Ponemon INSTITUTE

nCIPHER
AN ENTRUST DATACARD COMPANY

2019/20 ESTUDIO DE TENDENCIAS DE CIFRADO - EDICIÓN MÉXICO

Resumen Ejecutivo

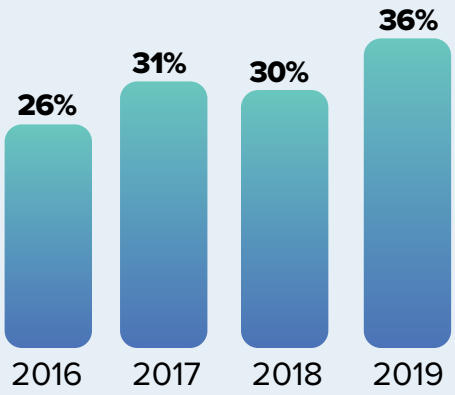
PONEMON INSTITUTE SE COMPLACE EN PRESENTAR LOS RESULTADOS DEL *ESTUDIO DE TENDENCIAS DE CIFRADO EN MÉXICO 2019*, PATROCINADO POR NCIPHER SECURITY.

Encuestamos a 499 personas en México para analizar el uso del cifrado y el impacto de esta tecnología y la postura de seguridad en las organizaciones en esta región.

El primer Estudio de Tendencias de Cifrado se llevó a cabo en 2005 tomando como muestra únicamente a encuestados en Estados Unidos. A partir de entonces hemos decidido ampliar la investigación del estudio e incluir otros países en el mundo.

Desde 2015, el porcentaje de organizaciones con una estrategia de cifrado general que se aplica de manera consistente en toda la empresa ha aumentado del 26% al 36%, tal como se muestra en la figura a continuación. Las organizaciones con un plan o estrategia de cifrado limitado aumentaron del 26% al 47%.

El **36%** de las organizaciones cuenta ahora con una estrategia de cifrado consistente para toda la empresa.



Las páginas a continuación ofrecen un resumen de nuestros resultados principales.

ESTRATEGIA Y ADOPCIÓN DEL CIFRADO

Ninguna función influye por sí sola en el curso de las estrategias de cifrado. Si bien la responsabilidad por la estrategia de cifrado está dispersa en toda la organización, el 31% de los encuestados afirma que ninguna función es responsable por sí sola de la estrategia de cifrado; este indicador es seguido por la seguridad (el 24% de los encuestados) y las operaciones de TI (el 22% de los encuestados).

¿Qué tipo de datos se cifran con mayor frecuencia? En su mayoría, las empresas están cifrando datos relacionados con pagos e información financiera. El cifrado de registros de clientes ha aumentado significativamente desde 2015.

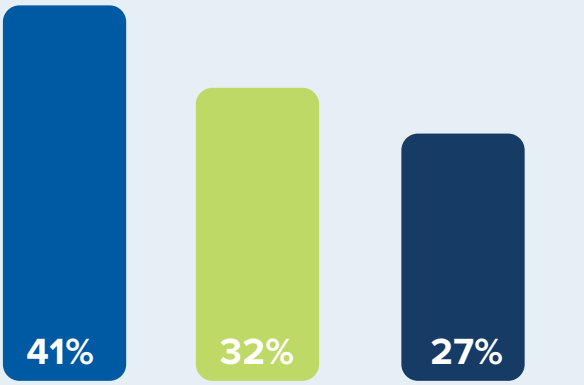
> Desde 2015, el porcentaje de organizaciones con una estrategia de cifrado general que se aplica de manera consistente en toda la empresa ha aumentado del 26% al 36%.

AMENAZAS, PRINCIPALES IMPULSORES Y PRIORIDADES

Los errores de los empleados son la mayor amenaza contra los datos confidenciales. La amenaza más importante de vulnerabilidad de información confidencial o sensible son los errores de los empleados, según el 41% de los encuestados. El 32% de los encuestados dice que los hackers representan la mayor amenaza y el 27% dice que son los agentes internos malintencionados.

El **41%**

Los errores de los empleados son la amenaza más significativa para los datos confidenciales



Errores de los empleados

Hackers

Agentes internos maliciosos *(segunda más alta de la región)*

La protección de la información personal de los clientes es el principal factor impulsor del uso de tecnologías de cifrado. La importancia de proteger la información personal de los clientes y el cumplimiento de las normas y los requisitos externos en materia de seguridad de datos o privacidad, son los principales factores impulsores según el 56% y el 46% de los encuestados, respectivamente.

El **56%**

La protección de la información personal del cliente es la razón principal para **cifrar los datos.**

> El 32% de los encuestados dice que los hackers representan la mayor amenaza y el 27% dice que son los agentes internos malintencionados.

Descubrir dónde residen los datos confidenciales en la organización continúa siendo el mayor desafío. Descubrir dónde residen los datos confidenciales en la organización y la implementación inicial de la tecnología de cifrado son los mayores desafíos en la planificación y ejecución de una estrategia de cifrado de datos, según el 56% y el 48% de los encuestados, respectivamente.

OPCIONES DE IMPLEMENTACIÓN

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 comunicaciones por Internet, bases de datos, copias de seguridad y archivos es más propenso a ser implementado de manera más amplia. Por el contrario, la implementación en las plataformas y dispositivos del Internet de las cosas (IoT) y los repositorios de Big Data tienen menores probabilidades de implementarse parcial o ampliamente.

Ciertas características del cifrado se consideran más críticas que otras. Las características más importantes son la administración de claves (el 81% de los encuestados), la aplicación de políticas (el 79% de los encuestados) y la escalabilidad del sistema (el 70% de los encuestados). Las características que no se consideran importantes son la integración con otras herramientas de seguridad (el 46% de los encuestados) y la compatibilidad con algoritmos emergentes (el 35% de los encuestados).

ACTITUDES FRENTE A LA ADMINISTRACIÓN DE CLAVES

¿Por qué es difícil la administración de claves? El 69% de los encuestados califica como muy alta la dificultad en la administración de claves. Las principales razones son: la falta de personal calificado (el 82% de los encuestados), la falta de claridad con respecto a quiénes están a cargo (el 48% de los encuestados) y la deficiencia de las herramientas de administración de claves (el 43% de los encuestados).

El **69%** de los encuestados otorga a la dificultad en la administración de claves de cifrado una calificación de **7** o más en una escala de **10** puntos.

1 = impacto mínimo, 10 = impacto severo

¿Qué claves son las más difíciles de administrar? Las claves más difíciles de administrar son las claves de cifrado del usuario final (por ejemplo, el correo electrónico, el cifrado de disco completo), las claves del protocolo Secure Shell Session (SSH) y las claves de firma.

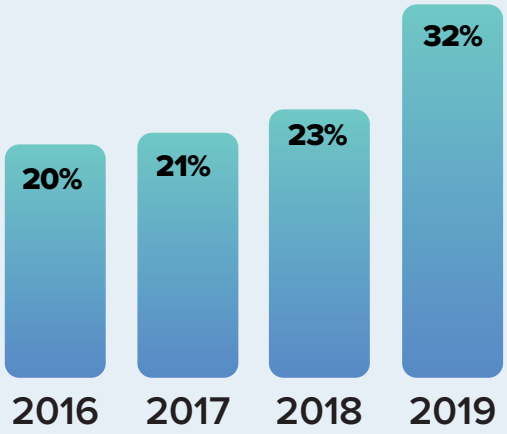
Las empresas de los encuestados utilizan una variedad de sistemas de administración de claves. Los sistemas que más se suelen implementar son: la política formal de administración de claves (KMP) y los procesos manuales (el 56% y el 55% de los encuestados, respectivamente).

> El 69% de los encuestados califica de manera muy alta la dificultad que tienen para administrar las claves

IMPORTANCIA DE LOS MÓDULOS DE SEGURIDAD DE HARDWARE (HSM)

La adopción de HSM está en crecimiento. El 32% de las empresas reportaron que su organización utiliza HSM en la actualidad. Esto indica un aumento del 23% con respecto al año pasado.

El **32%**
DE LOS ENCUESTADOS
UTILIZA **HSMs**



La importancia de los HSMs 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 HSMs qué tan importantes son para su estrategia de administración de cifrado o de claves. El 39% de los encuestados dice que son importantes en la actualidad y el 55% de los encuestados dice que serán importantes en los próximos 12 meses. El principal caso de uso de los HSMs es el cifrado a nivel de la aplicación. Se prevé que el cifrado de la base de datos crezca en los próximos 12 meses.

Cómo están utilizando los HSM las organizaciones. El 61% de los encuestados dice tener un equipo centralizado que brinda criptografía como servicio y el 39% dice que los dueños de las aplicaciones son los responsables de sus propios servicios criptográficos. México ha demostrado el mismo progreso al pasar a un modelo centralizado de criptografía: el promedio global es del 60% de los encuestados.

El **61%**
de las organizaciones usa los HSMs para proporcionar cifrado **interno como servicio.**

CIFRADO EN LA NUBE

La mayoría de las organizaciones envía a la nube datos sensibles o confidenciales. El 49% 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 26% planea hacerlo en un período de 12 a 24 meses. El 40% 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.

¿Cómo se protegen los datos en reposo en la nube? El 35% 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 25% de los encuestados dice que el cifrado se realiza en la nube utilizando claves generadas o administradas por el proveedor de servicios en la nube.

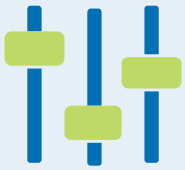
¿Cuáles son las características de cifrado específicas para la nube más importantes? Las características más importantes son el soporte para el estándar de KMIP para la administración de claves (el 88% de los encuestados), la integración SIEM (el 54% de los encuestados) y los controles de acceso a usuarios privilegiados (el 46% de los encuestados).

LAS CARACTERÍSTICAS MÁS IMPORTANTES DEL CIFRADO EN LA NUBE SON:

88%
Soporte para el estándar KMIP para la administración de claves

54%
Integración SIEM, visualización y análisis de registros

46%
Control de acceso a usuarios con información privilegiada



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 investigaciones independientes, educa a los líderes del sector público y del privado, y verifica las prácticas de privacidad y de protección de datos de las organizaciones en una variedad de industrias.

ACERCA DE NCIPHER SECURITY

nCipher Security, una empresa de Entrust Datacard, lidera el mercado de Módulos de Seguridad de Hardware (HSMs) de propósito general y con ello fortalece a las organizaciones líderes en el mundo al brindarles confianza, integridad y control sobre la información y las aplicaciones críticas de sus negocios. El rápido entorno digital de hoy en día mejora la satisfacción del cliente, proporciona una ventaja competitiva y mejora la eficiencia operativa. Y también multiplica los riesgos en seguridad. Nuestras soluciones criptográficas protegen las tecnologías emergentes, tales como la nube, el IoT, el blockchain, los pagos digitales, y ayudan a cumplir con las nuevas exigencias en materia de cumplimiento. Esto lo llevamos a cabo utilizando la misma tecnología comprobada de la que dependen las organizaciones globales en la actualidad para protegerse contra las amenazas a sus datos confidenciales, las comunicaciones de red y la infraestructura empresarial. Le ofrecemos confianza para las aplicaciones críticas de su negocio, aseguramos la integridad de sus datos y le damos el control completo, hoy, mañana y en todo momento. **www.ncipher.com**

HAGA CLIC PARA DESCARGAR EL INFORME COMPLETO

Buscar: nCipherSecurity

www.ncipher.com

nCIPHER
AN ENTRUST DATACARD COMPANY