



CIBERSEGURIDAD



Sean bienvenidos una vez más a Código Seguro, en el día de hoy estimados lectores, les hablaré acerca de la seguridad en la nube. La computación en la nube se refiere al uso de una red de servidores remotos conectados a Internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software en general.

En lugar de depender de un servicio físico instalado localmente, se tiene acceso a una estructura donde el software y el hardware están virtualmente integrados. Como tal, no es considerada una nueva tecnología, sino un nuevo modelo de suministro de información y servicios que utiliza tecnologías ya existentes. En este caso, emplea la infraestructura de Internet para permitir la comunicación entre servicios/aplicaciones del lado del cliente y del lado del servidor.

Por su parte, los proveedores de servicios en la nube (CSP) ofrecen plataformas en la nube para que sus clientes utilicen y creen sus servicios web, del mismo modo que los proveedores de servicios de internet (ISP) ofrecen a los clientes banda ancha de alta velocidad para acceder a la red de redes. Tanto los CSP como los ISP ofrecen servicios. La nube proporciona una capa de abstracción entre los recursos informáticos y la arquitectura de bajo nivel implicada. Los clientes no son propietarios de la infraestructura física real, sino

que se limitan a pagar una cuota de suscripción y el proveedor de servicios en la nube les da acceso a los recursos y la propia infraestructura.

Un concepto clave es que los clientes pueden reducir el gasto en recursos como licencias de software, hardware y otros servicios, como por ejemplo pudiera ser el de correo electrónico, ya que pueden obtener todo esto de una sola fuente, el proveedor de servicios en nube. Según estudios recientes, las empresas disciplinadas consiguen una reducción media del 18% en su presupuesto de tecnologías de la información (TI) gracias a esto y una reducción del 16% en los costos de energía que consumen normalmente los centros de datos.

Entre sus características principales se encuentran:

Disponibilidad a pedido: Permite acceder a los recursos del sistema informático, como almacenamiento de datos y capacidad de cómputo, sin una gestión activa directa por parte del usuario. Estos recursos están disponibles desde cualquier lugar a través de Internet, ya sea desde dispositivos móviles o fijos.

Modelos de servicio en la nube:

Software como servicio (SaaS): Puede describirse como un proceso por el cual los proveedores de servicios de aplicaciones (ASP) proporcionan diferentes aplicaciones de software a través de Internet. De este modo, el cliente se libra de instalar y utilizar la aplicación en su propia computadora y también elimina la tremenda carga que supone el mantenimiento del software, el funcionamiento continuo, la protección y el soporte.

Plataforma como servicio (PaaS): Es la entrega de una plataforma informática y un conjunto de soluciones como servicio sin descarga ni instalación de software para desarrolladores, responsables de TI o usuarios finales. Proporciona una infraestructura con un alto nivel de integración para implantar y probar aplicaciones en la nube.

Infraestructura como servicio (IaaS): Se refiere a la compartición de recursos de hardware para ejecutar servicios mediante la tecnología de virtualización. Su principal objetivo es facilitar el acceso de aplicaciones y sistemas operativos a recursos como servidores, redes y almacenamiento.

Acceso remoto: Otras computadoras pueden acceder a los recursos a través de una red.

Escalabilidad: Los recursos son flexibles y se pueden ajustar según las necesidades.

Virtualización: La infraestructura de nube utiliza sistemas de software y hardware para diseñar y usar las nubes.

Tener en cuenta los elementos de seguridad siempre resulta imprescindible y en el ámbito de la computación basada en la nube es

un tema especialmente preocupante, fundamentalmente por el hecho de que los dispositivos utilizados para prestar los servicios no pertenecen directamente a los propios usuarios. Estos ya no tienen total control ni conocimiento de lo que puede ocurrir muchas veces con sus datos. Y recabe destacar lo preocupante que resulta en los casos en que los usuarios tienen información valiosa y personal almacenada en un servicio de computación en la nube.

Los usuarios prefieren por defecto no comprometer su privacidad, por lo que los proveedores de servicios de computación en la nube deben garantizar la seguridad de la información de sus clientes. Esto, sin embargo, se está convirtiendo en un reto cada vez mayor, ya que a medida que se realizan avances en materia de ciberseguridad, siempre parece haber alguien que encuentra la manera de desactivar dichos elementos y aprovecharse de la información de los usuarios. De ahí la importancia que tiene para Cuba contar una Ley No. 149 de Protección de Datos Personales desde agosto del 2022. En esta se establece según su artículo 44.1 que todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Por otra parte, ya en el orden tecnológico, la seguridad en la nube es una disciplina de la ciberseguridad, dedicada a proteger los sistemas informáticos en la nube. Esto incluye mantener los datos privados y seguros en la infraestructura, las aplicaciones y las plataformas en línea. La seguridad en la nube abarca las siguientes categorías:

Seguridad de los datos: Garantiza que los datos almacenados en la nube estén protegidos contra accesos no autorizados o pérdidas.

Gestión de identidades y accesos (IAM): Controla quién tiene acceso a los recursos en la nube y cómo se autentican.

Gobernanza: Define políticas para prevenir, detectar y mitigar amenazas.

Planificación de la retención de datos y la continuidad del negocio: Asegura que los datos estén disponibles incluso en situaciones de desastre.

Cumplimiento legal: Garantiza que las operaciones en la nube cumplan con las regulaciones y leyes aplicables.

La seguridad es fundamental para proteger tanto a los proveedores de servicios como a los clientes que utilizan estos servicios. Los proveedores alojan los servicios en sus servidores a través de conexiones de Internet siempre activas, y su responsabilidad es mantener la confidencialidad y seguridad de los datos de los clientes. Sin embargo, los usuarios también deben configurar adecuadamente los

servicios y adoptar prácticas seguras para garantizar una solución saludable de seguridad en la nube. A continuación, te sugerimos las siguientes buenas prácticas:

Evaluación de los riesgos: Comienza por evaluar los riesgos específicos para tu caso. Identifica las amenazas potenciales y los activos críticos que necesitas proteger.

Políticas de acceso y permisos: Establece políticas de acceso y permisos adecuadas. Limita el acceso solo a las personas que realmente necesitan acceder a los recursos en la nube.

Autenticación multifactorial (MFA): Implementa MFA para agregar una capa adicional de seguridad. Esto requiere que los usuarios proporcionen más de una forma de autenticación antes de acceder a los datos o aplicaciones.

Encriptación de datos: Asegúrate de que los datos estén encriptados tanto en tránsito como en reposo. Utiliza protocolos seguros como HTTPS y TLS.

Auditoría y monitoreo: Configura registros de auditoría y monitorea continuamente los eventos en la nube. Esto te ayudará a detectar actividades sospechosas o no autorizadas.

Actualizaciones y parches: Mantén tus sistemas actualizados con los últimos parches de seguridad. Esto es esencial para proteger contra vulnerabilidades conocidas.

Respuesta a incidentes: Prepara un plan de respuesta a incidentes. Define cómo manejarás situaciones de seguridad, cómo notificarás a los afectados y cómo restaurarás los servicios.

Educación y capacitación: Educa a tus empleados sobre las mejores prácticas de seguridad en la nube. La concienciación es clave para prevenir errores y ataques.

En resumen, la computación en la nube es un modelo de prestación de servicios tecnológicos que impacta en diversos negocios. Se basa en infraestructuras tecnológicas dinámicas, caracterizadas por la virtualización de recursos y una alta automatización para atender demandas variables. Recuerda además que la seguridad es un proceso continuo. Mantente informado sobre las últimas amenazas y ajusta tus medidas según sea necesario.

Por hoy nos despedimos, no sin antes hacer alusión a la historia de la informática que también es importante. Y es que justamente ayer cumplió sus 53 años, el archiconocido Protocolo de Transferencias de Archivos (FTP), quien hasta la fecha ha permitido el intercambio de ficheros, entre numerosos dispositivos conectados a una red de computadoras. Seguro estoy que se estarán preguntando en este momento, si está bien usar FTP para transferir archivos en la nube. ¿Será seguro? Pero no tenemos tiempo para más, la respuesta en esta ocasión la dejaremos abierta, quizás para otra de nuestras historias, que

seguro compartimos como cada miércoles con ustedes, nuestros asiduos lectores. Solo me resta decirles que les vaya bien. Nos vemos la próxima semana.

(Tomado de Cubadebate)