la normativa.

Tampoco le será aplicable la normativa a la información referente a personas físicas en su calidad de comerciantes y profesionistas.

(art. 3 RLFPDPP)

DATO PERSONAL SENSIBLE - DEFINICIÓN

El consentimiento para el tratamiento de este tipo de datos debe ser expreso y por escrito, y con firma autógrafa o medio de autenticación equivalente.

Las medidas de seguridad son mucho más elevadas.

Las sanciones, en caso de infracciones en el tratamiento de estos datos alcanzan su mayor rango.

En todo caso, la LFPDPPP prohíbe la creación de bases de datos con información que directa o indirectamente contenga datos personales sensibles, sin que se justifique la creación de dichas bases para finalidades legítimas y concretas

"Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual" (art. 3 .VI. LFPDPPP)

EJEMPLOS DE DATOS PERSONALES Y DATOS SENSIBLES

Datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas

Datos biométricos sobre características físicas

Huella digital, el rostro (reconocimiento facial), la retina, el iris, la geometría de la mano o de los dedos, la estructura de las venas de la mano, la forma de las orejas, la piel o textura de la superficie dérmica, el ADN, la composición química del olor corporal y el patrón vascular, pulsación cardíaca, entre otros.

Características del comportamiento y los rasgos de la personalidad

La firma autógrafa, la escritura, la voz, la forma de oprimir un teclado y la forma de caminar, entre otros.

Datos patrimoniales

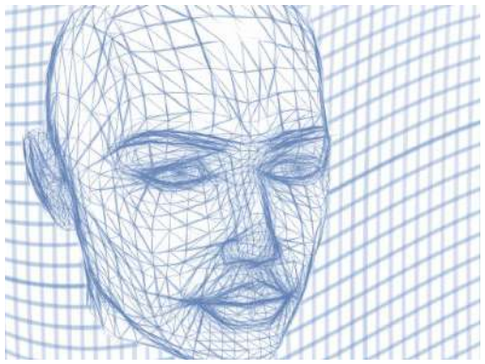
Información sobre la cuenta de ahorro individual del trabajador, cuenta de pensión y demás datos que revelen el patrimonio del trabajador.

BASES DE DATOS - DEFINICIÓN

Conjunto ordenado de datos:

¿en un documento?, ¿una tabla en una base de datos?,

¿varias bases de datos interrelacionadas en un sistema de información?



Otros aspectos a considerar: hosting, cloud computing, etc

Clases

- Jurídico: finalidad del tratamiento
- Lógico: estructura lógica y tratamiento informático

"El conjunto ordenado de datos personales referentes a una persona identificada o identificable"
(art. 3.II. LFPDPPP)

TRATAMIENTO - DEFINICIÓN

Obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio.

El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales

Por cualquier medio: “automatizado •o no”

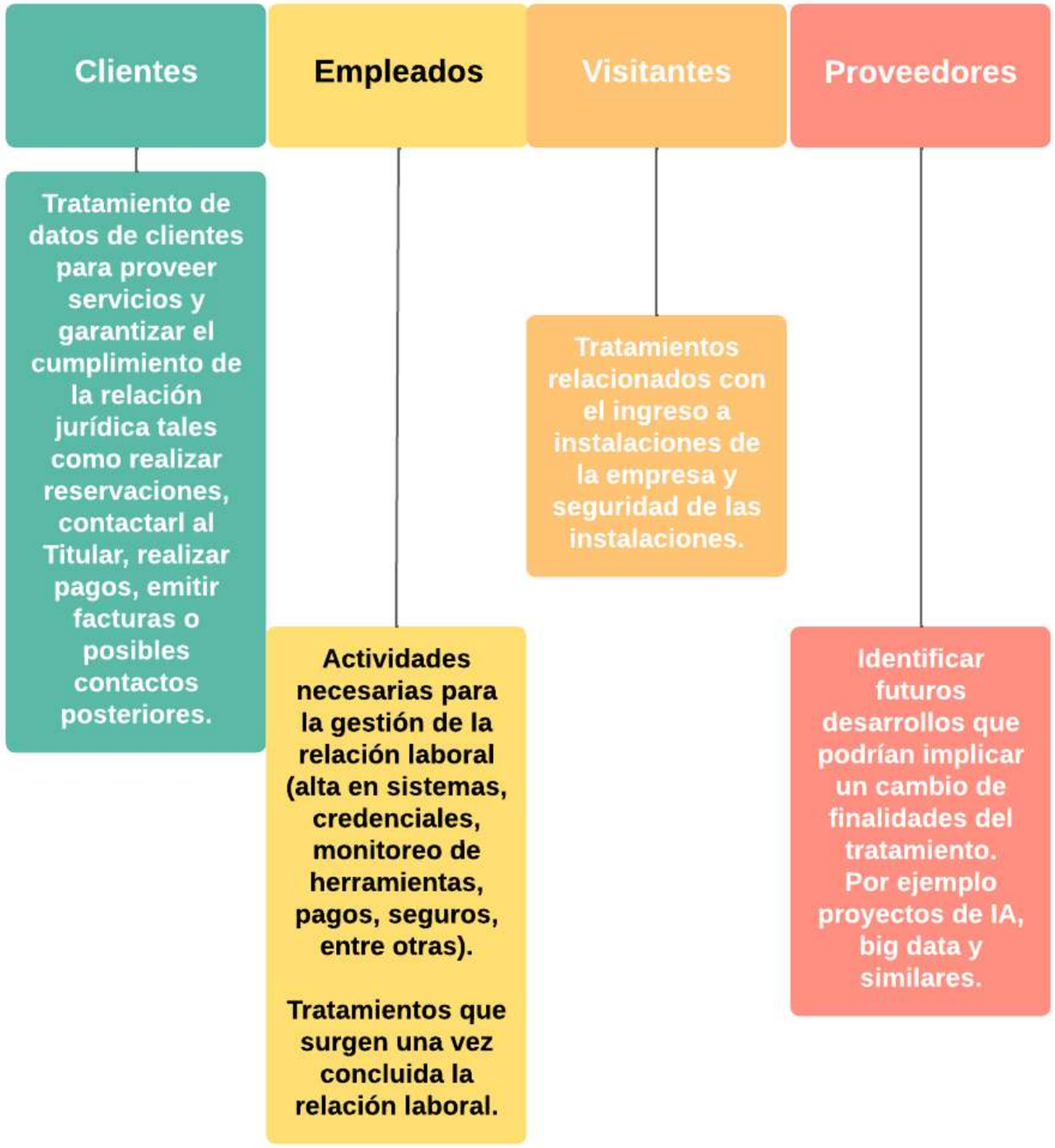
Temporal o definitivo: mero alojamiento de datos o realización de una operación necesaria

Fases:

1. obtener
2. usar
3. eliminar

“La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.”
(art. 3 .XVIII. LFPDPPP)

EJEMPLOS DE TRATAMIENTOS



INTELIGENCIA ARTIFICIAL

BIG DATA

COMPUTACIÓN DISTRIBUIDA

MACHINE LEARNING

IoT

DEEP LEARNING

Tecnologías emergentes: concepto

En términos generales, las tecnologías emergentes son herramientas que, dentro de 5 o 10 años, pueden provocar una gran revolución empresarial. Es decir, son las innovaciones que cambiarán la forma en que operamos en el mercado. Sin embargo, todavía no están bien establecidas o no se han desarrollado lo suficiente.

DISOCIACIÓN - DEFINICIÓN

La disociación es un tratamiento de datos

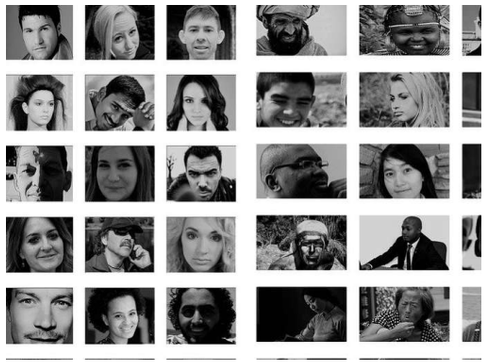
Es más que un mero enmascaramiento de los datos

El dato disociado no puede identificar, en modo alguno, a quien era su titular

Si los datos han sido disociados, deja de aplicarse la LFPDPPP

> ***"El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo"***
> ***(art. 3.VIII. LFPDPPP)***

TITULAR DE LOS DATOS - DEFINICIÓN



Cualquier persona: nacional, extranjero, residente, ilegal, etc

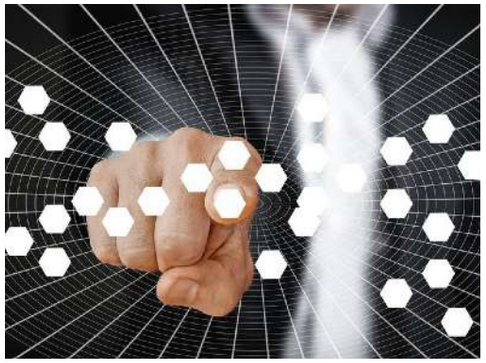
Supuestos de incapacidad legal

Exclusión de personas morales (públicas o privadas) y empresarios individuales

"La persona física a quien corresponden los datos personales"
(art. 3.XVII LFPDPPP)

INFORMACIÓN A LA QUE NO LE APLICA LA LEY

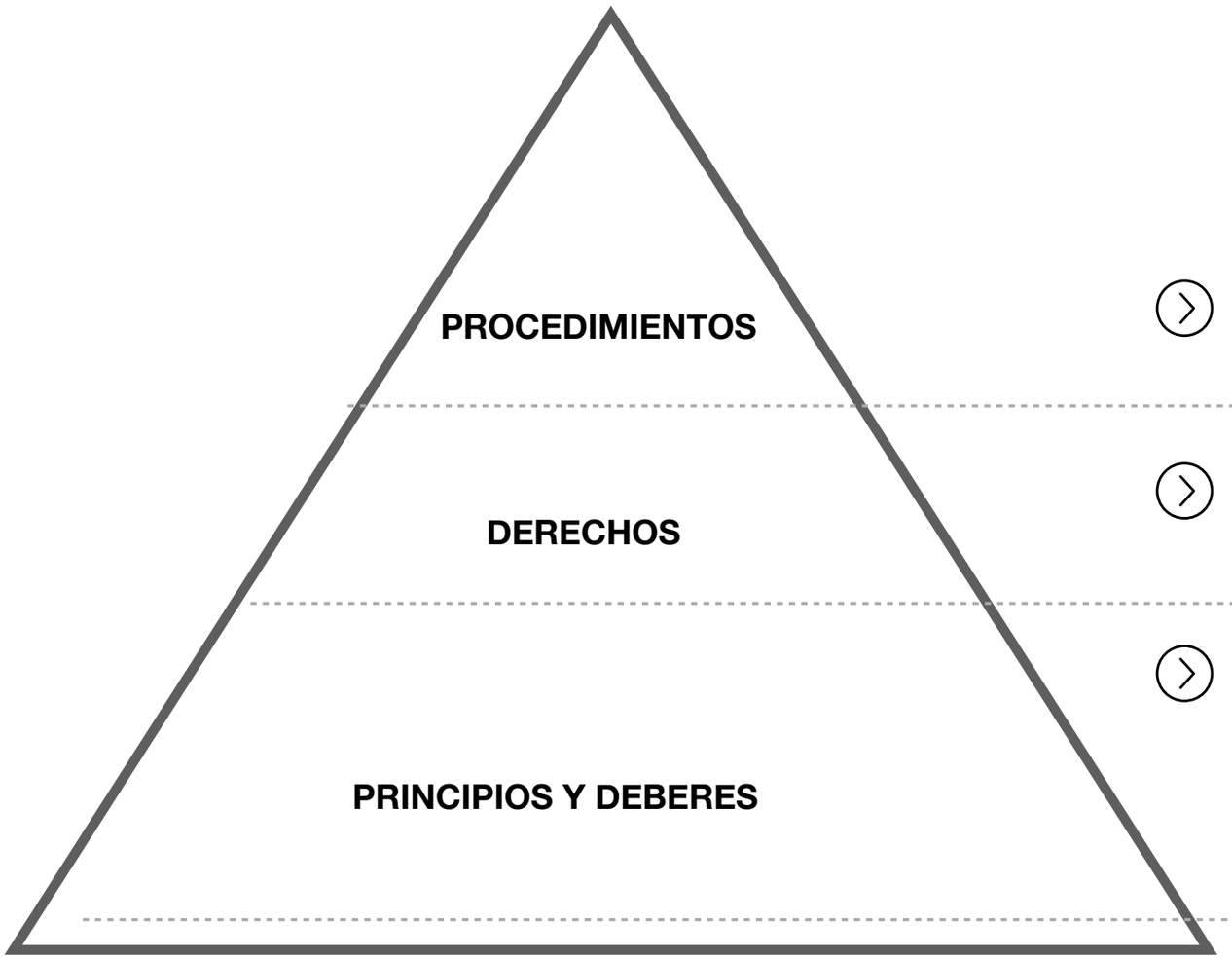
1. La relativa a **personas morales**



2. Aquélla que refiera a personas físicas en su calidad de **comerciantes y profesionistas.**

3. La de personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o prestación de servicios, consistente únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como algunos de los siguientes datos laborales: domicilio físico, dirección electrónica, teléfono y número de fax; siempre que esta información sea tratada para fines de representación del empleador o contratista.

EJES RECTORES DE LA NORMATIVIDAD



PROCEDIMIENTOS

INAI: PPD, PI, PV y PISAN

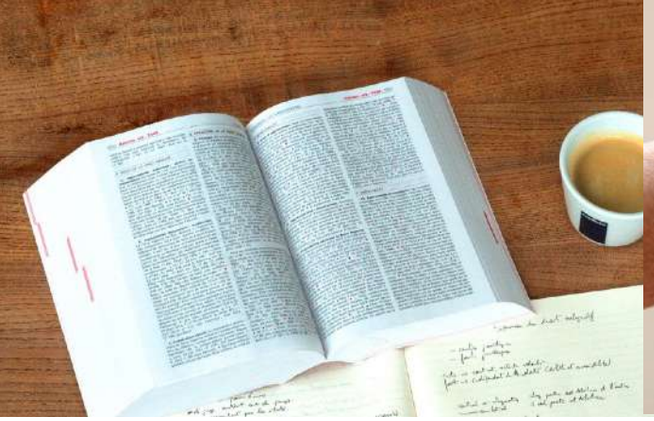
DERECHOS DE LOS TITULARES DE LOS DATOS

(Acceso, Rectificación, Cancelación y Oposición)

PRINCIPIOS Y DEBERES

Principios: licitud, consentimiento, finalidad, proporcionalidad, calidad, información y responsabilidad.

Deberes: seguridad y confidencialidad.



LICITUD

El tratamiento debe ser conforme con la normatividad aplicable

LEALTAD

El tratamiento debe privilegiar la protección de los intereses del titular y su expectativa razonable de privacidad

PROPORCIONALIDAD

Los datos deben tratarse para las finalidades necesarias, adecuadas y relevantes informadas en el aviso de privacidad

CALIDAD

Los datos personales tratados deben ser pertinentes, correctos y actualizados

PRINCIPIOS

FINALIDAD

Tratar los datos para las finalidades informadas en el aviso de privacidad

INFORMACIÓN

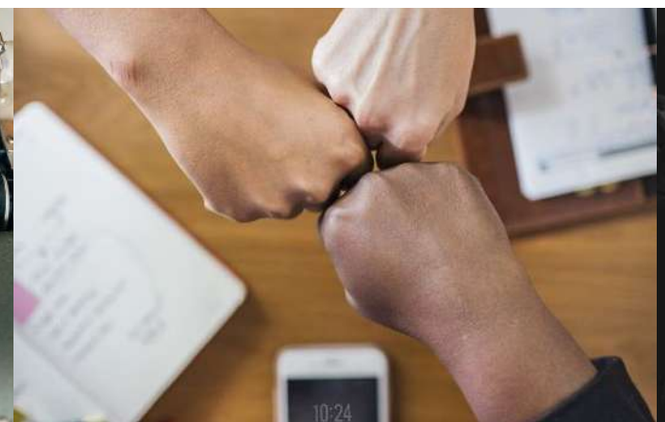
El responsable tiene la obligación de informar a los titulares las condiciones a las que se sujetará el tratamiento, a través del aviso de privacidad

CONSENTIMIENTO

Todo tratamiento de datos personales debe contar con el consentimiento de su titular, salvo las excepciones previstas por la Ley

RESPONSABILIDAD

Cumplir con los principios y deberes establecidos y vigilar que los encargados también los cumplan.



PRINCIPIO DE LICITUD

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

Cámara de Diputados del H. Congreso de la Unión
Secretaría General
Secretaría de Servicios Parlamentarios

Nueva Ley DOF 05-07-2010

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

TEXTO VIGENTE

Nueva Ley publicada en el Diario Oficial de la Federación el 5 de julio de 2010

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Presidencia de la República.

FELIPE DE JESÚS CALDERÓN HINOJOSA, Presidente de los Estados Unidos Mexicanos, a sus habitantes sabed:

Que el Honorable Congreso de la Unión, se ha servido dirigirme el siguiente

DECRETO

"EL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, DECRETA:

SE EXPIDE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES Y SE REFORMAN LOS ARTÍCULOS 3, FRACCIONES II Y VII, Y 33, ASÍ COMO LA DENOMINACIÓN DEL CAPÍTULO II, DEL TÍTULO SEGUNDO, DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL.

ARTÍCULO PRIMERO. Se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS

Obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo previsto en la normatividad

Legislación mexicana

Derecho internacional

"Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable. "
(art. 7.I LFPDPPP)

PRINCIPIO DE LEALTAD

Obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

No se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales.

Existe una actuación fraudulenta o engañosa:

1. Exista dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento
2. Se vulnere la expectativa de privacidad
3. Las finalidades no son las informadas en el aviso de privacidad

"La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.

En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley. "
(art. 7 LFPDPPP)

PRINCIPIO DE LEALTAD

La propaganda e información dirigida al público inversionista sobre las características y desempeño de los fondos de inversión, los Activos Objeto de Inversión o sobre los servicios u operaciones que presten las sociedades o entidades señaladas en el artículo 109 anterior, deberá circunscribirse a la naturaleza y características propias de los Valores de que se trate, o bien a la organización, actividades u operaciones que pueden prestar las sociedades o entidades conforme a las disposiciones aplicables.

La propaganda e información a que se refiere este Título, deberá expresarse en forma clara y veraz, procurando la mayor objetividad posible, de tal forma que **no induzca a confusión o errores de interpretación** que redunden en perjuicio o engaño del público inversionista, ni se resalten las cualidades de un cierto Valor o entidad del mercado de valores en demérito de otra.

La propaganda e información deberá difundirse en idioma español, pudiendo utilizarse cualquier otro idioma siempre y cuando enseguida se haga la traducción correspondiente. Asimismo, deberán evitarse modismos, giros vulgares, extranjerismos o expresiones que signifiquen un deterioro del idioma español.

(arts. 110, 111 y 112 de las Disposiciones de carácter general Disposiciones de carácter general aplicables a los fondos de inversión y a las personas que les prestan servicios.

PRINCIPIO DE FINALIDAD

Los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad, en términos del art. 12 de la LFPDPPP.

Las finalidades deberán ser determinadas, lo cual se logra cuando con claridad, sin lugar a confusión, y de manera objetiva se especifica para qué objeto serán tratados los datos personales.

No se podrán llevar a cabo tratamientos para finalidades distintas que no resulten compatibles o análogas con aquellas que hayan sido previstas en el aviso de privacidad.

El titular podrá negar o revocar su consentimiento, así como oponerse al tratamiento de sus datos personales para las finalidades secundarias

"El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular. " (art. 12 LFPDPPP)

PRINCIPIO DE PROPORCIONALIDAD

PROPORCIONALIDAD

Sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido.

MINIMIZACIÓN

El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.

"En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley. " (art. 7 LFPDPPP)

"El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar." (art. 46 RLFPDPPP)

PRINCIPIO DE CALIDAD

Se cumple cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.

Se presume que se cumple con la calidad cuando los datos son proporcionados directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga.

Cuando los datos no fueron obtenidos directamente del titular, el responsable deberá adoptar medidas razonables para que estos respondan al principio de calidad, de acuerdo con el tipo de datos personales y las condiciones del tratamiento.

El responsable deberá adoptar los mecanismos que considere necesarios para procurar que los datos personales que trate sean exactos, completos, pertinentes, correctos y actualizados , a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

"El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados. (…) "
(art. 11 LFPDPPP, entre otros)

PRINCIPIO DE CONSENTIMIENTO

El consentimiento del titular debe ser:

1. Libre
2. Inequívoco
3. Específico
4. Informado

La carga de la prueba recae en el responsable.

Consentimiento tácito: Cuando habiendo puesto a disposición el aviso de privacidad y hasta en tanto el titular no ejerza sus derechos de oposición o cancelación o no revoque su consentimiento.

En el consentimiento tácito debemos tomar en cuenta la forma mediante la cual el responsable pretenda recabar los datos personales:

1. Cuando se recaban directa o personalmente de su titular.
2. Cuando los datos personales se obtienen de manera indirecta del titular.
3. Utilice comunicación electrónica.

El responsable deberá obtener el consentimiento expreso del titular cuando:

1. lo exija la Ley,
2. se trate de datos financieros o patrimoniales,
3. se trate de datos sensibles,
4. lo solicite el responsable para acreditar el mismo y
5. lo acuerden el titular y responsable

"Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley" (art. 8 LFPDPPP)

EXCEPCIONES AL CONSENTIMIENTO

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

Nueva Ley DOF 05-07-2010

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

TEXTO VIGENTE

Nueva Ley publicada en el Diario Oficial de la Federación el 5 de julio de 2010

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos - Presidencia de la República.

FELIPE DE JESÚS CALDERÓN HINOJOSA, Presidente de los Estados Unidos Mexicanos, a sus habitantes sabed:

Que el Honorable Congreso de la Unión, se ha servido dirigirme el siguiente

DECRETO

"EL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, DECRETA:

SE EXPIDE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES Y SE REFORMAN LOS ARTÍCULOS 3, FRACCIONES II Y VII, Y 33, ASÍ COMO LA DENOMINACIÓN DEL CAPÍTULO II, DEL TÍTULO SEGUNDO, DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL.

ARTÍCULO PRIMERO. Se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Previsto en una Ley

Los datos figuren en fuentes de acceso público

Los datos personales se sometan a un procedimiento previo de disociación

Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica

Exista una situación de emergencia

Sean indispensables para la atención médica, la prevención

Se dicte resolución de autoridad competente

PRINCIPIO DE INFORMACIÓN

FINALIDAD

Dar a conocer al titular, de manera efectiva, la existencia del tratamiento de su información personal y sus características esenciales

¿CÓMO?

El principio de información se materializa físicamente a través de la **puesta a disposición del aviso de privacidad al titular.**

El aviso de privacidad permite al titular decidir de manera libre e informada sobre el tratamiento de sus datos personales.

¿PARA QUÉ?

Para que el titular pueda ejercer su derecho a la autodeterminación informativa y protección de datos personales ante el responsable.

"El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad." (art. 15 LFPDPPP)

PRINCIPIO DE RESPONSABILIDAD

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

Nueva Ley DOF 05-07-2010

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

TEXTO VIGENTE

Nueva Ley publicada en el Diario Oficial de la Federación el 5 de julio de 2010

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos - Presidencia de la República.

FELIPE DE JESÚS CALDERÓN HINOJOSA, Presidente de los Estados Unidos Mexicanos, a sus habitantes sabed:

Que el Honorable Congreso de la Unión, se ha servido dirigirme el siguiente

DECRETO

"EL CONGRESO GENERAL DE LOS ESTADOS UNIDOS MEXICANOS, DECRETA:

SE EXPIDE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES Y SE REFORMAN LOS ARTÍCULOS 3, FRACCIONES II Y VII, Y 33, ASÍ COMO LA DENOMINACIÓN DEL CAPÍTULO II, DEL TÍTULO SEGUNDO, DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL.

ARTÍCULO PRIMERO. Se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

Velar por el cumplimiento de los principios

Asegurarse de que el tratamiento por terceros (nacional e internacionalmente), cumple la normativa

Rendir cuentas al titular

Cuidar porque lo asegurado en el Aviso de Privacidad se respete

La empresa es responsable de velar por el cumplimiento de la normatividad aplicable, incluso en aquellos datos en que el tratamiento sea realizado por terceros.

"El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica." (art. 14 LFPDPPP)

SEGURIDAD

El responsable del tratamiento y todo aquél que intervenga de alguna manera en el mismo está obligado a establecer medidas de seguridad físicas, técnicas y administrativas

DEBERES

CONFIDENCIALIDAD

El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos

Existe un deber de secreto específico en protección de datos de no divulgar los datos a los que tienen acceso.

LOS DERECHOS ARCO

Acceso

Derecho que tiene del titular de los datos a obte
responsable sus datos personales, así como info
relativa a las condiciones y generalidades del tra

Rectificación

Derecho que tiene el titular de rectificar sus dat
estos sean inexactos o incompletos.

Cancelación

Implica el cese en el tratamiento por parte del R
partir de un bloqueo de los mismos y su posteric

Oposición

Derecho que tiene el titular a oponerse al tratar
datos personales o exigir que se cese en el misr
exista causa legítima y su situación específica a
cuando requiera manifestar su oposición a fin d
lleve a cabo el tratamiento de sus datos para fir

1. Los derechos ARCO sólo pueden ejercerse por el titular o su representante legal debidamente acreditado.

2. Para ello, el titular deberá seguir el procedimiento seguido en el aviso de privacidad.

3. El Departamento de Datos Personales es la única entidad que puede dar trámite a este tipo de peticiones.

4. En la normatividad del sector público existe además el derecho de “portabilidad”

FASES EN LAS QUE PUEDE OCURRIR EL TRATAMIENTO DE DATOS PERSONALES






1. Evaluación preliminar (Prospectos)	2. Alta de cliente	3. Ciclo de vida del cliente	4. Cumplimiento obligaciones legales	5. Elaboración de perfiles	6. Cancelación

En cada una de las fases del tratamiento se deben cumplir diversas obligaciones:

- Revisar que el aviso de privacidad respectivo se encuentre debidamente actualizado e indique todos los tratamientos que se van a realizar.
- Poner a disposición de los titulares el aviso de privacidad previo al uso de los datos personales y generar prueba.
- Recabar el consentimiento del titular para el tratamiento de sus datos, a menos de que se actualice alguno de los supuestos previstos en el artículo 37 de la LFPDPPP.
- Tratar los datos para los fines autorizados por su titular.
- Revisar que los datos sean correctos y actualizados.
- Aplicar las medidas de seguridad administrativas, físicas y técnicas para garantizar la seguridad y confidencialidad de los datos personales.
- Cancelar los datos una vez concluida la finalidad de su tratamiento.

2. Comunicaciones de datos personales: remisiones y transferencias

SUJETOS QUE INTERVIENEN EN EL TRATAMIENTO

RESPONSABLE

quien DECIDE sobre el tratamiento de los datos personales. Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

ENCARGADO

el que realiza una prestación de servicios sobre los datos, un tratamiento a nombre y POR CUENTA del responsable.

TERCERO

la persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

TIPOS DE COMUNICACIONES

TRANSFERENCIA

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

Toda transferencia se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en la Ley.

REMISIÓN

Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

El encargado debe realizar las actividades de tratamiento sin modificar las finalidades o decidir sobre el alcance y contenido del tratamiento.

2.A. Remisiones

REMISIÓN DE DATOS PERSONALES

CONCEPTO

La comunicación de datos personales entre el responsable y el encargado

TIPOS

Pueden darse dentro o fuera del territorio nacional

¿CONSENTIMIENTO?

No requieren del consentimiento del titular

¿INFORMACIÓN?

No requieren ser informadas en el aviso de privacidad

EL ENCARGADO DEL TRATAMIENTO

Regularmente cuando se presta cualquier tipo de servicio en calidad de prestador de servicios, la empresa que presta el servicio de tratamiento de datos actúa como encargado del tratamiento.

Proveedor de servicios de cómputo en la nube

La figura del encargado es muy común, ya que el tratamiento de datos personales es imprescindible en cualquier actividad empresarial y, a su vez, hay multitud de tratamientos que requieren de la intervención de un tercero prestador de servicios.

Call centers
Actividades de contacto telefónico, por correo, chatbots o redes sociales.

Ser encargado del tratamiento implica no tener capacidad de decisión sobre el tratamiento. Es decir, el encargado trata los datos siguiendo el mandato dado por el responsable, que es quien decide sobre la finalidad, contenido y uso del tratamiento.

Terceros independientes que presten servicios como auditores, aplicación de exámenes, encuestas, entre otros.

OBLIGACIONES DEL ENCARGADO

1

No transferir los datos personales

2

Suprimir los datos personales una vez concluida la prestación de servicios

3

Guardar confidencialidad sobre los datos personales comunicados

4

Implementar las medidas de seguridad necesarias conforme a la normatividad aplicable

5

Tratar los datos conforme a las instrucciones del Responsable en el contrato de prestación de servicios y en su aviso de privacidad

2.B. Transferencias

TRANSFERENCIA

TRANSFERENCIA

1. Trata los datos para un fin propio y
2. Asume las mismas obligaciones que el responsable transferente

FORMALIZACIÓN

Deberá formalizarse mediante cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

CONDICIONES

Cuando la transferencia sea nacional, el receptor de los datos personales deberá tratar los datos personales, comprometiéndose a garantizar su confidencialidad y únicamente los utilizará para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.

EJEMPLO: TRASPASO

ADMINISTRADORA TRANSFERENTE

Cumpliendo con las formalidades previstas en la normatividad de datos personales y la LSAR realiza el traspaso de datos y recursos en la cuenta del trabajador.

ADMINISTRADORA RECEPTORA

1. Recibe datos y recursos de la cuenta del trabajador.
2. Debe **cumplir** con las obligaciones previstas en la LSAR y la LFPDPPP.

3. El Departamento de Datos Personales

FUNCIONES DEL DEPARTAMENTO DE DATOS PERSONALES

Atender los Derechos ARCO de los Titulares

El **personal de la organización no puede dar trámite directo a estas solicitudes**

En caso de recibir una solicitud ARCO deberá remitirla al Departamento para que esta la atienda en tiempo y forma .

Fomentar la cultura de protección de datos

Todas las áreas de la empresa están obligadas a cooperar con el Departamento para atender los Derechos ARCO y a mediante la localización y envío de información que este requiera.

Responde quejas sobre temas de privacidad

Desarrollar políticas y procesos en PDP

5. Sanciones por incumplimiento

La Ley Federal de Protección de Datos Personales en Posesión de Particulares (“LFPDPPP”) es aplicable a todos los particulares sean personas físicas o morales que lleven a cabo el tratamiento de datos personales.

Proteger los datos personales es una **obligación** de todas las empresas

Incumplir las obligaciones de la LFPDPPP puede dar lugar a un incumplimiento de políticas internas y a una responsabilidad personal y directa.

Incumplir con las obligaciones previstas en la LFPDPPP puede dar lugar a la imposición de MULTAS de **hasta 27 millones de pesos.**

Actualmente la **multa más alta** impuesta por el INAI es de 32 millones de pesos por violar el principio de proporcionalidad al recabar datos no necesarios para la solicitud de un crédito

CASO MARRIOT

- La cadena de hoteles Marriott informó de una de las mayores violaciones de seguridad de la historia, con robo de datos personales y financieros de 500 millones de clientes. La brecha de seguridad se remonta -nada menos- que a 2014 y se habría originado en la cadena de hoteles Starwood adquirida por Marriott en 2016.
- La firma anunció que los datos sustraídos de sus clientes incluyen el nombre, la dirección de correo, el número de teléfono, el correo electrónico, el número de pasaporte o la fecha de nacimiento.
- El caso Marriott/Starwood es el incidente de piratería más serio hasta la fecha, tanto por el número de clientes afectados como por el tipo de información sensible a la que se ha tenido acceso.
- La brecha de Marriott y Starwood se diferencia de la mayoría de las brechas recientes que han sufrido los hoteles en que esta ha llegado al sistema principal de reservas de la compañía, una base de datos de alta prioridad y seguridad, pues recoge, por ejemplo, la información de los pasaportes

Procedimiento de verificación

INAI.3S.07.02-0028/2016

Conducta

Responsable: Hotel

El Responsable recaba datos personales del Titular, sin contar con un aviso de privacidad el cual ponga a disposición de sus huéspedes, previo a recabar o dar tratamiento a sus datos personales.

Criterios DGIV-INAI

El Responsable aportó dos fotografías de la rececpión del Hotel en las que se aprecia su aviso de privacidad; sin embargo, las mismas no contienen la certificación que acredite las circunstancias de lugar y tiempo en que fueron tomadas, y que corresponde a lo representado en ellas.

La Responsable incumplió con los principios de consentimiento, información, responsabilidad y licitud.

Ordena iniciar PISAN

Recomendaciones

- Capacitar a los empleados sobre la puesta a disposición del aviso de privacidad de la empresa.
- Contar en las áreas de recepción con un aviso de privacidad visible al público.
- Generar prueba plena de la puesta a disposición de los avisos de privacidad.

Procedimiento de Protección de Derechos

PPD.0146/15

Conducta

Responsable: Empresa hotelera

El Responsable fue omisa en atender el derecho de acceso formulado por el Titular, por lo que, el INAI requirió a la Responsable para que emitiera respuesta favorable para el Titular y presentara las pruebas correspondientes ante el Instituto.

El Titular solicitó acceso a registro de huéspedes y visitantes.

Criterios DGPDS-INAI

El INAI consideró fundada la solicitud de protección de datos y determinó que el Hotel no estaba obligado a dar acceso a los datos en virtud de que demostró que estos no obraban en sus bases de datos a la fecha de presentación de la solicitud.

Se ordenó el inició del Procedimiento de Imposición de Sanciones por actualizarse la infracción prevista en la fracción II del artículo 63 de la Ley consistente en actuar con negligencia o dolo en la atención de Derechos ARCO.

Se inició PISAN

Recomendaciones

- **Se debe capacitar al personal para conocer sus obligaciones de protección de datos, entre ellas, atender los Derechos de los Titulares.**
- **Se debe establecer un procedimiento estandarizado para registrar y procesar cada una de las solicitudes ARCO recibidas en tiempo y forma.**

Procedimiento de verificación

IFAI.3S.07.02-043/2016

Conducta

Responsable: Agencia de Viajes

Una empleada de la Responsable adjunto por error un archivo relativo al reporte de ventas del mes de mayo del año dos mil quince, el cual contenía base de datos personales de 95 clientes, incluyendo datos relativos al número de viajes realizados, destinos de los viajes, datos personales de contacto, e incluso, datos personales patrimoniales y financieros

Criterios DGIV-INAI

La Responsable dio tratamiento a los datos personales para una finalidad sustancialmente distinta que aquélla para la que originalmente se obtuvieron e incumplió el deber de confidencialidad.

La Responsable incumplió con los principios de lealtad, responsabilidad y licitud.

Recomendaciones

- **Capacitar al personal sobre sus obligaciones en materia de protección de datos.**
- **Contar con un plan de respuesta ante vulneraciones de seguridad.**
- **Contar con una política de atención a vulneraciones y generar prueba de las medidas correctivas que se han adoptado.**

Ordena iniciar PISAN

Procedimiento de verificación

INAI.3S.07.02-062/2016

Conducta

Responsable: Restaurante

Uno de los empelados del Responsable divulgó uno de los videos grabados con el sistema de video vigilancia de circuito cerrado, en u sitio web, en el cual se logra distinguir la imagen personal del Titular; el cual nunca fue informado, ni dio su consentimiento para la captación de video de su persona, ni para la divulgación de dicho video.

Criterios DGIV-INAI

El Responsable no logró acreditar contar con un aviso de privacidad para su sistema de video vigilancia de circuito cerrado e impide el conocimiento del procedimiento debido para el ejercicio de los Derechos ARCO.

La Responsable incumplió con los principios de información, responsabilidad y licitud.

Ordena iniciar PISAN

Recomendaciones

- **Elaborar un aviso de privacidad para zonas de videovigilancia.**
- **Generar prueba de la puesta a disposición del Aviso de Privacidad.**
- **Recabar el consentimiento expreso y por escrito para el tratamiento de Imagen personal de los titulares.**

Procedimiento de Revisión

3S.07.02-081/2019

Conducta

Responsable:Persona moral que utiliza servicio de vigilancia (fraccionamiento)

El titular tuvo que entregar una identificación en un punto de seguridad para ingresar a las instalaciones. La persona encargada de seguridad perteneciente a una empresa que presta servicios a la responsable dijo perder la identificación, pero posteriormente fue utilizada con fines malisciosos.

Criterios DGIV-INAI

Tanto la empresa responsable como la que le presta servicios de seguridad infrigieron la norma puesto que realizaron una transferencia de datos y las dos se convirtieron en responsables. La primera porque es la responsable original y cae sobre ella primeramente la protección de los datos y la segunda porque es la que recabó dichos datos

Existe una violación de los principios de consentimiento, información, lealtad y licitud

Se inició PISAN

Recomendaciones

- **Contar con un aviso de privacidad y generar la prueba de puesta a disposición y de obtención del consentimiento.**
- **Contar con las medidas de seguridad sobre los datos personales que obtenga y de los que actualice la figura de responsable.**

Procedimiento de verificación

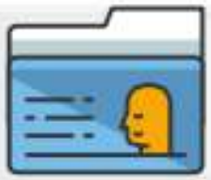
INAI.3S.07.02-065/2016

Conducta

Responsable: Empresa de outsourcing

La Titular otorgó a una empresa prestadora de servicios de personal su CV, así como sus datos personales; posteriormente, dicha empresa transfirió los datos personales de la Titular a una empresa de Outsourcing, quien se comunico con la Titular de manera directa con ella, sin que ninguna de ambas empresas pusera a disposición de la Titular su aviso de privacidad.

Criterios DGIV-INAI



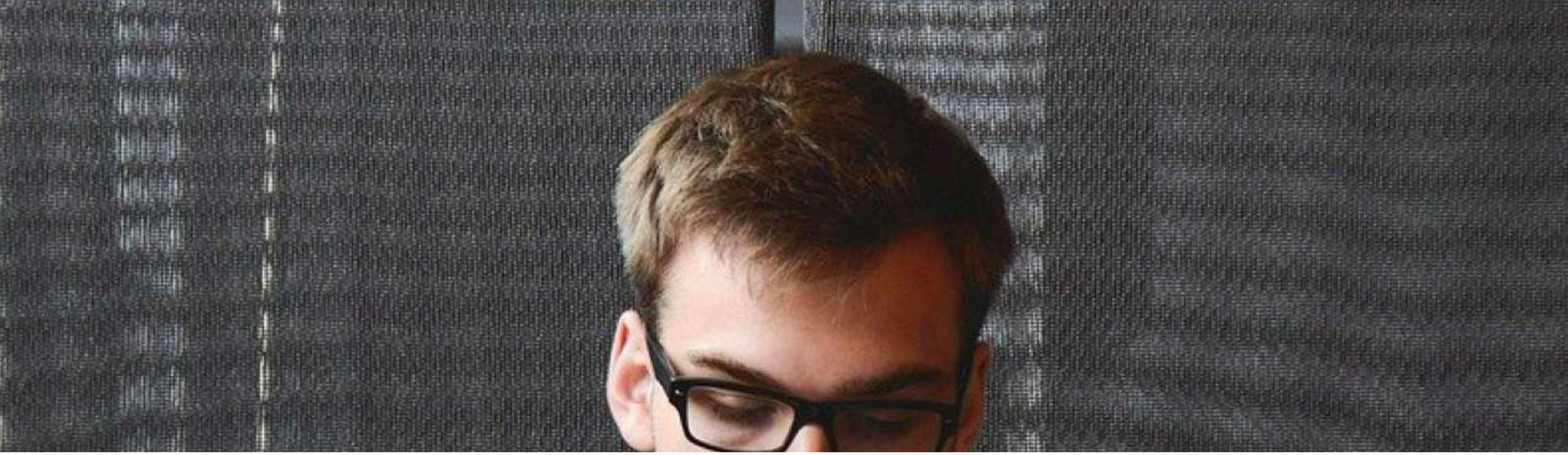
El primer contacto que tuvo la Responsable con la Titular fue a través de correo electrónico para la contratación de sus servicios, por lo que debe de entenderse que a partir de ese momento la Responsable dio tratamiento a los datos personales de la Titular.

Si bien la Responsable no recabo de manera directa los datos personales de la Titular, al recibir su CV, se convirtió en nuevo Responsable de los datos personales de la Titular, y a partir del envío del correo electrónico, nació la relación jurídica entre ambas partes.

Ordena iniciar PISAN

Recomendaciones

- Informar las transferencias en el Aviso de Privacidad y solicita, en caso de ser necesario el consentimiento del titular para el tratamiento.
- Generar prueba de la puesta a disposición del Aviso de Privacidad.
- Formalizar las transferencias de datos personales entre responsables.



6. Mejores Prácticas

MEJORES PRÁCTICAS

***1. Análisis de la información*:** Realizar un análisis de las bases de datos y sistemas de tratamiento para identificar el flujo de los datos personales y conocer los tratamientos de datos personales presentes en la organización.

***2. Transparencia*:** Revisar los avisos de privacidad y establecer un plan de acción para adecuar el contenido de estos a la normativa aplicable. Poner a disposición el aviso de privacidad que corresponda de forma previa al tratamiento.

3. Consentimiento: Revisar cómo se obtiene, registra y gestiona el consentimiento para verificar que los procedimientos relacionados con su gestión se ajusten a la normatividad. No dar tratamiento a los datos de los titulares para fines no consentidos por este. Además, es importante que cuando sea requerido se genere prueba de su obtención y se conserve dicha prueba.

4. Derechos*:* Conocer los medios existentes para el ejercicio de Derechos ARCO para que se pueda orientar a los titulares sobre los mecanismos existentes para la tramitación de sus solicitudes y remitirlas al Departamento de Datos Personales.

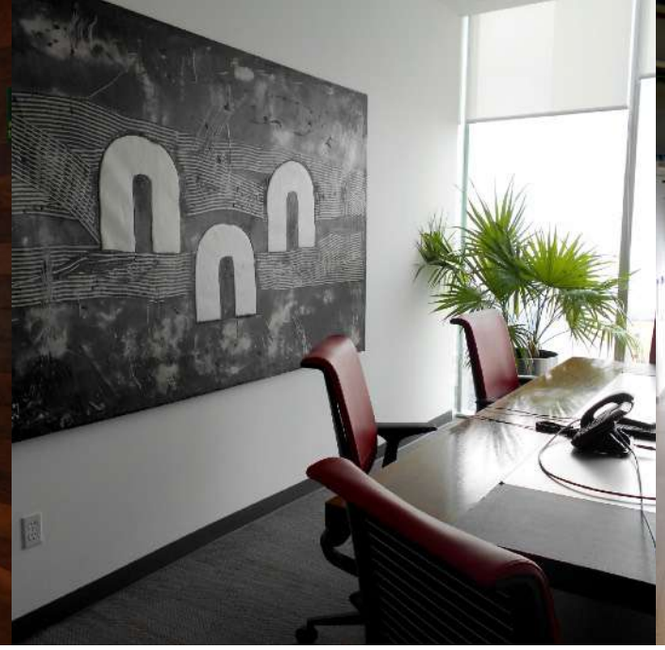
MEJORES PRÁCTICAS

5. Protección de datos por diseño y evaluaciones de protección de datos: Adoptar la privacidad desde el diseño de los productos y como medida incorporada a los mismos. En aquellos casos en los que se identifiquen tratamientos de alto riesgo será necesario consultar al DPDP para que se realice una evaluación de impacto a la privacidad.

6. Comunicaciones de datos: Realizar actividades de revisión a los terceros para verificar la forma en la que estos cumplen sus obligaciones de protección de datos. Solicitar el apoyo de legal para que en las prestaciones que involucren el uso de datos se regulen las comunicaciones de datos con terceros (remisiones y transferencias).

***7. Políticas y procesos*:** Conocer las políticas y procesos de la empresa y asegurarse de cumplir con las mismas para evitar la imposición de sanciones internas y el incumplimiento a la normatividad.

8. Concienciación: Conocer y difundir el cumplimiento de las obligaciones en materia de protección de datos personales aplicables.



Gracias por su atención

info@davara.com.mx @DavaraAbogados T + 52 (55) 56 52 34 55 F + 52 (55) 56 52 19 85