**El surgimiento de la seguridad en la nube**

Uno de los desarrollos tecnológicos más importantes de este siglo ha sido la aparición de la computación en la nube. Según el Centro Nacional de Ciberseguridad del Reino Unido, la computación en la nube se define como “un servicio escalable masivamente bajo demanda, alojado en una infraestructura compartida y accesible a través de Internet”.

Anteriormente, aprendiste que la mayor parte de la información se encuentra en forma de datos, los cuales están en constante cambio. En los últimos años, las empresas comenzaron a migrar sus datos a la nube. La adopción de servicios basados en la nube generó nuevas complejidades en la manera en que se protege la información en línea. En esta lectura, explorarás estos desafíos y las oportunidades surgidas  para los/as profesionales de la seguridad.

**Subirse a la nube**

Iniciar un negocio en línea solía ser un proceso complicado y costoso. En el pasado, las empresas debían crear y mantener sus propias soluciones internas para operar en el mercado digital. Sin embargo, gracias a la nube, en la actualidad es mucho más sencillo hacerlo, para cualquier persona.

La disponibilidad de tecnologías en la nube ha transformado radicalmente la forma en que las empresas operan en línea. Estas nuevas herramientas permiten a las empresas escalar y adaptarse rápidamente, al tiempo que reducen sus costos. Sin embargo, a pesar de estos beneficios, el cambio hacia servicios basados en la nube también ha presentado una serie de nuevos desafíos de ciberseguridad que ponen en riesgo los activos.

**Servicios basados en la nube**

Al hablar de “servicios basados en la nube” se hace referencia a una variedad de soluciones empresariales disponibles bajo demanda o basadas en la web. En función de las necesidades y el presupuesto con el que cuente una organización, estos servicios pueden abarcar desde el alojamiento de sitios web hasta entornos de desarrollo de aplicaciones, pasando por toda la infraestructura de backend.

Existen tres categorías principales de servicios basados en la nube:

* Software como servicio (SaaS)
* Plataforma como servicio (PaaS)
* Infraestructura como servicio (IaaS)

**Software como servicio (SaaS)**

El software como servicio (SaaS) hace referencia a aplicaciones de front-end a las que los/as usuarios/as acceden a través de un navegador web. Las empresas proveedoras de servicios alojan, gestionan y mantienen todos los sistemas de backend para esas aplicaciones. Algunos ejemplos comunes de servicios SaaS incluyen aplicaciones como el servicio de correo electrónico Gmail™, la plataforma de comunicación y colaboración en equipo Slack y el software de videoconferencias Zoom.

**Plataforma como servicio (PaaS)**

La plataforma como servicio (PaaS) se refiere a las herramientas de desarrollo de aplicaciones de backend a las que los/as clientes/as pueden acceder en línea. Los desarrolladores utilizan estos recursos para escribir código y crear, gestionar e implementar sus propias aplicaciones. Mientras tanto, las empresas proveedoras de servicios en la nube alojan y mantienen el hardware y software de backend que las aplicaciones utilizan para funcionar. Algunos ejemplos de servicios PaaS incluyen la plataforma Google App Engine™, Heroku® y VMware Cloud Foundry.

**Infraestructura como servicio (IaaS)**

Los clientes de infraestructura como servicio (IaaS) obtienen acceso remoto a una variedad de sistemas de backend que son alojados por el proveedor de servicios en la nube. Esto incluye servidores de procesamiento de datos, almacenamiento, recursos de redes y más. Los recursos suelen licenciarse según las necesidades, lo que lo convierte en una alternativa rentable en comparación con la compra y el mantenimiento de infraestructura local.

Los servicios basados en la nube permiten a las empresas conectar con sus clientes, empleados y socios comerciales a través de Internet. Algunas de las organizaciones más grandes del mundo ofrecen servicios basados en la nube, como:

* Plataforma Google Cloud
* Microsoft Azure

**Seguridad en la nube**

Migrar aplicaciones e infraestructura a la nube puede facilitar el funcionamiento de un negocio en línea. Sin embargo, también puede complicar la tarea de mantener los datos privados y seguros. La seguridad en la nube es un campo en crecimiento dentro de la ciberseguridad, que se enfoca específicamente en la protección de datos, aplicaciones e infraestructuras en la nube.

En un modelo tradicional, las organizaciones tenían toda su infraestructura de TI en sus instalaciones. La protección de esos sistemas recaía por completo en el equipo de seguridad interno de ese entorno. No obstante, estas responsabilidades no están tan claramente definidas cuando parte o todo el entorno operativo se encuentra en la nube.

Por ejemplo, un cliente de PaaS paga para acceder a los recursos que necesita para crear sus aplicaciones. En este sentido, es razonable esperar que se encargue de la seguridad de las aplicaciones que genera por su cuenta. Por otro lado, la responsabilidad de mantener la seguridad de los servidores a los que acceden debe ser de la empresa proveedora de servicios en la nube, ya que hay otros clientes que utilizan los mismos sistemas.

En seguridad en la nube, este concepto se conoce como modelo de responsabilidad compartida. Por lo general, los clientes son responsables de asegurar todo lo que esté directamente bajo su control:

* Gestión de identidades y accesos
* Configuración de recursos
* Manejo de datos

**Nota:** El grado de responsabilidad que se delega a un proveedor de servicios varía según el servicio que se utilice: SaaS, PaaS e IaaS.

**Desafíos de la seguridad en la nube**

Las empresas proveedoras de servicios hacen todo lo posible para ofrecer productos seguros a sus clientes. Gran parte de su éxito depende de prevenir vulnerabilidades y de la eficacia con la que puedan proteger la información confidencial. Sin embargo, como los datos se almacenan en la nube y se accede a ellos a través de Internet, surgen varios desafíos:

* Una de las mayores preocupaciones es una **configuración incorrecta**. Los clientes de servicios basados en la nube son responsables de configurar su propio entorno de seguridad. En muchas ocasiones, pueden utilizar configuraciones predeterminadas que no abordan sus objetivos de seguridad específicos.
* Es más probable que se produzcan **violaciones de seguridad nativas** de la nube debido a servicios mal configurados.
* **Controlar el acceso puede ser difícil** segúnel cliente y el nivel de servicio.
* **Cumplir con los estándares regulatorios** también es un problema, particularmente en las industrias que están obligadas por ley a seguir requisitos específicos como los de la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA), los del Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS) y los del Reglamento General de Protección de Datos (RGPD)..

Además de estos, existen muchos otros desafíos. A medida que más organizaciones adoptan servicios basados en la nube, aumenta la necesidad de contar con profesionales de la seguridad en la nube para hacer frente a un número cada vez mayor de  riesgos. Burning Glass, una destacada empresa en análisis del mercado laboral, [sitúa a la seguridad en la nube entre las habilidades más demandadas en ciberseguridad](https://www.burning-glass.com/wp-content/uploads/2020/10/Fastest_Growing_Cybersecurity_Skills_Report.pdf).

**Conclusiones clave**

El mercado global ha experimentado un cambio significativo hacia los servicios basados en la nube. La tecnología en la nube todavía es relativamente nueva, lo que ha dado lugar al surgimiento de nuevos modelos de seguridad y a una variedad de desafíos en este ámbito. Es probable que surjan otras preocupaciones a medida que más empresas se vuelvan dependientes de la nube. Por ello, familiarizarse con la nube y los diferentes servicios disponibles es un paso importante para apoyar los esfuerzos de cualquier organización en la protección de la información en línea.

**Recursos para obtener información adicional**

La seguridad en la nube es uno de los campos de la ciberseguridad que mayor crecimiento está experimentando. Existen diversos recursos disponibles en línea para aprender más sobre este tema especializado.

* [El Centro Nacional de Ciberseguridad del Reino Unido](https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model) dispone de una guía detallada para elegir, utilizar e implementar servicios en la nube de forma segura, basada en el modelo de responsabilidad compartida.
* [Cloud Security Alliance®](https://cloudsecurityalliance.org/) es una organización dedicada a la creación de entornos seguros en la nube. Ofrece acceso a investigaciones específicas sobre seguridad en la nube, certificaciones y productos a través de una membresía de pago.
* [CompTIA Cloud+](https://www.comptia.org/blog/your-next-move-cloud-security-specialist) es un programa de certificación diseñado para enseñarte las habilidades fundamentales necesarias para convertirte en un/a especialista en seguridad en la nube.