Deloitte.

Termómetro:
Privacidad y Protección de datos en México 2014

Segunda Edición

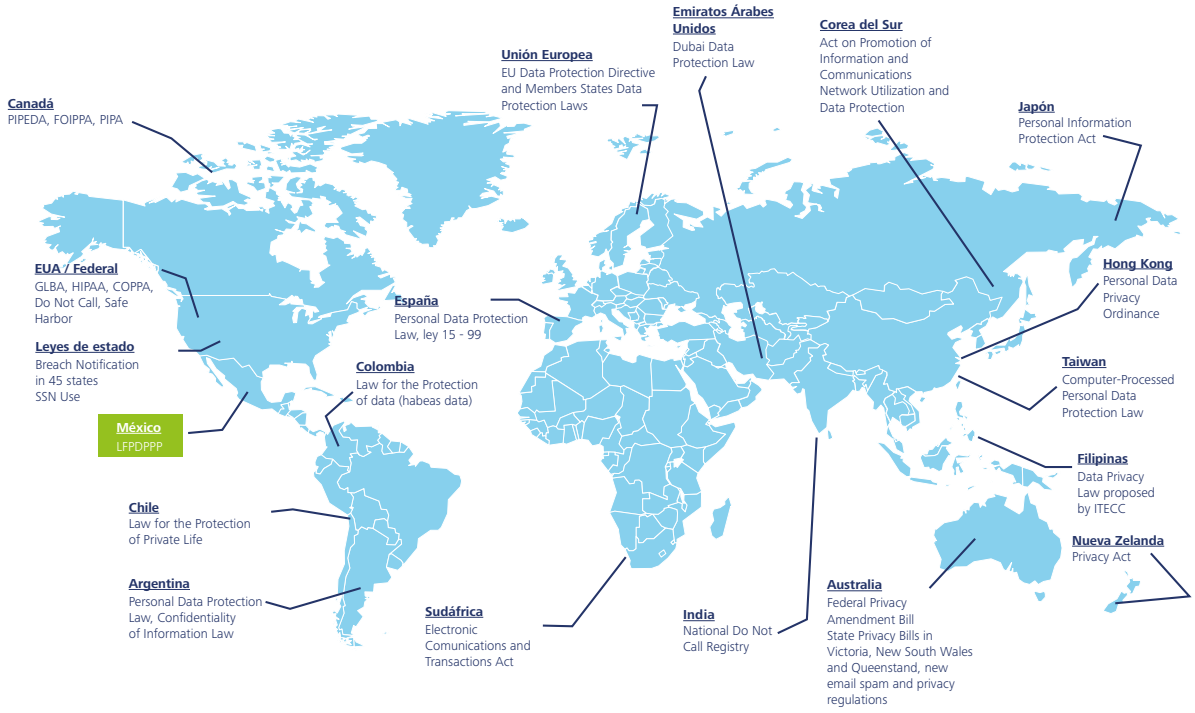
Índice

Introducción

México no es el único país en el mundo que debe velar por la salvaguarda e integridad de los datos personales. En diferentes países alrededor del mundo se han promulgado leyes de protección de datos personales, las cuales han sido adecuadas a las necesidades culturales, económicas y políticas de cada país. De esta manera, observamos la existencia de diferentes regulaciones que han sido pioneras en la protección de datos personales y que sirven de ejemplo para nuestro país. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en México fue publicada el 5 de julio del 2010 y entró en vigor al siguiente día. A nivel mundial, existen alrededor de 99 países que cuentan con leyes de protección de datos personales, algunos de ellos se mencionan a continuación:

- Alemania, que en 1970 aprobó la primera ley de protección de datos.
- Suecia, aprobó su ley en 1973 (Personal Data Act 1998:2004).
- Estados Unidos de Norteamérica, donde la protección de datos tiene base en la Privacy Act de 1974. Existen varias regulaciones GLBA, HIPPA, COPA, Do not call y Safe Harbor.
- España, aprobó su Ley Orgánica de Protección de Datos 15, en 1999.
- Rusia, aprobó su ley en 2006.
- Canadá, aprobó su ley en 2000 (PIPEDA, FOIPPA, PIPA).

Leyes de protección de datos personales en el mundo



En el caso de países Latinoamericanos identificamos que algunas de las leyes que han sido adaptadas se asemejan al modelo Europeo, entre ellas encontramos:

Para el caso de la ley mexicana, se asemeja más al modelo español y canadiense.

Protección de Datos Personales en el Mundo

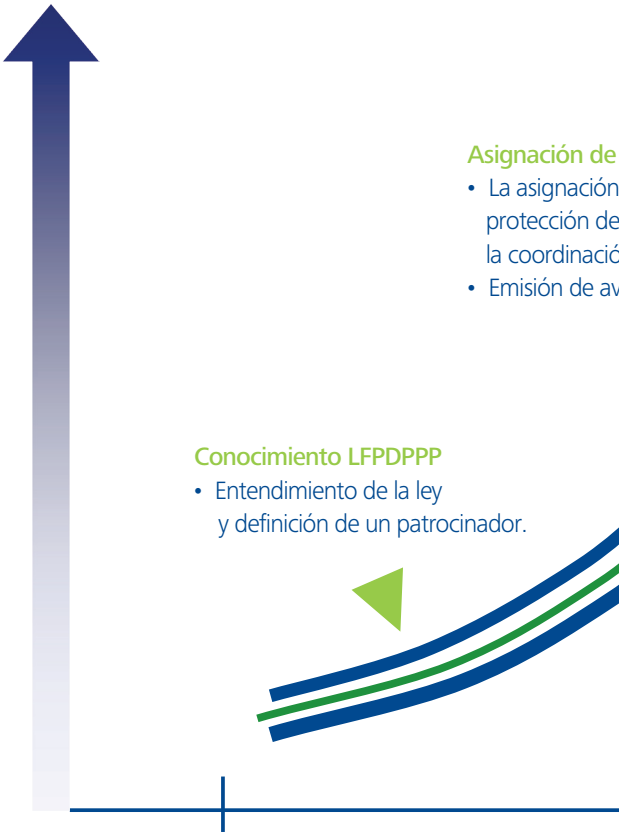
Contexto regional

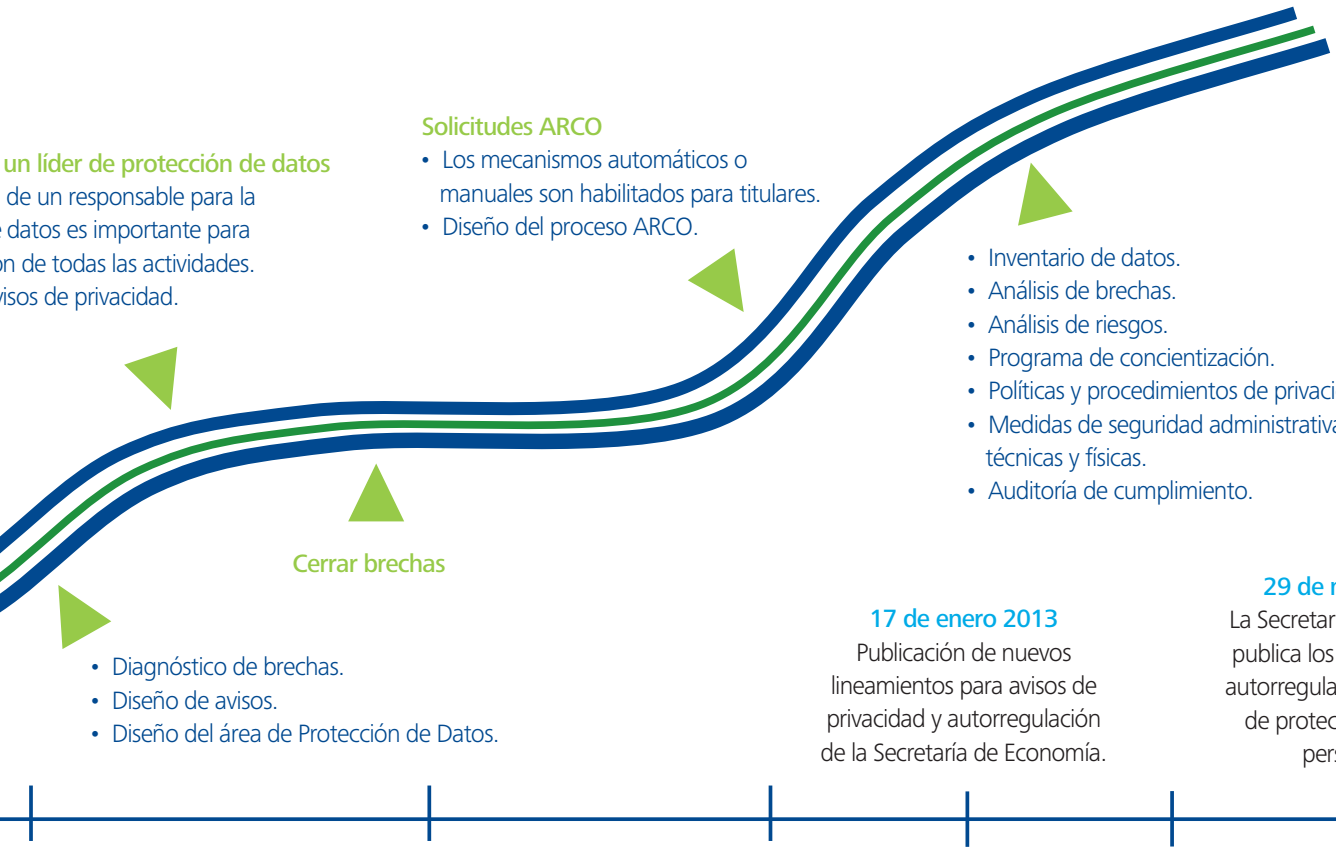
A la fecha, todos los plazos de cumplimiento con la LFPDPPP se encuentran vencidos, por lo que es de vital importancia que las empresas realicen un diagnóstico de avances y cumplimientos en el proceso de adopción de la LFPDPPP que les permita brindar certidumbre a sus clientes, proveedores y empleados respecto al manejo de los datos personales con que cuenta la organización; además de evitar posibles sanciones por incumplimientos a la misma.

Con esto en mente se plantearon tres objetivos para este estudio:

- Identificar el nivel de cumplimiento con la LFPDPPP en el mercado mexicano, considerando los aspectos técnicos, organizacionales, operativos y legales.
- Conocer la existencia de incidentes de fuga o pérdida de datos personales en las empresas encuestadas.
- Conocer las prácticas de seguridad para la privacidad y protección de la información utilizadas en el mercado mexicano.

Fechas de cumplimiento de la LFPDPPP





un líder de protección de datos
de un responsable para la
e datos es importante para
ón de todas las actividades.
visos de privacidad.

Solicitudes ARCO
- Los mecanismos automáticos o manuales son habilitados para titulares.
- Diseño del proceso ARCO.

- Inventario de datos.
- Análisis de brechas.
- Análisis de riesgos.
- Programa de concientización.
- Políticas y procedimientos de privacidad.
- Medidas de seguridad administrativas, técnicas y físicas.
- Auditoría de cumplimiento.

Cerrar brechas

- Diagnóstico de brechas.
- Diseño de avisos.
- Diseño del área de Protección de Datos.

17 de enero 2013
Publicación de nuevos lineamientos para avisos de privacidad y autorregulación de la Secretaría de Economía.

29 de mayo 2014
La Secretaría de Economía publica los parámetros de autorregulación en materia de protección de datos personales.

lio de 2011
ón de persona
mento de datos
es y avisos de
l a los titulares.

21 de diciembre de 2011
Publicación del reglamento.

6 de enero de 2012
Ejercicio de derechos ARCO.
Inicia el procedimiento de protección de derechos.

22 de junio 2013
diseñar e implementar las medidas de seguridad administrativas, técnicas y físicas.

Metodología y perfil de los participantes

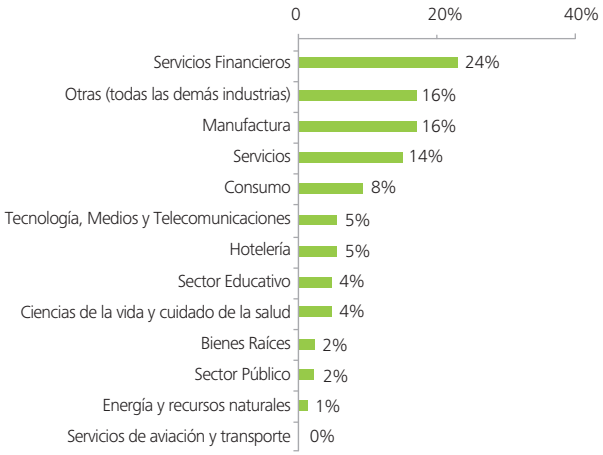
Cuestionario	Universo	Proceso de levantamiento	Participantes
• Cuestionario con una duración de 20 minutos para aplicación telefónica y electrónica	• Directores de Auditoría interna y/o Riesgos, Directores de Tecnología, Directores de Finanzas, Directores de áreas legales • Multi-industrias • Nacional	• Periodo de levantamiento de información: 12 de marzo al 3 de abril de 2014 Aplicación multicanal. Medios utilizados: › Correo electrónico › Telemarketing › Redes sociales	• 169 ejecutivos de alto nivel (siendo éste el universo utilizado para las gráficas)

Nota: Las respuestas a los temas tratados en este estudio pueden no representar la suma del 100 por ciento, debido al redondeo de decimales al momento de elaborar las gráficas.

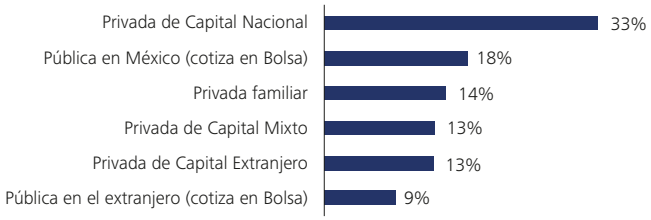
Perfil de los participantes

El perfil de empresa predominante en la encuesta fue el de **servicios financieros,** representados en la gráfica con un 24% del total. El 33% de las empresas participantes son **privadas de capital nacional,** seguidas por empresas que cotizan en la BMV (18%), las empresas públicas o privadas extranjeras son los perfiles con una menor participación.

Industria

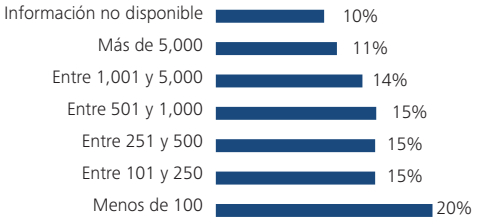


Tipo de empresa

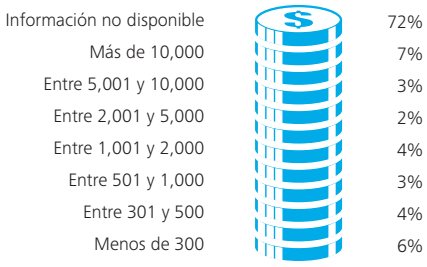


Resulta importante destacar del perfil de las organizaciones, que el 59% es representado por la suma de las barras que van desde 101 hasta 5,000 empleados, con lo cual podemos determinar que la mayor participación se obtuvo de empresas que por su volumen de empleados, consideraríamos como grandes. Por otro lado, el 72% de los participantes no proporcionó la cantidad de sus ingresos; del 28% que lo proporcionó, el 7% tiene ingresos mayores de 10,001 millones de pesos y el 6% cuenta con ingresos menores de 300 millones de pesos, siendo estos dos perfiles los predominantes.

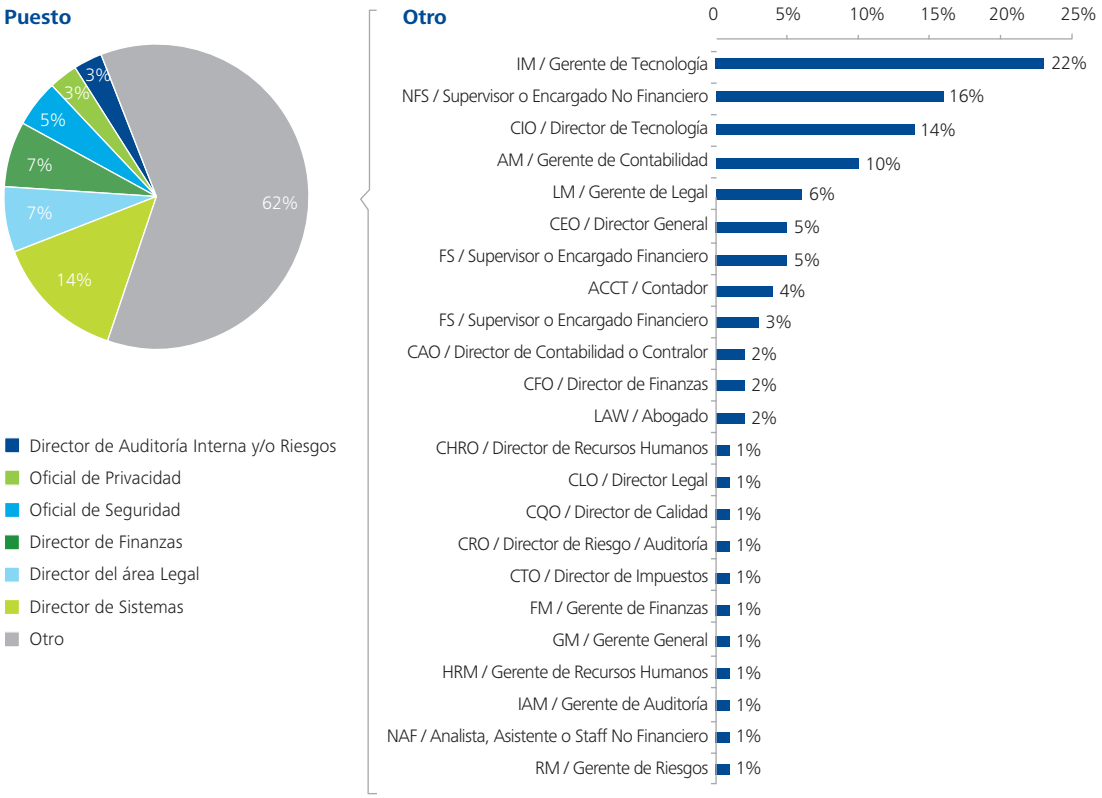
Empleados



Ingresos



Dentro de la encuesta, entre los puestos con mayor participación se encuentran el de Director de Sistemas, con un 14%, seguido del Director de Finanzas y el Director del área Legal con un 7% respectivamente. El 62% está representado por otros puestos: encontramos a Gerentes de Tecnología (22%), Supervisores no financieros (16%), Directores de Tecnología (14%) y Gerentes de Contabilidad (10%).



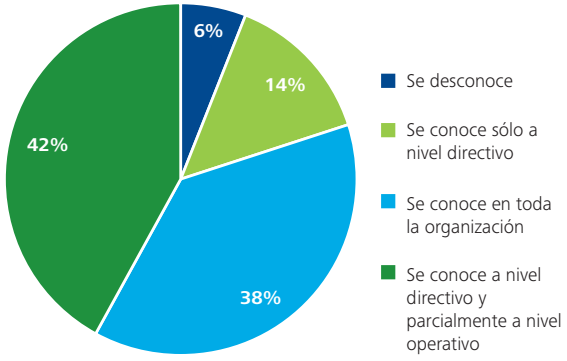
Resultados generales

La primer pregunta realizada en la encuesta está enfocada a conocer si todos los niveles de la organización conocen la LFPDPPP. Se observa, según los resultados obtenidos, que a casi cuatro años de la entrada en vigor de la ley, el 42% de los encuestados dice que ésta es conocida a nivel directivo y parcialmente a nivel operativo; seguido de un 38%, que indica que se conoce en toda la organización. Sólo un 6% dice desconocerla. Por lo que es probable que las empresas se hayan asesorado y que la ley resulte del conocimiento de la mayoría de los encuestados.

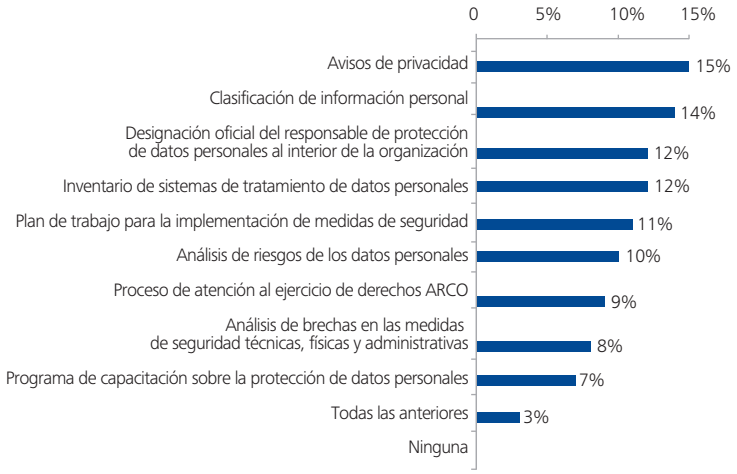
Entre las acciones tomadas por las empresas a partir de la entrada en vigor de la ley, se destacan como principales actividades los avisos de privacidad (15%) y la clasificación de información personal (14%). Estas actividades pueden aparentar el cumplimiento con la ley.

No resulta del todo sorprendente que la prioridad esté enfocada en estos temas. Sin embargo, se observa un déficit en el entrenamiento al interior de las organizaciones para el cumplimiento, dado que únicamente un 7% menciona haber realizado un entrenamiento sobre el tema.

¿Qué tan al tanto está su organización de la LFPDPPP, en todos los niveles?



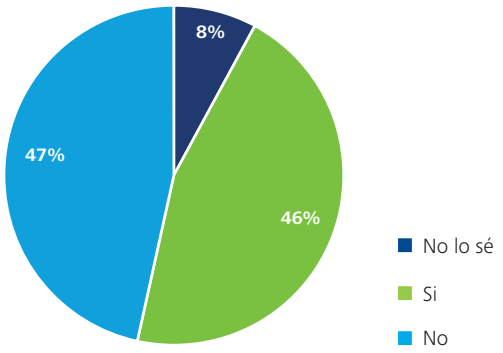
¿Qué actividades se han llevado a cabo en su organización?



Ante estos resultados, la incógnita que surge es: ¿De qué manera las organizaciones están capacitando a sus empleados para evitar vulneraciones por errores humanos?, ¿qué recomendaciones están siguiendo para mantener la privacidad de los datos?, ¿qué sistemas de gestión de seguridad de datos personales (SGSDP) están siendo implementados para el cumplimiento con la LFPDPPP?

Según la encuesta, un 47% indica que no cuenta aún con un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), mientras que el 46% indica que sí, por lo que estos resultados muestran que existe una oportunidad para casi la mitad de los encuestados para reforzar los temas de seguridad en su organización.

¿Su organización cuenta con un Sistema de Gestión de Seguridad de Datos Personales (SGSDP)?



En las recomendaciones en materia de Seguridad de Datos Personales publicadas en el Diario Oficial de la Federación, el 30 de octubre de 2013, el IFAI recomendó la implementación de un SGSDP (Sistema de Gestión de Seguridad de Datos Personales) basado en PHVA (Planear-Hacer-Verificar-Actuar), para la protección de los datos personales para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley, su Reglamento, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Las condiciones para obtener resultados más alentadores en la adopción de la Ley comprenden el implementar un sistema de gestión de seguridad de datos personales al interior de la organización que se adecúe al giro y tamaño de la organización, así como a la clasificación de los datos personales obtenidos.

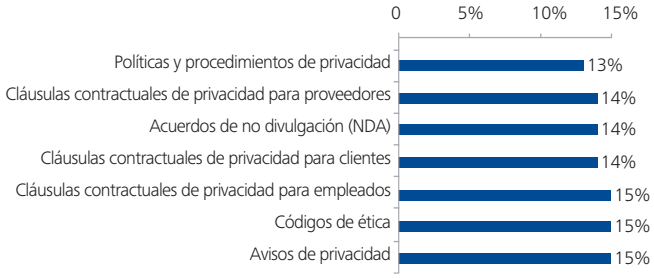
Por ello es necesario que las organizaciones consideren:

1. Elaborar un inventario de datos personales (clasificado) y de los sistemas donde se tratan.
2. Determinar los roles y responsabilidades de las personas que traten datos personales.
3. Realizar un análisis de riesgos de datos personales y asignar prioridades de atención de acuerdo a su impacto.
4. Establecer las medidas de seguridad técnicas, físicas y administrativas aplicables a los datos personales de acuerdo a su clasificación.
5. Mantener un análisis de brechas que identifique las diferencias entre las medidas de seguridad existentes y aquéllas faltantes que resulten necesarias para la protección de los datos personales.
6. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.
7. Llevar a cabo revisiones o auditorías.
8. Capacitar al personal que efectúe el tratamiento.
9. Realizar un registro de los medios de almacenamiento de los datos personales.

Marco jurídico y normativo

De acuerdo con los encuestados, las organizaciones están considerando la implementación de cláusulas contractuales de privacidad para clientes, empleados y proveedores, así como acuerdos de no divulgación, códigos de ética, políticas de privacidad y avisos de privacidad por igual, como parte importante para la protección de información dentro de un marco jurídico y normativo, con ligeras tendencias en cuanto al nivel de importancia como se muestra en la gráfica.

¿Con cuáles de los siguientes elementos cuenta su organización para proteger la información en un marco jurídico y/o normativo?



Esto implica que las organizaciones han tomado conciencia de la igualdad que requiere la protección de los datos tanto a nivel interno como externo a través de los diferentes apoyos contractuales o jurídicos que los ayudan a respaldar el tratamiento de los datos personales.

Avisos de privacidad

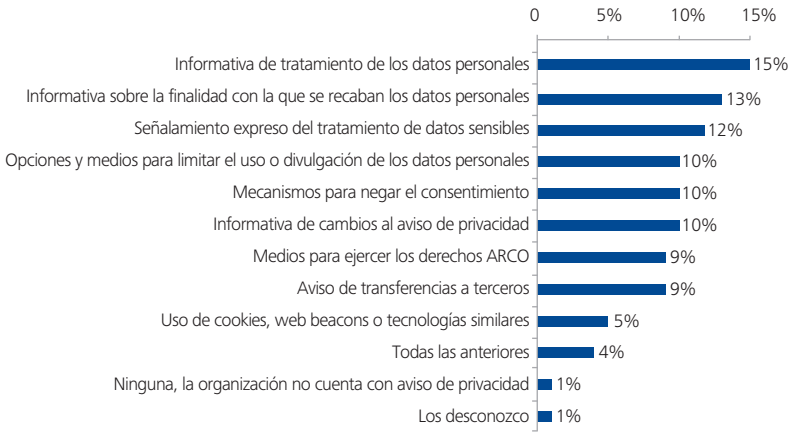
Como ya se había comentado en párrafos anteriores, los avisos de privacidad han sido los elementos que más han sido implementados en las organizaciones; la mayoría de los encuestados cuenta actualmente con avisos de privacidad; sólo un 1% menciona no contar con uno aún. Como referencia, en el estudio anterior, realizado en el 2011, un 16% no contaba con un plan para la protección de datos y un 16% estaba en proceso de implementación.

Los tres elementos más utilizados por las organizaciones en sus avisos de privacidad son:

- Señalamiento expreso del tratamiento de datos sensibles.
- Informativa sobre la finalidad con la que se recaban los datos personales.
- Informativa de tratamiento de los datos personales.

El 4% integra todos los elementos que deben informar en los avisos de privacidad y el menos utilizado por las organizaciones es el uso de cookies, web beacons o tecnologías similares (5%) según la gráfica que se muestra a continuación.

Indique los elementos que integran su aviso de privacidad.



Uso de cookies y web beacons

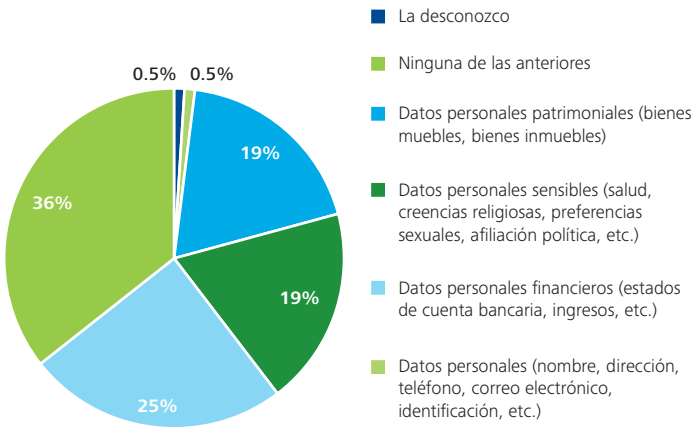
Según los lineamientos del aviso de privacidad publicados en el Diario Oficial de la Federación (DOF) el 17 de enero del 2013 el uso de cookies y web beacons deben ser informados en los avisos de privacidad.

Para entender de mejor manera las razones de la obligación anterior se hace necesario comprender ¿Qué son las cookies y las web beacons?

Cookie. Archivo de datos que se almacena en el disco duro del equipo de cómputo o del dispositivo de comunicaciones electrónicas de un usuario al navegar en un sitio de internet específico, el cual permite intercambiar información de estado entre dicho sitio y el navegador del usuario. La información de estado puede revelar medios de identificación de sesión, autenticación o preferencias del usuario, así como cualquier dato almacenado por el navegador respecto al sitio de internet.

Web beacon. Imagen visible u oculta insertada dentro de un sitio web o correo electrónico que se utiliza para monitorear el comportamiento del usuario en estos medios. A través de estas se puede obtener información como la dirección IP de origen, navegador utilizado, sistema operativo, momento en que se accedió a la página, y en el caso del correo electrónico, la asociación de los datos anteriores con el destinatario.

De las siguientes categorías de datos personales, ¿qué categoría(s) abarca su organización?



Derivado de lo anterior, identificar a un usuario se considera como dato personal y por consecuencia está dentro del alcance de la Ley. Todas las empresas que recaben datos personales a través de Internet deberían cubrir con dicho requisito; en la actualidad se observa que no todas las empresas informan sobre dichos elementos, y de los participantes que recaban datos personales por estos medios, sólo el 5% contempla el cumplimiento de la Ley.

Dentro de la categoría de datos personales recabados que se informan en los avisos de privacidad (como nombre, dirección y teléfono, entre otros), el 36% de las organizaciones entrevistadas reportan que sí son considerados en su organización, seguido por los datos financieros (25%) y por último, se encuentran los datos personales sensibles y los patrimoniales en igual proporción (19%).

Entrenamiento

Además, el 33% de los encuestados menciona que realizan entrenamientos periódicamente sobre la importancia de conocer y cumplir con la Ley, mientras que el 20% declara nunca haber realizado un entrenamiento; el resto asegura haber brindado entrenamiento en al menos una ocasión.

¿En su organización con qué periodicidad se ha brindado entrenamiento y se ha concientizado sobre la importancia de conocer y cumplir con la LFPDPPP?

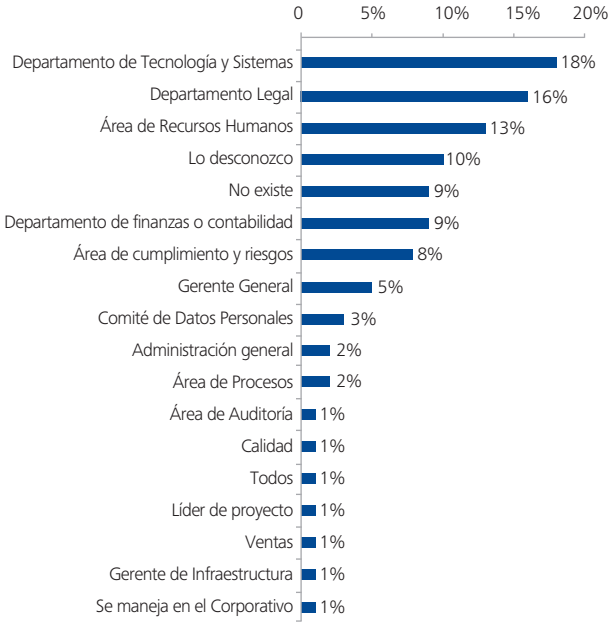
Líder responsable de protección de datos

En la medida en que los datos personales, sensibles, financieros o patrimoniales pueden resultar atractivos para terceros, los procesos de privacidad de la organización podrían verse involucrados en temas de vulneración. Es entonces cuando resulta de especial atención la identificación del líder responsable de protección de datos personales con la intención de definir el rol y tener un responsable del seguimiento.

A partir de la encuesta observamos que un 18% de los profesionistas que forman parte del área de tecnología y sistemas son los principales responsables de la protección de datos personales, seguido por profesionistas del departamento legal con un 16%; en tercer lugar con un 13% se encuentra el área de recursos humanos. Sin embargo, en ningún momento se debe pensar que el área de auditoría interna deba ser quien ejecute dichas tareas, debido a los conflictos de interés que representa para el área ser juez y parte de la protección y privacidad de datos.

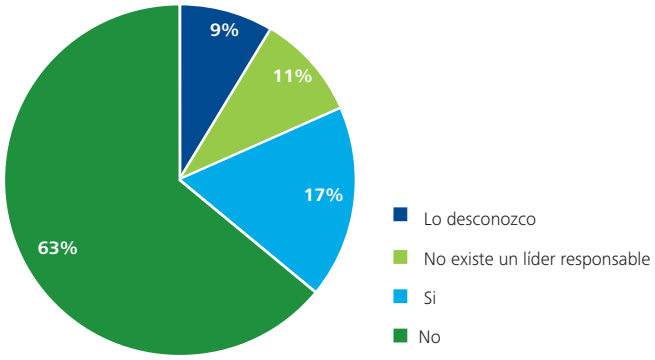
Resulta de vital importancia la participación de todas las áreas operativas de la organización, considerando que el flujo de datos y de información es transversal, por lo que las diferentes funciones y áreas deben colaborar en equipo, alineadas a una estrategia de protección en común.

¿Quién es el líder responsable de la protección de datos personales al interior de su organización?



El 63% de los encuestados declaró que el líder responsable de la protección de datos personales no está dedicado de tiempo completo a estas actividades, lo cual resulta directamente proporcional a ciertos factores como podrían ser los casos de derechos ARCO presentados por los titulares desde la vigencia de la Ley, la probabilidad de vulneración de datos personales, lo atractiva de la base de datos, los controles implementados para minimizar la vulnerabilidad de los datos, experiencias pasadas, riesgos identificados, entre otros, que ayudan a determinar las necesidades que la organización manifieste para mantener una persona dedicada de tiempo completo a velar por la privacidad de los datos.

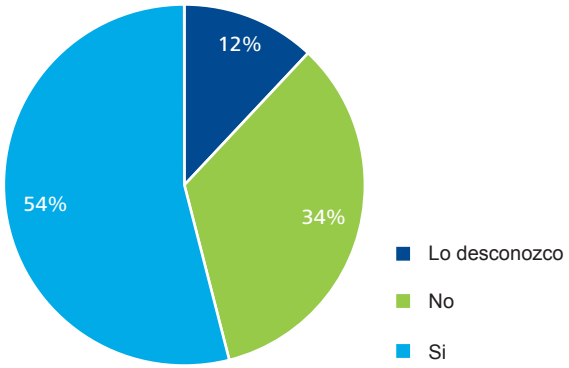
¿El líder responsable de la protección de datos personales está dedicado de tiempo completo a estas actividades?



El proceso para la atención de derechos ARCO inició el 6 de enero de 2012, por lo que resulta positivo que algunas empresas (54% de las participantes) actualmente ya cuenten con los procesos para la atención de los derechos ARCO; sin embargo, es indispensable acelerar la introducción de este tipo de prácticas, a fin de cumplir con los requisitos de la Ley.

Para lograrlo, las empresas deben establecer un nuevo proceso, a manera de ventanilla, por ejemplo, para poder atender a los titulares que soliciten revisar sus datos personales y sus derechos ARCO. Posteriormente se debe seguir el proceso de revisión delimitado por la empresa y dar respuesta en el plazo establecido por la Ley. Adicionalmente, las organizaciones deberán establecer métricas de evaluación.

¿Su organización cuenta con procedimientos y medios para la atención de los derechos ARCO (Acceso, Rectificación, Cancelación, Oposición)?

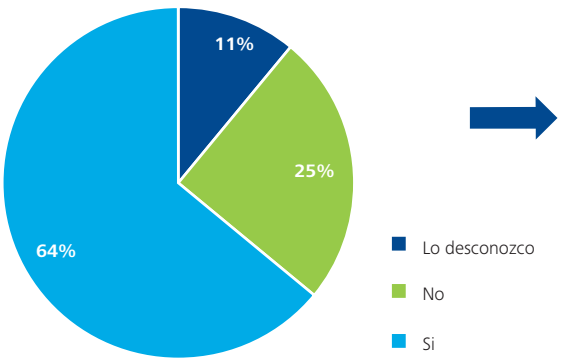


Herramientas para prevenir fugas de información

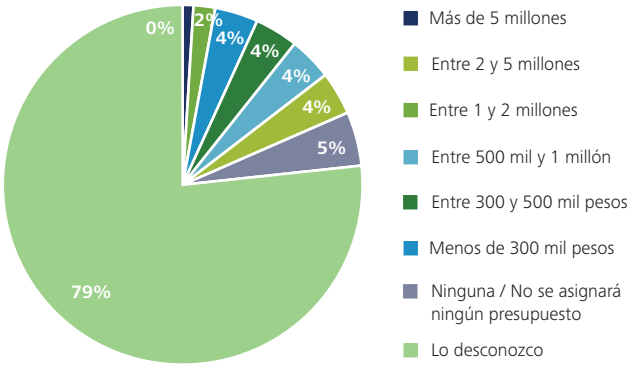
Las implicaciones de cumplimiento con la LFPDPPP suponen que las organizaciones deben mantener medidas de seguridad físicas, técnicas y administrativas para la protección de los datos. De lo contrario existen sanciones económicas y penales impuestas por Ley. Otras consecuencias pueden ser daños en la reputación de la marca, así como disminución de la confianza de clientes, empleados y proveedores, por mencionar algunas.

Por tal motivo es urgente para las organizaciones la asignación de presupuestos para cerrar brechas y riesgos en el tratamiento de datos personales. Los resultados de la encuesta revelan que el 64% planea implementar herramientas como un DLP (Data Loss Prevention) para la prevención de fuga de información aunque la mayoría (79%) desconoce aún el presupuesto que se asignará a esta actividad.

¿Su organización ha pensado implementar herramientas para prevenir la fuga de información (DLP, por sus siglas en inglés)?



¿Qué cantidad se estima asignar como presupuesto?



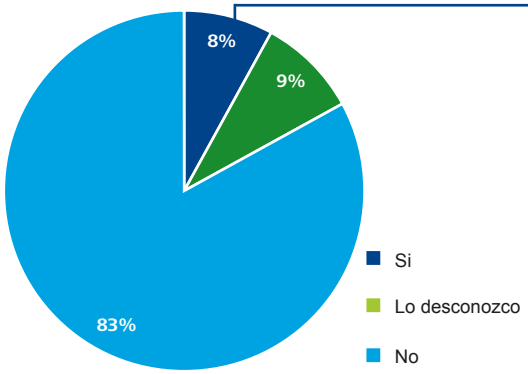
Aunque existen muchas herramientas en el mercado, el DLP se utiliza comúnmente para la protección de datos, pues la herramienta previene la fuga de información, tanto la que está en medios móviles (laptops, tablets, etc.), como la que corre en la red y la que está en reposo (servidores, mainframes, etc.). Además, permite clasificar la información de acuerdo a lo estipulado en la ley, monitorear e identificar dichos tipos de información y llevar a cabo acciones particulares según órdenes preestablecidas. Un sistema DLP debe implementarse junto con una estrategia de privacidad y protección de información, que incluya entre otros aspectos la clasificación de información, políticas y procedimientos de protección y uso de información, análisis de riesgos de datos personales, procesos de incidentes, capacitación y concientización de personal.

Toda organización que trate datos personales debe planificar e implementar sistemas de prevención de intrusos, o bien, aplicar procedimientos de análisis de la información y contención del ataque ante una incidencia detectada, analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia.

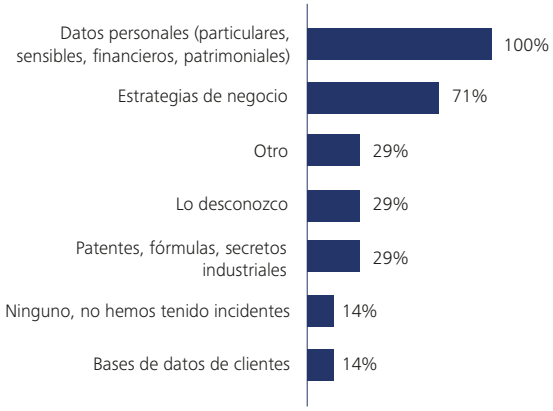
Dentro de la encuesta, la mayoría (83%) declara no haber tenido algún incidente relacionado con fuga, robo o pérdida de información en su compañía. Sin embargo, esto puede deberse a la falta de controles para identificar este tipo de fugas.

Sólo un 9% declaró haber tenido incidentes. De este 9% de encuestados que han sufrido algún incidente, el 100% declara haber tenido problemas con los datos personales, el 71% en las estrategias de negocios y el 29% en patentes, fórmulas y secretos industriales.

¿Su compañía ha tenido algún incidente relacionado con fuga, robo o pérdida de información?



¿Qué tipo de datos se vieron comprometidos?



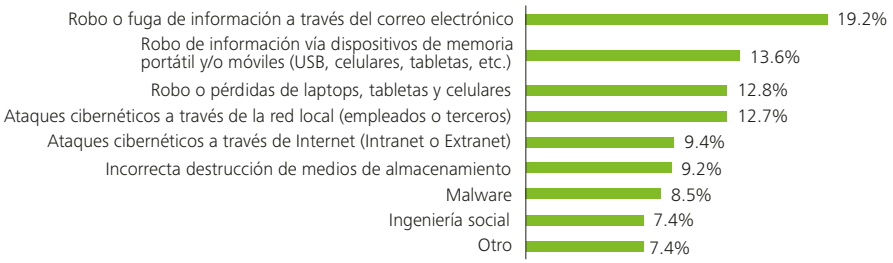
Rubros vulnerables

Las amenazas y vulneraciones de información se dan en muy diversas formas, por mencionar algunas:

- Suplantación de identidad.
- Revelación de información.
- Denegación de servicios.
- Elevación de privilegios.
- Interrupción de servicios.
- Intercepción de datos o recursos.
- De fabricación, cuando se insertan objetos falsificados en el sistema.

El robo o fuga de información a través del correo electrónico es el rubro más vulnerable para las organizaciones con un 19.2%; en segundo lugar encontramos al robo de información vía dispositivos de memoria portátil y/o móviles con un 13.6%, seguido del robo o pérdidas de laptops, tabletas y celulares con un 12.8%.

Numere en orden de importancia para su compañía los siguientes rubros de acuerdo a su nivel de vulnerabilidad.

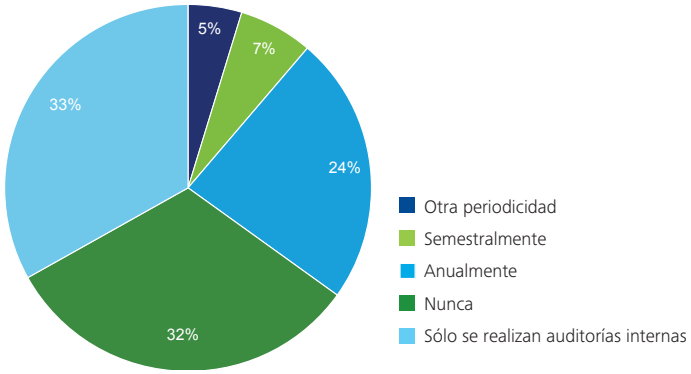


El primer lugar de importancia de acuerdo a su nivel de vulnerabilidad es el de robo o fuga de información a través de correo electrónico (19.2%).

Auditoría interna y externa

Abordando el tema de auditorías internas y/o externas para el cumplimiento con la LFPDPPP, la encuesta realizada revela que el 65% de los encuestados no realiza auditorías externas de cumplimiento con la ley; de este porcentaje, un 33% realiza auditorías internas y un 32% declara no haber realizado nunca una auditoría externa. El artículo 61-VII del reglamento de la LFPDPPP indica llevar a cabo revisiones o auditorías.

¿Con qué periodicidad realiza auditorías externas de cumplimento de la LFPDPPP?



Las auditorías externas o internas de cumplimiento tienen un gran impacto en las empresas que las aplican, pues llegan a sensibilizarse con nuevos temas (riesgos, amenazas, vulnerabilidades) que anteriormente no eran vistos y atacados por las organizaciones; de ahí la necesidad de contar con una asesoría externa que permita identificar las situaciones y procesos que terminarían en consecuencias de incumplimiento ante la ley; agregado a lo anterior, del 36% de las organizaciones que realizan auditorías externas, sólo un (24%) las realiza anualmente, mientras que un 7% las realiza semestralmente.

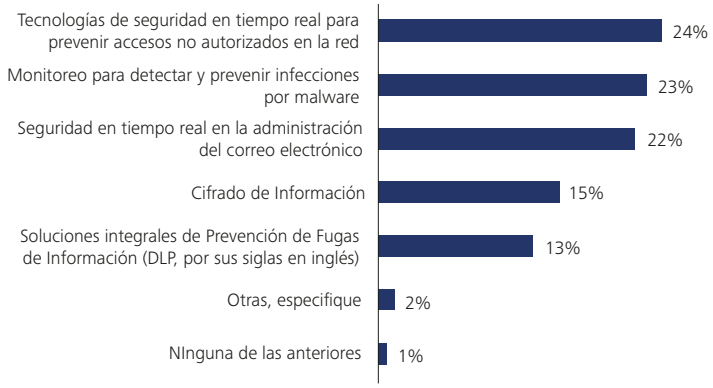
Este tema comienza a ser preocupante cuando el hábito de hacer las cosas siempre de la misma forma afecta esencialmente de dos maneras: la primera, impide ver las situaciones de modo diferente, de ver más allá de lo ordinario, de visualizar nuevos escenarios; la segunda, las acciones cotidianas se convierten en hábitos o vicios que difícilmente se podrán cambiar.

Cuidado y seguridad de los datos

De las diversas acciones tecnológicas que ayudan a evitar la pérdida de información, la más implementada en las organizaciones son las tecnologías de seguridad en tiempo real (24%), seguido de un monitoreo para detectar y prevenir infecciones por malware.

El cifrado de información (15%) y soluciones integrales DLP (por sus siglas en inglés), son las menos implementadas en las organizaciones (13%). Esto se debe a las malas experiencias derivadas de una inadecuada estrategia de implementación. Estas soluciones deben considerar aspectos tanto técnicos como del negocio.

Para evitar la pérdida de información, ¿qué acciones tecnológicas ha implementado en su organización?



Mantener un programa de seguridad de datos en una organización es una solución integral que no sólo busca proteger, preservar y administrar de una manera eficiente todo tipo de recursos con los que cuenta la organización, sino que también busca dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que pudiesen afectarla. Por esta razón las organizaciones deben trabajar en diferentes acciones que permitan mejorar dichos programas. Según los resultados de la encuesta, el control de acceso y política de seguridad son las soluciones más implementadas en las organizaciones con un 15%.

De las siguientes acciones orientadas a un programa de seguridad de los datos personales, ¿cuáles se han implementado en su organización?

Al implementar un programa de protección de datos dentro de una organización, un 33% de los encuestados considera como prioridad asegurar el cumplimiento regulatorio, seguido de incrementar la confianza y lealtad de los clientes (19%) y mantener la reputación de la marca (18%).

Numere de acuerdo al nivel de importanca en el establecimiento de un programa de protección de datos dentro de su organización los siguientes rubros.

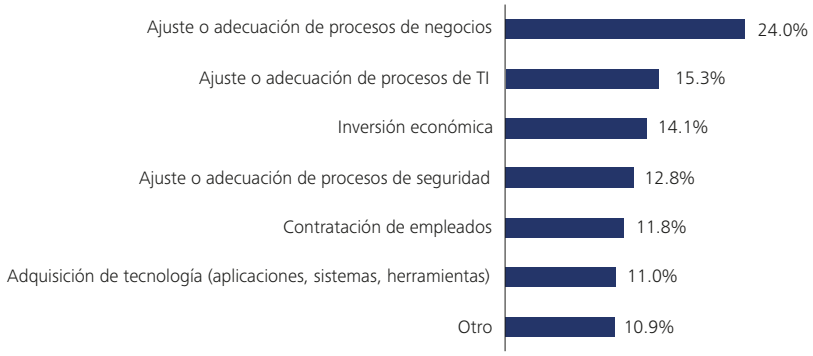
Cumplimiento de la LFPDPPP

A partir de la entrada en vigor de la LFPDPPP las organizaciones tienen que alinear sus brechas de cumplimiento, por lo que han tenido que enfocarse en metodologías, procesos, gente, tecnologías, estrategias, entre otras actividades que les permitan alcanzar sus objetivos de cumplimiento.

Pero, según las organizaciones, ¿qué factores al interior de la organización requieren de más apoyo para el cumplimiento con la LFPDPPP? La encuesta revela que en primer lugar y con una marcada preferencia según el orden de importancia, son los procesos y prácticas internas, con un 24.7%, en segundo lugar, políticas y estándares (14.9%) y en tercer lugar, gente (13.1%). Los últimos lugares están conformados por los factores de estrategia, tecnología y legal (12%).

¿Qué factor necesita mayor apoyo para el cumplimiento de la LFPDPPP en su compañía?

¿Qué factor impacta más a su compañía en lo referente al cumplimiento con la LFPDPPP?



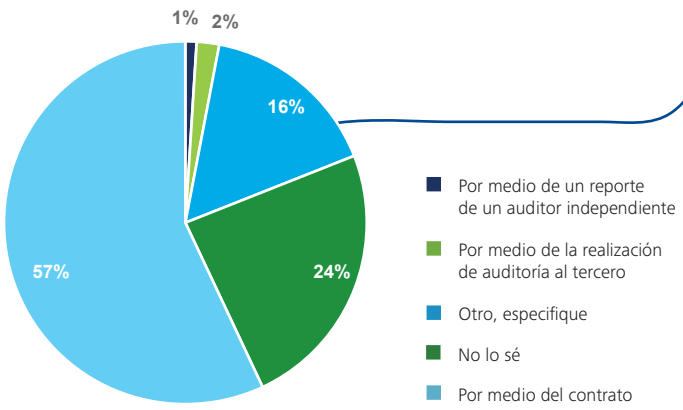
Y por otro lado, ¿qué factor impacta más a las organizaciones para el cumplimiento con la ley? El resultado de la encuesta revela que las organizaciones califican con mayor impacto el tener que ajustar o adecuar sus procesos de negocios actuales con los requerimientos de Ley con un 24%, seguido del ajuste o adecuación de los procesos de TI (15%). En tercer y cuarto lugar encontramos la inversión económica (14%) y al ajuste o adecuación de los procesos de seguridad (12.8%). Por último, la contratación de empleados (11.8%) y la adquisición de tecnología (11%) son los factores que menos impactan a la compañía en relación con la ley.

Transferencia de información a terceros

Otro factor de importancia para la protección de datos personales es la transferencia a terceros. Distintas organizaciones, por diferentes motivos, tienen la necesidad de transferir información para estar en posibilidades de ofrecer servicios como pagos de nómina, seguros de gastos médicos, aplicación de exámenes psicométricos, etc. Pero, ¿cuáles son las medidas de seguridad utilizadas por las organizaciones para la protección de la información por el tercero y el cumplimiento con la Ley al momento de la transferencia?

La encuesta revela que los contratos son el medio por el cual las organizaciones se aseguran de que un tercero cuente con las medidas de seguridad y privacidad requeridas por la L ey para proteger los datos personales al momento de compartirlos y un 57% de los encuestados declaran hacer uso de estos. El 24% de los participantes no tiene el conocimiento de cómo se asegura esta información en sus procesos de negocio. Del 16% que respondió Otros, el 89% aseguró no compartir o transferir información a terceros.

Cuando comparte (transfiere o remite) datos personales con un tercero para un proceso de negocios, ¿cómo se asegura de que el tercero cuente con las medidas de seguridad y privacidad requeridas por la Ley para proteger los datos personales?



Otros

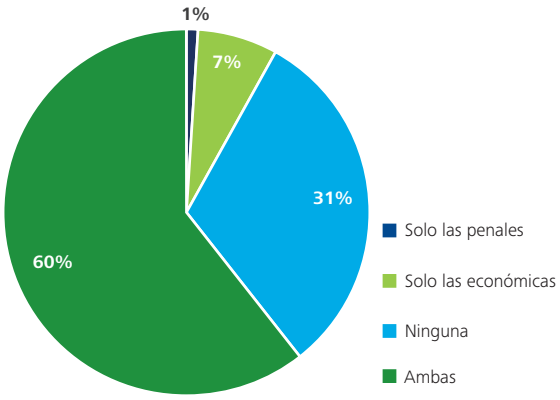
No se comparte / Transfiere información a terceros	89%
Aviso de Privacidad	4%
Físicamente en presencia de abogados	4%
Programa especial	4%

Según los resultados obtenidos en gráficas anteriores, las organizaciones consideran como prioridad asegurar el cumplimiento regulatorio para la protección de datos en lugar de la salvaguarda de la infraestructura crítica de TI. Esto se puede deber al conocimiento de las sanciones impuestas por la Ley. El 60% de las organizaciones tiene conocimiento de las sanciones penales y económicas que impone la autoridad en los casos de tratamiento indebido o fuga de información de datos personales.

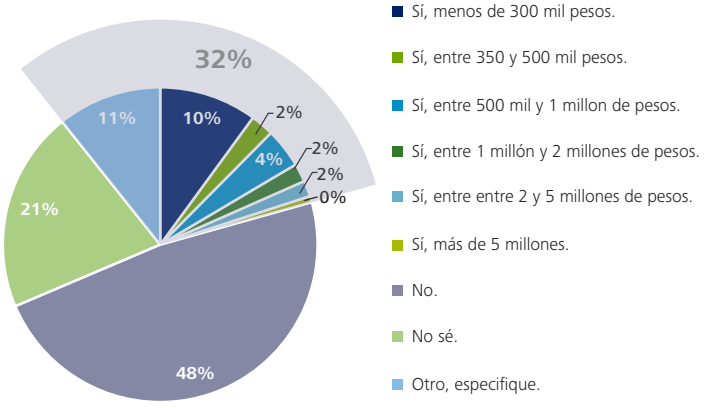
En el estudio anterior se realizó la misma pregunta y a lo largo de estos tres años se pudo observar que el conocimiento de las sanciones ha mejorado. En el estudio realizado en el 2011, el 53% mencionó no conocer ninguna de las sanciones impuestas por la autoridad y sólo un 24% declaró tener conocimiento de ambas. En el presente estudio, el porcentaje que dice sólo conocer una categoría de las sanciones impuestas, declara que las sanciones económicas son las más conocidas (7%).

Todas las organizaciones requieren realizar esfuerzos de inversión económica para mejorar sus prácticas de protección de datos actuales, y esperan que las mismas rindan frutos tanto en el presente (para las organizaciones que ya han realizado esfuerzos), así como en el futuro para las que apenas comienzan o continúan haciéndolo, el resultado revela que el 48% de los encuestados dice no haber realizado alguna inversión económica para el cumplimiento de la Ley en el último año, mientras que un 32% afirma haber realizado alguna inversión.

¿Conoce las sanciones que impone la autoridad en los casos de tratamiento indebido o fuga de información de datos personales?



En el último año, ¿hizo alguna inversión económica para el cumplimiento de la LFPDPPP?

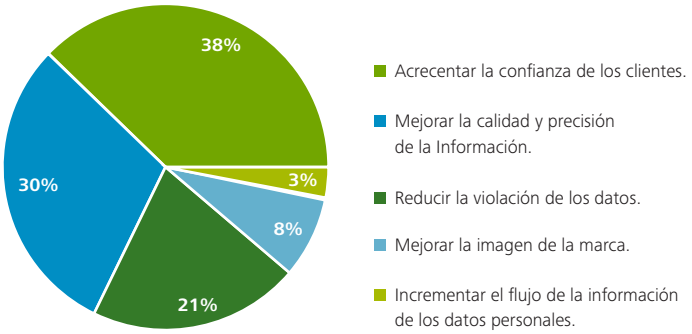


Parece lógico esperar que las organizaciones que invierten en mejorar sus prácticas de protección de datos esperen como resultado no sólo ser exentos de multas o sanciones económicas, sino también ganar confianza de clientes. Los participantes en la encuesta consideran que es valioso para su organización que el IFAI otorgue alguna certificación a las empresas que cumplen con la Ley; sólo un 18% no lo considera valioso.

El mayor beneficio que perciben las organizaciones al cumplir con la Ley según la encuesta es acrecentar la confianza de los clientes con un porcentaje de 38 por ciento, seguido por una mejora en la calidad y precisión de la información y la reducción de la violación de los datos. El beneficio calificado con menor importancia, es el incremento del flujo de la información de los datos personales (3%).

¿Considera valioso que el IFAI otorgue alguna certificación a las empresas que cumplen con la ley?

¿Cuál es el mayor beneficio que el cumplimiento de la LFPDPPP aportará a su compañía?



Conclusión

La privacidad, sin duda alguna, representa un cambio cultural en nuestro país, el cual requiere de tiempo, participación, inversión, esfuerzos y flexibilidad para aceptar esta nueva cultura que hasta la aparición de la Ley, era ignorada.

Posterior al análisis anterior y de los resultados obtenidos a partir de la encuesta es necesario considerar que a casi 4 años de entrada en vigor de la Ley, las organizaciones aún presentan oportunidades de mejora en diferentes aspectos de cumplimiento, toda vez que los planteamientos de la Ley no involucren únicamente la protección de datos, sino además el establecimiento de una serie de procesos y que apoyarán el ejercicio de los derechos de los titulares, los cuales buscan respaldar primordialmente los principios de privacidad establecidos (licitud, consentimiento, calidad, lealtad, proporcionalidad, finalidad, lealtad, información).

Para cumplir con dichos principios es necesario establecer una metodología, que de manera integral, involucre gente, procesos, tecnología y asesoría legal que de manera acertada guíen en la implementación de un programa de privacidad.

Servicios Deloitte México en privacidad y protección de información

Nuestro principal objetivo en materia de privacidad y protección de información es proveer soluciones integrales que contemplen el diseño e implementación de controles durante el ciclo de vida de los datos, que permitan salvaguardar la confidencialidad de su información.

El enfoque de solución que Deloitte México pone a su alcance, permite la alineación de los procesos de las compañías a los requerimientos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), reglamento y normatividad nacional relacionada. Al mismo tiempo, nuestro marco de referencia se basa en mejores prácticas y estándares internacionales.

Deloitte México analiza las medidas de seguridad técnicas, físicas y administrativas de las organizaciones y evalúa si son suficientes para permitir la privacidad y la protección de los datos de sus accionistas, clientes, empleados y terceros.

Nuestros servicios incluyen:

- Análisis y diagnósticos del grado de cumplimiento de los procesos de la compañía con la normatividad nacional y las buenas prácticas internacionales.
- Asesoría en los planes para la adaptación de los procesos de la organización a los requerimientos en materia de protección de datos personales.
- Automatización de controles para la prevención de fuga de información mediante soluciones de DLP.
- Evaluación a terceros sobre el grado de cumplimiento de los procesos y del tratamiento seguro de los datos.
- Auditoría de cumplimiento para verificar el grado de alineación y cumplimento con respecto a la LFPDPPP.

Podemos armar un proceso integral de implementación en un periodo flexible, el cual comprende un análisis profesional por tipo y volumen de datos, un diagnóstico de acuerdo al tamaño de la empresa y al grado de complejidad tecnológica de los procesos, y, finalmente, la detección de necesidades.

¿Por qué Deloitte?

Porque tenemos:

- Amplia experiencia nacional e internacional en administración de proyectos, basada en estándares y normas nacionales e internacionales.
- Sólida metodología.
- Conciencia de la importancia de conectar la tecnología con la estrategia de todo negocio.
- A nivel mundial, obtuvimos el grado de Empresa Líder por la Evaluación de Controles de Seguridad de la Información y Riesgos de las Tecnologías de la Información de Forrester Wave. ™
- Integramos un gran entendimiento del negocio con gran profundidad técnica para nuestros clientes nacionales e internacionales. Deloitte está en más de 150 países en el mundo, y toda nuestra experiencia y conocimientos son para su organización.

Contactos

Región Centro
Santiago Gutierrez
Tel. +52 (55) 50806533
sangutierrez@deloittemx.com

Eduardo Cocina
Tel. +52 (55) 5080 6936
ecocina@deloittemx.com

Pedro Hill
Tel. +52 (55) 59002911
pehill@deloittemx.com

Región Frontera
Mario García
Tel. +52(664) 6227810
magarcia@deloittemx.com

Región Bajío
Victor Rizo
Tel. +52 (55) 50806827
vrizo@deloittemx.com

Jose Luis Ceballos
Tel. +52 (33) 36690404
jlceballos@deloittemx.com

Región Norte
Kristian Ayala
Tel. +52 (81) 81337380
krayala@deloittemx.com

www.deloitte.com/mx