

IBM presenta nuevos servicios de ciberseguridad cuántica para proteger los datos en el entorno cloud

- Este lanzamiento es posible gracias al liderazgo de IBM en nube híbrida, computación cuántica y seguridad

- La compañía ofrece mayor protección en la transferencia de datos a la nube para garantizar la privacidad de la información sensible a través de cifrado al más alto nivel de la industria

ARMONK, N.Y., 30 de noviembre de 2020. Los datos y su seguridad son y seguirán siendo activos importantes para las empresas y los consumidores en la era de la computación cuántica. Por ello, IBM acaba de anunciar una serie de servicios y tecnologías en la nube que ayudarán a proteger los datos alojados en el entorno cloud y a que estén preparados para futuras ciberamenazas cuánticas. Estos servicios y tecnologías incluyen nuevas capacidades como:

“ A medida que crece nuestra dependencia de los datos en la era de la nube híbrida y avanzan las capacidades de computación cuántica, la necesidad de privacidad de los datos es cada vez más crítica ”

- Quantum Safe Cryptography Support (soporte en criptografía cuántica segura): mediante el uso de tecnología de código abierto, este servicio mejora los estándares utilizados para transmitir datos entre la empresa y la nube, ayudando a asegurar esa información mediante el uso de un algoritmo de seguridad cuántica.
- Extended IBM Cloud Hyper Protect Crypto Services (Servicios de cifrado Hyper Protect en IBM Cloud): estas nuevas capacidades mejoran la privacidad de los datos en las aplicaciones en la nube. La información enviada a través de la red a las aplicaciones en la nube y los datos sensibles —como las de una tarjeta de crédito—, se almacenan en una base de datos que puede ser encriptada a nivel de aplicación con la capacidad “Keep Your Own Key” (KYOK), la protección de cifrado de claves criptográficas con el más alto nivel de la industria.

"A medida que crece nuestra dependencia de los datos en la era de la nube híbrida y avanzan las capacidades de computación cuántica, la necesidad de privacidad de los datos es cada vez más crítica, por lo que estamos ofreciendo nuevas tecnologías para ayudar a las empresas a proteger los datos existentes y ayudar a protegerse contra las amenazas futuras", ha apuntado Hillery Hunter, vicepresidente y director de Tecnología de IBM Cloud. "La seguridad y el cumplimiento siguen siendo una prioridad para IBM Cloud mientras continuamos invirtiendo en computación confidencial y nuestras capacidades de encriptación líderes para ayudar a las empresas de todo tipo -especialmente aquellas en industrias altamente reguladas- a mantener los datos seguros".

Prepararse para futuras amenazas con el soporte de criptografía cuántica segura

Mientras que la computación cuántica tiene como objetivo resolver problemas complejos que ni siquiera los superordenadores más poderosos del mundo pueden abordar, puede suponer una amenaza al tener la capacidad de romper rápidamente los algoritmos de cifrado, exponiendo los datos sensibles. Para mitigar estos riesgos, IBM ha desarrollado una agenda estratégica para ayudar a proteger la seguridad a largo plazo de sus plataformas y servicios. Esta agenda incluye la investigación, el desarrollo y la estandarización de los principales algoritmos de criptografía cuántica como herramientas de código abierto, como CRYSTALS y OpenQuantumSafe. También incluye la gestión, las herramientas y la tecnología para apoyar a los clientes en su viaje hacia un futuro más seguro.

Como parte de este plan, IBM está aportando su [liderazgo en capacidades de encriptación](#) desarrolladas por investigadores en criptografía para ayudar a los clientes a proteger sus datos en la nube de IBM con un enfoque de criptografía cuántica segura. Esas capacidades están concebidas para ayudar a las empresas a prepararse para las amenazas futuras y que pueden ser

útiles contra los ciberdelincuentes, que en la actualidad recopilan datos cifrados para descifrarlos más adelante.

Para proteger el encriptado en la era de la computación cuántica, IBM ha presentado una nueva característica en su servicio basado en la nube IBM Key Protect, que gestiona el ciclo de vida de las claves de cifrado que se utilizan en IBM Cloud o en las aplicaciones creadas por el cliente. Con esta novedad, se puede utilizar una conexión de seguridad en la capa de transporte (TLS) habilitada para la criptografía cuántica, lo que ayuda a proteger los datos durante la gestión del ciclo de vida de las claves.

Asimismo, IBM Cloud también está añadiendo capacidades de apoyo a la criptografía de seguridad cuántica para permitir las transacciones de las aplicaciones. Cuando las aplicaciones nativas en contenedores de la nube se ejecutan en Red Hat OpenShift, en IBM Cloud o en IBM Cloud Kubernetes Services, las conexiones TLS seguras pueden ayudar a las transacciones de las aplicaciones con soporte de criptografía cuántica durante el tránsito de datos y protegerlas de posibles infracciones.

Protección de datos confidenciales con IBM Cloud Hyper Protect Crypto Services

Las empresas también deben mitigar los riesgos de las amenazas externas e internas, así como abordar el cumplimiento de la normativa. En este sentido, IBM Cloud ofrece nuevas funciones para ayudar a asegurar las transacciones de las aplicaciones y los datos sensibles utilizando los servicios de cifrado de [IBM Cloud Hyper Protect Crypto Services](#). Estos ofrecen el nivel más alto de protección de cifrado de claves criptográficas de la industria al proporcionar a los clientes la capacidad de "conservar su propia clave" (KYOK). Construido sobre hardware con certificación FIPS-140-2 Nivel 4 -el nivel más alto de seguridad ofrecido por cualquier proveedor de nube en la industria para módulos criptográficos- permite a los clientes tener un control exclusivo de la clave, y por lo tanto la autoridad sobre los datos y las cargas de trabajo protegidas por las mismas.

Esta función está diseñada para aquellas transacciones en aplicaciones en las que se necesita una criptografía más avanzada. Con este servicio los clientes de IBM Cloud pueden mantener sus claves privadas protegidas dentro del módulo de seguridad del hardware de la nube mientras descargan TLS a IBM Cloud Hyper Protect Crypto Services para ayudar a establecer una conexión segura con el servidor web. También pueden lograr la encriptación de datos sensibles a nivel de aplicación, como el número de una tarjeta de crédito, antes de que se almacenen en un sistema de base de datos.

Cumpliendo con las demandas de seguridad de las industrias altamente reguladas

IBM ha estado invirtiendo en tecnologías de [computación confidencial](#) durante más de una década y hoy en día ofrece estas soluciones para ayudar a los clientes a proteger sus datos, las aplicaciones y los procesos. De hecho, IBM sigue colaborando con sus homólogos de la industria para seguir avanzando en las iniciativas de estandarización, a la par que fomenta su compromiso con la seguridad y el cumplimiento. Por ejemplo, las mejores prácticas de seguridad en IBM Cloud están ahora disponibles como un punto de referencia del Center for Internet Security (CIS) Foundations para IBM Cloud, y los criptógrafos de IBM Research son colaboradores clave en los algoritmos QSC que están preseleccionados por el National Institute of Standards and Technology (NIST).

Para más información visite: www.ibm.com/cloud/

For further information: Patricia Torralba IBM Comunicación Tlf.- 637 80 41 48 patricia.torralba@es.ibm.com
