INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"MEDIDAS DE SEGURIDAD DE PROTECCIÓN DE DATOS PERSONALES EN MI LUGAR DE TRABAJO"

SOLUCIÓN ESTRATÉGICA EMPRESARIAL
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Esteban Ramón Rodríguez Jiménez

Asesor:

Mtro. Rigoberto Martínez Becerril

Ciudad de México, julio de 2020

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 10 de noviembre de 2020
INFOTEC-DAIC-GCH-SE-0593/2020.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

MEDIDAS DE SEGURIDAD DE PROTECCIÓN DE DATOS PERSONALES EN MI LUGAR DE TRABAJO

Desarrollado por el alumno **Esteban Ramón Rodríguez Jiménez** y bajo la asesoría del **Mtro. Rigoberto Martínez Becerril**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.

Mtra. Julieta Alcibar Hermosillo
Coordinadora de Biblioteca

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

C.p.p Servicios Escolares

Agradecimientos

Agradezco:

A Dios, ¡Siempre!

A mis padres, mi esposa y mis hijas por su amor, comprensión y apoyo total.

Al INFOTEC, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (TIC), de la red Centros Públicos de Investigación (CPI) del Consejo Nacional de Ciencia y Tecnología (CONACYT), por contribuir enormemente a mi formación académica en el ámbito de las TIC, a través de los diversos programas académicos en los que he tenido la dicha de formar parte.

A la Doctora Issa Luna Pla por la confianza depositada en mi persona para integrarme a la primera generación de la Maestría en Derecho de las Tecnologías de Información y Comunicación (MDTIC).

Al Doctor Miguel Ángel Mesa Carrillo y al Maestro Moisés Octavio Limón Ortega por sembrar en mi el interés hacia el ámbito político-jurídico en México.

A Diego García Vélez y Jonathan López Torres por todo su apoyo para materializar este y otros proyectos relacionados con la materia.

A Joel Gómez Treviño y a todos los colegas de la Academia Mexicana de Derecho Informático (AMDI) por su orientación y apoyo.

A todos los catedráticos y compañeros de estudio. Compartir sus experiencias y conocimientos, fue un privilegio.

Al Maestro Rigoberto Martínez Becerril en la guía para la consecución de este texto.

A todas las personas que contribuyeron a la realización de esta Maestría.

Tabla de Contenido

Índice de Cuadros

Siglas y Abreviaturas

CPEUM	Constitución Política de los Estados Unidos Mexicanos
DOF	Diario Oficial de la Federación
Empresa	Tecnologías en Información del Norte, S.A. de C.V.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
UMA	Unidad de Medida y Actualización

Introducción

El desarrollo tecnológico y el Internet[1] han traído consigo la necesidad de proteger diversos aspectos inherentes a las personas, la privacidad[2] y la información de carácter personal son algunos de ellos. Esta necesidad de proteger los datos personales, la información y la privacidad, deriva del derecho que poseen las personas a la protección de sus datos personales, que se traduce en su derecho a la autodeterminación informativa, es el individuo quien decide qué se hace, qué no se hace, quién puede poseerla y para qué fines puede ser utilizada su información personal.

En este sentido, el Derecho se ha visto obligado a evolucionar a través del diseño y creación de nueva normatividad y entes reguladores, en el caso mexicano el INAI como máximo órgano constitucional autónomo que tiene por objeto garantizar el derecho a la protección de los datos personales en posesión de los particulares en toda la República.

En este orden de ideas, en estricto sentido entre los mecanismos a través de los cuales se puede garantizar el derecho a la protección de datos personales en cualquier organización pública o privada en cualquier parte del mundo son las medidas de seguridad, las cuales se agrupan en administrativas, técnicas y físicas. Si no existen tales mecanismos de protección resulta imposible lograr la protección de información personal y, por ende, hacer efectivo el derecho humano a la protección de datos personales.

En virtud de lo anterior, el presente trabajo constituye una "Solución Estratégica Empresarial" que tiene como finalidad solventar una problemática que enfrenta la empresa en la que laboro (la Empresa), la cual consiste en que, al

---

1 "[…] el Internet no es una entidad física tangible, sino más bien una red gigante que interconecta innumerables grupos de menor tamaño de redes de computadoras interconectadas. Es pues la red de redes". Álvarez, Clara Luz, *Internet y derechos fundamentales*, México, Porrúa, 2011, p. 1.

2 Un concepto relacionado es el de intimidad el cual se refiere en términos generales a las cosas que una persona desea mantener para sí misma de forma reservada. Véase más en: Méjan Carrer, Luis Manuel Camp, *El Derecho a la Intimidad y la Informática*, México, editorial Porrúa, México, 1996.

trabajar con diversos flujos de información de carácter personal, la Empresa, aunado a cumplir con el resto de obligaciones en materia de protección de datos personales en términos de la legislación aplicable, cuenta con distintas medidas de seguridad de carácter administrativas, técnicas y físicas, no obstante, la problemática que se plantea es que dichas medidas no han sido revisadas ni están concentradas en un solo documento, sino que están contenidas en diversos documentos, lo que hace necesario para la Empresa revisarlas, actualizarlas de ser necesario y unificarlas en un solo documento.

Con la adecuada revisión, documentación y unificación de las medidas de seguridad, la Empresa:

1. Fortalecerá la protección de los datos personales en su posesión, brindando seguridad jurídica y una expectativa razonable de privacidad a los titulares de los datos personales y

2. Garantizará su cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, a efecto de evitar contingencias de carácter legal.

La problemática anterior se reconoció por la Dirección General de la Empresa, quien asumió el tema como prioritario, por lo que, a petición del suscrito y en compatibilidad con los conocimientos adquiridos en la Maestría en Derecho de las Tecnologías de la Información y Comunicación cursada en INFOTEC, el suscrito propuso el presente trabajo como “Solución Estratégica Empresarial” a efecto de resolver el problema de la Empresa anteriormente citado, el cual está directamente relacionado con el Derecho y con las tecnologías de la información y comunicación.

Por lo anterior, el presente trabajo como “Solución Estratégica Empresarial” es viable a efecto de dar solución al problema planteado y cumple, a su vez, con los objetivos de la modalidad referida, de conformidad con los lineamientos de INFOTEC.

Adicionalmente, el presente trabajo será de gran valor para la Empresa ya que permitirá blindar sus obligaciones de *compliance* de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, y brindará seguridad y confianza a su personal, clientes y socios de negocio.

Señalado lo anterior, en el capítulo 1 se aborda el derecho a la protección de datos personales en las empresas, en el cual se incluye una introducción al derecho a la protección de datos personales en México, la importancia de la protección de datos personales en las empresas y los riesgos de no proteger los mismos.

En el capítulo 2 se abordan las medidas de seguridad para la protección de datos personales, el cual incluye la importancia de las mismas, el marco normativo, las sanciones por su incumplimiento y sus distintos tipos, las de carácter administrativas, técnicas y físicas.

Por su parte, en el capítulo 3 se abordan los datos personales objeto de tratamiento por la Empresa, la identificación de las medidas de seguridad actuales y la adición de nuevas medidas de seguridad, cuya identificación e incorporación es resultado del presente trabajo.

Para finalizar, se presenta un apartado con las conclusiones del presente trabajo.

Capítulo 1

El derecho a la protección de datos personales en las empresas en México

Capítulo 1: El derecho a la protección de datos personales en las empresas en México

Parte de la actual economía se distingue por el incremento de productos y servicios creados, distribuidos y comercializados a través de las tecnologías de la información y comunicación (TIC), de ahí el inicio de la llamada economía digital, en donde oferentes y demandantes están en constante contacto intercambiando diferentes tipos y cantidades de información.

La información de carácter personal es uno de los principales tipos de información objeto de intercambio en el mundo de los negocios, en donde el inadecuado uso de la misma ha dado lugar al diseño y creación de nueva normatividad que tiene por objeto proteger a las personas respecto al tratamiento de sus datos personales, constituyéndose así el derecho a la protección de datos personales, siendo México un claro ejemplo de ello.

1.1 Marco jurídico del derecho a la protección de datos personales en México

Los datos personales —como derecho objeto de protección— son cualquier información concerniente a una persona física identificada o identificable y adquieren el carácter de sensibles "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."[3]

3 Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010, artículo 3, fracciones V y VI, México. Disponible en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf* (Fecha de consulta: 05 de enero de 2020).

En este sentido, en México el derecho a la protección de datos personales[4] tiene un fundamento y protección de carácter constitucional, al ser reconocido en la Carta Magna en el artículo 16, segundo párrafo, que a la letra señala:

> Artículo 16. […]
> 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[5] 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.[6]

El artículo anterior constituye el fundamento de un derecho humano de reciente creación, el cual se adicionó a la CPEUM mediante decreto publicado en el DOF el primero de junio de 2009.[7] Como se puede observar, este derecho, con

---

4 El derecho a la protección de datos es un "[…] derecho subjetivo, autónomo y de tercera generación, que constituye un instrumento jurídico imprescindible en el desarrollo de una sociedad democrática y que garantiza la libertad del individuo en el seno de la misma." Peschard Mariscal, Jacqueline, *El derecho fundamental a la protección de datos personales en México*, en: Nuñez Ornelas, Lina, y Piñar Mañas, José Luis, La protección de datos personales en México, Tirant lo Blanch, México, 2013, p. 19.

5 En cuanto a las excepciones al derecho a la protección de datos personales véase: López Torres, Jonathan. La Constitución y la protección de datos personales en México: las inconsistencias en el esquema de excepciones". Revista Tohil de la Facultad de Derecho de la Universidad Autónoma de Yucatán. ISSN 2007-6673, año 16, número 38, enero-junio 2016. Disponible en: *http://www.derecho.uady.mx/tohil/rev38/art2rev38.pdf* (Fecha de consulta: 05 de enero de 2020).

6 Constitución Política de los Estados Unidos Mexicanos, "Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos", publicado en el DOF el primero de junio de 2009, México.
Disponible en: *https://www.dof.gob.mx/nota_detalle.php?codigo=5092143&fecha=01/06/2009* (Fecha de consulta: 05 de enero de 2020).

7 Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el DOF el primero de junio de 2009. Disponible en:

apenas 10 años en el marco jurídico mexicano, tiene por objeto garantizar a toda persona la protección de su información personal, derecho que se materializa a través de los llamados derechos ARCO, cuyas siglas significan "Acceso, Rectificación, Cancelación y Oposición" al tratamiento de datos personales.[8]

Al respecto, el Poder Judicial de la Federación ha señalado que el segundo párrafo del artículo 16 de la CPEUM "[…] establece el derecho a la protección de datos personales de los gobernados como medio para garantizar la facultad de los individuos a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de la sociedad, y la posibilidad de exigir su cumplimiento a las autoridades y particulares que conocen, usan o difunden dicha información."[9]

En ese orden de ideas, los tribunales judiciales federales han señalado que, la protección de datos personales constituye un derecho humano vinculado con la salvaguarda de otros derechos fundamentales inherentes al ser humano en los términos siguientes:

> El párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce los denominados derechos ARCO, relativos al acceso, rectificación, cancelación y oposición de datos personales, como un medio para garantizar el derecho de los individuos a decidir qué aspectos de

---

https://www.dof.gob.mx/nota_detalle.php?codigo=5092143&fecha=01/06/2009 (Fecha de consulta: 05 de enero de 2020).

8 No sobra señalar que, en la fracción II del apartado A del artículo 6 de la CPEUM se establece el derecho a la protección de datos personales en posesión de las autoridades del estado mexicano, conocidos como "sujetos obligados", los cuales se conforman por cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal.

9 Tesis: XXI.3o.C.T.11 C (10a.), *Semanario Judicial de la Federación*, Décima Época, t. III, febrero de 2020, p. 2399. Disponible en: *https://sjf.scjn.gob.mx/SJFSist/Paginas/DetalleGeneralV2.aspx?ID=2021622&Clase=DetalleTesisBL&Semanario=1* (Fecha de consulta: 21 de febrero de 2020).

su vida deben o no ser conocidos o reservados por el resto de la sociedad, y la posibilidad de exigir su cumplimiento a las autoridades y particulares que conocen, usan o difunden dicha información. Así, dichas prerrogativas constituyen el derecho a la protección de los datos personales, como un medio de salvaguarda de otros derechos fundamentales previstos en la propia Constitución y en los tratados internacionales de los que México es Parte, conforme a los cuales, el Estado tiene la obligación de garantizar y proteger el derecho de todo individuo a no ser interferido o molestado por terceros o por una autoridad, en ningún aspecto de su persona –vida privada–, entre los que se encuentra el relativo a la forma en que se ve a sí mismo y cómo se proyecta a los demás –honor–, así como de aquellos que corresponden a los extremos más personales de la vida y del entorno familiar –intimidad–, o que permiten el desarrollo integral de su personalidad como ser humano –dignidad humana–.[10]

Vital importancia ha cobrado el derecho a la protección de información personal que, el deber del Estado mexicano de salvaguardarlo debe potenciarse ante los riesgos que representan las nuevas herramientas tecnológicas, en virtud del "[…] efecto multiplicador de los medios de comunicación digitales de Internet y las redes sociales, a través de los cuales se facilita la difusión y durabilidad de su contenido, al permanecer de manera indefinida en los medios electrónicos en los que se publican, sin restricción territorial alguna […]"[11]

---

10 Tesis: I.10o.A.5 CS (10a.), *Semanario Judicial de la Federación*, Décima Época, t. III, septiembre de 2019, p. 2199. Disponible en: *https://sjf.scjn.gob.mx/SJFSist/paginas/DetalleGeneralV2.aspx?ID=2020563&Clase=DetalleTesisBL&Semanario=0* (Fecha de consulta: 21 de febrero de 2020).

11 Tesis: I.10o.A.6 CS (10a.), *Semanario Judicial de la Federación*, Décima Época, tomo III, septiembre de 2019, p. 2200. Disponible en: *https://sjf.scjn.gob.mx/SJFSist/Paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=datos%2520personales&Dominio=Rubro&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=47&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=2020564&Hit=5&IDs=2021622,2020995,20*

Señalados los alcances del derecho a la protección de datos personales, es conveniente destacar que, en México este derecho se regula de conformidad con la naturaleza pública o privada de quien los posee, es decir, si la información personal está en posesión de una autoridad, identificadas como "sujetos obligados", se aplica una ley especial, en este caso, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual, de conformidad con su artículo 1, es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la CPEUM, en materia de protección de datos personales en posesión de sujetos obligados, y tiene por objeto:

> […] establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.
> Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.[12]

En lo que respecta al ámbito privado, es decir, cuando los datos personales están en posesión de un particular resulta aplicable la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la cual, de conformidad con su artículo 1 es "[…] de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación

---

20767,2020575,2020564,2020563,2020549,2020542,2019839,2019836,2018263,2017930,2017650,2016812,2015849,2015581,2015442,2015433,2015432,2015163&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema= (Fecha de consulta: 21 de febrero de 2020)

12 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017, artículo 1, México. Disponible en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf* (Fecha de consulta: 22 de febrero de 2020).

informativa de las personas.” La aplicación al ámbito privado se observa a continuación en su artículo 2 con sus respectivas excepciones:

> Artículo 2.- Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:
> I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
> II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Por último, es importante mencionar que, la autoridad garante en México del derecho humano a la protección de datos personales en posesión de particulares y autoridades es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual tiene una naturaleza jurídica de organismo constitucional autónomo creado en virtud de la reforma constitucional en materia de transparencia publicada en el DOF el 07 de febrero de 2014.[13]

Las atribuciones para garantizar el derecho a la protección de datos personales en posesión de los sujetos obligados se observan en la fracción VIII del artículo 6 de la CPEUM, conforme a lo siguiente:

> VIII. La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de

13 Véase el: Decreto por el que se reforman y adicionan diversas disposiciones de la CPEUM, en materia de transparencia. Publicado en el DOF el 07 de febrero de 2014. Disponible en: *http://dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014* (Fecha de consulta: 22 de febrero de 2020).

> garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.[14]

Por su parte, las atribuciones —temporales— de garantizar el derecho a la protección de datos personales en posesión de los particulares se establecieron en el artículo séptimo transitorio de la citada reforma constitucional en materia de transparencia de 2014, en donde se señaló que:

> SÉPTIMO. En tanto se determina la instancia responsable encargada de atender los temas en materia de protección de datos personales en posesión de particulares, el organismo garante que establece el Artículo 6o. de esta Constitución ejercerá las atribuciones correspondientes.

Para concluir el presente apartado, es importante mencionar que, el derecho a la protección de datos personales nace como una medida para garantizar la protección de las personas mediante el legítimo, controlado e informado tratamiento de sus datos personales, lo que se conoce también como el derecho a la autodeterminación informativa, que no es otra cosa que, las personas decidan quiénes puedan usar sus datos personales, cuántos datos personales pueden recabar y utilizar, y decidir para qué fines pueden ser utilizados los mismos, lo cual,

14 Ídem.

a su vez, garantizará la privacidad de las personas,[15] Derecho que se estima ser desarrollado de mejor manera.[16]

1.2 La importancia de la protección de datos personales para las empresas

Las empresas dadas sus actividades operativas y de negocio recopilan y procesan cantidades importantes de información todos los días, lo cual se debe tanto a la naturaleza de sus operaciones como a la adopción de las TIC, lo que ha implicado la digitalización y modernización de sus procesos de negocio, toda vez que:

> Los negocios buscan de manera continua mejorar la eficiencia de sus operaciones para poder obtener una mayor rentabilidad. Los sistemas y tecnologías de la información son algunas de las herramientas más importantes disponibles para que los gerentes obtengan mayores niveles de eficiencia y productividad en las operaciones […][17]

En este sentido, las empresas tratan distintos tipos de información: de carácter operacional, administrativa, financiera, de propiedad industrial e intelectual, legal, entre otros tipos, y, por supuesto, información de carácter personal.

---

15 Para más información relativa al marco jurídico nacional e internacional en materia del derecho a la protección de datos personales véase el "*Corpus Iuris en materia de Protección de Datos Personales*", una herramienta desarrollada por el INAI en conjunto con la Red Iberoamericana de Protección de Datos, el cual tiene por objeto permitir el acceso, "de manera sencilla y sistematizada a un nutrido conjunto de documentos, normas y precedentes que muestren el desarrollo que ha tenido la protección de datos personales como un derecho humano, las direcciones y grados de avance que éste ha alcanzado, así como las áreas que es necesario reforzar, continuar desarrollando, o bien, que representan nuevos retos en la materia." Disponible en: *http://corpusiurispdp.inai.org.mx/Pages/home.aspx* (Fecha de consulta: 22 de febrero de 2020).

16 *Cfr*. Piñar Mañas, José Luis, y Recio Gayo Miguel, *Código de Protección de Datos Personales México*, Tirant lo Blanch, México, 2013, p. 13 .

17 Laudon, Kenneth, y Laudon Jane, *Sistemas de información gerencial*, Decimocuarta edición, Pearson Educación, México, 2016, pp. 13 y 14.

Las empresas recopilan y procesan datos personales en todo momento, información que proviene de forma interna, desde sus socios, directivos y todos los empleados, hasta información de terceros, que pueden ser desde sus clientes proveedores hasta sus clientes en calidad de usuarios finales. Los tipos de información que recaban las empresas dependen de las actividades comerciales de las mismas, ya que mientras una empresa de telecomunicaciones puede recabar información de identificación, de contacto, fiscal y datos financieros para el pago de los servicios, un hospital recaba desde información de identificación y contacto, hasta datos personales sensibles, que son los relativos al estado de salud de las personas que se concentra en un expediente clínico.

A manera de ejemplo, los datos personales de identificación y contacto son tan importantes porque permiten al menos dos aspectos básicos a las empresas: 1) identificar a las personas (datos personales de identificación, como el nombre completo) y, 2) contactar a las personas (datos personales de contacto, como correo electrónico, domicilio y número telefónico).

Los datos personales de identificación y contacto parecieran menos importantes, pero no es así ¿qué pasaría si una empresa no pudiera identificar a sus clientes? y bien ¿qué pasaría si una empresa no pudiera contactar a sus clientes? De no contar con tal información sería muy difícil para una empresa seguir prestando cierto servicio o entregando cierto producto, e incluso no podría contactar a sus clientes para cobrar los productos y/o servicios correspondientes.

Ahora bien, pareciera que recabar información personal constituye una tarea fácil para las empresas, pero no es así, las empresas en muchos casos tienen que realizar múltiples actividades para llegar a tener la oportunidad de que un usuario les brinde su información de carácter personal (en otras ocasiones no es así y adquieren de forma ilegal la información), actividades que consisten desde contar con productos y servicios de buena calidad, cantidad y precio, una adecuada publicidad, conocimiento de la empresa por el público consumidor, posicionamiento entre sus competidores e incluso contar con referencias de terceros respecto a la

formalidad de la empresa. Todas estas actividades y gestiones constituyen inversiones por parte de las empresas para hacer notar a sus clientes y usuarios que son su mejor opción para adquirir sus productos o servicios.

Logrado lo anterior, es decir, una vez que las empresas recopilan los datos personales de sus potenciales clientes o usuarios finales e incluso cuando logran hacerlos sus clientes, es cuando surge la necesidad e importancia de la protección de datos personales para las empresas, importancia que en muchos casos se debe al cumplimiento de obligaciones de carácter legal, como en el caso de México con la obligación de cumplir con la LFPDPPP y en otros casos, adicional al anterior, cuando las empresas reconocen que sus clientes y su información personal son lo más importante para su negocio.

En nuestro caso, la Empresa reconoce la importancia de proteger la información personal tanto interna como de sus clientes, y esto lo tiene muy presente porque tanto el personal interno como sus clientes le han otorgado su confianza al brindar su información personal, compromiso que la Empresa observa más allá que solo el cumplimiento legal, motivo del presente trabajo.

1.3 Riesgos a la protección de datos personales en las empresas

Recabar y utilizar información de carácter personal conlleva una obligación de carácter ética y legal en México, lo cual conlleva a la exposición de distintos riesgos. Por ello, los principales riesgos a la protección de datos personales en las empresas se pueden clasificar en dos tipos y pueden consistir en los siguientes:

Riesgos internos

a) No les importe proteger los datos personales;
b) Desconozcan que tienen una obligación legal de proteger los datos personales y cuáles son las normas jurídicas que deben cumplir;
c) Desconozcan la existencia del derecho humano a la protección de datos personales;

d) Falta de personal capacitado para el tratamiento de datos personales;
e) Estrategias limitadas o no adecuadas para proteger datos personales,
f) Entrega o acceso de forma irresponsable de información personal a terceros proveedores y/o socios de negocio;
g) Venta de bases de datos con información personal;
h) Desconocimiento de plazos de conservación y de eliminación de forma segura de información personal;
i) Colapso de equipos de cómputo y de almacenamiento de información en virtud de su falta de mantenimiento técnico y/o por el término de su vigencia de vida operativa, y
j) Robo, filtración y/o divulgación de datos personales por parte de empleados, y
k) Ausencia o limitadas medidas de seguridad administrativas, técnicas y físicas.

Los riesgos internos anteriores, que se caracterizan por una ausencia de control o control limitado de protección de los datos personales, predisponen a las empresas a contingencias que puedan desembocar en pérdida o robo de información personal, con consecuencias no solo de carácter legal, sino en la afectación en la confidencialidad de la información como afectaciones a la privacidad de las personas y que merman la imagen y confianza de las empresas.

Los riesgos internos se atribuyen de forma directa e indirecta a las empresas por su ausencia de mecanismos de protección o por la limitación de los mismos.

Riesgos externos

a) Robo de datos personales por parte de terceros, mediante el robo de dispositivos de cómputo y de comunicación móvil utilizados para realizar actividades laborales, y

b) Ataques cibernéticos, que tengan por objeto robar, dañar, secuestrar y/o eliminar bases de datos o documentos con información de carácter personal.

Los riesgos externos anteriores, que se caracterizan por ser atribuibles a factores externos, es decir, están fuera del control de las empresas, comparten las mismas contingencias que los riesgos internos, no solo de carácter legal, sino en la afectación en la confidencialidad de la información como afectaciones a la privacidad de las personas.

Los riesgos externos son cada vez más frecuentes y pueden, a su vez, tener consecuencias reputacionales, legales y económicas, toda vez que pueden afectar a cualquier tipo de información, no solo la personal, sino financiera, legal, de negocios, de propiedad intelectual y hasta secretos industriales.

Tanto los riesgos internos como externos perjudican a las empresas y a los propios titulares de la información, en donde la información de estos últimos puede ser utilizada para cometer delitos como el robo de identidad y fraudes, entre muchos otros.

Como es posible observar, a lo largo del presente capítulo se ha descrito brevemente el marco jurídico que regula del derecho a la protección de los datos personales en México, cuál es la importancia de la protección de los datos personales para las empresas, así como los riesgos internos y externos a los que se enfrentan dichas unidades económicas para proteger los datos personales de sus clientes y personal interno.

En el siguiente capítulo se abordarán diversos aspectos relacionados con las medidas de seguridad para la protección de los datos personales en las empresas.

Capítulo 2

Medidas de seguridad para la protección de datos personales

Capítulo 2: Medidas de seguridad para la protección de datos personales

La seguridad de los datos personales es un tema que debería importar seriamente a individuos y organizaciones, tanto por ser titulares de la información como por tener la obligación legal para hacerlo. No obstante, persiste al día de hoy tanto desconocimiento como falta de consciencia respecto al cuidado de los datos personales, así como de los mecanismos o controles necesarios para proteger dicha información.

Crear consciencia en individuos y organizaciones respecto a la importancia de la protección de datos personales es uno de los primeros pasos para garantizar la seguridad de los mismos.

2.1 Importancia de las medidas de seguridad

Las medidas de seguridad administrativas, técnicas y físicas son —en estricto sentido— los esfuerzos que materializan y hacen realidad la protección de datos personales en México y en cualquier parte del mundo, sean organizaciones públicas o privadas, las cuales, a su vez, contribuyen a hacer efectivo el derecho humano a la protección de datos personales en México, previsto en el segundo párrafo del artículo 16 de la CPEUM. En particular, las medidas de seguridad son el control o grupo de controles de seguridad para proteger los datos personales.[18]

En este sentido, no puede existir protección de datos personales en las empresas, si las mismas no emplean controles o mecanismos de seguridad para proteger tal información, mecanismos que son de diferentes tipos (de ahí la clasificación general de medidas de seguridad en administrativas, técnicas y

18 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2011, artículo 57, párrafo primero, México. Disponible en: *http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf* (Fecha de consulta: 16 de febrero de 2020).

físicas), que dependen de las cantidades de datos personales a proteger, su sensibilidad, los riesgos a los que están expuestos, entre otros.

Las cuales van desde la concientización al interior de las organizaciones de proteger la información personal y el empleo de contraseñas robustas en equipos de cómputo, hasta políticas laborales de no uso de dispositivos personales para realizar actividades de las empresas.

A efecto de ejemplificar la importancia de las medidas de seguridad para las empresas como herramientas de negocios esenciales,[19] tales como son la protección contra *software* espía, sistemas de detección de intrusos y el *software* antivirus, entre otros, a continuación se señalan algunos casos que tuvieron incidentes de seguridad graves, de los que la opinión pública tuvo conocimiento a través de diversos medios de comunicación impresos y electrónicos, donde se filtraron datos personales y sus implicaciones:

a) eBay

Un ataque cibernético en los servidores de la empresa dedicada al comercio electrónico de productos a través de Internet denominada eBay, durante febrero y marzo de 2014, comprometió la base de datos que contiene nombres de clientes, contraseñas cifradas, direcciones de correo electrónico, direcciones físicas, números telefónicos y fechas de nacimiento. Aunque se dijo que no se accedió a los datos financieros, la información obtenida es útil para el posible robo de identidad de sus clientes.[20]

b) Heartland Payment Systems

En 2008, criminales cibernéticos, encabezados por el hacker de Miami Albert González, instalaron software espía (en inglés spyware) en la red computacional de Heartland Payment Systems, Inc., una empresa dedicada

19 Laudon, Kenneth, y Laudon Jane, *op. cit.,* p. 314.

20 Véase CNNExpansión, "*eBay es víctima de ataque cibernético*". Disponible en: *https://expansion.mx/tecnologia/2014/05/21/ebay-es-victima-de-un-ciberataque* (Fecha de consulta: 20 de febrero de 2020).

al procesamiento de pagos y proveedora de tecnología relacionada con los mismos, ubicada en Princeton, New Jersey, Estados Unidos de America, y robaron los números de alrededor de 100 millones de tarjetas de crédito y débito, según la información que es pública. González fue capturado y sentenciado en el 2010 a cumplir una condena de 20 años en una prisión federal y, Heartland tuvo que pagar alrededor de $140 millones USD. en multas y resoluciones.[21]

c) Sony

En abril de 2011, el gigante tecnológico japonés de los videojuegos, fue victima de piratas informáticos que obtuvieron información personal de sus clientes, incluyendo números de tarjetas de crédito, débito y cuentas bancarias, además de 100 millones de cuentas de usuarios de PlayStation Network y de Sony Online Entertainment. La filtración de datos significó un costo a Sony y a los emisores de las tarjetas de crédito de alrededor de los $2 mil millones USD.[22]

En México, las medidas de seguridad para la protección de datos personales son obligatorias para las empresas en términos de lo ordenado por la LFPDPPP, por lo que su ausencia de implementación puede acarrear sanciones de carácter económico a las mismas, pero:

> Más allá de minimizar el posible impacto económico por la imposición de sanciones por parte de la autoridad, el principal beneficio de establecer medidas de seguridad, documentarlas y mantenerlas, radica en el aumento de la certidumbre y confianza de los titulares de los datos personales. Al

21 Véase Bank Info Security, "*Heartland Hacker Sentenced to 20 Years*". Disponible en: *https://www.bankinfosecurity.com/heartland-hacker-sentenced-to-20-years-a-2344* (Fecha de consulta: 20 de febrero de 2020).

22 Véase The Guardian, "*PlayStation Network hackers access data of 77 million users*". Disponible en: *https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data* (Fecha de consulta: 20 de febrero de 2020).

mismo tiempo, se aumenta la competitividad del mercado en general, se mejoran los procesos de la organización y la eficiencia y se facilita la inversión, incluso desde otros países.[23]

De lo anterior se puede observar que, las medidas de seguridad, entre otros beneficios, fortalecen la expectativa razonable de privacidad de los titulares de los datos personales, consistente en que, los titulares incrementan su confianza o esperanza en que las empresas que recaban y utilizan sus datos personales los protegerán contra cualquier daño, perdida, robo, uso o acceso no autorizado.

En consecuencia, es importante reiterar que, no es factible la protección de datos personales en las empresas si no existen medidas de seguridad y como se puede observar en los tres ejemplos anteriores de EBay, Heartland Payment Systems y Sony, se trata de compañías grandes que aunado —se presume— invierten grandes cantidades de capital en medidas de seguridad para proteger sus activos de información, en particular la información personal de sus clientes, aun así son vulnerables a ataques cibernéticos que no solo ponen en riesgo la disponibilidad de sus operaciones comerciales, sino también ponen en riesgo la confidencialidad e integridad de la información que poseen, como en los ejemplos señalados: datos personales.

2.2 Marco normativo de las medidas de seguridad para las empresas

En México la obligación expresa de contar con medidas de seguridad para proteger los datos personales en posesión de las empresas lo constituye el artículo 19 de la LFPDPPP y 57 de su Reglamento. La LFPDPPP señala lo siguiente:

23 INAI, *Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas*, México, junio 2015, p. 4. Disponible en: *http://inicio.inai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf* [Fecha de consulta: 23 de febrero de 2020]

> Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información.
>
> Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Por su parte, el Reglamento de la LFPDPPP señala que:

> Artículo 57. El responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Capítulo, con independencia del sistema de tratamiento. Se entenderá por medidas de seguridad para los efectos del presente Capítulo, el control o grupo de controles de seguridad para proteger los datos personales.
>
> Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento.

De los preceptos anteriores, se observa que todo responsable o empresa que realice tratamiento de datos personales (obtenga, use, acceda a, maneje, aproveche, divulgue o almacene datos personales, por cualquier medio)[24] o los

24 Definición de tratamiento prevista en el artículo 3, fracción XVIII, de la LFPDPPP.

encargados,[25] tienen la obligación de establecer y mantener medidas de seguridad administrativas, técnicas y físicas para proteger la información de carácter personal contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Aunado a lo anterior, el artículo 19 de la LFPDPPP y 57 del Reglamento establecen los siguientes aspectos de carácter puntual que tienen que observar las empresas en su obligación de proteger los datos personales, sean responsables o encargados:

a) *No podrán adoptar medidas de seguridad menores a aquellas que mantengan para el manejo de su información.* Este aspecto es de vital importancia y a la vez contradictorio, ya que, por un lado, establece un grado mínimo de protección para las empresas para proteger la información personal, consistente en que, las empresas deberán proteger los datos personales en su posesión tal como protegen su información operativa, comercial, financiera, etc., y por otro lado, no bastará para las empresas proteger los datos personales tal como protegen la última información señalada, ya que la LFPDPPP y su Reglamento señalan obligaciones adicionales para proteger los datos personales.
b) *Tomarán en cuenta el riesgo existente al que está expuesta la información personal que posea.* Este aspecto implica que las empresas tienen que analizar los riesgos de los datos personales que poseen tanto por el tipo de información como por su cantidad, ya que una empresa que recaba datos personales de identificación y contacto, tal información estará —presumiblemente— menos expuesta, que una empresa del sector bancario que recabe datos personales de carácter financiero de un número amplio de personas.

25 De conformidad con el artículo 3, fracción IX, el encargado es la "persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable".

c) *Tomarán en cuenta las posibles consecuencias para los titulares de los riesgos a los que están expuestos sus datos personales.* Relacionado con el criterio anterior, este aspecto se enfoca en el riesgo para el titular de los datos personales que su información personal sea dañada, pérdida, alterada, destruida o usada, accedida o tratada de forma no autorizada, es decir, en las consecuencias directas e indirectas al propio titular de los datos personales.
d) *Tomarán en cuenta la sensibilidad de los datos personales.* Vinculado al criterio B anterior, este aspecto implica que las empresas tienen que analizar la sensibilidad de los datos personales que poseen, ya que una empresa que recaba datos personales de identificación y contacto, tal información estará —presumiblemente— menos expuesta, que una empresa del sector salud que recabe datos personales sensibles relativos al estado de salud de las personas.
e) *Tomarán en cuenta el desarrollo tecnológico.* Este aspecto transversal a los anteriores tiene en cuenta el desarrollo tecnológico, donde es necesario considerar el soporte en formato electrónico de la información de carácter personal y si la información es procesada a través de medios electrónicos, así como las amenazas cibernéticas que pueden poner en riesgo tales datos personales.
f) *Deberán tomar en cuenta lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda.* Este aspecto se refiere prácticamente a la regulación sectorial, es decir, la regulación que se expide de manera especial en cada sector, sea el financiero, contable, de salud, entre otros, por lo que las empresas deberán cumplir tanto con la regulación sectorial correspondiente como con la LFPDPPP y su Reglamento.

Adicionalmente, es necesario señalar que el deber de adoptar e implementar medidas de seguridad a su vez parte de la obligación de las empresas de observar

y cumplir con el principio de responsabilidad —uno de los ocho principios para la protección de los datos personales.[26]

De lo anterior, es posible concluir que las empresas tienen la obligación con fundamento en los artículos 19 de la LFPDPPP y 57 de su Reglamento, así como en virtud del principio de responsabilidad de adoptar e implementar medidas de seguridad para la protección de los datos personales en su posesión, para lo cual tienen que tener en cuenta diversos aspectos como la sensibilidad de los datos personales, los riesgos a los que están expuestos, el desarrollo tecnológico y la forma en que protegen su información operativa, comercial y financiera. Aunado a ello, para lograr el objetivo de adoptar e implementar medidas de seguridad, es necesario que las empresas tengan un profundo conocimiento de su operación diaria, solo así podrán identificar de forma clara los tipos y cantidades de información personal en su posesión que es objeto de tratamiento, el ciclo de vida de tal información, así como su finalidad.

La LFPDPPP como marco jurídico de las medidas de seguridad para la protección de datos personales contiene un Capítulo III titulado; “De las medidas de seguridad en el tratamiento de datos personales”, del Reglamento de la LFPDPPP (artículos 57 a 66), en donde se abarcan distintos aspectos relacionados con las medidas de seguridad, en los cuales destacan: la atenuación de sanciones por cumplir con recomendaciones emitidas por el INAI; las funciones de seguridad que pueden recaer en la empresa o en un tercero subcontratado; factores para determinar las medidas de seguridad, actualizaciones de las medidas de seguridad, así como vulneraciones de seguridad y notificación a los titulares cuyos datos personales hayan sido vulnerados.

Asimismo, es importante señalar que en complemento al tema que nos ocupa, el entonces Instituto Federal de Acceso a la Información y Protección de

26 El artículo 6 de la LFPDPPP señala que los principios de protección de datos personales son los siguientes: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

Datos emitió en octubre de 2013 las Recomendaciones en materia de seguridad de datos personales.[27]

Los distintos tipos de medidas de seguridad se desarrollan en el Reglamento de la LFPDPPP, conforme a los apartados subsecuentes.

2.2.1 Medidas de seguridad administrativas

Las medidas de seguridad administrativas se definen en el artículo 2, fracción V, del Reglamento de la LFPDPPP, de conformidad con lo siguiente:

> "Artículo 2. Además de las definiciones establecidas en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para los efectos del presente Reglamento se entenderá por:
> […]
> V. Medidas de seguridad administrativas: Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales;
> […]"

Las medidas de seguridad administrativas están enfocadas al aspecto organizacional o administrativo de las empresas, es decir, cómo las personas que dirigen o están al frente de las empresas planean, diseñan, adoptan e implementan medidas de seguridad a efecto de que todas las personas al interior de las empresas protejan los datos personales.

Este tipo de medidas de seguridad se caracterizan por tratarse del compromiso a nivel gerencial en las empresas en cuanto a la importancia de la

27 Instituto Federal de Acceso a la Información y Protección de Datos, *Recomendaciones en materia de seguridad de datos personales*, publicadas en el DOF el 30 de octubre de 2013. Disponibles en: *https://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013* (Fecha de consulta: 16 de febrero de 2020).

protección de información personal, como por ser las medidas de seguridad que se enfocan en el factor humano, de ahí que abarcan desde el establecimiento de mecanismos para brindar seguridad a los datos personales en toda la organización y la identificación y clasificación de información personal, hasta la capacitación y desarrollo de conocimientos para la protección de datos personales.

2.2.2 Medidas de seguridad físicas

Las medidas de seguridad físicas se definen en el artículo 2, fracción VI, del Reglamento de la LFPDPPP, de conformidad con lo siguiente:

> "Artículo 2. Además de las definiciones establecidas en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para los efectos del presente Reglamento se entenderá por:
> […]
> VI. Medidas de seguridad físicas: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:
> a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;
> b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;
> c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y
> d) Garantizar la eliminación de datos de forma segura;
> […]"

Las medidas de seguridad físicas están enfocadas en los controles de seguridad físicos y/o tecnológicos que tienen que adoptar e implementar las empresas para proteger el acceso a las áreas críticas de las empresas y a equipos en donde se almacenen datos personales, así como proteger los dispositivos móviles. Adicionalmente, se puede observar que se trata de controles de mantenimiento y soporte técnico a equipos de cómputo o dispositivos, así como de

herramientas que son necesarias para realizar un borrado seguro de información personal, como garantía de no recuperación.

2.2.3 Medidas de seguridad técnicas

Las medidas de seguridad técnicas se definen en el artículo 2, fracción VII, del Reglamento de la LFPDPPP, de conformidad con lo siguiente:

> "Artículo 2. Además de las definiciones establecidas en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para los efectos del presente Reglamento se entenderá por:
> […]
> VII. Medidas de seguridad técnicas: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:
> a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;
> b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
> c) Se incluyan acciones para la adquisición¸ operación, desarrollo y mantenimiento de sistemas seguros, y
> d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales;
> […]"

Las medidas de seguridad técnicas se distinguen por el uso de controles tecnológicos que tienen que adoptar e implementar las empresas para proteger la información de carácter personal, independientemente del dispositivo o solución tecnológica en donde se almacenen (equipos de cómputo, discos duros, bases de datos, portales web, entre otros). Este tipo de medidas se complementan con medidas de carácter administrativo u organizacional, ya que requieren ser implementadas al amparo de una política integral de seguridad de la información

que define, entre otros aspectos, quiénes pueden acceder a la información personal en posesión de las empresas, con qué atributos (lectura, escritura y/o copia) y para qué fines.

Asimismo, las medidas de seguridad técnicas también se encargan de adquirir, operar y desarrollar sistemas de información de datos personales seguros, que permiten la confidencialidad, seguridad, disponibilidad e integridad de la información, para lo cual requieren de monitoreo y soporte técnico continuo.

Hoy en día las medidas de seguridad técnicas constituyen el último candado en las empresas para proteger los datos personales en su posesión, después de las medidas de seguridad administrativas y físicas.

2.3 Sanciones por incumplimiento

La LFPDPPP establece un marco de infracciones y sanciones a las mismas cuando se contravengan sus disposiciones y si bien, de forma expresa no señala una sanción por incumplir con las medidas de seguridad, sí establece una sanción por incumplir con el principio de responsabilidad previsto en el artículo 6 de la LFPDPPP, principio que sustenta el deber ser de las medidas de seguridad para la protección de los datos personales.

En este sentido, las infracciones a la LFPDPPP relacionadas con la no adopción e implementación de las medidas de seguridad para la protección de información personal son principalmente las siguientes:

> "Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:
> […]
> IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;
> […]
> VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;

[…]

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;

[…]"

Las infracciones anteriores son sancionadas por el INAI con fundamento en el artículo 64 en los términos siguientes:

- Multa de 100 a 160,000 veces el valor diario de la UMA:[28] en los casos previstos en la fracción IV del artículo 63 de la LFPDPPP. Esta multa de conformidad con el valor diario de la UMA para 2020[29] asciende a las cantidades de $8,600.00 a $13,900,800.00.
- Multa de 200 a 320,000 veces el valor diario de la UMA: en los casos previstos en las fracciones VIII y XI del artículo 63 de la LFPDPPP. Esta multa de conformidad con el valor diario de la UMA para 2020 asciende a las cantidades de $17,376.00 a $27,801,600.00, y
- Multa adicional de 100 a 320,000 veces el valor diario de la UMA: en caso de que de manera reiterada persistan las infracciones y tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos. Esta multa de conformidad con el valor diario

28 De conformidad con el artículo tercero transitorio del Decreto por el que se declara reformadas y adicionadas diversas disposiciones de la CPEUM, en materia de desindexación del salario mínimo "[…] todas las menciones al salario mínimo como unidad de cuenta, índice, base, medida o referencia para determinar la cuantía de las obligaciones y supuestos previstos en las leyes federales, estatales, del Distrito Federal, así como en cualquier disposición jurídica que emane de todas las anteriores, se entenderán referidas a la Unidad de Medida y Actualización." Decreto publicado en el DOF el 27 de enero de 2016. Disponible en:
https://dof.gob.mx/nota_detalle.php?codigo=5423663&fecha=27/01/2016 (Fecha de consulta: 16 de febrero de 2020).

29 Valor de la Unidad de Medida y Actualización para 2020. Publicado en el DOF el 10 de enero de 2020. Disponible en: *http://www.dof.gob.mx/nota_detalle.php?codigo=5583733&fecha=10/01/2020* (Fecha de consulta: 16 de febrero de 2020).

de la UMA para 2020 asciende a las cantidades de $8,688.00 a $27,801,600.00.

Adicionalmente, es necesario destacar que, con fundamento en el artículo 66 de la LFPDPPP, las sanciones anteriores se impondrán sin perjuicio de la responsabilidad civil[30] o penal[31] que resulte.

Para concluir este apartado es menester señalar que, las empresas deben cumplir con su obligación de adoptar e implementar medidas de seguridad para la protección de información personal por su compromiso y lealtad hacia sus clientes o usuarios y personal. En caso de no hacerlo, las empresas tendrán que hacer frente a las sanciones de carácter económico que puede imponer el INAI, aunado de la responsabilidad civil y penal que pueda derivarse, así como los daños reputacionales y de posicionamiento en el mercado que puede generar una sanción de una autoridad.

Las empresas como en la que trabajo tienen una sola opción positiva para su posicionamiento en el mercado: cumplir con el derecho a la protección de datos personales mediante el diseño, adopción, implementación, monitoreo, evaluación y actualización de medidas de seguridad administrativas, técnicas y físicas para proteger los datos personales en su posesión.

Como es posible observar, a lo largo del presente capítulo se ha abordado la importancia de las medidas de seguridad para la protección de datos personales en las empresas, el marco normativo, tipos y características de dichas medidas, así como las sanciones por incumplir la obligación de adoptarlas.

En el siguiente capítulo se abordarán las medidas de seguridad para la protección de los datos personales en la Empresa.

---

30 De conformidad con lo previsto en el artículo 58 de la LFPDPPP, los titulares que consideren que han sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la LFPDPPP por el responsable o el encargado, podrán ejercer los derechos que estimen pertinentes para efectos de la indemnización que proceda, en términos de las disposiciones legales correspondientes.

31 Véanse los delitos en materia del tratamiento indebido de datos personales en los artículos 67, 68 y 69 de la LFPDPPP.

Capítulo 3

Medidas de seguridad en la Empresa

Capítulo 3: Medidas de seguridad en la Empresa

Para que cualquier empresa pueda proteger los datos personales en su posesión es importante conocer a detalle su modelo de negocio, así como todas y cada una de sus operaciones, áreas y funciones de su personal. Una empresa que no se conoce así misma se predispone a no proteger de manera efectiva los datos personales en su posesión.

3.1 Datos personales objeto de tratamiento

En la Empresa se recaban datos personales de las siguientes categorías:

- Internos: en esta categoría se incluyen datos personales de identificación, contacto, fiscales, laborales, académicos, de seguridad social, y experiencia laboral de empleados, y
- Externos: en esta categoría se incluyen datos personales de clientes, representantes legales y prestadores de servicios.

La información anterior es la que es objeto de protección mediante las medidas de seguridad de la Empresa.

3.2 Identificación de las medidas de seguridad

Del análisis a la normativa interna de la Empresa se han identificado diversas medidas de seguridad a efecto de proteger los datos personales que son objeto de tratamiento, las cuales se señalan y describen a continuación, de acuerdo con el tipo de medida:

Nombre	Descripción
Aviso de privacidad	Documento que se pone a disposición del titular de los datos personales previo al tratamiento de estos, con el que se da cumplimiento a lo ordenado por los artículos 15 y 16 de la LFPDPPP.

Cláusula laboral de confidencialidad	Esta cláusula está inserta en los contratos individuales de trabajo y tiene como finalidad hacer mención al trabajador de su obligación de mantener con carácter confidencial toda la información que con motivo de sus funciones conozca o llegare a conocer, lo cual incluye datos personales, obligación que se asienta con carácter permanente.
Cláusula de confidencialidad en contratos con terceros	En las relaciones comerciales de la Empresa con terceros que implican el acceso a datos personales en posesión de la Empresa por un tercero (remisión de datos personales a un encargado), en los contratos respectivos se incluye una cláusula de protección de datos personales que observa lo previsto en los artículos 19 y 21 de la LFPDPPP, y 51 de su Reglamento, así como lo previsto en el Aviso de Privacidad de la Empresa.
Capacitación de nuevo ingreso	Es una capacitación integral que tiene como finalidad integrar al personal de nuevo ingreso para que conozca a detalle todo lo que es la Empresa, misión, visión, modelo de negocio, principales actividades a desarrollar por la persona y sus obligaciones de confidencialidad de toda la información que conozca o llegare a conocer, incluida la información de carácter personal de los clientes, esto es, entre otra, sus datos personales.
Prohibición de utilizar equipos de cómputo y móviles personales	En la Empresa se tiene una política de asignar equipo de cómputo y de telefonía propiedad de la empresa, por lo que está prohibido que el personal interno utilice equipo de cómputo y teléfonos

	celulares personales, a efecto de evitar que sustraigan cualquier tipo de información de la Empresa, incluidos datos de carácter personal.
Prohibición de tomar fotografías o publicar fotografías del interior de la Empresa o de la información de la Empresa	En la Empresa se tiene una política de no tomar fotografías o publicar fotografías de las instalaciones de la Empresa o de su información, a efecto de evitar la divulgación de cualquier tipo de información, incluidos datos personales.

Cuadro 1. Medidas de Seguridad Administrativas en la Empresa
Fuente: Elaboración propia.

Nombre	Descripción
Cerraduras en puertas de acceso al domicilio	Las puertas de acceso al domicilio de la Empresa cuentan con cerraduras, los cuales son mecanismos de metal para cerrar con llave las puertas de acceso, con lo cual se impide el acceso a personal no autorizado al interior del domicilio donde se encuentra la información en posesión de la Empresa, incluidos los datos personales.
Alarma	El domicilio de la Empresa cuenta con un sistema electrónico de alarma contratada con un proveedor. Esta medida de seguridad constituye un mecanismo de seguridad adicional que avisa a cierto personal de la Empresa si una persona accede sin estar autorizada para ello, así como a personal de seguridad del proveedor. El sistema de alarma se activa y desactiva con un nombre de usuario y contraseña.
Cámaras de videovigilancia	Las instalaciones de la Empresa cuentan con un sistema de cámaras de videovigilancia que monitorean la actividad del domicilio de la

	empresa, tanto a las afueras como al interior. Con este sistema es posible vigilar la actividad al interior de la organización.

Cuadro 2. Medidas de Seguridad Físicas en la Empresa
Fuente: Elaboración propia.

Nombre	Descripción
Contraseñas en equipos de cómputo	Los equipos de cómputo con los que cuenta la Empresa están protegidos con contraseñas impuestas por cada colaborador, quienes las resguardan con carácter confidencial.
Contraseñas para bases de datos y carpetas virtuales compartidas	Las bases de datos y carpetas virtuales compartidas con información personal de clientes y personal interno están protegidas con contraseñas, aunado a que solo pueden acceder a ellas personal previamente autorizado con motivo de sus funciones al interior de la Empresa.
Acceso a la red de Internet a personal autorizado	La red de Internet de la Empresa solo se permite su acceso a personal interno y a aquel previamente autorizado.

Cuadro 3. Medidas de Seguridad Técnicas en la Empresa
Fuente: Elaboración propia.

3.3 Adición de nuevas medidas de seguridad

En la Empresa se realizó un análisis de lo dispuesto en el Capítulo 1 y 2 de la presente Solución Estratégica Empresarial así como de lo dispuesto en los artículos 60, 61 y 62 del Reglamento de la LFPDPPP, del cual se desprendió que, si bien se tienen diversas medidas de seguridad administrativas, físicas y técnicas las cuales son adecuadas y necesarias para la protección de cualquier tipo de información, incluidos datos personales, es necesario fortalecer las mismas con la adopción e implementación de medidas de seguridad adicionales a efecto de incrementar la protección de información personal en posesión de la Empresa.

Por tanto, en la Empresa se adicionan para su implementación de forma inmediata las siguientes nuevas medidas de seguridad:

Nombre	Descripción
Análisis de riesgos	Se adopta la política de implementar análisis de riesgos en la Empresa con relación a los datos personales en su posesión, a efecto de conocer los mismos, sus alcances, medidas que sean necesarias para mitigarlos, entre otras cuestiones. Se adoptará como marco de referencia la "Metodología de Análisis de Riesgo BAA" emitida por el INAI.[32]
Cláusula de borrado seguro de información en contratos con terceros	En las relaciones comerciales de la Empresa con terceros que implican el tratamiento de datos personales en posesión de la Empresa por un tercero (remisión de datos personales a un encargado), se incluirá de forma obligatoria en todos los contratos una cláusula de borrado seguro de la información cuando así sea procedente, para lo cual se pondrá como referencia la "Guía para el Borrado Seguro de Datos Personales" emitida por el INAI.[33]
Responsabilidad laboral	Se adiciona a los contratos individuales de trabajo la responsabilidad de los trabajadores en la observación de las medidas de seguridad para la

32 Véase en: Metodología de Análisis de Riesgo BAA. INAI, México, 2015. Disponible en: *http://inicio.inai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf* (Fecha de consulta: 20 de febrero de 2020).

33 Véase en: Guía para el Borrado Seguro de Datos Personales. INAI, México, 2016. Disponible en: *http://inicio.inai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf* (Fecha de consulta: 20 de febrero de 2020).

	protección de información de la Empresa incluidos datos personales, cuya inobservancia y/o violación traerá como consecuencia la rescisión de la relación laboral.
Prohibición de medios de almacenamiento personales	Se adopta la política de no uso de medios de almacenamiento (USB y/o discos duros) personales para información de la Empresa, además de restringir los puertos de manera lógica en los equipos informáticos, para lo cual la Empresa asignará, en su caso, los medios encriptados de almacenamiento necesarios al personal que con motivo de sus funciones tenga que hacer uso de esto.
Autorización para la descarga e instalación de software	Se adopta la política de previa autorización para la descarga e instalación de software en los equipos de cómputo y dispositivos móviles de los colaboradores de la Empresa, con lo cual se evitará la descarga de software malicioso que comprometa la información de la Empresa, incluida la información de carácter personal.
Elaboración de documentación responsiva sobre equipos de cómputo y su uso	Se implementará la elaboración de documentación responsiva sobre la asignación de equipos de cómputo y su uso, con la cual se busca identificar de forma clara qué equipo de cómputo se asigna a determinado colaborador, en qué estado (nuevo o usado) y su responsabilidad de devolverlo en buenas condiciones, así como de reportar cualquier tipo de falla, robo y/o extravío y las responsabilidades y prohibiciones en su uso.
Capacitación en seguridad de la información y	Se implementará una capacitación sobre seguridad de la información y protección de datos

protección de datos personales	personales de carácter obligatoria y permanente para todos los colaboradores de la Empresa que abarcará al menos el contenido de la presente Solución Estratégica Empresarial.
Autorización para la extracción de equipos de cómputo	Se adopta la política de no sacar los equipos de cómputo fuera de las instalaciones de la Empresa, con las excepciones previamente autorizadas en razón del perfil o solicitudes previas de autorización.
Auditorías sorpresa	Se adopta la política de auditorías sorpresa a efecto de revisar que las áreas competentes y los colaboradores de la Empresa observen en todo momento las medidas de seguridad previstas en el presente documento. El factor sorpresa será un elemento disuasivo en la inobservancia de las políticas de seguridad de la Empresa.
Cultura de seguridad de la información	Se adopta la política de creación de una cultura de seguridad de la información a cargo del área de TI, la cual se encargará de difundir a través de trípticos y correo electrónico institucional las medidas de seguridad para la protección de información, incluida la protección de los datos personales.
Revisión anual de las medidas de seguridad	Se adopta la política de revisión anual con carácter obligatorio de las medidas de seguridad administrativas, técnicas y físicas de la Empresa para la protección de cualquier tipo de información, incluidos datos personales. Esta revisión podrá ser a cargo de personal interno de la Empresa o de una compañía externa.

Cuadro 4. Nuevas Medidas de Seguridad Administrativas en la Empresa
Fuente: Elaboración propia.

Nombre	Descripción
Identificación y documentación del personal con accesos a los controles de seguridad físicos de la Empresa	Se identificará y documentará el personal con accesos a los controles de seguridad físicos a la Empresa (incluye al personal con llaves a las instalaciones, control de alarma y del sistema de videovigilancia). Con esta medida se podrá conocer y determinar quiénes pueden tener acceso a las instalaciones de la Empresa en caso de cualquier contingencia de robo o sustracción de información.
Eliminación de información en papel con máquinas trituradoras	Se adopta la política de eliminación de información soportada en papel únicamente a través de máquinas trituradoras, para lo cual la Empresa hará la adquisición de las mismas.
Mantenimiento preventivo	Se adopta la política a cargo del área de TI de brindar un mantenimiento preventivo al menos cada 3 meses a todos los equipos de cómputo de todos los colaboradores de la Empresa.
Borrado seguro de información en equipos de cómputo y portátiles	Se adopta la política de borrado seguro de la información contenida en equipos de cómputo, teléfonos celulares y tabletas cuando las mismas sean cambiadas o renovadas al personal, con lo cual se garantiza la eliminación de información en tales dispositivos una vez que dejan de ser utilizados al interior de la Empresa, y a su vez se evita la fuga de cualquier tipo de información, incluidos datos personales. Se adoptará como referencia la “Guía para el Borrado Seguro de Datos Personales” emitida por el INAI.

Cuadro 5. Nuevas Medidas de Seguridad Físicas en la Empresa
Fuente: Elaboración propia.

Nombre	Descripción
Prohibición de modificación a la configuración de equipos de cómputo y dispositivos móviles	Se adopta la política de prohibición expresa de la modificación a la configuración de equipos de cómputo y dispositivos móviles, por lo que se deberá respetar la configuración corporativa a cargo del Área de TI.
Análisis automático de antivirus	Se adopta la política de análisis automático de antivirus en todos los equipos de cómputo de la Empresa.
Respaldos de información	Se adopta la política de respaldos periódicos de información almacenada en los equipos de cómputo de la Empresa a cargo del Área de TI.
Accesos no autorizados	Se adopta la política de notificaciones a la Dirección General de la Empresa de usuarios que deseen acceder a recursos no autorizados.

Cuadro 6. Nuevas Medidas de Seguridad Técnicas en la Empresa
Fuente: Elaboración propia.

Como se puede apreciar, derivado de la revisión y análisis de las medidas de seguridad administrativas, técnicas y físicas de la Empresa vigentes se pudo observar que es necesario la adopción de nuevas medidas de seguridad adicionales para fortalecer los controles de seguridad actuales, con los cuales se busca erradicar comportamientos por acción u omisión, intencionales o no, que puedan poner en riesgo los datos personales en posesión de la Empresa.

Finalmente, para efecto de concentrar en un solo apartado, como anexo único a la presente Solución Estratégica Empresarial, se integran todas las medidas de seguridad administrativas, técnicas y físicas de la Empresa, que constituyen la suma de las medidas de seguridad para la protección de datos personales en posesión de las empresas en México, identificadas en los apartados 3.2 y 3.3 del presente trabajo.

Conclusiones

Conclusiones

La protección de datos personales en México es un derecho humano protegido por la CPEUM en su artículo 16, párrafo segundo, con el cual se protege el derecho a la autodeterminación informativa de las personas. Todas las personas físicas y morales de carácter privado, incluso las instituciones públicas, tienen la obligación de respetar, garantizar, proteger y hacer efectivo tal derecho, con el cual, a su vez, se protege la privacidad de las personas, derecho que comienza a ser estudiado e interpretado por la Suprema Corte de Justicia de la Nación, de ahí su relevancia y pertinencia en el sistema jurídico mexicano.

Los datos personales, como objeto de protección de este citado derecho, son información con un valor económico en el mercado, tanto para los que utilizan tal información de forma legítima, como para aquellos que la adquieren de forma ilegal. En México y en cualquier parte del mundo se aspira a proteger los datos personales por ser el combustible del comercio electrónico, la publicidad y le economía digital.

Esta protección de datos personales no puede hacerse realidad sin medidas de seguridad administrativas, técnicas y físicas, son estas medidas o controles los que permiten en estricto sentido proteger los datos personales.

En la Empresa se protegen los datos personales, no solo por su obligación legal derivada de la LFPDPP analizada en los Capítulos 1 y 2, sino porque conoce y comprende lo importante que es para las personas su información que los identifica o los hace identificables y los riesgos que se pueden derivar de un mal uso, robo, divulgación y/o daño. Riesgos que son tanto de carácter interno como externos tal como se abordó en el apartado 1.3 de este trabajo, riesgos que se maximizan con motivo del imparable desarrollo y dependencia tecnológica.

En este sentido, la identificación y análisis de las medidas de seguridad de la Empresa, que se realizaron en el apartado 3.2 de este trabajo, ha sido de una relevancia y utilidad invaluables, ya que fue posible conocer qué mecanismos se han tenido para proteger los datos personales en su posesión; es decir, responde a la pregunta ¿qué medidas de seguridad tiene la Empresa?, lo cual, a su vez, originó los siguientes cuestionamientos ¿son suficientes las medidas de seguridad actuales

para proteger los datos personales? ¿hacen falta medidas adicionales? Las respuestas a tales preguntas fueron: no y sí, respectivamente, originando una nueva serie de medidas de seguridad adicionales que buscan fortalecer las actuales y subsanar áreas de oportunidad que no se tenían identificadas.

Estas nuevas medidas de seguridad en la Empresa tienen como finalidad no dejar huecos que pongan en riesgo la protección de datos personales en su posesión, desde la implementación de análisis de riesgos, uso de técnicas de borrado seguro, responsabilidades laborales para los colaboradores, control de medios de almacenamiento de información y auditorías sorpresa, hasta la revisión anual obligatoria de las medidas de seguridad, la capacitación constante en seguridad de la información, respaldos periódicos de información y cláusulas contractuales en relaciones con terceros, entre otros.

Por tanto, en el presente trabajo, como Solución Estratégica Empresarial, se comprueba que, al revisarse periódicamente las medidas de seguridad de la Empresa es posible identificar áreas de oportunidad que permiten la adopción e implementación de nuevas medidas de seguridad para proteger de mejor manera los datos personales en su posesión, mejorando con ello, a su vez, el cumplimiento del marco normativo aplicable, consistente en: la CPEUM, la LFPDPPP y su Reglamento.

Bibliografía

ÁLVAREZ, Clara Luz, *Internet y derechos fundamentales*, México, Porrúa, 2011.

BANK INFO SECURITY, "*Heartland Hacker Sentenced to 20 Years*", 26 de marzo de 2010. https://www.bankinfosecurity.com

CNNExpansión, "*eBay es víctima de ataque cibernético*", 21 mayo 2014. https://expansion.mx

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

CORPUS IURIS en materia de Protección de Datos Personales. Red Iberoamericana de Protección de Datos-INAI. Disponible en: *http://corpusiurispdp.inai.org.mx/Pages/home.aspx*

DECRETO por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Publicado en el DOF el primero de junio de 2009. Disponible en: *http://www.dof.gob.mx/avisos/1889/SG_010609/SG_010609.htm*

DECRETO por el que se declara reformadas y adicionadas diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de desindexación del salario mínimo. Publicado en el DOF el 27 de enero de 2016.

DECRETO por el que se reforman y adicionan diversas disposiciones de la CPEUM, en materia de transparencia. Publicada en el DOF el 07 de febrero de 2014.

GUÍA PARA EL BORRADO SEGURO DE DATOS PERSONALES. INAI, México, 2016. Disponible en: *http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf*

INAI. *Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas. México, junio 2015. Disponible en: http://inicio.ifai.org.mx/nuevo/Manual%20seguridad%20MIPYMES.pdf*

LAUDON, Kenneth, y LAUDON, Jane, *Sistemas de información gerencial*, Decimocuarta edición, Pearson Educación, México, 2016.

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

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS.

LÓPEZ TORRES, Jonathan. La Constitución y la protección de datos personales en México: las inconsistencias en el esquema de excepciones". Revista Tohil de la Facultad de Derecho de la Universidad Autónoma de Yucatán. ISSN 2007-6673, año 16, número 38, enero-junio 2016.

MÉJAN CARRER, Luis Manuel Camp, *El Derecho a la intimidad y la informática*, México, editorial Porrúa, México, 1996.

METODOLOGÍA DE ANÁLISIS DE RIESGO BAA. INAI, México, 2015. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf

NUÑEZ ORNELAS, Lina, y PIÑAR MAÑAS, José Luis, *La protección de datos personales en México*, Tirant lo Blanch, México, 2013.

PIÑAR MAÑAS, José Luis, y RECIO GAYO, Miguel, *Código de Protección de Datos Personales México*, Tirant lo Blanch, México, 2013.

PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO. Tesis: I.10o.A.5 CS (10a.), Semanario Judicial de la Federación, Época: Décima Época, t. III, septiembre de 2019, p. 2199.

PROTECCIÓN DE DATOS PERSONALES. EL DEBER DEL ESTADO DE SALVAGUARDAR EL DERECHO HUMANO RELATIVO DEBE POTENCIALIZARSE ANTE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS, DEBIDO A LOS RIESGOS QUE ÉSTAS REPRESENTAN POR SUS CARACTERÍSTICAS. Tesis: I.10o.A.6 CS (10a.), Semanario Judicial de la Federación, Décima Época, tomo III, septiembre de 2019, p. 2200.

RECONOCIMIENTO DE PATERNIDAD. LA ORDEN DE GIRAR OFICIO PARA CONOCER LOS BIENES E INGRESOS DEL DEMANDADO EN EL JUICIO RELATIVO VULNERA SU DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, SI NO SE HA DEMOSTRADO LA FILIACIÓN ENTRE LAS PARTES PARA TENER DERECHO A RECIBIR ALIMENTOS (INAPLICABILIDAD DEL ARTÍCULO 563 DEL CÓDIGO PROCESAL CIVIL DEL ESTADO DE GUERRERO). Tesis: XXI.3o.C.T.11 C (10a.), *Semanario Judicial de la Federación*, Décima Época, t. III, febrero de 2020, p. 2399.

RECOMENDACIONES EN MATERIA DE SEGURIDAD DE DATOS PERSONALES. Publicadas en el DOF el 30 de octubre de 2013. Disponible en: *https://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013*

REGLAMENTO DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES.

VALOR DE LA UNIDAD DE MEDIDA Y ACTUALIZACIÓN PARA 2020. Publicado en el DOF el 10 de enero de 2020. Disponible en: *http://www.dof.gob.mx/nota_detalle.php?codigo=5583733&fecha=10/01/2020#:~:text=Con%20base%20en%20lo%20anterior,del%201o.%20de%20febrero*

THE GUARDIAN, “PlayStation Network hackers access data of 77 million users”, 26 de Abril de 2011. https://www.theguardian.com

ANEXO

ANEXOS

ANEXO I. Medidas de Seguridad en la Empresa

Medidas de Seguridad Administrativas	
Nombre	**Descripción**
Aviso de privacidad	Documento que se pone a disposición del titular de los datos personales previo al tratamiento de estos, con el que se da cumplimiento a lo ordenado por los artículos 15 y 16 de la LFPDPPP.
Cláusula laboral de confidencialidad	Esta cláusula está inserta en los contratos individuales de trabajo y tiene como finalidad hacer mención al trabajador de su obligación de mantener con carácter confidencial toda la información que con motivo de sus funciones conozca o llegare a conocer, lo cual incluye datos personales, obligación que se asienta con carácter permanente.
Cláusula de confidencialidad en contratos con terceros	En las relaciones comerciales de la Empresa con terceros que implican el acceso a datos personales en posesión de la Empresa por un tercero (remisión de datos personales a un encargado), en los contratos respectivos se incluye una cláusula de protección de datos personales que observa lo previsto en los artículos 19 y 21 de la LFPDPPP, y 51 de su Reglamento, así como lo previsto en el Aviso de Privacidad de la Empresa.
Capacitación de nuevo ingreso	Es una capacitación integral que tiene como finalidad integrar al personal de nuevo ingreso para que conozca a detalle todo lo que es la Empresa, misión, visión, modelo de negocio, principales actividades a desarrollar por la persona y sus obligaciones de

	confidencialidad de toda la información que conozca o llegare a conocer, incluida la información de carácter personal de los clientes, esto es, entre otra, sus datos personales.
Prohibición de utilizar equipos de cómputo y móviles personales	En la Empresa se tiene una política de asignar equipo de cómputo y de telefonía propiedad de la empresa, por lo que está prohibido que el personal interno utilice equipo de cómputo y teléfonos celulares personales, a efecto de evitar que sustraigan cualquier tipo de información de la Empresa, incluidos datos de carácter personal.
Prohibición de tomar fotografías o publicar fotografías del interior de la Empresa o de la información de la Empresa	En la Empresa se tiene una política de no tomar fotografías o publicar fotografías de las instalaciones de la Empresa o de su información, a efecto de evitar la divulgación de cualquier tipo de información, incluidos datos personales.
Análisis de riesgos	Se adopta la política de implementar análisis de riesgos en la Empresa con relación a los datos personales en su posesión, a efecto de conocer los mismos, sus alcances, medidas que sean necesarias para mitigarlos, entre otras cuestiones. Se adoptará como marco de referencia la "Metodología de Análisis de Riesgo BAA" emitida por el INAI.[34]
Cláusula de borrado seguro de información en contratos con terceros	En las relaciones comerciales de la Empresa con terceros que implican el tratamiento de datos personales en posesión de la Empresa por un tercero (remisión de datos personales a un encargado), se incluirá de forma obligatoria en todos los contratos

34 Véase en: Metodología de Análisis de Riesgo BAA. INAI, México, 2015. Disponible en: *http://inicio.inai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf* (Fecha de consulta: 20 de febrero de 2020).

	una cláusula de borrado seguro de la información cuando así sea procedente, para lo cual se pondrá como referencia la "Guía para el Borrado Seguro de Datos Personales" emitida por el INAI.[35]
Responsabilidad laboral	Se adiciona a los contratos individuales de trabajo la responsabilidad de los trabajadores en la observación de las medidas de seguridad para la protección de información de la Empresa incluidos datos personales, cuya inobservancia y/o violación traerá como consecuencia la rescisión de la relación laboral.
Prohibición de medios de almacenamiento personales	Se adopta la política de no uso de medios de almacenamiento (USB y/o discos duros) personales para información de la Empresa, para lo cual la Empresa asignará tales medios de almacenamiento al personal que con motivo de sus funciones tenga que hacer uso de tales medios de almacenamiento.
Autorización para la descarga e instalación de software	Se adopta la política de previa autorización para la descarga e instalación de software en los equipos de cómputo y dispositivos móviles de los colaboradores de la Empresa, con lo cual se evitará la descarga de software malicioso que comprometa la información de la Empresa, incluida la información de carácter personal.
Elaboración de documentación responsiva sobre equipos de cómputo y su uso	Se implementará la elaboración de documentación responsiva sobre la asignación de equipos de cómputo y su uso, con la cual se busca identificar de forma clara qué equipo de cómputo se asigna a

35 Véase en: Guía para el Borrado Seguro de Datos Personales. INAI, México, 2016. Disponible en: *http://inicio.inai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf* (Fecha de consulta: 20 de febrero de 2020).

	determinado colaborador, en qué estado (nuevo o usado) y su responsabilidad de devolverlo en buenas condiciones, así como de reportar cualquier tipo de falla, robo y/o extravío y las responsabilidades y prohibiciones en su uso.
Capacitación en seguridad de la información y protección de datos personales	Se implementará una capacitación sobre seguridad de la información y protección de datos personales de carácter obligatoria y permanente para todos los colaboradores de la Empresa que abarcará al menos el contenido de la presente Solución Estratégica Empresarial.
Autorización para la extracción de equipos de cómputo	Se adopta la política de no sacar los equipos de cómputo fuera de las instalaciones de la Empresa, con las excepciones previamente autorizadas en razón del perfil o solicitudes previas de autorización.
Auditorías sorpresa	Se adopta la política de auditorías sorpresa a efecto de revisar que las áreas competentes y los colaboradores de la Empresa observen en todo momento las medidas de seguridad previstas en el presente documento. El factor sorpresa será un elemento disuasivo en la inobservancia de las políticas de seguridad de la Empresa.
Cultura de seguridad de la información	Se adopta la política de creación de una cultura de seguridad de la información a cargo del área de TI, la cual se encargará de difundir a través de trípticos y correo electrónico institucional las medidas de seguridad para la protección de información, incluida la protección de los datos personales.
Revisión anual de las medidas de seguridad	Se adopta la política de revisión anual con carácter obligatorio de las medidas de seguridad administrativas, técnicas y físicas de la Empresa

	para la protección de cualquier tipo de información, incluidos datos personales. Esta revisión podrá ser a cargo de personal interno de la Empresa o de una compañía externa.

Medidas de Seguridad Físicas	
Nombre	**Descripción**
Cerraduras en puertas de acceso al domicilio	Las puertas de acceso al domicilio de la Empresa cuentan con cerraduras, los cuales son mecanismos de metal para cerrar con llave las puertas de acceso, con lo cual se impide el acceso a personal no autorizado al interior del domicilio donde se encuentra la información en posesión de la Empresa, incluidos los datos personales.
Alarma	El domicilio de la Empresa cuenta con un sistema electrónico de alarma contratada con un proveedor. Esta medida de seguridad constituye un mecanismo de seguridad adicional que avisa a cierto personal de la Empresa si una persona accede sin estar autorizada para ello, así como a personal de seguridad del proveedor. El sistema de alarma se activa y desactiva con un nombre de usuario y contraseña.
Cámaras de videovigilancia	Las instalaciones de la Empresa cuentan con un sistema de cámaras de videovigilancia que monitorean la actividad del domicilio de la empresa, tanto a las afueras como al interior. Con este sistema es posible vigilar la actividad al interior de la organización.
Identificación y documentación del	Se identificará y documentará el personal con accesos a los controles de seguridad físicos a la

personal con accesos a los controles de seguridad físicos de la Empresa	Empresa (incluye al personal con llaves a las instalaciones, control de alarma y del sistema de videovigilancia). Con esta medida se podrá conocer y determinar quiénes pueden tener acceso a las instalaciones de la Empresa en caso de cualquier contingencia de robo o sustracción de información.
Eliminación de información en papel con máquinas trituradoras	Se adopta la política de eliminación de información soportada en papel únicamente a través de máquinas trituradoras, para lo cual la Empresa hará la adquisición de las mismas.
Mantenimiento preventivo	Se adopta la política a cargo del área de TI de brindar un mantenimiento preventivo al menos cada 3 meses a todos los equipos de cómputo de todos los colaboradores de la Empresa.
Borrado seguro de información en equipos de cómputo y portátiles	Se adopta la política de borrado seguro de la información contenida en equipos de cómputo, teléfonos celulares y tabletas cuando las mismas sean cambiadas o renovadas al personal, con lo cual se garantiza la eliminación de información en tales dispositivos una vez que dejan de ser utilizados al interior de la Empresa, y a su vez se evita la fuga de cualquier tipo de información, incluidos datos personales. Se adoptará como referencia la “Guía para el Borrado Seguro de Datos Personales” emitida por el INAI.

Medidas de Seguridad Técnicas	
Nombre	**Descripción**
Contraseñas en equipos de cómputo	Los equipos de cómputo con los que cuenta la Empresa están protegidos con contraseñas

	impuestas por cada colaborador, quienes las resguardan con carácter confidencial.
Contraseñas para bases de datos y carpetas virtuales compartidas	Las bases de datos y carpetas virtuales compartidas con información personal de clientes y personal interno están protegidas con contraseñas, aunado a que solo pueden acceder a ellas personal previamente autorizado con motivo de sus funciones al interior de la Empresa.
Acceso a la red de Internet a personal autorizado	La red de Internet de la Empresa solo se permite su acceso a personal interno y a aquel previamente autorizado.
Prohibición de modificación a la configuración de equipos de cómputo y dispositivos móviles	Se adopta la política de prohibición expresa de la modificación a la configuración de equipos de cómputo y dispositivos móviles, por lo que se deberá respetar la configuración corporativa a cargo del Área de TI.
Análisis automático de antivirus	Se adopta la política de análisis automático de antivirus en todos los equipos de cómputo de la Empresa.
Respaldos de información	Se adopta la política de respaldos periódicos de información almacenada en los equipos de cómputo de la Empresa a cargo del Área de TI.
Accesos no autorizados	Se adopta la política de notificaciones a la Dirección General de la Empresa de usuarios que deseen acceder a recursos no autorizados.

Cuadro 7. Medidas de Seguridad en la Empresa
Fuente: Elaboración propia.