THALES

Ponemon INSTITUTE

ESTUDIO DE TENDENCIAS DE CIFRADO EN MÉXICO

Julio de 2018

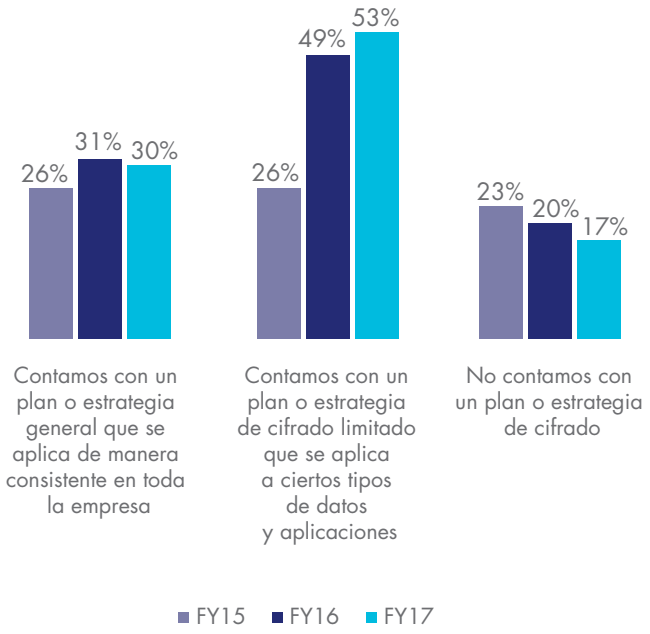
RESUMEN EJECUTIVO

El Ponemon Institute se complace en presentar los resultados del *Estudio de Tendencias en Cifrado en México 2018,* patrocinado por Thales eSecurity. Encuestamos a 468 personas en México para examinar el uso del cifrado y el impacto de esta tecnología en la posición en cuanto a la seguridad de las organizaciones en esta región.

El primer Estudio de Tendencias de Cifrado se realizó en 2005 para una muestra de encuestados de EE. UU. Desde entonces hemos ampliado el alcance del estudio para incluir a encuestados de 11 países además de México. Los 11 países incluyen a: Australia, Brasil, Francia, Alemania, India, Japón, Medio Oriente, la Federación Rusa, el Reino Unido, los Estados Unidos y, por primera vez, Corea del Sur.

Como se muestra en la Figura 1, un mayor número de organizaciones representadas en este estudio continúan reconociendo la importancia de contar con una estrategia de cifrado, ya sea a nivel empresarial (30% de los encuestados) o de una estrategia limitada que apunta a ciertas aplicaciones y tipos de datos (53% de los encuestados).

Figura 1. ¿Qué describe mejor la estrategia de cifrado de su organización?



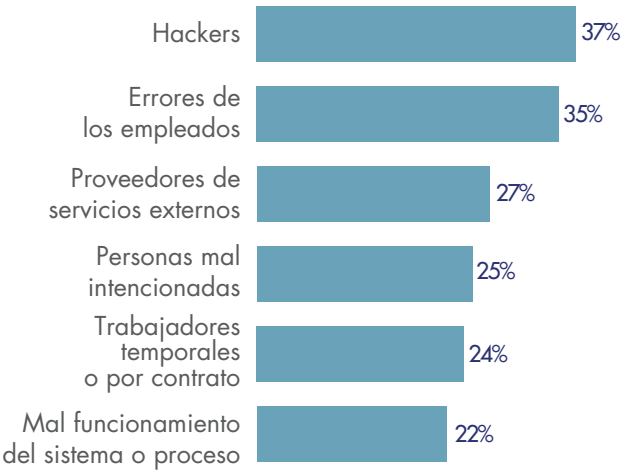
A continuación presentamos un resumen de nuestros resultados principales. En la siguiente sección de este informe se proporcionan detalles de cada uno de los resultados principales.

La influencia para dirigir las estrategias de cifrado se encuentra dispersa en toda la organización. El 27% de los encuestados dice que no hay un solo departamento que tenga la responsabilidad de dirigir las estrategias de cifrado y el 26% de los encuestados dice que las líneas de negocios son las más influyentes. Solo el 23% de los encuestados dice que el área de operaciones de TI tiene influencia.

¿Qué tipos de datos se cifran con mayor frecuencia? Cada vez más empresas están cifrando información financiera, información de clientes y datos relacionados con pagos. Desde 2015, solo algunas empresas cifran los datos de los empleados o de recursos humanos y propiedad intelectual.

Los hackers son la amenaza más importante para los datos confidenciales. Según el 37%, la amenaza más importante para la exposición de datos sensibles o confidenciales son los hackers. El 35% de los encuestados dice que se debe a errores de los empleados, mientras que el 27% respondieron que los proveedores de servicios de terceros representan la mayor amenaza.

Amenazas a los datos confidenciales

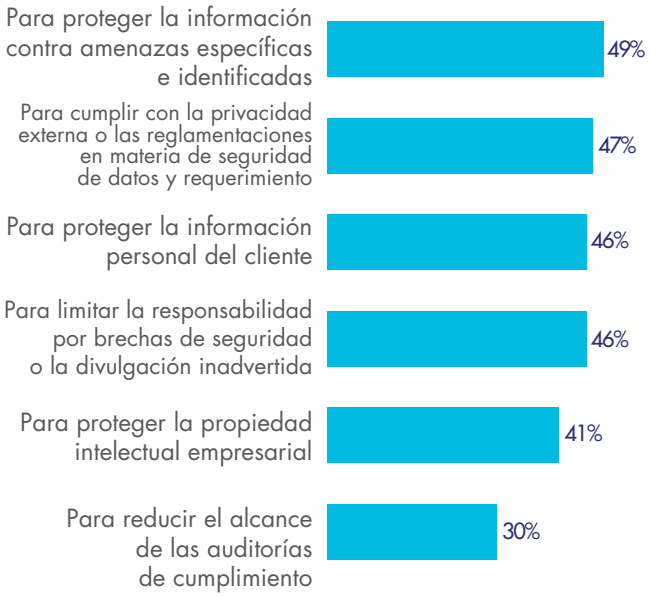


30%

de las organizaciones cuentan ahora con una estrategia de cifrado que se aplica de manera sistemática en toda la empresa

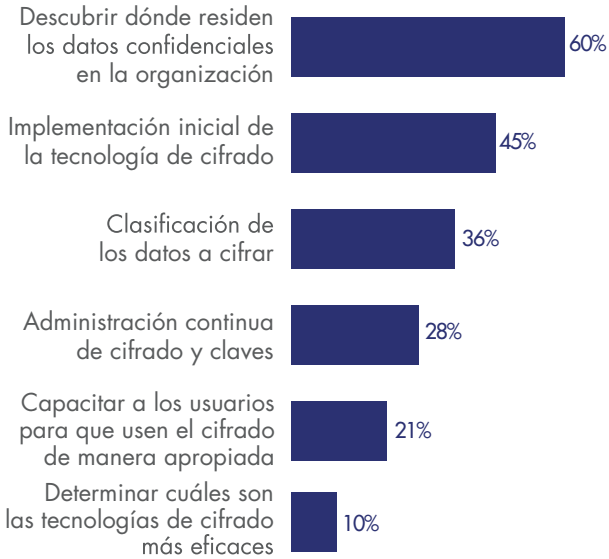
La protección en contra de amenazas identificadas es el principal impulsor para usar tecnologías de cifrado. Varios de los principales impulsores del uso del cifrado han disminuido ligeramente en los últimos tres años, mientras que otros han aumentado. Los cuatro impulsores principales son la protección de la información contra amenazas específicamente identificadas (49%), el cumplimiento y requisitos regulatorios para la seguridad de los datos y privacidad externa (47%), la protección de la información personal del cliente (46%) y para limitar la responsabilidad por brechas de seguridad o divulgación inadvertida (46%).

Qué factores impulsan el cifrado



Descubrir dónde residen los datos confidenciales en la organización sigue siendo el mayor desafío. En los últimos tres años, el mayor reto consiste en la capacidad de descubrir dónde residen los datos confidenciales en la organización (60% de los encuestados) seguido de la implementación inicial de la tecnología de cifrado (45% de los encuestados). El reto de capacitar a los usuarios para que usen el cifrado de manera apropiada ha disminuido en los últimos tres años.

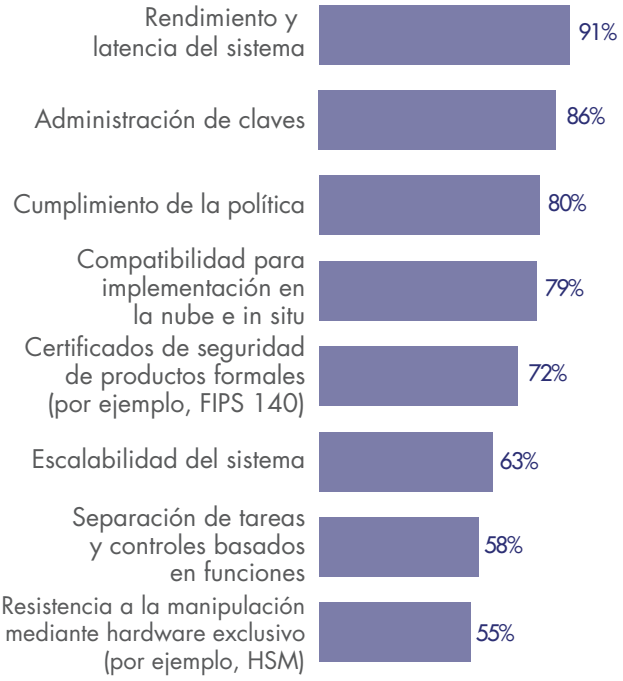
Por qué el cifrado desafía a las organizaciones



No hay una sola tecnología de cifrado que predomine en las organizaciones. Ninguna tecnología domina porque las organizaciones tienen necesidades muy diversas. El cifrado para bases de datos, comunicaciones sobre Internet y los discos duros de las computadoras portátiles son más propensos a ser implementados de manera más amplia. Por el contrario, la implementación en las plataformas y dispositivos del Internet de las cosas (IoT), un caso de uso reciente pero emergente, los repositorios de Big Data y los contenedores Docker tienen menores probabilidades de implementarse parcial o completamente.

Ciertas características de cifrado se consideran más críticas que otras. En los últimos tres años, las siguientes características han aumentado en importancia: la aplicación de políticas, el apoyo para la nube e implementación in situ, la separación de tareas y los controles basados en funciones. El rendimiento del sistema, así como la latencia y la administración de claves, siguen siendo las dos principales características.

¿Cuál es el nivel de importancia de estas características específicas?



¿Qué tan dolorosa es la administración de claves? Usando una escala de 10 puntos, se les pidió a los encuestados que calificaran el "dolor" general asociado con la administración de claves dentro de su organización, donde 1 = impacto mínimo y 10 = impacto severo. El 64% de los encuestados eligió puntuaciones de 7 o más, lo que sugiere un umbral de dolor bastante alto. La razón por la que la administración de claves es difícil se debe a la falta de personal calificado y a que las herramientas para administrarlas son inadecuadas.

¿Cuáles son las claves más difíciles de administrar? El dolor al administrar ciertas claves ha aumentado significativamente. Estas son: claves de cifrado del usuario final (por ejemplo, correo electrónico, cifrado de disco completo), claves de firma (por ejemplo, firma de códigos, firmas digitales) y claves relacionadas con pagos (por ejemplo, cajero automático (ATM), punto de venta (POS), etc.). La dificultad en la administración de claves de cifrado del usuario final es la que más ha aumentado.

La administración de claves continúa siendo problemática, con **las claves para servicios en la nube calificadas como las más difíciles de administrar**

La importancia de los HSM para una estrategia de cifrado o administración de claves crecerá en los próximos 12 meses. Les preguntamos a los encuestados en organizaciones que actualmente implementan HSM qué tan importantes son para su estrategia de administración de cifrado o de claves. El 42% respondió que son importantes actualmente, y el 45% mencionó que serán importantes en los próximos 12 meses. El cifrado de base de datos y el cifrado de nube pública, incluyendo BYOK, son casos de uso que están en crecimiento.

"LES PREGUNTAMOS A LOS ENCUESTADOS EN ORGANIZACIONES QUE ACTUALMENTE IMPLEMENTAN HSM QUÉ TAN IMPORTANTES SON PARA SU ESTRATEGIA DE ADMINISTRACIÓN DE CIFRADO O DE CLAVES. EL 42% RESPONDIÓ QUE SON IMPORTANTES ACTUALMENTE, Y EL 45% MENCIONÓ QUE SERÁN IMPORTANTES EN LOS PRÓXIMOS 12 MESES".

42%

Los HSM fueron calificados ya sea como *muy importantes o importantes* **por el** 42% de los encuestados

Cómo usan los HSM las organizaciones. El 65% de los encuestados dice tener un equipo centralizado que brinda criptografía como servicio y el 35% dijo que los dueños de las aplicaciones son los responsables de sus servicios criptográficos.

71%

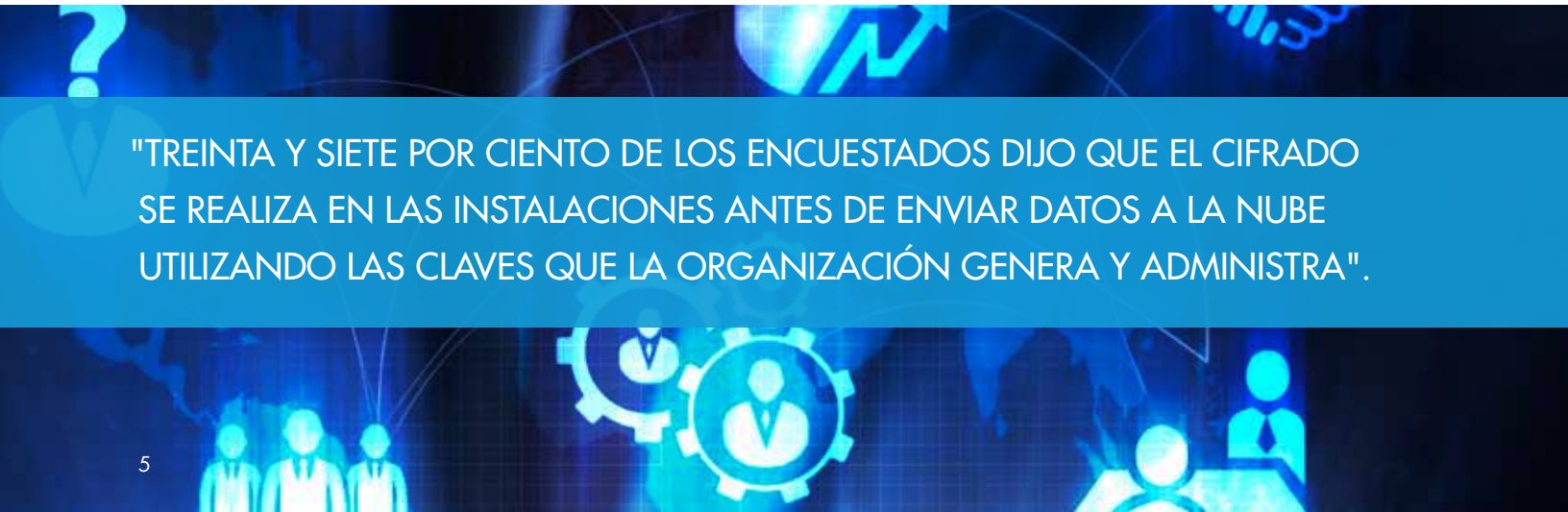
usará **múltiples proveedores de servicios en la nube pública** en los próximos dos años

La mayoría de las organizaciones envían a la nube datos sensibles o confidenciales. El 52% de los encuestados dice que sus organizaciones actualmente envían a la nube datos sensibles o confidenciales (estén o no cifrados, o que no se puedan leer a través de algún otro mecanismo) y el 24% respondió que planea hacerlo en un período de 12-24 meses. El 36% de los encuestados dice que el proveedor de servicios en la nube es el principal responsable de proteger los datos sensibles o confidenciales que se envían a la nube.

37%

El cifrado en servicios en la nube pública creció un **11% durante el año pasado**.

¿Cómo se protegen en la nube los datos en reposo? El 37% de los encuestados dice que el cifrado se realiza in situ antes de enviar datos a la nube utilizando claves que la organización genera y administra y el 33% respondió que el cifrado se realiza en la nube utilizando claves generadas/administradas por el proveedor de servicios de la misma.



"TREINTA Y SIETE POR CIENTO DE LOS ENCUESTADOS DIJO QUE EL CIFRADO SE REALIZA EN LAS INSTALACIONES ANTES DE ENVIAR DATOS A LA NUBE UTILIZANDO LAS CLAVES QUE LA ORGANIZACIÓN GENERA Y ADMINISTRA".

"EL 52% DE LOS ENCUESTADOS DICE QUE SUS ORGANIZACIONES ACTUALMENTE ENVÍAN A LA NUBE DATOS SENSIBLES O CONFIDENCIALES (ESTÉN O NO CIFRADOS, O QUE NO SE PUEDAN LEER A TRAVÉS DE ALGÚN OTRO MECANISMO) Y EL 24% RESPONDIÓ QUE PLANEA HACERLO EN UN PERÍODO DE 12 A 24 MESES".

Acerca de Ponemon Institute

Ponemon Institute© se dedica a promover prácticas de gestión de información y privacidad responsables en las empresas y el gobierno. Para lograr este objetivo, el Instituto lleva a cabo una investigación independiente, educa a los líderes de los sectores público y privado y verifica las prácticas de privacidad y protección de datos de las organizaciones en una variedad de industrias.

Acerca de Thales eSecurity

Thales eSecurity es un líder en soluciones y servicios avanzados de seguridad de datos que ofrece confianza en todo lugar donde se genera, transmite o almacena información. Nos aseguramos de que los datos que le pertenecen a las empresas y entidades de gobierno estén seguros y sean confiables en cualquier entorno, en sus instalaciones, en la nube, en centros de datos o en entornos de Big Data, sin sacrificar la agilidad empresarial. La seguridad no sólo minimiza el riesgo, también facilita las iniciativas digitales que ahora impregnan nuestra vida cotidiana: el dinero digital, las identidades electrónicas, la atención de la salud, los automóviles conectados, y con el internet de las cosas (IoT), incluso los electrodomésticos. Thales proporciona todo lo que una organización necesita para proteger y administrar sus datos, identidades y propiedad intelectual, así como el cumplimiento de las reglamentaciones, a través del cifrado, la administración de claves avanzada, la tokenización, los controles de acceso de usuario a información privilegiada y las soluciones de alta seguridad. Los profesionales en seguridad de todo el mundo confían en Thales para acelerar la transformación digital de su organización de manera confiable. Thales eSecurity forma parte de Thales Group.

Acerca de Thales

Las personas en las que todos confiamos para hacer que el mundo gire confían en Thales. Nuestros clientes vienen a nosotros con grandes ambiciones: para hacer la vida mejor, para mantenernos más seguros. Con la combinación de una diversidad única de experiencia, talentos y culturas, nuestros arquitectos diseñan y entregan extraordinarias soluciones de alta tecnología. Soluciones que hacen posible el mañana, hoy. Desde el fondo de los océanos hasta la profundidad del espacio y el ciberespacio, ayudamos a nuestros clientes a pensar de forma más inteligente y a actuar más rápido: dominando una complejidad cada vez mayor y cada momento decisivo en el camino. Con 65 000 empleados en 56 países, Thales reportó ventas de €15.8 mil millones en 2017.

HAGA CLICK AQUÍ PARA LEER EL INFORME COMPLETO

NUESTROS PATROCINADORES

VENAFI

GEOBRIDGE

cloud security alliance

GuidePoint SECURITY

CRITICALSTART

OASIS

THALES

www.thalesesecurity.com