# GSISS 2018

## Proteger la información y prosperar en una economía digital


pwc

## *Más información, nuevos riesgos*

Conforme las compañías de todos los sectores se mueven hacia nuevos modelos digitales, generan mayores volúmenes de información que, en gran medida, es compartida y transmitida a terceros, que incluyen socios de negocio y proveedores.

Al generar una mayor cantidad de información en formato digital, surgen nuevos riesgos que pueden pasar desapercibidos, aumentando la probabilidad de fugas de información, pérdida o destrucción de la misma.

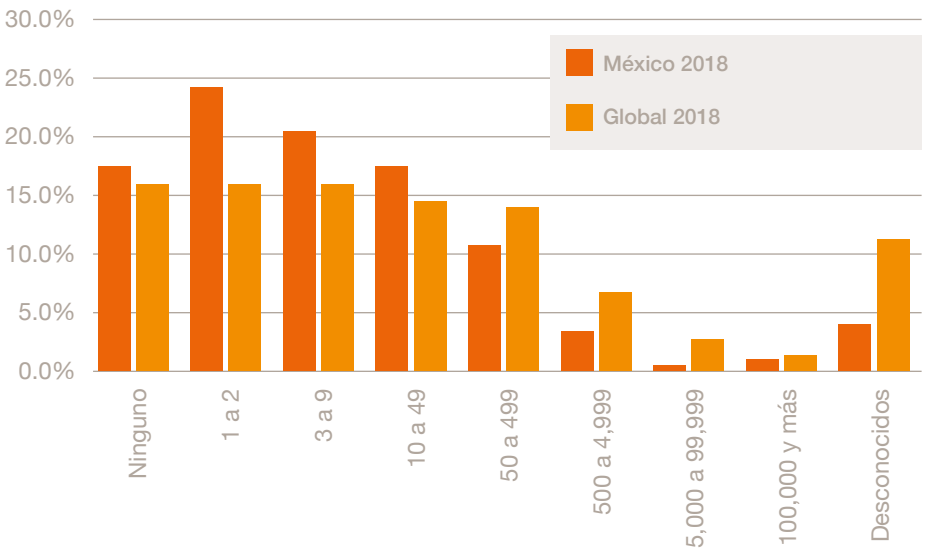
Debido a ello, las compañías pueden quedar expuestas ante las autoridades regulatorias al violar leyes o normativas con las que deben cumplir, lo que, por otro lado, podría lastimar su reputación de manera importante.

Los resultados del *Global State of Information Security Survey (GSISS)*, de PwC, muestran que las organizaciones aún deben esforzarse en crear un verdadero gobierno de datos y en diseñar e instrumentar una estrategia de seguridad contra las amenazas e incidentes de información.

Este reto también es imperativo para México. El 78.6% de las empresas del país que participaron en el estudio declaró haber detectado al menos un incidente de seguridad en los últimos 12 meses. Este indicador es mayor al que reportaron las empresas a nivel global (72.2%).

***Las organizaciones deben esforzarse en crear un verdadero gobierno de datos***

**Número de incidentes de seguridad detectados en los últimos 12 meses**




**78.6%**

de las empresas del país declaró haber detectado al menos un incidente de seguridad en los últimos 12 meses

En la actualidad, adoptar nuevas tecnologías sin pensar primero en los riesgos para la seguridad de la información, puede traer consecuencias sin precedentes para las empresas.

Según el Foro Económico Mundial (WEF, por sus siglas en inglés), la creciente interconexión de dispositivos y la mayor dependencia tecnológica amplía los riesgos para las organizaciones. En su *Informe de Riesgos Mundiales 2018,* el organismo indica que los ataques cibernéticos son la primera preocupación para los líderes de negocios, aun por encima de los ataques terroristas. Las fallas en el software y otros factores podrían provocar errores sistémicos que "caen como cascada a través de las redes y afectan a la sociedad de formas imprevistas".

Se espera que las empresas que aprovechen la oportunidad de gestionar la protección de datos y los riesgos de privacidad estén mejor posicionadas para prosperar en una economía impulsada por los datos y para desarrollar la resiliencia en la sociedad digital.

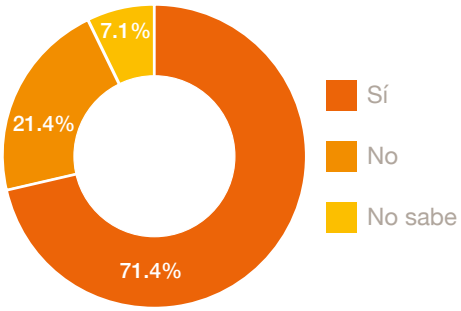
## *Causas de los ataques, presupuesto en seguridad y controles*

A pesar de que ha aumentado la conciencia sobre la necesidad de mejorar en materia de seguridad y privacidad, muchas empresas en riesgo de sufrir ataques cibernéticos no están preparadas para lidiar con estos temas. Las crecientes amenazas a la integridad de los datos podrían socavar los sistemas de seguridad y causar daños físicos a la infraestructura crítica.

A nivel global, el 44% de los 9,500 ejecutivos encuestados en 122 países para el GSISS 2018, manifestó que no tiene una estrategia general de seguridad de la información. El 48% declaró que no cuenta con un programa de capacitación para la conciencia de seguridad del empleado, mientras que el 54% indicó que carece de un proceso de respuesta ante incidentes.

Por su parte, el 44% de los encuestados en México respondió que no cuenta con una estrategia general de seguridad de la información, aunque 71.4% de las empresas en el país señaló que tiene un programa de respuesta ante incidentes.

**¿Cuenta con un plan de respuesta ante incidentes?**

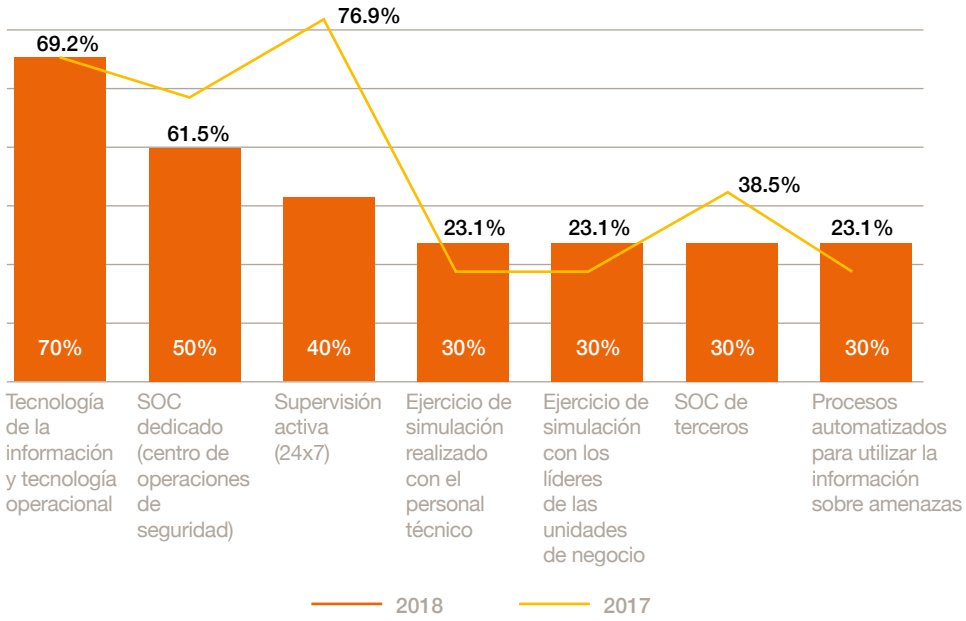



**44%**

de los encuestados en México respondió que no cuenta con una estrategia general de seguridad de la información

De los que cuentan con un plan de supervisión y respuesta ante ataques cibernéticos, el 70% de los participantes mexicanos declaró contar con tecnología de la información y tecnología operacional, el 50% dispone de un centro de operaciones de seguridad y el 40% hace una supervisión activa 24/7.

**¿Cuál de los siguientes aplica dentro de tu programa de incidentes de ciberseguridad?**



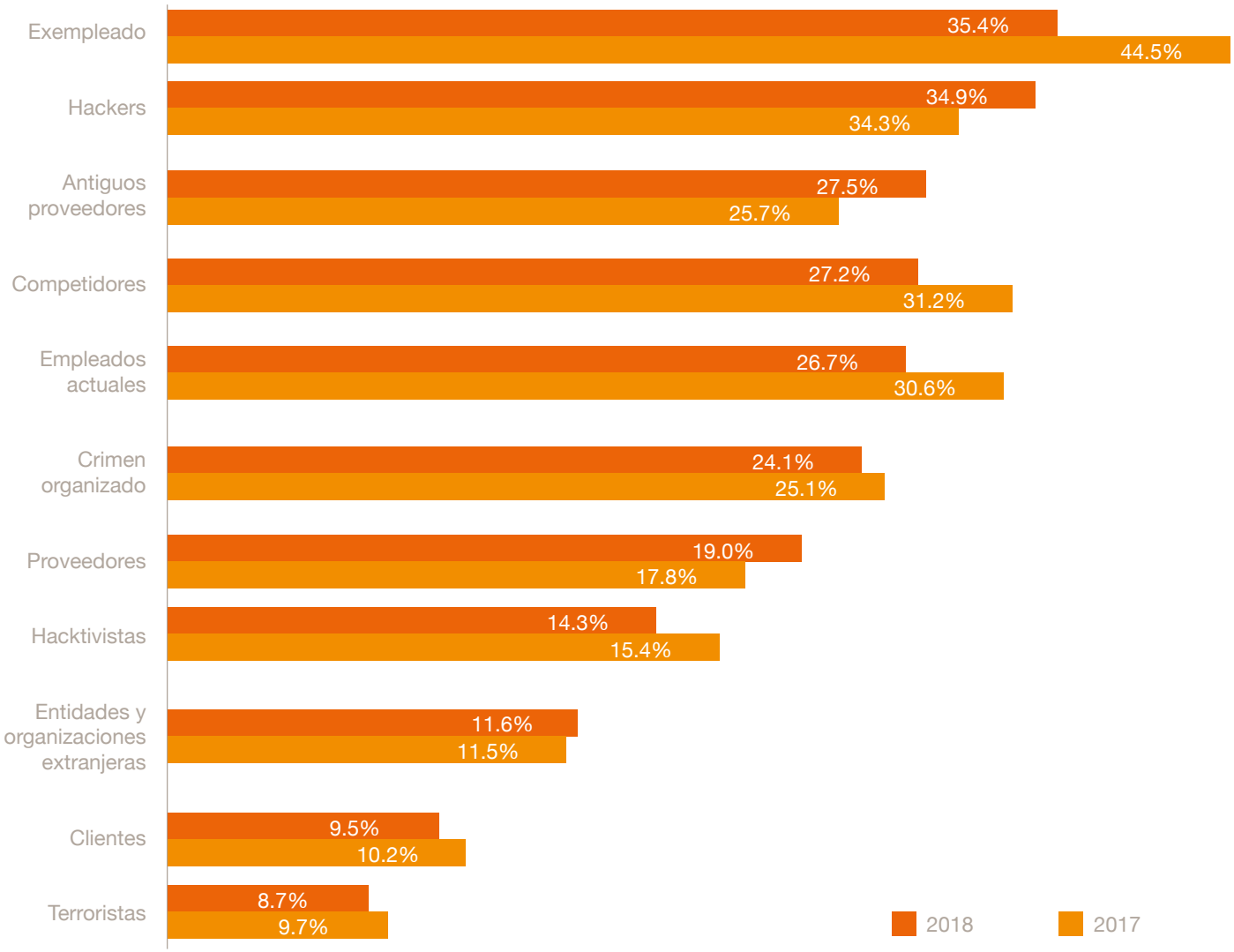

**35.4%**

de las empresas entrevistadas indicó que los exempleados son la principal causa de incidentes de seguridad

Para los participantes mexicanos, las mayores amenazas externas a la seguridad de la información son los hackers (34.9%), la competencia (27.2%) y el crimen organizado (24.1%).

Los ejecutivos de las compañías con operaciones en México también identificaron las siguientes amenazas internas para la seguridad de la información: 35.4% de las empresas entrevistadas indicó que los exempleados son la principal causa de incidentes de seguridad. Les siguen los hackers (34.9%), antiguos proveedores (27.5%), competidores (27.2%) y empleados actuales (26.7%).

**¿Quiénes son los principales autores de los ataques?**




*No establecer controles en el acceso a la información para el personal de la empresa y monitorear lo que hace, puede resultar en un incidente*

Además de las amenazas internas, también se debe poner atención en los ataques que ocurren a través de terceros. No establecer controles en el acceso a la información para el personal de la empresa y monitorear lo que hace, sobre todo en las transacciones críticas, puede resultar en un incidente. Por otro lado, no controlar a los terceros o no conocer qué tipo de controles tiene para resguardar o transmitir la información, aumenta el riesgo.

Cabe destacar que en México, las empresas destinan un mayor porcentaje de su presupuesto de Tecnologías de la Información (TI) a seguridad de la información. El monto promedio es de 4.2 millones de dólares, equivalente al 5.1% del presupuesto total destinado a TI, mientras que a nivel global se destina en promedio 4% del presupuesto a este rubro.

| | Global | | Latinoamérica | | México | |
|---|---|---|---|---|---|---|
| | 2017 | 2018 | 2017 | 2018 | 2017 | 2018 |
| Presupuesto de seguridad de la información (millones de dólares) | 5.060 | 5.131 | 4.772 | 4.412 | 5.020 | 4.246 |
| Porcentaje | 3.7% | 4.1% | 3.9% | 4.1% | 3.9% | 5.1% |

*El monto promedio es de 4.2 millones de dólares, equivalente al 5.1% del presupuesto total destinado a TI*

Es común que la seguridad aún se perciba como una cuestión de TI, aunque es un asunto que debe contar con su propio responsable y un presupuesto que no esté supeditado a otra área. Todavía es una práctica usual que el equipo encargado de seguridad dependa del *Chief Information Officer* (CIO) o del director de TI. El efecto es que, si el responsable de seguridad no puede tomar decisiones propias, comienza a generarse un problema de independencia.

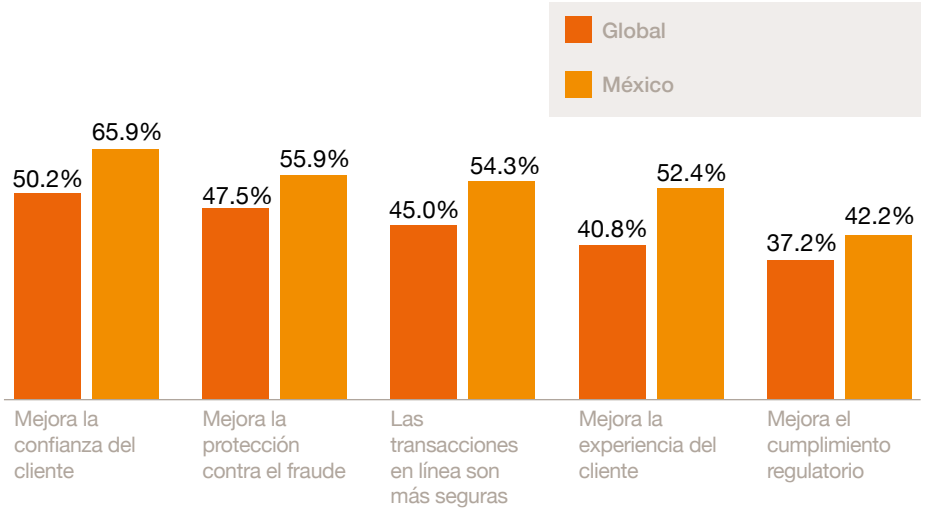
Las empresas requieren una estructura que les convenga en el manejo de la información y prevención de ataques. Por ello, se debe desconcentrar el presupuesto de seguridad de TI y dar más autonomía en la toma de decisiones en este rubro.

## *Tecnologías de autenticación, factor para aumentar confianza*

Las mejoras en tecnologías de autenticación podrían ayudar a los líderes de negocios a construir redes más confiables.

En el GSISS 2018, el 66% de los encuestados en México afirmó que el uso de tecnologías avanzadas de autenticación ha mejorado la confianza de los clientes y los socios comerciales en las capacidades de privacidad y seguridad de la información de la organización; además, el 56% aseguró que estas han ayudado a reducir el fraude y el 52%, que han mejorado la experiencia del cliente.

**¿Qué impacto tiene el uso de tecnologías avanzadas de autenticación en tu organización?**




Las principales tecnologías de autenticación que están implementando las empresas en México son: múltiples factores de autenticación (48.8%), llaves criptográficas (43.9%) y mobile tokens (43.7%).

| Tecnologías de autenticación actuales | |
|---|---|
| Múltiples factores de autenticación | 48.8% |
| Llaves criptográficas | 43.9% |
| Mobile tokens | 43.7% |
| Hard tokens | 41.8% |
| Biométricos | 36.7% |
| Soft tokens | 35.3% |
| Identificaciones oficiales | 34.2% |

En cuanto a las tecnologías que piensan instrumentar en los próximos 12 meses, en primer lugar, están los sistemas biométricos (65.8%), los soft tokens (64.9%) y las identificaciones oficiales (63.7%).

| Tecnologías de autenticación a implementar en los próximos 12 meses | |
|---|---|
| Biométricos | 65.8% |
| Soft tokens | 64.9% |
| Identificaciones oficiales | 63.7% |
| Hard tokens | 60.1% |
| Llaves criptográficas | 58.5% |
| Mobile tokens | 55.4% |
| Múltiples factores de autenticación | 49.1% |

Si bien en nuestro país el uso de sistemas biométricos ya es un requerimiento estipulado por la Comisión Nacional Bancaria y de Valores (CNBV) para las entidades del sector financiero, cada vez más empresas planean incorporarlos en su seguridad.

En la actualidad, algunas instituciones financieras hacen uso de la tecnología biométrica como un doble factor de autenticación, es decir, que ya no solo se valida la identidad con el nombre de usuario y la contraseña, además de ello se utilizan, por ejemplo, la huella digital y el reconocimiento facial, entre otros. En algunos casos, este tipo de verificación está siendo usada únicamente para transacciones cuyos montos superen determinados límites.

La autenticación a través de doble factor de autenticación también tiene aplicaciones en el sector público (control de inmigración en fronteras, agencias de seguridad) y aplicaciones más avanzadas en el sector salud (identificación de pacientes en hospitales y acceso a expedientes médicos).

El uso de estas tecnologías va en aumento en nuestro país, lo que claramente indica que la industria en general está tomando cartas en el asunto respecto a la Seguridad y Privacidad de la información.

## *La confianza como estrategia de negocio*

El aumento en escala y sofisticación de los ataques cibernéticos debe poner en alerta a las organizaciones y aumentar su resiliencia ante estas amenazas, cuyos daños no se limitan solamente a las operaciones comerciales.

De acuerdo con el Reporte de Riesgos Globales del WEF, las empresas deben anticiparse a los objetivos de los atacantes, que pueden ser desde el robo y la interrupción del negocio, hasta la extorsión, espionaje económico, daño reputacional y la infiltración de infraestructura y servicios críticos. Estos adversarios, cada vez más diversos y activos, hacen que los riesgos cibernéticos se vuelvan difíciles de gestionar.

La estrategia de administración de riesgos de una empresa debe basarse en una sólida comprensión de las amenazas cibernéticas a las que se enfrenta la organización y una conciencia de los activos clave que requieren mayor protección. Debe haber un apetito al riesgo coherente. Los líderes deben impulsar el desarrollo de una cultura de gestión del riesgo cibernético en todos los niveles de la organización.

Las organizaciones de todos los tamaños están obligadas a impulsar la participación de la junta directiva en la supervisión de la gestión del riesgo cibernético y de privacidad. En México, el 40% de los encuestados opina que su junta directiva participa directamente en la supervisión de los riesgos cibernéticos y de privacidad actuales. Sin una sólida comprensión de los mismos, los consejos no están bien posicionados para ejercer sus responsabilidades de supervisión en materia de protección de datos y privacidad.

De acuerdo al GSISS 2018, el 65% de los encuestados en México dice que su organización ha puesto un *Chief Privacy Officer* (CPO) o a un ejecutivo de nivel similar a cargo de la privacidad de la empresa. Esta cifra es ligeramente menor a la que arroja la encuesta a nivel global, que es de 68%. Resulta interesante que 24% de los participantes de nuestro país no está considerando contratar a un CPO como encargado del cumplimiento de la privacidad, aun cuando los riesgos de incumplimiento son elevados.

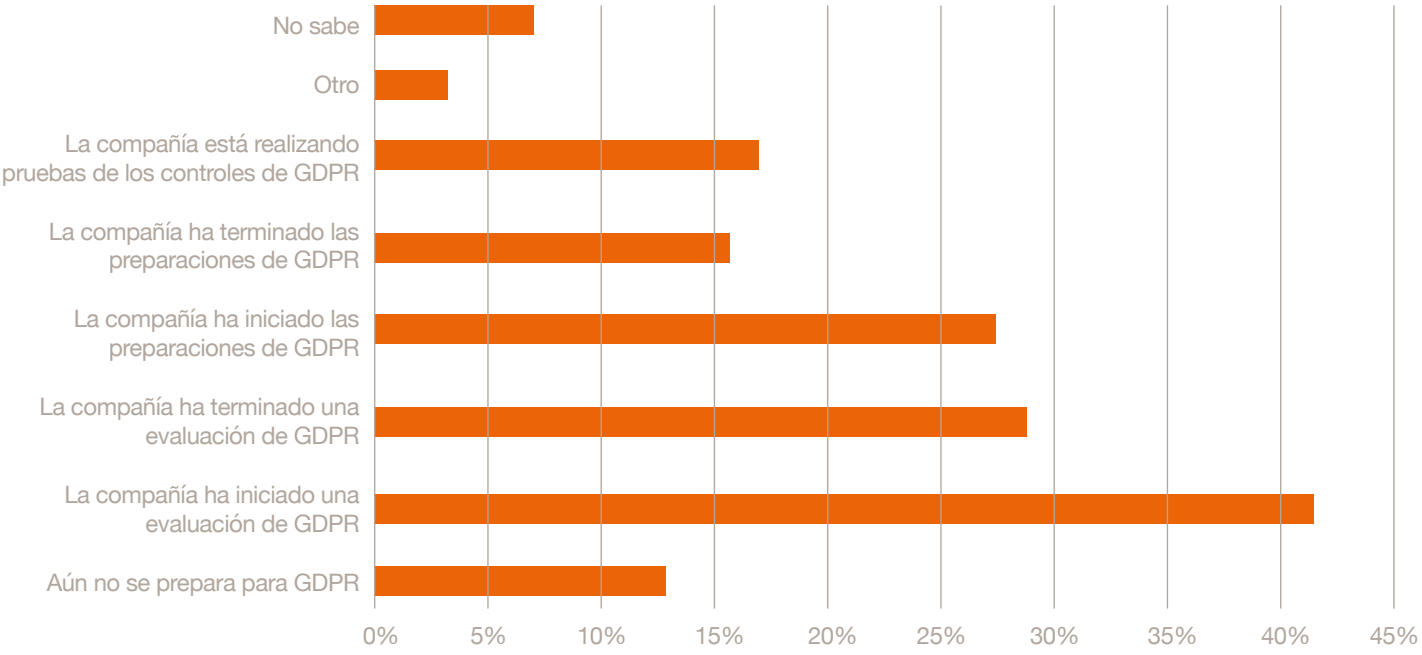
Las empresas también se enfrentan a nuevas normas de privacidad y seguridad de datos, incluida la Regulación General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea (UE), que aplica a cualquier organización que realice negocios con la UE y maneje datos de ciudadanos europeos. La regulación entró en vigor en mayo de 2018.


***Algunas instituciones financieras utilizan ya la tecnología biométrica como un doble factor de autenticación***

**40%**

de los encuestados opina que su junta directiva participa directamente en la supervisión de los riesgos cibernéticos y de privacidad

**De las siguientes respuestas, ¿cuál se ajusta a la etapa en la que está tu compañía respecto al cumplimiento de GDPR?**




Los líderes empresariales deberían ver GDPR como una oportunidad para alinear sus organizaciones a donde deben estar para el éxito futuro, no sólo para el cumplimiento, sino para la gestión estratégica de riesgos.

Es importante resaltar que la ciberseguridad también puede aprovecharse como una estrategia de negocio para demostrar a los consumidores que su información está protegida y, por ende, consolidará más oportunidades de negocio.

De acuerdo con la 21 Encuesta Global de CEOs de PwC, el 87% de los directivos dice que está invirtiendo en ciberseguridad para generar confianza con los clientes. Casi la misma cantidad (81%) afirma que está mejorando en la transparencia con respecto al uso y almacenamiento de datos.

Por otro lado, una encuesta de opinión pública hecha en la Unión Europea en 2017 revela que el 61% de los entrevistados considera la seguridad y la privacidad como un elemento importante en su decisión de compra de un producto de tecnologías de la información. El 27% de los encuestados afirmó que está dispuesto a pagar un costo adicional por estas características.

Lo anterior refleja que los consumidores dan un valor monetario a la privacidad, es decir, puede concluirse que están dispuestos a pagar más por los productos de tecnología diseñados con un enfoque en seguridad y privacidad. Sin embargo, los consumidores, a menudo, no tienen esa opción, debido a que muchos dispositivos son producidos y vendidos a bajo costo, y no cuentan con protección de seguridad. Las empresas pueden aprovechar la oportunidad para demostrarle a sus clientes que su información está protegida.

Las economías y las sociedades viven una gran transformación a causa de las tecnologías digitales que, pese a todas las ventajas que ofrecen, también amplían las posibilidades de ataques cibernéticos. Para que las empresas progresen en un entorno con riesgos más sofisticados, diseñar una estrategia con las mejores prácticas y herramientas es el mejor escudo ante estas amenazas y refuerza la confianza de los consumidores en las organizaciones.

**Sobre el GSISS 2018**

El Global State of Information Security Survey (GSISS) 2018 de PwC se realizó en línea entre el 24 de abril y el 26 de mayo de 2017. Los informes se basan en las respuestas de más de 9,500 CEO, CFO, CIO, CISO, OSC, VP y directores de Tecnologías de la Información (TI) de más de 122 países. Para la encuesta 2018 en México, respondieron 465 personas, de los cuales el 18% fue CEO, el 12% CIO y el 10% COO. El rango de empresas de 101 a 500 empleados fue el más representativo (23%).

## *Contactos*


***Fernando Román***
Socio Líder
Cybersecurity & Privacy
fernando.roman@pwc.com
(55) 5263 5898

***Yonathan Parada***
Socio
Cybersecurity & Privacy
yonathan.parada@pwc.com
(81) 8881 4106

***Ana Cristina Cajiga***
Gerente
Cybersecurity & Privacy
ana.cristina.cajiga@pwc.com
(55) 5263 6138