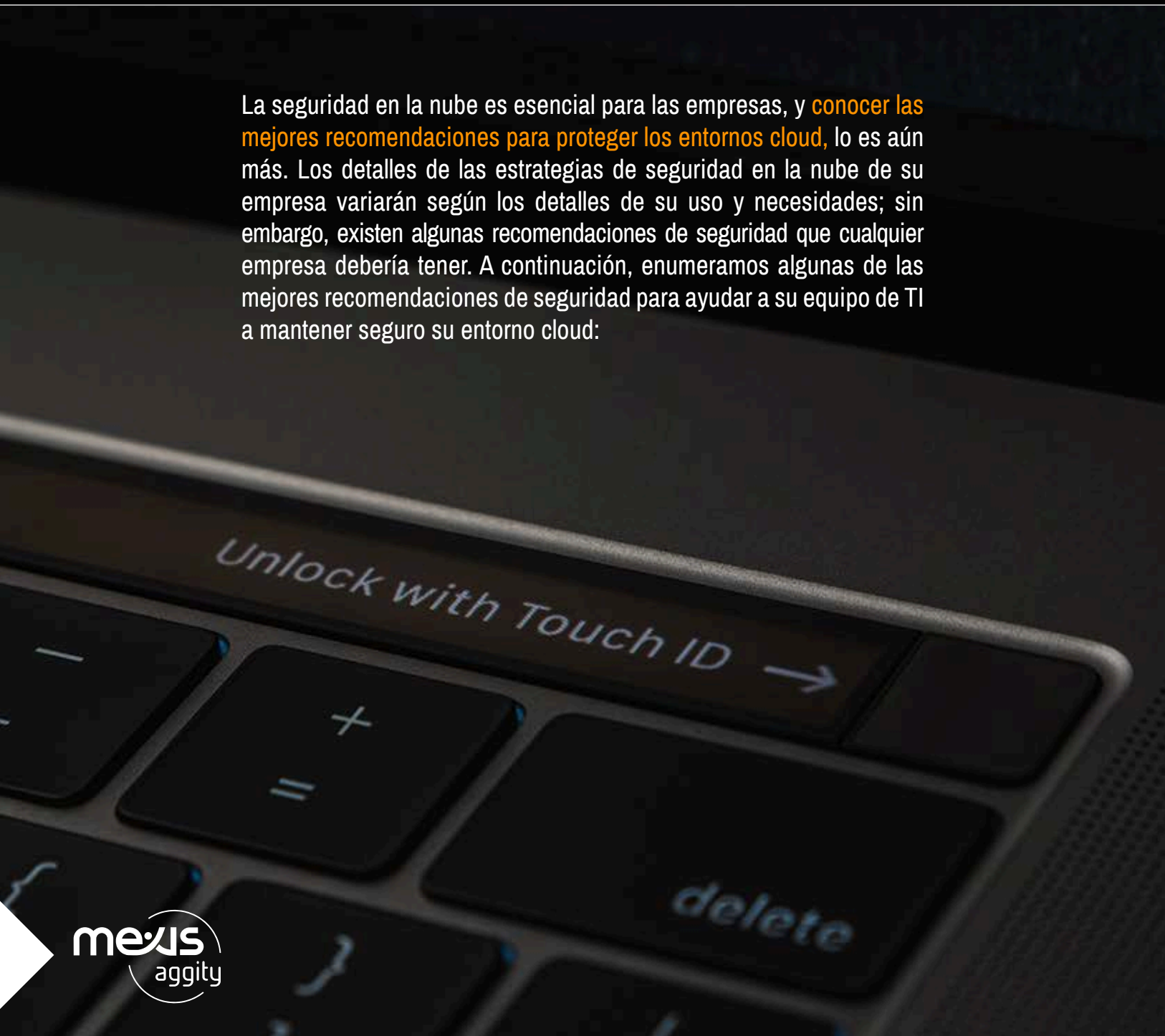
Las mejores recomendaciones para mantener seguros los entornos cloud de las empresas

mexus aggity

Los entornos cloud confiables y de alta disponibilidad son necesarios para que las empresas desplieguen sus aplicaciones con el mínimo esfuerzo. La infraestructura como servicio (IaaS), la plataforma como servicio (PaaS) y el software como servicio (SaaS), brindan importantes ahorros de costes (personal y propiedad), rendimiento mejorado, mayor confiabilidad, escalabilidad y, sobre todo, importantes beneficios de seguridad.

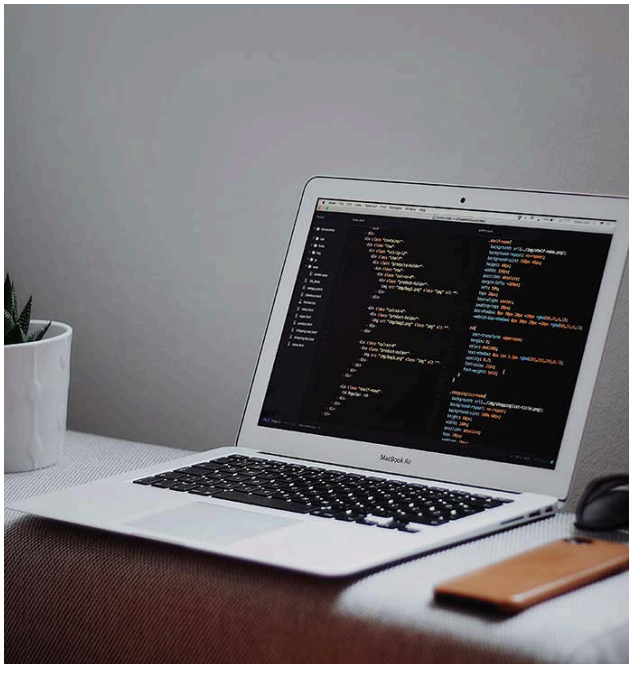
La seguridad en la nube es esencial para las empresas, y conocer las mejores recomendaciones para proteger los entornos cloud, lo es aún más. Los detalles de las estrategias de seguridad en la nube de su empresa variarán según los detalles de su uso y necesidades; sin embargo, existen algunas recomendaciones de seguridad que cualquier empresa debería tener. A continuación, enumeramos algunas de las mejores recomendaciones de seguridad para ayudar a su equipo de TI a mantener seguro su entorno cloud:

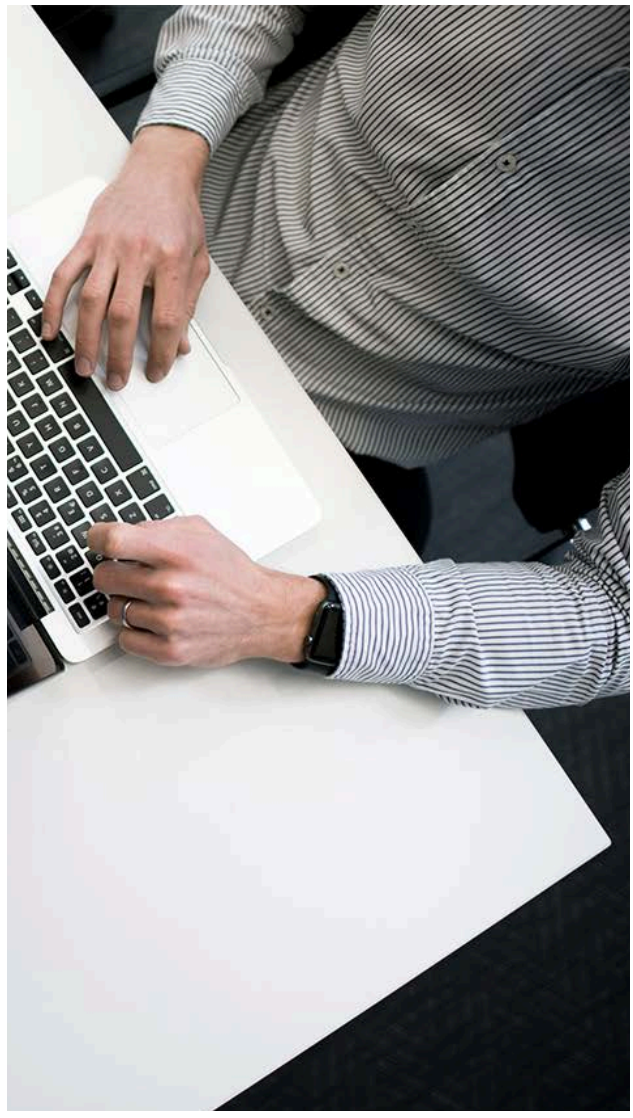


Responsabilidades compartidas de seguridad en la nube

Elegir cargar sus datos en la nube es, en su mayor parte, un punto discutible; las ventajas de la movilidad, la escalabilidad y la comodidad han demostrado que las plataformas en la nube son una herramienta necesaria y vital para el avance de la industria moderna. Sin embargo, algunos problemas siguen siendo un desafío para el mundo en línea, incluido el cumplimiento normativo y la protección de datos confidenciales.

Lo primero que debe comprender acerca de estas recomendaciones es que tanto el proveedor como el usuario de la nube son responsables de la seguridad. Cuando firma un acuerdo con un proveedor, este debe distinguir de qué aspectos de la seguridad es responsable el usuario y de qué aspectos se ocupará el proveedor. **Asegurar el cumplimiento es el camino correcto para administrar un negocio con tranquilidad,** ya que las sanciones pueden ser severas e incluso un factor decisivo para el negocio.



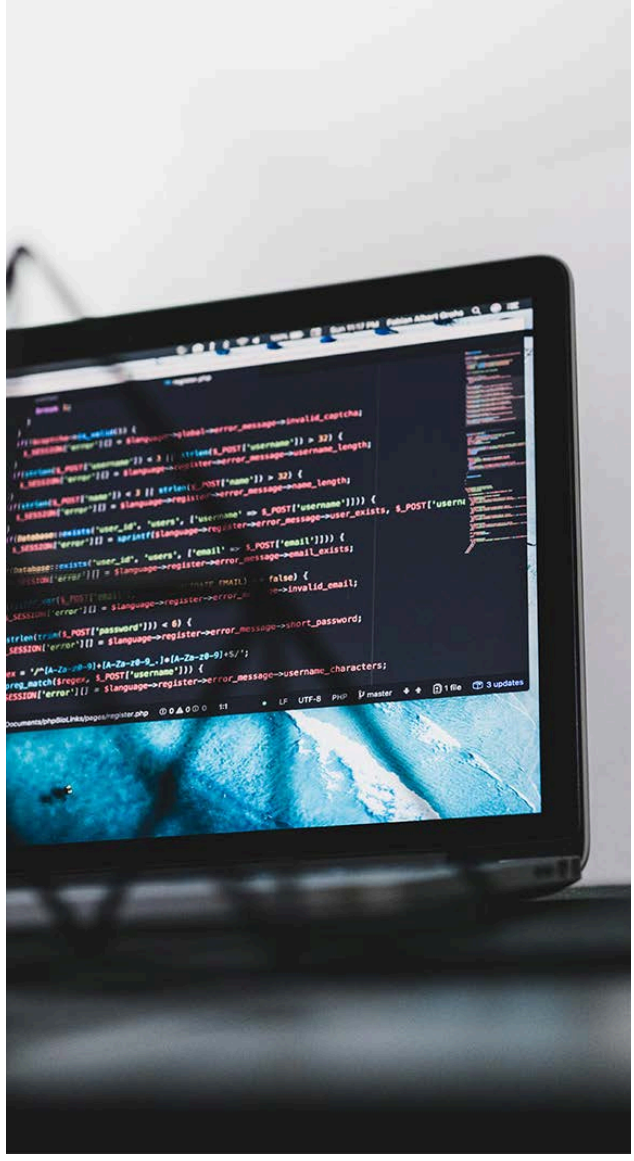


Cifrado de datos en la nube

Cuando almacena datos en la nube, debe asegurarse de que esos datos estén debidamente protegidos. Igualmente, asegurar el cifrado en tránsito de los datos es clave para evitar que estos puedan ser interceptados por un actor malicioso. Un entorno en la nube debe admitir el cifrado de datos para los datos que se mueven hacia y desde la nube. Consulte con su proveedor de servicios para ver qué políticas de cifrado ofrecen. Cada proveedor debe tener pautas detalladas que muestren cómo protegen los datos almacenados en sus servidores en la nube; su empresa necesita conocer estas pautas antes de migrar datos.

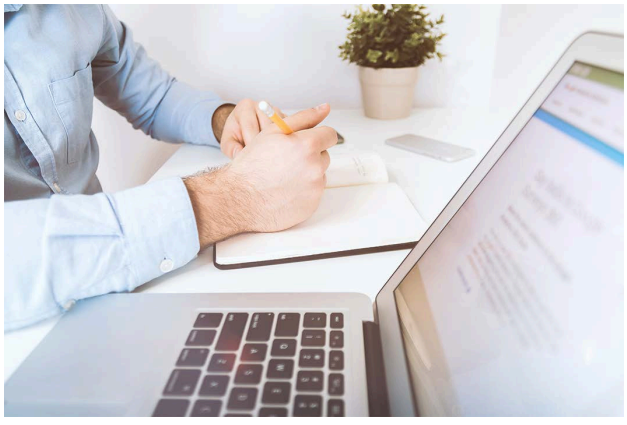
Establecer políticas de gobierno de datos en la nube

En todo sistema de información, asegurar la confidencialidad, integridad y disponibilidad de los datos es la clave de bóveda. Por motivos regulatorios, en algunos casos, es necesario tener políticas que mantengan los datos sensibles de clientes o de terceros en general almacenados de manera segura. Disponer de mecanismos que muevan los datos a almacenes de archivo privados ayudará tanto al control de costes como a mantener un alto nivel de privacidad. Esto en el cloud se puede conseguir con pocos clicks muy rápidamente. Igualmente en el caso de que su empresa abandone el entorno de nube que está utilizando actualmente, bien migrando a un nuevo proveedor de nube o volviendo a una arquitectura local o por que deba eliminar los datos de un cliente, ya que ha dejado de trabajar con él, su empresa necesita establecer políticas de eliminación de datos que eliminen de manera segura estos datos de su sistema, mientras mantiene el cumplimiento.



Gestionar el control de acceso

Entre todos los requisitos de seguridad de la computación en la nube, el control de acceso es uno de los requisitos fundamentales para evitar el acceso no autorizado a los sistemas y proteger los activos de las organizaciones. “Es esencial dominar el concepto de roles, usuarios y grupos para conceder permisos temporales de accesos a recursos y mantener el mínimo permiso de acceso”, comenta Urbano. Es recomendable que ningún operador, máquina o humano, acceda a los datos almacenados en su nube a menos que sea estrictamente necesario para realizar su trabajo. La promulgación de políticas de control de acceso le permite administrar los operadores que intentan ingresar a su entorno cloud. También puede asignar derechos específicos y políticas de acceso a diferentes usuarios y recursos; con esto, los recursos de la nube de bajo nivel no tendrán los mismos derechos de acceso que los administradores de seguridad de alto nivel.



Capacite a sus empleados en sus recomendaciones de seguridad en la nube

A veces, la mayor amenaza de seguridad para sus tecnologías en la nube es su propia empresa y sus empleados. Un empleado que hace un mal uso de su entorno cloud, ya sea por negligencia o falta de conocimiento, puede abrir las compuertas a los actores dañinos que buscan ingresar a su sistema. Al igual que con cualquier tecnología, su empresa debería tomarse un tiempo para capacitar a los empleados que utilizarán el entorno de nube en las mejores recomendaciones de seguridad que ha adoptado. De esta manera, puede prevenir las amenazas de seguridad internas y al mismo tiempo prepararse para las externas.

Nuestra recomendación es planificar e implementar un **plan de ciberseguridad** que garantice la protección de su empresa.

Los beneficios de la seguridad basada en los entornos cloud, continúan atrayendo empresas a esta tecnología. La combinación de la escalabilidad y los costes reducidos de la nube con una mejor protección, mayor inteligencia sobre amenazas y un cumplimiento más rápido de las reglas, regulaciones y estándares normativos, aseguran la mejor estrategia de seguridad en los entornos cloud.

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