Entrust Datacard®

NCIPHER
AN ENTRUST DATACARD COMPANY

2020/21
ESTUDIO DE TENDENCIAS DE CIFRADO EN MÉXICO

Ponemon INSTITUTE

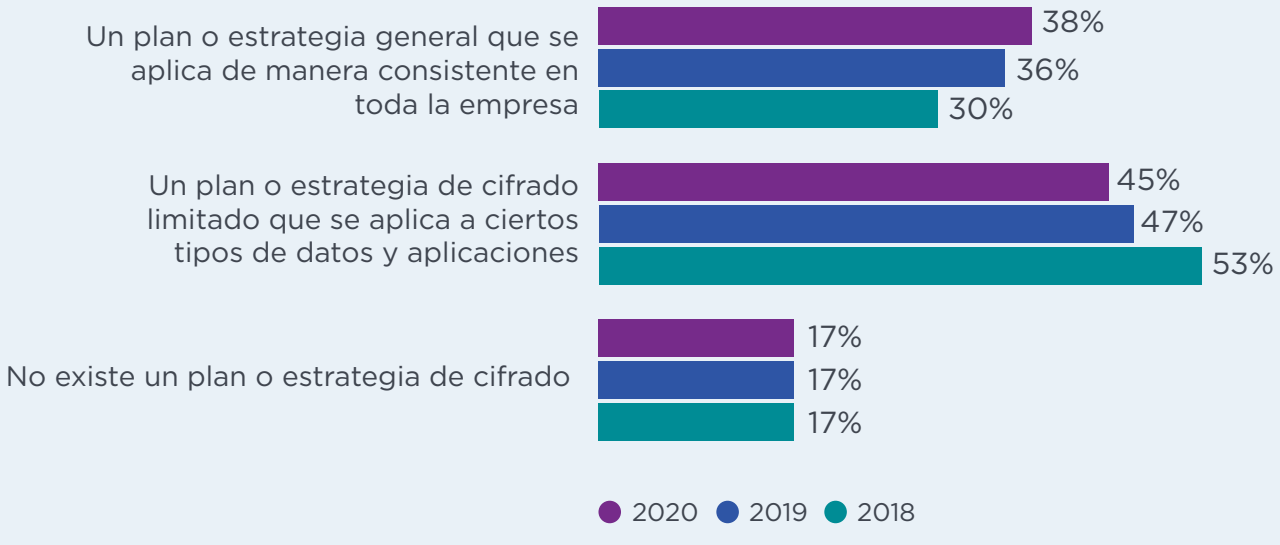
PONEMON INSTITUTE SE COMPLACE EN PRESENTAR LOS RESULTADOS DEL ESTUDIO DE TENDENCIAS DE CIFRADO EN MÉXICO DE 2020, PATROCINADO POR NCIPHER.

Encuestamos a 353 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. A nivel global realizamos una encuesta a 6.457 personas en varios sectores de la industria en 17 países: Australia, Brasil, Francia, Alemania, India, Japón, México, Oriente Medio (una combinación de encuestados ubicados en Arabia Saudita y los Emiratos Árabes Unidos), los Países Bajos, la Federación Rusa, el Sudeste asiático, Corea del Sur, Suecia, Taiwán, el Reino Unido, los Estados Unidos.

El 38% de los encuestados dice que sus organizaciones tienen una estrategia de cifrado general que se aplica de manera uniforme en toda la empresa. Las organizaciones con un plan o estrategia de cifrado limitado corresponden al 45%.

Las páginas a continuación ofrecen un resumen de los resultados de 2020.

El 38% de las organizaciones cuenta con una estrategia de cifrado



ESTRATEGIAS EN LA ADOPCIÓN DEL CIFRADO

Las operaciones de TI continúan teniendo la mayor influencia en la dirección de las estrategias de cifrado. Si bien la responsabilidad de la estrategia de cifrado está distribuida en toda la organización, las operaciones de TI (25% de los encuestados) tienen la mayor influencia. El 31% de los encuestados dice que ninguna función es responsable de la estrategia de cifrado.

¿Qué tipo de datos se cifran con mayor frecuencia? El 62% de los encuestados dice que sus organizaciones están cifrando datos relacionados con los pagos y el 55% de los encuestados dice que sus organizaciones cifran los registros financieros.

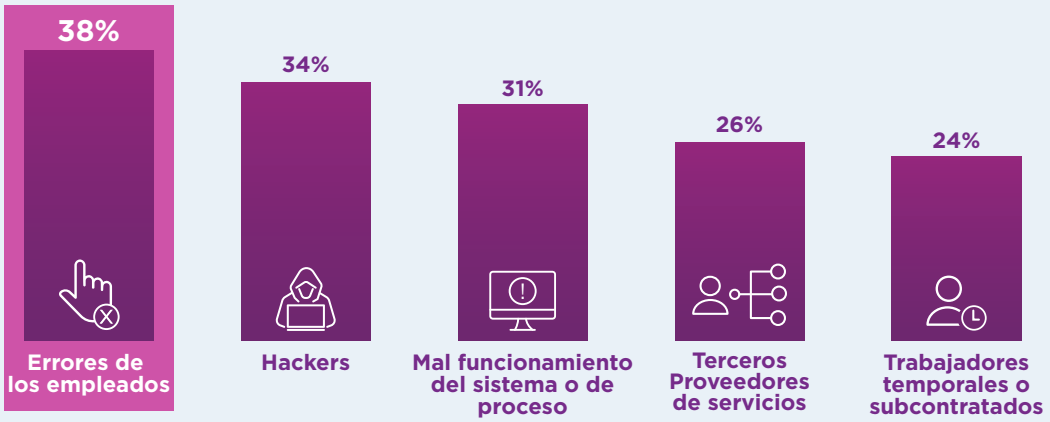
AMENAZAS, PRINCIPALES IMPULSORES Y PRIORIDADES

Los intrusos negligentes y los hackers representan la mayor amenaza para los datos confidenciales. Las amenazas más importantes de vulnerabilidad de información confidencial o sensible son los errores de los empleados (38% de los encuestados), seguido por los hackers, según el 34 por ciento de los encuestados.

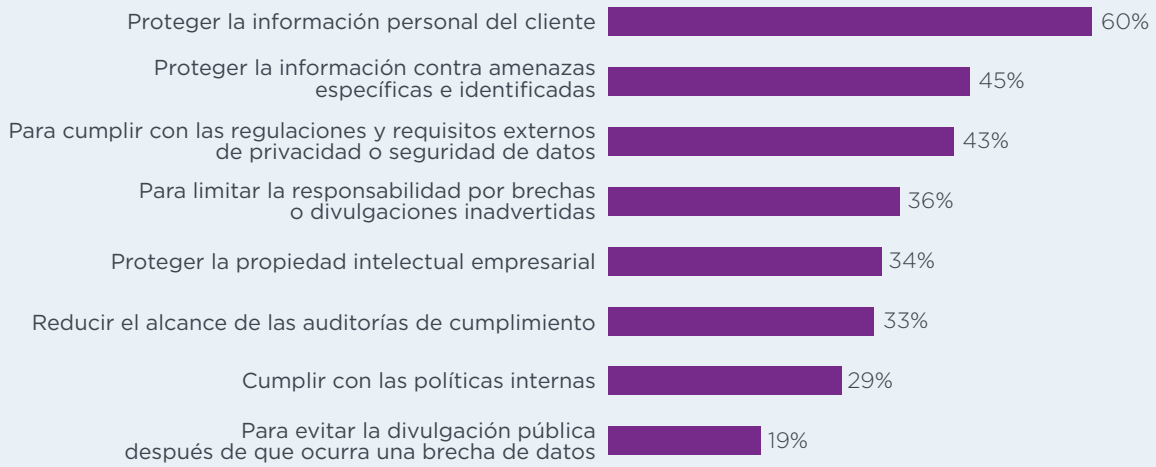
La protección de la información del cliente es la principal razón por la que las organizaciones cifran los datos. La protección de la información del cliente es el principal impulsor del cifrado según el 60% de los encuestados, seguida de la protección de la información contra amenazas específicas identificadas (45 por ciento de los encuestados).

Principales tipos de datos cifrados

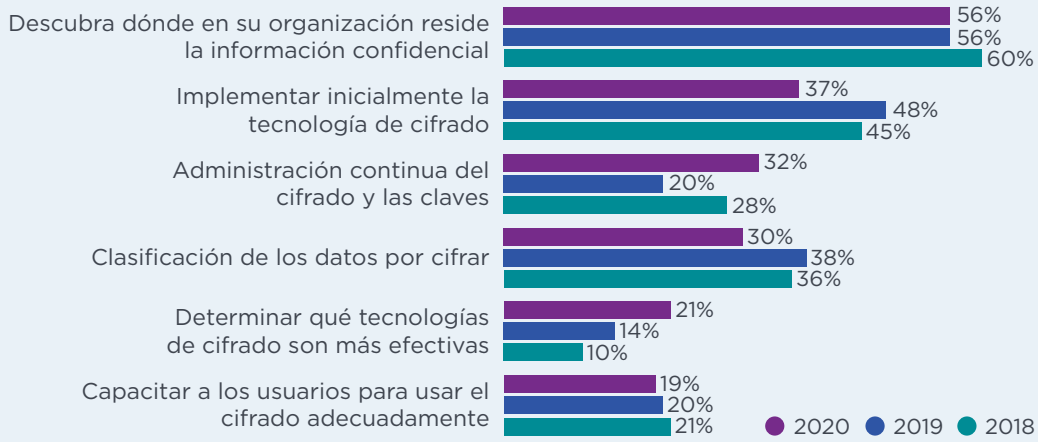
Las principales amenazas a los datos confidenciales



Los principales motivadores para usar tecnología de cifrado



¿Cuáles son los mayores desafíos en la planificación y ejecución de una estrategia informática de cifrado de datos?



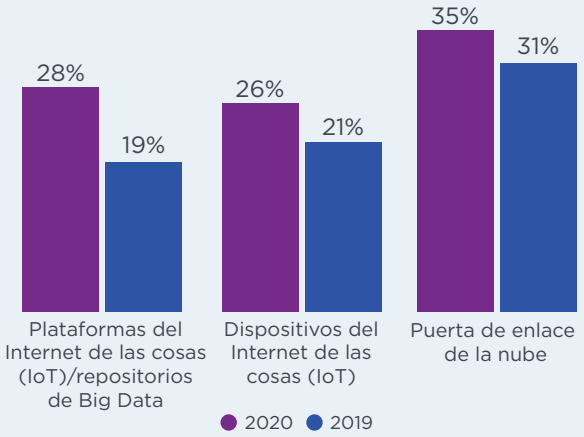
Descubrir dónde residen los datos confidenciales en la organización continúa siendo el mayor desafío. El 56% de los encuestados dice que descubrir dónde residen los datos confidenciales en la organización es el mayor desafío en la planificación y ejecución de una estrategia de cifrado de datos. A esto le sigue la implementación inicial de las tecnologías de cifrado (37% de los encuestados).

OPCIONES DE IMPLEMENTACIÓN

No predomina ninguna tecnología 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, según el 50% y el 42% de los encuestados, respectivamente. El cifrado de plataformas de Internet de las cosas (IoT)/repositorios de datos y dispositivos de IoT se implementa al menos de forma parcial según el 50% y el 47% de los encuestados respectivamente.

Desde el año pasado, las tasas de uso de cifrado para plataformas/repositorios de IoT, dispositivos de IoT y puertas de enlace en la nube han aumentado en un 9%, 5% y 4% respectivamente.

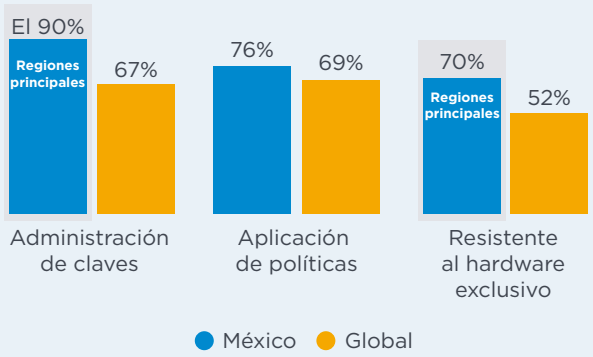
Desde el año pasado, las organizaciones han aumentado su adopción de cifrado para los siguientes casos de uso:



Ciertas características de cifrado se consideran más críticas que otras. A los encuestados se les pidió que calificaran las características de la tecnología de cifrado consideradas como las más importantes para la posición de su organización en cuanto a la seguridad. La mayoría de los encuestados califica la administración de claves (90% de los encuestados) y la aplicación de políticas (76% de los encuestados) como características muy importantes de las tecnologías de cifrado.

México muestra una fuerte preferencia por las soluciones de cifrado que cuentan con administración de claves, la aplicación de políticas y resistencia a las manipulaciones indebidas

¿Qué importancia tienen las siguientes funciones asociadas con las soluciones de cifrado que su organización está utilizando?
Respuestas muy importantes e importantes combinadas

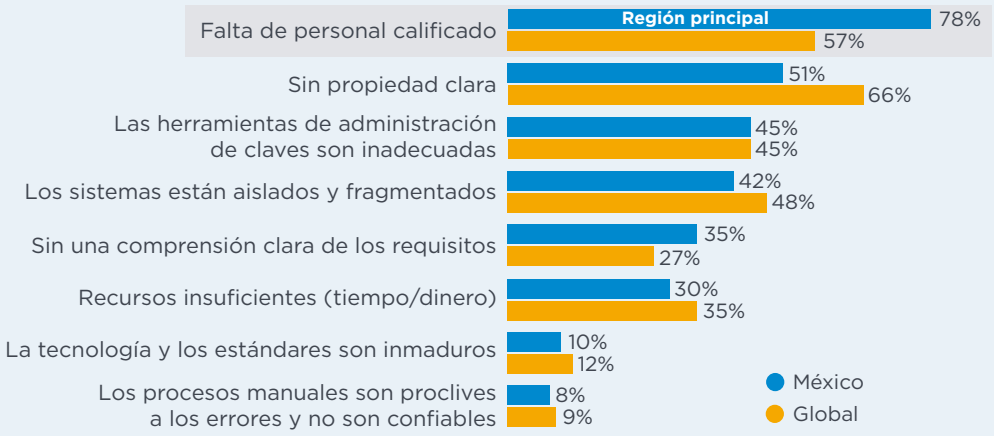


ACTITUDES ANTE LA ADMINISTRACIÓN DE CLAVES

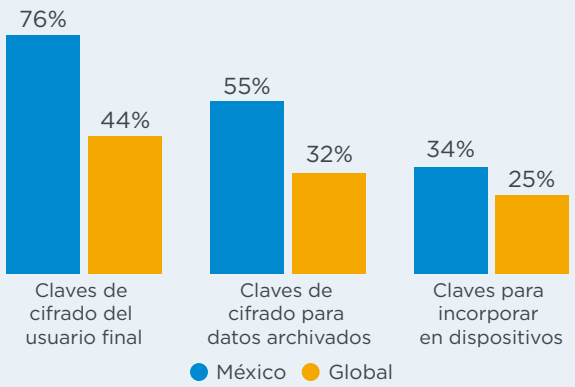
¿Qué tan difícil es la administración de claves? El 62% de los encuestados califica como muy alta la dificultad en la administración de claves. Las principales razones son: la falta de personal calificado, no existe un claro propietario y que las herramientas de administración de claves son inadecuadas.

¿Cuáles claves son las más difíciles de administrar? Las claves de cifrado del usuario final son las más difíciles de administrar, según el 76% de los encuestados (la tasa más alta en todo el mundo), seguidas de las claves para servicios alojados o en la nube externa, incluidas Traiga su propia clave (BYOK, por sus siglas en inglés, el 66% de los encuestados) y claves SSH (64% de encuestados).

¿Qué hace tan complicada la administración de claves?



México califica la dificultad asociada con la administración de los siguientes tipos de claves de cifrado con las tasas más altas en todo el mundo



Las organizaciones utilizan principalmente procesos manuales para administrar claves. El 58% de los encuestados dice que sus organizaciones utilizan procesos manuales seguidos por el 56% de los encuestados que dicen que sus organizaciones utilizan una infraestructura formal de administración de claves (KMI).

Las criptomonedas/billeteras y las transacciones/administración de activos son las aplicaciones para las que las organizaciones tienen planeado utilizar el blockchain. El 43% de los encuestados dice que sus organizaciones planean usar blockchain.

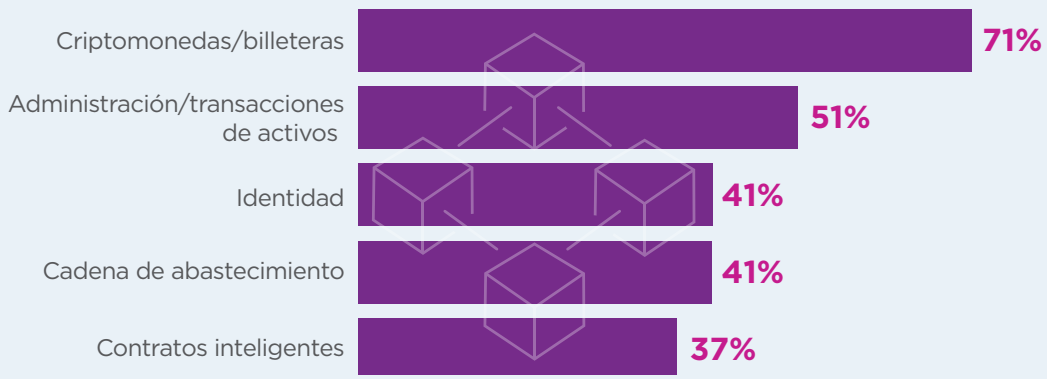
Los dos casos de uso principales serán criptomonedas/billeteras y transacciones/administración de activos, según el 71% y el 51% de los encuestados respectivamente.

La computación multipartita alcanzará la adopción empresarial generalizada mucho antes que los algoritmos cuánticos. Se pidió a los encuestados que estimaran cuánto tiempo pasará antes de que se adopten los algoritmos cuánticos, el cifrado homomórfico y la computación multipartita. Si bien se estima que los algoritmos cuánticos se adoptarán en un promedio de ocho años, se espera que la computación multipartita se adopte en un promedio de cinco años y medio.

IMPORTANCIA DE LOS MÓDULOS DE SEGURIDAD DE HARDWARE (HSMs)

La importancia de los HSMs para una estrategia de cifrado o administración de claves crecerá en los próximos 12 meses. El 80% de los encuestados tiene conocimientos sobre HSMs. Les preguntamos a los encuestados en organizaciones que actualmente implementan HSMs (31% de los encuestados) qué tan importantes son para su estrategia de administración de cifrado o de claves. El 50% 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.

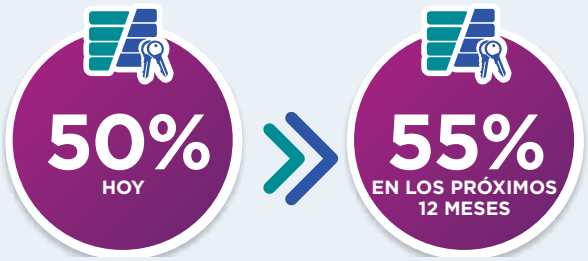
El 43% de las organizaciones planea usar blockchain
Los 5 principales casos de uso son:



La creciente importancia de los Módulos de Seguridad de Hardware (HSMs) para el cifrado o la administración de claves

¿Qué tan importantes son los HSMs para su estrategia de administración de cifrado y claves?

Respuestas muy importantes e importantes combinadas



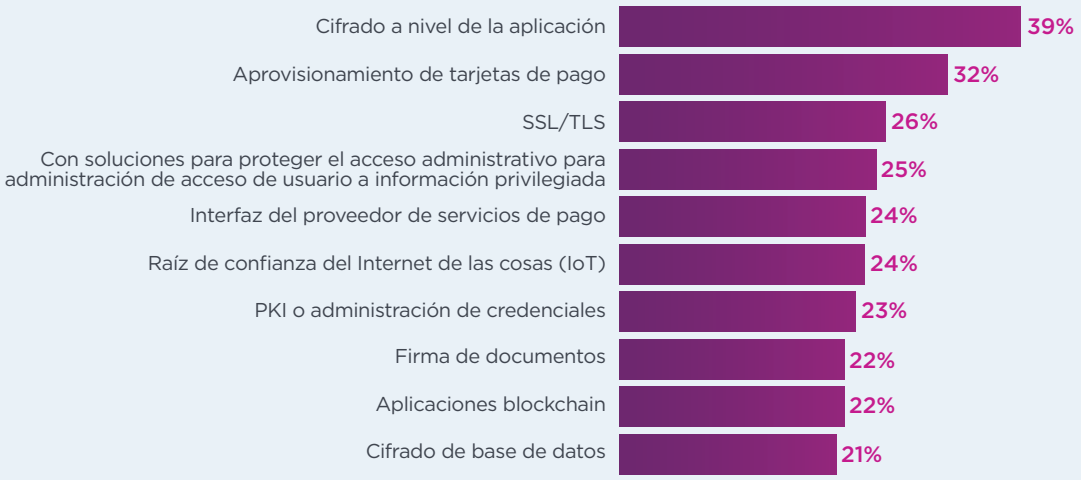
Cómo están utilizando los HSMs las organizaciones. El 71% de los encuestados dice tener un equipo centralizado que brinda criptografía como servicio y el 29% dice que los dueños de las aplicaciones son los responsables de sus propios servicios criptográficos. En la actualidad, el 39% de los encuestados usa HSMs para el cifrado de nivel de aplicación y el 32 por ciento de los encuestados dice que los usa para el aprovisionamiento de credenciales de pago. En los próximos 12 meses, el 54% de los encuestados dice que usará HSMs para el cifrado de nivel de aplicación.

CIFRADO EN LA NUBE

Menos de la mitad de las organizaciones envía a la nube datos sensibles o confidenciales. El 46% 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% planea hacerlo en un período de 12 a 24 meses. El 37% de los encuestados dice que es responsabilidad del proveedor de servicios en la nube proteger los datos confidenciales en la nube o es una responsabilidad compartida.

Las organizaciones utilizan una variedad de enfoques para proteger los datos en reposo en la nube. El 39% 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, el 28% de los encuestados dice que el cifrado se realiza en la nube utilizando claves generadas/administradas por el proveedor de servicios en la nube y 28% de los encuestados dice que el cifrado se realiza en la nube utilizando claves que su organización genera y administra in situ.

Los 10 principales casos de uso para los Módulos de Seguridad de Hardware (HSMs) en 2020



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. Pero también multiplica los riesgos en seguridad. Nuestras soluciones criptográficas protegen las tecnologías emergentes, tales como la nube, el IoT, el blockchain y los pagos digitales, además de ayudar 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**

ACERCA DE ENTRUST DATACARD

Los empleados, ciudadanos y consumidores esperan cada vez más experiencias en cualquier lugar y en cualquier momento, ya sea que inicien sesión en redes corporativas, crucen fronteras, accedan a servicios de gobierno electrónico o realicen compras. También esperan que los ecosistemas que permiten esta libertad y flexibilidad sean completamente confiables y seguros. Entrust Datacard ofrece la identidad confiable y tecnologías de transacción seguras que hacen posibles estos ecosistemas. Nuestros más de 45 años de especialización y experiencia como líderes en la industria se extienden por todo el mundo, con más de 2000 empleados que atienden a clientes en 150 países de todo el mundo. Para más información, visite **www.entrustdatacard.com**