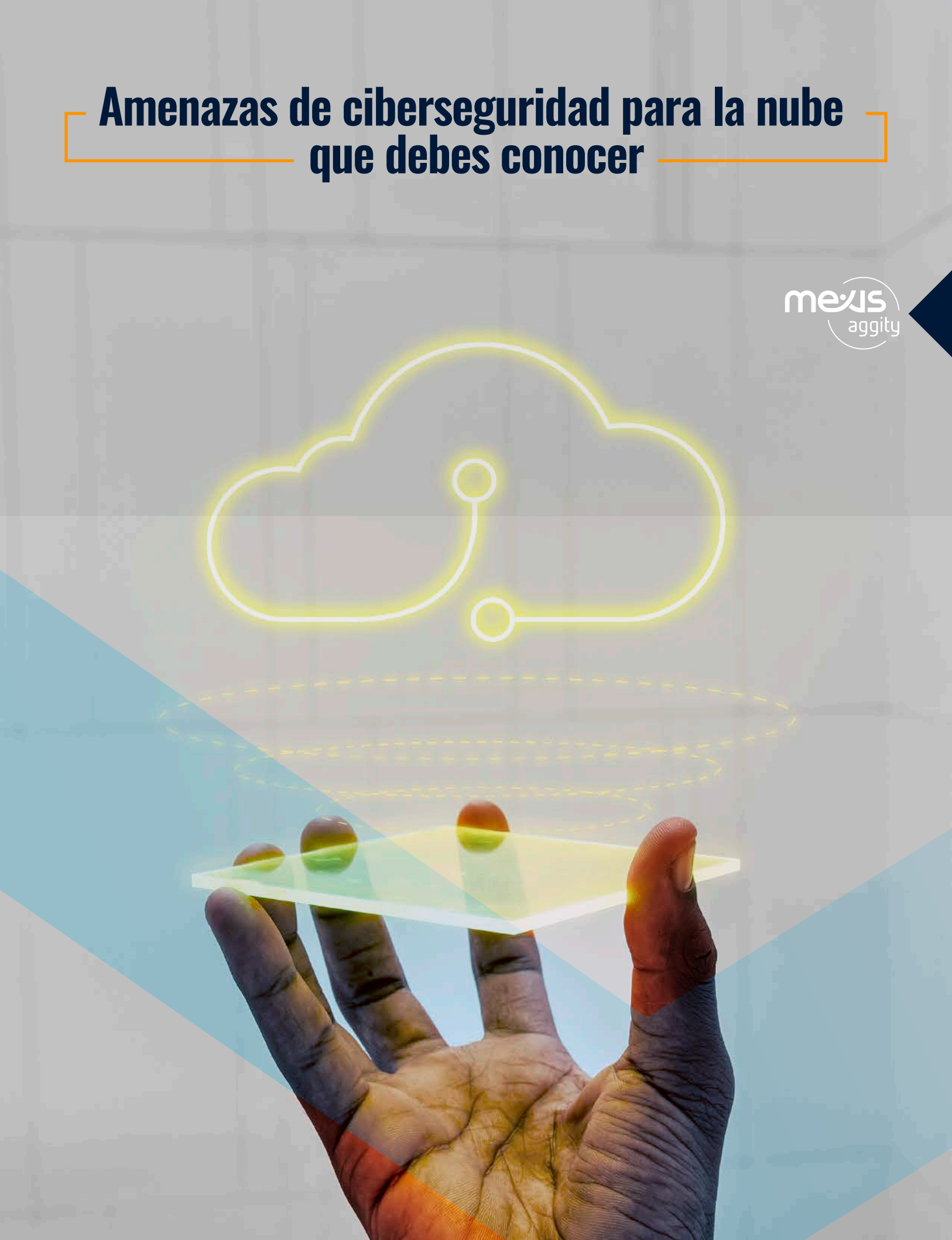
Amenazas de ciberseguridad para la nube que debes conocer



La llegada del internet ha permitido revolucionarlo todo, desde los medios de comunicación y entretenimiento hasta la forma en la que trabajamos y estudiamos. Tal ha sido su impacto que incluso el internet ha sido la punta de lanza para el desarrollo de nuevas herramientas.

Un ejemplo perfecto es la computación en la nube o los servicios en la nube, los cuales han llegado para seguir con la revolución.

Lamentablemente, como siempre, hay un lado malo, ya que **existen potenciales amenazas que pueden poner en peligro el éxito de la computación en la nube** en un futuro no muy lejano.

¿Qué son los servicios en la nube?

Los servicios en la nube son un tipo de servicio el cual se distingue por usar el internet como alojamiento de todos los archivos y programas. Y es que, en lugar de tener una sede física, el cloud computing utiliza el internet como un alojamiento o hosting.
Por ejemplo, en lugar de tener un ordenador con todos los programas y el sistema operativo, este se encuentra alojado en la nube. Lo mismo sucede con el almacenamiento, en lugar de usar un disco duro, todo se guarda en la nube.

Las amenazas que enfrenta la computación en la nube

Cripto Hacking

Este método bastante innovador de hackeo utiliza el mismo sistema de minado de las criptomonedas para vulnerar los sistemas de seguridad. Para ello es necesario contar con un gran poder de computación para poner en marcha el minado.

Una de las principales señales de alarma de este sistema es que no suele ser fácil de detectar. Si acaso verás que el servicio de nube se hace más lento, aunque esto podría pasar por alto pensando que es el internet, cuando en realidad es porque los delincuentes están atacando.

Aplicaciones inseguras

Vincular aplicaciones de dudosa procedencia a tu servicio de computación en la nube puede poner en riesgo la seguridad. Y es que muchas de estas apps sirven como un caballo de troya el cual se encarga de filtrar los softwares maliciosos a la nube.

Te recomendamos que, para evitar este tipo de filtraciones utilices siempre un antivirus para proteger tu PC. Estos te permitirán detectar caballos de troya y otros tipos de virus potencialmente riesgosos, los cuales pueden pasar desapercibidos. Así garantizamos que todas las aplicaciones instaladas son realmente confiables y seguras.

Fuga de datos

La fuga de datos es considerada como uno de los principales problemas a los que se enfrentan los servicios en la nube. Y es que cada vez es más frecuente ver brechas de seguridad en las cuales los datos terminan por fugarse y caer en manos equivocadas.

Es muy importante, como usuarios, conocer cuáles son los sistemas de seguridad con los que cuentan con los servicios en la nube.

Además, hay estrategias que podemos utilizar como contraseñas de mayor seguridad o encriptado para evitar que nuestros datos caigan en manos de delincuentes que les den mal uso.

Denegación de servicio (DDoS)

La modalidad de ataque DDoS consiste en saturar los servidores de la nube con una gran cantidad de tráfico web. Esto hace que las plataformas no puedan procesar toda la información separándolas y provocando que los servicios terminen por caerse o estar “No disponibles”.

Si bien el riesgo de fuga de datos no es tan alto, ya que aquí el objetivo es bloquear los servidores y no vulnerarlos. En realidad, sí hay un gran riesgo detrás de un ataque DDoS, pues al saturarse los servidores te denegarán el acceso a la nube, por lo que no podrás usarla.

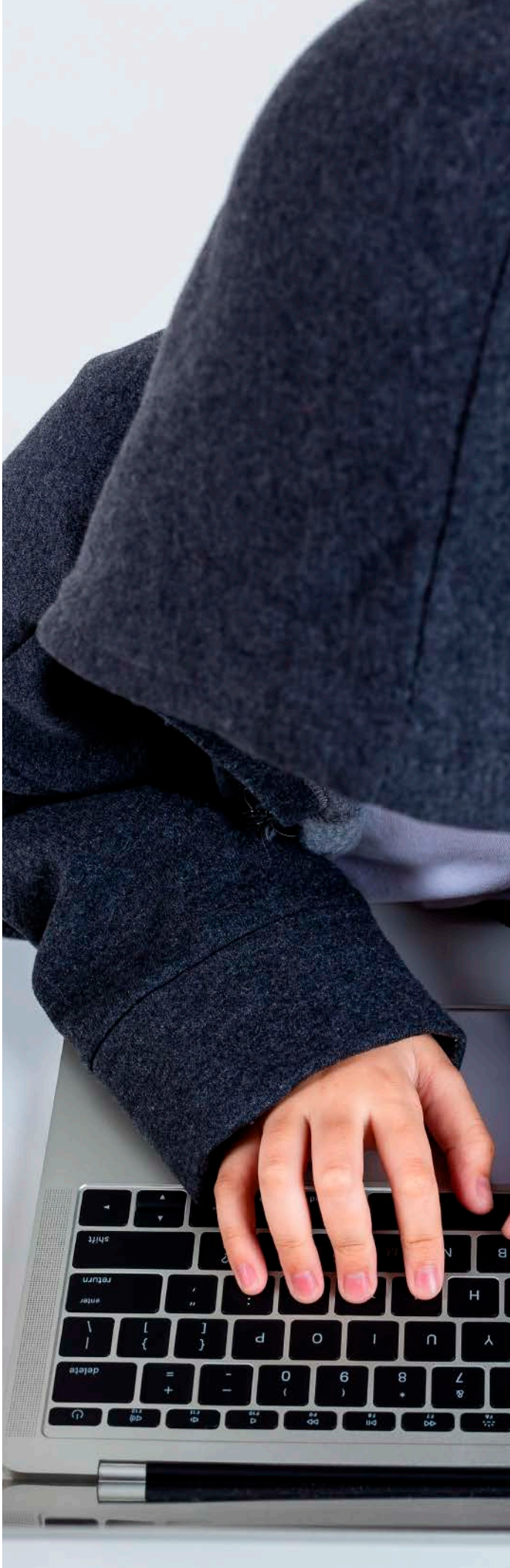
Amenazas internas

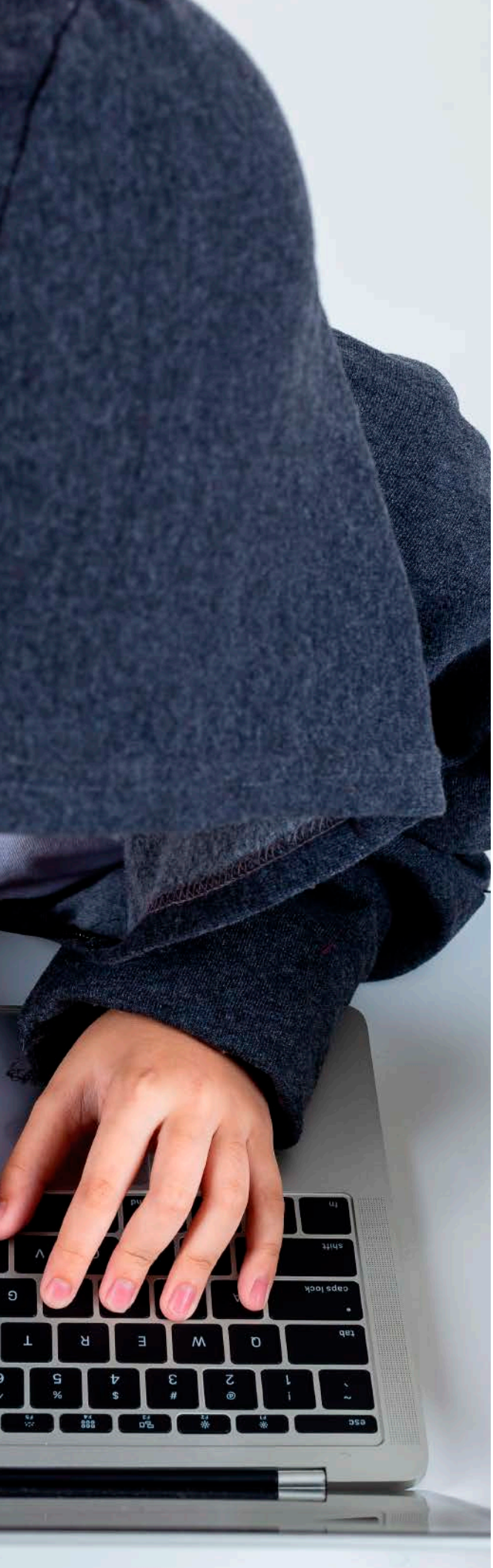
Aunque no lo creas, expertos revelan que 43% de las violaciones de datos proviene de fuentes internas. Esto quiere decir que algún usuario, como pasa en películas de espías, fue el encargado de vulnerar desde adentro la seguridad al filtrar los datos de los usuarios.

Pueden darse casos de empleados o exempleados con accesos a las plataformas de la nube los cuales pueden llegar a filtrar la información. Es por eso que la cultura de prevención y los acuerdos de confidencialidad son muy importantes para evitar este tipo de incidencias y filtraciones.

Secuestro de cuentas

Hay virus los cuales tienen la capacidad de secuestrar las cuentas de los usuarios, bloqueándolas para así exigir un pago. Lamentablemente, esto es muy común, ya que, a lo largo de años recientes, una gran cantidad de empresas se han visto afectadas por este tipo de ataques.





El riesgo está en que para desbloquear o liberar tu cuenta, muchos hackers solicitan el pago de un rescate el cual puede ser muy costoso. Lo peor de todo es que muchos ciberdelincuentes no solo cobran un rescate, también se encargan de extorsionar a las empresas solicitando más y más pagos.

Capacitación inadecuada

Además, tener una mala capacitación puede hacer que tus usuarios no sepan cómo proteger su información y mantener sus datos fuera del alcance de los hackers. Es por eso que resulta muy importante realizar una capacitación adecuada antes de comenzar a aprovechar la computación en la nube.

Muchos usuarios sin saberlo, ponen en riesgo su información a y accesos usando contraseñas inseguras, redes de internet abiertas, entre otras situaciones que parecerían normales, pero que están llenas de riesgo. Así que, es importante tomar en cuenta este punto a la hora de conocer cuáles son las amenazas que enfrenta la computación en la nube.

Los programas de protección para tu seguridad

Si realmente quieres mantenerte protegido, es necesario considerar el uso de aplicaciones especiales las cuales se encargarán de mantener toda tu información segura.

Uno de los ejemplos más claros es el uso de un antivirus que sea potente y preciso.

En el caso de la nube, hay sistemas de encriptación los cuales garantizan la seguridad en la transmisión de datos. Por último, tenemos opciones como el uso de una VPN, un servidor Proxy, protección de nuestro internet, así como el uso de cortafuegos que eviten la incursión a nuestra computadora en la nube.

Fuente de información:
https://www.revistacloudcomputing.com