Ponemon INSTITUTE

ENTRUST

Usted está aquí, al igual que sus datos.
Las amenazas están por todas partes.

ESTUDIO GLOBAL SOBRE LAS TENDENCIAS DE CIFRADO PARA 2021

Resumen ejecutivo

PONEMON INSTITUTE PRESENTA LOS RESULTADOS DEL ESTUDIO GLOBAL SOBRE LAS TENDENCIAS DE CIFRADO PARA 2021[1]

Encuestamos a 6610 personas de diversos sectores industriales, ubicadas en 17 países o regiones: Alemania, Australia, Brasil, Corea del Sur, España, Estados Unidos, Federación Rusa, Francia, Hong Kong, Japón, México, Oriente Medio (que agrupa encuestados ubicados en Arabia Saudita y los Emiratos Árabes Unidos), Países Bajos, Reino Unido, Sudeste Asiático, Suecia y Taiwán[2].

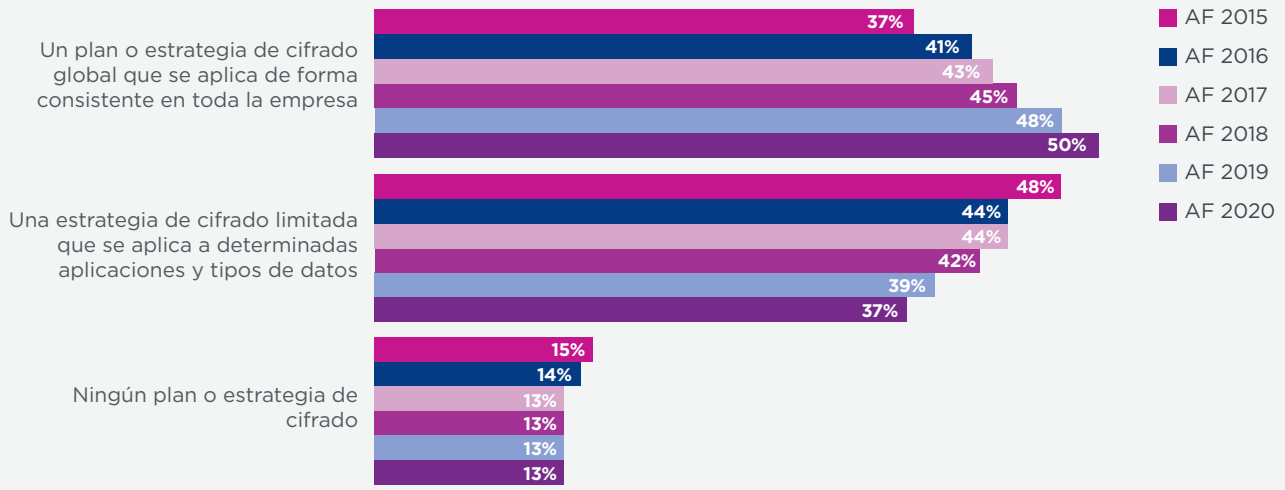
El objetivo de esta investigación es determinar cómo ha evolucionado el uso del cifrado en los últimos 16 años y qué efectos ha tenido esta tecnología en las percepciones sobre la seguridad de las organizaciones. El primer estudio sobre las tendencias de cifrado se llevó a cabo en 2005, con un muestreo de encuestados de Estados Unidos[3].

Desde entonces, hemos ampliado el alcance de la investigación para incluir encuestados de todas las regiones del mundo.

Como se ilustra en la Figura 1, desde 2015 se ha producido un crecimiento constante de la implementación de una estrategia general de cifrado. Este año, el 50% de los encuestados señala que sus organizaciones cuentan con un plan de cifrado global que se aplica de forma consistente en toda la empresa, mientras que el 37% dice tener un plan o una estrategia de cifrado limitada, que se aplica a determinadas aplicaciones y tipos de datos. Esto representa un leve descenso con respecto al año pasado.

A continuación, se encuentran los resultados del estudio de este año.

Figura 1. **¿Tiene su empresa una estrategia de cifrado?**
El muestreo de los países se presenta consolidado.



[1] La recopilación de datos para este estudio comenzó en diciembre de 2020 y finalizó en enero de 2021. Los datos de tendencias presentados a lo largo del informe se basan en el año fiscal en el que se inició la encuesta y no en el año en el que concluyó la preparación de este informe. Por lo tanto, los resultados que se presentan actualmente corresponden al año fiscal 2020.

[2] Los resultados por país se muestran abreviados de la siguiente manera: Alemania (DE), Australia (AU), Brasil (BZ), Corea (KO), España (SP), Estados Unidos (US), Francia (FR), Hong Kong (HK), Japón (JP), México (MX), Oriente Medio (AB), Países Bajos (NL), Reino Unido (UK), Rusia (RF), Sudeste Asiático (SA), Suecia (SW) y Taiwán (TW).

[3] El análisis de tendencias que se muestra en este estudio se ha generado a partir de muestras combinadas de distintos países a lo largo de 16 años (desde 2005).

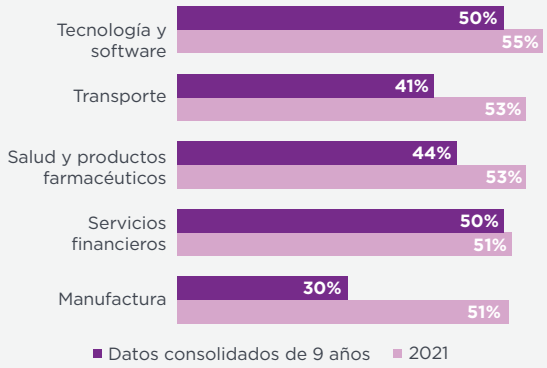
ESTRATEGIA Y ADOPCIÓN DEL CIFRADO

Aumentan las estrategias de cifrado para toda la empresa. Desde que se comenzó a llevar a cabo este estudio hace 16 años, se ha producido un aumento constante de la cantidad de organizaciones que cuentan con una estrategia de cifrado aplicada de forma consistente en toda la empresa. A su vez, se ha producido una disminución constante de la cantidad de organizaciones que no cuentan con ningún plan o estrategia de cifrado. Básicamente, los resultados se han invertido a lo largo de los años del estudio.

Algunos países tienen estrategias de cifrado más consolidadas. La preponderancia de una estrategia de cifrado corporativa varía entre los distintos países representados en esta investigación. La mayor presencia de una estrategia de cifrado corporativa se registra en Alemania, Estados Unidos, Japón y los Países Bajos. Los menores niveles de adopción de una estrategia corporativa, según los encuestados, se encontraron en la Federación Rusa y Brasil. El promedio mundial de adopción es del 50%.

La función de operaciones de TI es la que más ha influido en la estructuración de la estrategia de cifrado de las organizaciones en los últimos 14 años. Sin embargo, en Estados Unidos, las áreas más influyentes son las líneas de negocio (35% de los encuestados). Operaciones de TI tiene mayor influencia en Suecia, Corea y Francia.

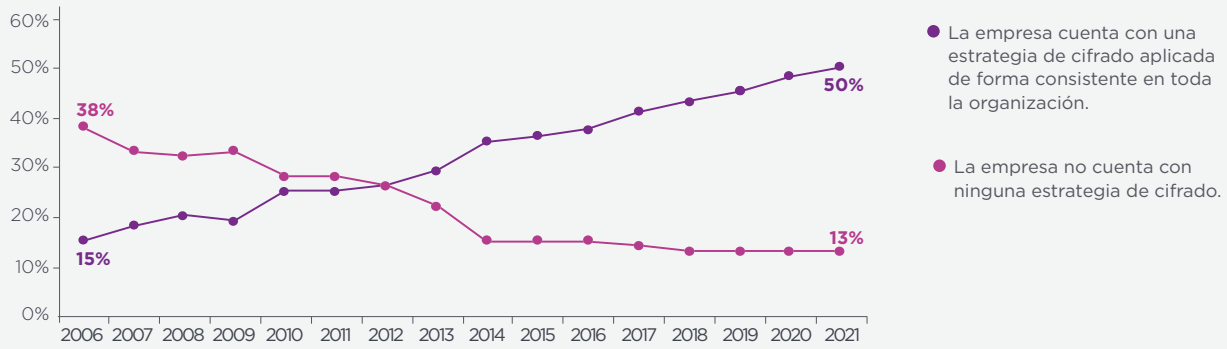
En aumento: las 5 industrias con mayor crecimiento del uso de cifrado



TENDENCIAS DE ADOPCIÓN DE CIFRADO

El uso de cifrado ha aumentado en todos los sectores. Los resultados indican un aumento constante en todos los sectores industriales, con la excepción de las organizaciones dedicadas a comunicaciones y servicios. Los aumentos más pronunciados en el uso extendido del cifrado se observan en la industria manufacturera, hotelería y productos de consumo.

Sus datos están por las nubes. ¿Su estrategia de cifrado está tomando mayor importancia?
Tendencias de estrategias de cifrado



Aumenta el uso generalizado de las tecnologías de cifrado. Desde que empezamos a medir el uso del cifrado en toda la empresa en 2005, hemos visto un aumento constante en el uso extendido de soluciones de cifrado en las organizaciones.

AMENAZAS, MOTIVACIONES PRINCIPALES Y PRIORIDADES

Los errores de los empleados siguen representando la amenaza más importante para los datos confidenciales. La principal amenaza para la exposición de datos delicados o confidenciales son los errores de los empleados.

En cambio, las amenazas menos significativas para estos datos son las escuchas gubernamentales y las solicitudes lícitas de datos. La preocupación por la exposición involuntaria (errores de empleados y mal funcionamiento del sistema) supera considerablemente la preocupación por ataques reales de trabajadores temporales o contratados y de personas malintencionadas.

Error o malicia: los resultados son los mismos
Las 6 amenazas principales para los datos confidenciales

La motivación principal para implementar el cifrado es la protección de la información personal de los clientes. Las organizaciones utilizan el cifrado para proteger la información personal de los clientes (54% de los encuestados), la información de amenazas específicas e identificadas (50% de los encuestados) y la propiedad intelectual de la empresa (49% de los encuestados).

Un obstáculo para el éxito de una estrategia de cifrado es la capacidad de determinar en qué parte de la organización se encuentran los datos confidenciales. El 65% de los encuestados afirma que el principal desafío es identificar en qué parte de la organización se encuentran los datos confidenciales. El 43% indicó que la implementación inicial de la tecnología de cifrado representa un esfuerzo considerable, mientras que el 34% mencionó que es difícil clasificar qué datos se deben cifrar.

¿Quién encontrará primero sus datos sin cifrar?

El **65**% de los encuestados afirma que el principal desafío de una estrategia de cifrado es identificar dónde se encuentran los datos confidenciales.

OPCIONES DE IMPLEMENTACIÓN

No hay ninguna tecnología de cifrado que sea la dominante entre las organizaciones. Las organizaciones tiene necesidades muy diversas. Las tecnologías en las que más probable se implemente el cifrado son las comunicaciones por internet, las bases de datos y las redes internas, que corresponden a los casos de uso más consolidados. Este es el cuarto año en el que el estudio mide la implementación del cifrado de plataformas y dispositivos de IoT. El 61% de los encuestados afirma que han implementado, al menos parcialmente, el cifrado de los dispositivos de IoT, mientras que también el 61% sostiene lo mismo para las plataformas de IoT.

CARACTERÍSTICAS DEL CIFRADO QUE SE CONSIDERAN MÁS IMPORTANTES

Algunas características de cifrado se consideran más importantes que otras. De acuerdo con los resultados consolidados del estudio, el rendimiento y la latencia del sistema, la administración de las claves y la aplicación de las políticas de seguridad son las tres características de cifrado más importantes.

Características imprescindibles de la protección de datos

Las 5 características principales de las soluciones de cifrado

¿Qué tipos de datos se cifran con mayor frecuencia? Debido a la vulneración de datos de alto perfil en los servicios financieros, los datos relacionados con los pagos y registros financieros son los más propensos al cifrado. El tipo de datos que es menos probable que se cifre es la información relacionada con la salud y la información no financiera. Este es un resultado sorprendente, dada la confidencialidad de la información médica.

ACTITUDES CON RESPECTO A LA ADMINISTRACIÓN DE CLAVES

¿Qué tan dificultosa es la administración de claves? El 56% de los encuestados califica la administración de claves como muy dificultosa, lo que indica que los encuestados consideran que la administración de claves es una actividad muy exigente.

El mayor porcentaje de sensación de dificultad se da en España, con el 69%. El nivel más bajo se encuentra en Francia, con el 37%. La falta de responsabilidades claramente definidas y la carencia de personal calificado son las principales razones por las que la administración de claves se considera una actividad dificultosa.

IMPORTANCIA DE LOS MÓDULOS DE SEGURIDAD DE HARDWARE (HSMs)

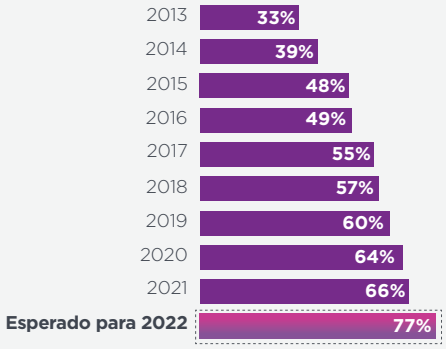
Las organizaciones de Estados Unidos, Alemania y Japón son más propensas a implementar HSMs. Es más probable que se implementen HSMs en Estados Unidos, Alemania y Japón que en otros países. El promedio general de implementación de HSMs es del 49%.

De qué forma se implementan principalmente los HSMs junto con aplicaciones basadas en la nube pública en la actualidad y cómo se implementarán en los próximos 12 meses. El 41% de los encuestados afirma que sus organizaciones poseen y operan HSMs locales, a los que acceden en tiempo real a través de aplicaciones hospedadas en la nube. En cambio, el 39% de los encuestados alquilan o utilizan HSMs de un proveedor de nube pública, con el mismo propósito. Se espera que el uso de HSMs a través de agentes de seguridad de acceso a la nube, así como la propiedad y operación de HSMs locales, aumenten considerablemente.

La valoración general promedio de la importancia de los HSMs como parte de una estrategia de cifrado y de administración de claves para este año es del 66%. Las respuestas indican que las organizaciones de Estados Unidos, Oriente Medio y los Países Bajos son las que más importancia atribuyen a los HSMs como parte de las actividades de cifrado o de administración de claves.

Las claves del éxito

Nivel de importancia de los HSMs en la estrategia de cifrado y administración de claves de la organización



¿De qué manera las organizaciones acceden a los HSMs? El 61% de los encuestados afirma que cuentan con un equipo centralizado que brinda servicios de criptografía (incluidos los HSMs) a múltiples equipos y aplicaciones de la organización (es decir, un modelo de nube privada). En cambio, el 39% sostiene que cada propietario o equipo a cargo de una aplicación en particular es responsable de sus propios servicios criptográficos (incluidos los HSMs), lo que representa un enfoque más tradicional de implementación en silos de centros de cómputos específicos por aplicación.

¿Cuáles son los principales objetivos o usos de los HSMs? Los tres usos principales son el cifrado en el nivel de la aplicación y TLS/SSL, seguidos, particularmente, por los servicios de cifrado y firma de contenedores. Durante los próximos 12 meses, se espera un aumento significativo del cifrado de bases de datos.

CIFRADO EN LA NUBE

El 60% de los encuestados afirma que sus organizaciones transfieren datos delicados o confidenciales a la nube, independientemente de si se cifran o se vuelven ilegibles por otro mecanismo, como la tokenización o el enmascaramiento de datos. Otro 24% de los encuestados prevé que comenzará a hacerlo en los próximos uno o dos años. Estos resultados indican que las ventajas de la informática en la nube superan los riesgos asociados a la transferencia de datos delicados o confidenciales a la nube.

¿Cómo protegen las organizaciones los datos en reposo en la nube? El 38% de los encuestados afirma que el cifrado se realiza de forma local, antes de enviar los datos a la nube, mediante claves generadas y administradas por la organización. Sin embargo, el 36% realiza el cifrado directamente en la nube, con claves generadas o administradas por el proveedor de la nube. El 21% de los encuestados utiliza algún enfoque de tipo Bring Your Own Key (BYOK).

¿Cuáles son las tres principales características de cifrado que son específicas para la nube? Las tres características más importantes son la compatibilidad con el estándar KMIP (Key Management Interoperability Protocol) para la administración de claves (59% de los encuestados), la integración, visualización y análisis de registros de SIEM (59% de los encuestados) y los controles de acceso pormenorizados (55% de los encuestados).

Cómo superar los desafíos de proteger los datos en múltiples nubes

Las 10 características principales del cifrado en la nube

ACERCA DE PONEMON INSTITUTE

Ponemon Institute© se dedica a promover prácticas responsables de administración de la información y la confidencialidad entre las empresas y los organismos públicos. Para lograr este objetivo, lleva a cabo investigaciones independientes, capacita a líderes del sector público y privado, y comprueba las prácticas de confidencialidad y protección de datos en organizaciones de una diversidad de industrias.

ACERCA DE ENTRUST

Entrust brinda seguridad a un mundo en constante movimiento al garantizar la confianza en las identidades, los pagos y la protección de datos. Hoy más que nunca, las personas exigen experiencias fluidas y seguras al cruzar fronteras, hacer compras, utilizar servicios de gobierno electrónico o acceder a redes corporativas. Entrust cuenta con una gama única de soluciones de seguridad digital y de emisión de credenciales que constituyen el aspecto clave de estas interacciones. Con más de 2500 colaboradores, una red global de socios tecnológicos y clientes en más de 150 países, las organizaciones más confiables del mundo confían en nosotros sin dudarlo. Para obtener más información, visite **entrust.com.**

PARA LEER LA VERSIÓN COMPLETA DE ESTE INFORME, VISITE: ENTRUST.COM/GO/2021-GETS

ENTRUST

SECURING A WORLD IN MOTION

Explore más en entrust.com