CYBER READINESS
INSTITUTE

Preguntas frecuentes sobre la nube:

Mejora de la ciberseguridad para trabajadores remotos

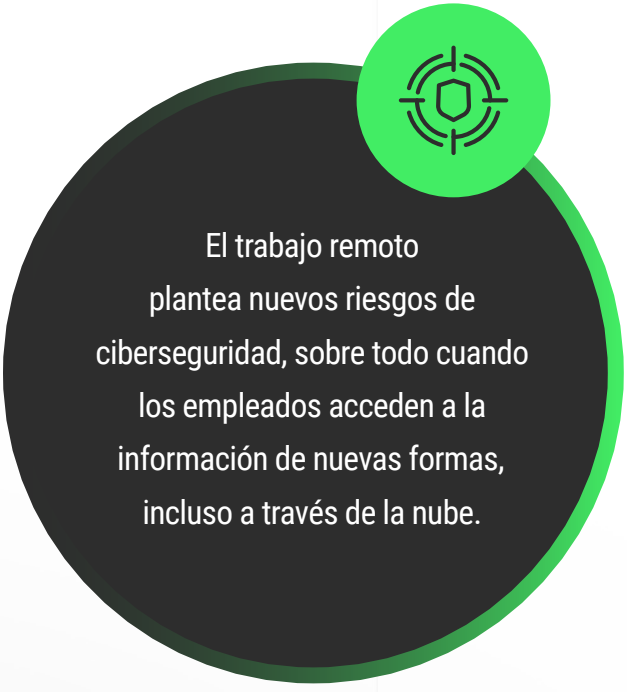
Como respuesta ante la pandemia de la COVID-19, las plantillas de la mayoría de las empresas han empezado a trabajar de forma remota. El trabajo remoto plantea nuevos riesgos de ciberseguridad, sobre todo cuando los empleados acceden a la información de nuevas formas, incluso a través de la nube.

Ahora es el momento de evaluar cómo usa la nube su organización. La nube presenta múltiples capacidades que pueden ayudar a que el trabajo remoto sea más práctico, eficiente y seguro. Estas preguntas frecuentes se han recopilado para ayudar a la alta dirección de pymes a familiarizarse con la terminología de la nube y a comprender los conceptos básicos de cómo la nube puede mejorar la ciberseguridad para la plantilla remota.

Oigo hablar mucho sobre “la nube”, pero ¿cuáles son los conceptos básicos que debo saber?

La “nube” se refiere a un grupo de ordenadores (conocidos colectivamente como servidores) que pertenecen a una empresa que los utiliza (por lo general, conocido como Proveedor de servicios en la nube o “CSP”, por sus siglas en inglés, Cloud Service Provider) y que le proporciona software o almacenamiento. Un cliente o una empresa autoriza el uso del software y/o el almacenamiento, por lo general mensualmente, y los costes cambian en función del uso, al igual que el coste mensual de los servicios públicos.

El CSP es responsable de utilizar, mantener y actualizar el hardware del ordenador (por ejemplo, almacenamiento, servidores), que se encuentra físicamente en un centro de datos y no en las instalaciones del cliente. Como cliente, paga por usar sus servicios.



guide@cyberreadinessinstitute.com

¿Qué términos habituales se utilizan al hablar de la nube?

CENTROS DE DATOS

Imagínese unos grandes almacenes llenos de ordenadores conectados a Internet que se llaman colectivamente "servidores". Cuando usted, como cliente, utiliza un servicio (por ejemplo, Outlook), básicamente está alquilando espacio (almacenamiento) y servicios (correo electrónico) para escribir, leer y enviar correos electrónicos.

SERVIDORES

Una conjunto de ordenadores y hardware conectados a Internet que prestan algún tipo de servicio, almacenamiento u otra función.

PROVEEDORES DE SERVICIOS EN LA NUBE (CSP)

Las empresas que le prestan servicios como cliente. Algunos ejemplos conocidos son Microsoft, Google o Amazon Web Services (AWS).

SOFTWARE COMO SERVICIO (SAAS) (pronunciado "sas")

Un CSP aloja en sus servidores el software al que su empresa accede a través de Internet. Las empresas suelen obtener licencias para el uso de muchos tipos de software, como correo electrónico (Google Mail), procesamiento de texto (Microsoft Word), hojas de cálculo (Google Sheets), contabilidad (QuickBooks) y gestión de ventas (Salesforce). Esta es la forma más habitual en la que las pequeñas empresas utilizan la nube y requiere la menor cantidad de mantenimiento para el cliente.

PLATAFORMA COMO SERVICIO (PAAS) (pronunciado "pas")

Un CSP proporciona la infraestructura (por ejemplo, un sistema operativo como Windows) y el software que le permite desarrollar, administrar y utilizar aplicaciones personalizadas (por ejemplo, aplicaciones de gestión de inventario o pedidos móviles de clientes).

INFRAESTRUCTURA COMO SERVICIO (IAAS) (pronunciado "ias")

Un proveedor de servicios en la nube aloja físicamente componentes que tradicionalmente se encontraban en un centro de datos "en las instalaciones del cliente", incluidos servidores, almacenamiento, hardware de red y software de servidores.

¿Cuáles son los beneficios de seguridad generales de trasladar las operaciones y la información a la nube?

Los CSP consideran la seguridad como una ***función principal del negocio*** y reconocen que la confianza es parte fundamental de su modelo empresarial. Se centran en actualizar continuamente los servicios y la infraestructura ofrecidos para aportar soluciones seguras para sus clientes. Usted se beneficia de su experiencia y su enfoque continuo en la seguridad.

La infraestructura física (por ejemplo, servidores, enrutadores, dispositivos de red) está alojada en centros de datos que son propiedad del CSP y que se encarga de mantener. Por lo general, esto a.) reduce los costes asociados con el mantenimiento, incluidas las tarifas y el mantenimiento del edificio, pero también b.) proporciona recursos dedicados para proteger la ubicación frente a problemas de seguridad física.

Los CSP hacen posible las ***economías de escala*** que le permiten acceder a recursos y servicios que superan lo que cualquier usuario individual podría implementar. Por ejemplo, los CSP agrupan recursos para comprender mejor los últimos ciberataques que utilizan los piratas informáticos y para implementar soluciones que protegen sus servicios y sus datos.

La mayoría de los proveedores de la nube de renombre definirán claramente qué controles de seguridad implementan y cuáles son sus responsabilidades en lo que respecta al uso de su servicio. Si no lo hacen, o si el proveedor en la nube que se está planteando contratar no le facilita directamente esa información, mejor que busque otro proveedor.

A medida que realizamos la transición a la nube, ¿cuáles son las responsabilidades continuas de ciberseguridad de mi organización?

Su principal responsabilidad es el comportamiento de sus empleados. Usted es responsable de formar a su personal sobre cómo evitar problemas y qué hacer si surge un problema. Debe asegurarse de que comprendan que estar preparados para la cibernética es una prioridad para su empresa.

Existe una serie de principios básicos que debe comprender en lo que respecta a las responsabilidades de seguridad de su organización al recurrir a un CSP:

- En primer lugar, el hecho de subcontratar servicios, una funcionalidad o infraestructura a un CSP no significa que subcontrate su responsabilidad en seguridad. Un ejemplo sencillo que se aplica a casi todo el mundo es la concienciación y el acceso de los empleados. ¿Sus empleados saben cómo detectar correos electrónicos sospechosos? ¿Su organización limita/restringe el acceso de los empleados al software (por ejemplo, aplicaciones de contabilidad) según la necesidad y sus responsabilidades)?
- En segundo lugar, los atacantes se centran en engañar a las personas (lo que se conoce como “phishing”) como una forma de obtener acceso no autorizado. Más del 90% de los ataques que tienen éxito comienzan cuando alguien hace clic en un enlace de correo electrónico sospechoso. La formación sobre ciberseguridad para los empleados es muy útil, incluida la práctica de una buena “higiene cibernética”, como no hacer clic en enlaces de remitentes desconocidos o validar con los supervisores los correos electrónicos que soliciten información confidencial.
- En tercer lugar, lo que sucede con los datos casi siempre es responsabilidad del cliente. Por ejemplo, la filtración de datos financieros confidenciales de clientes que no se han protegido correctamente (como la información de tarjetas de crédito) que se cargan en un CSP es responsabilidad del cliente, no del CSP. Y las consecuencias en la reputación, legales, financieras y de cumplimiento, por nombrar algunas, también son responsabilidad del cliente.

¿De qué manera el cambio a la nube mejora nuestra preparación cibernética en lo que respecta a la gestión de identidad de usuarios (por ejemplo, contraseñas y autenticación)?

Muchos proveedores de servicios en la nube disponen de equipos dedicados a la ciberseguridad y pueden responder a incidentes en tiempo real, identificando cuándo comienzan los problemas y adoptando medidas para mitigar los daños. Un gran proveedor de servicios en la nube recibe más de 200 millones de intentos de inicio de sesión **al día**. Este proveedor puede descubrir rápidamente cuando un nuevo tipo de ataque amenaza sus contraseñas y emprende medidas para evitar que le afecte a usted o a sus usuarios.

¿De qué manera el cambio a la nube mejora la preparación cibernética en lo que respecta al mantenimiento del software actualizado?

Mantener el software actualizado supone un gran beneficio para los clientes y, a menudo, constituye un punto de venta clave para los proveedores de la nube, sobre todo cuando se implementa una solución SaaS o PaaS. Cuando se cambia a un servicio en la nube, el proveedor es responsable de mantener las actualizaciones de software sin que usted tenga que realizar ninguna acción.

Sin embargo, esta función puede presentar un inconveniente, ya que es posible que los usuarios no estén preparados para adaptarse a las nuevas funciones tan rápido como las implementan las empresas en la nube. Si esto se aplica a su empresa, debe preguntar si existe una **opción de actualización diferida** para su licencia de software en la nube. Recuerde que los empleados pueden seguir siendo responsables de actualizar el software que se encuentra en su ordenador, tablet o teléfono individual.

¿De qué manera el cambio a la nube mejora nuestra preparación cibernética en lo que respecta a la prevención de correos electrónicos de phishing?

El phishing es difícil de abordar, ya que utiliza el engaño de la ingeniería social (a veces, adaptado específicamente a una persona, que es lo que se llama ***spear-phishing***) para acceder a una aplicación o a datos confidenciales (por ejemplo, información de inicio de sesión y contraseña).

Dicho esto, los proveedores de correo electrónico en la nube pueden descubrir y responder rápidamente a los ataques de phishing **una vez que se conocen**. Los proveedores de correo electrónico en la nube pueden prestar servicios para ayudar a informar y bloquear los correos electrónicos de phishing conocidos para que no lleguen a sus empleados. En última instancia, la mejor línea de defensa es un ***usuario con la formación correcta*** que sabe cómo son los correos electrónicos de phishing, así como qué hacer (¡y qué evitar!) cuando ve uno.

El uso de un proveedor de servicios en la nube mejora la preparación cibernética de su empresa para administrar la identidad de usuarios, mantener el software actualizado y evitar los correos electrónicos de phishing.

¿De qué manera el cambio a la nube mejora nuestra preparación cibernética en lo que respecta al uso de USB y medios extraíbles?

Pasarse a la nube supone una mejora espectacular, ya que no se requieren dispositivos “multimedia” extraíbles para utilizar el software basado en la nube. Todo lo que requiere la nube es un usuario con un inicio de sesión, un explorador y una conexión a Internet. Los USB y los medios extraíbles se vuelven en gran medida irrelevantes, siempre que forme a sus usuarios sobre cómo usar la nube para almacenar, transferir y acceder a la información que necesitan.

Seguirá siendo responsable de mantener la seguridad en los dispositivos físicos que habilitan los medios extraíbles y pueden impedir que el cliente acceda a los servicios. Sin embargo, una ventaja es que, si bien un dispositivo concreto (por ejemplo, un escritorio) podría verse afectado por un ataque de USB, los servicios “viven” en la nube y se puede acceder a ellos desde un dispositivo no infectado. Se trata de una potente función de la nube que ayuda a proteger la continuidad de su negocio.

¿Cómo me ayuda la nube si sufrimos un incidente cibernético?

Los proveedores de la nube invierten mucho tiempo y dinero en asegurarse de que sus servicios no se vean interrumpidos por un incidente cibernético. Los CSP ofrecen herramientas de software que pueden ayudarle a aislar la causa raíz (por ejemplo, servicios de registro de eventos, actividad sospechosa) de un incidente para reducir la posibilidad de que se repita. Los centros de datos de CSP también aplican sólidos controles de seguridad física, protección de energía y prevención de incendios para que pueda estar tranquilo de que la infraestructura de TI física real está bien protegida.

Nuestros empleados utilizan sus smartphones para trabajar. ¿Cómo me ayuda el uso de los servicios en la nube a reducir los riesgos de ciberseguridad relacionados?

Debe saber cómo acceden los usuarios a sus aplicaciones, sistemas e información. Debe crear una política de seguridad móvil que se aplique a todos los usuarios, independientemente del dispositivo que estén usando. La nube proporciona los mismos beneficios generales de seguridad para los empleados, independientemente de si están usando su smartphone u otro tipo de dispositivo. Es importante recordar que los smartphones suponen la mayor amenaza y que cada empresa debe ser diligente en cuanto a su política de seguridad móvil.

Acerca del Cyber Readiness Institute

El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de ciberseguridad gratuitas para las pequeñas y medianas empresas (pymes). El Programa de Preparación Cibernética autodirigido y disponible en línea se encuentra en chino, inglés, francés, español, portugués, árabe y japonés. Póngase en contacto con nosotros si tiene preguntas, comentarios o casos de éxito (**guides@cyberreadinessinstitute.org**).

¿Cómo puedo establecer prioridades para determinar qué debo trasladar a la nube?

No hay una respuesta que se aplique a todos los casos. La mayoría de las organizaciones disponen de lo que se denomina un entorno "híbrido" que utiliza una combinación de servicios en la nube con soluciones in situ autogestionadas (por ejemplo, una empresa puede utilizar su configuración de red para una oficina pequeña y un servicio de correo electrónico proporcionado por CSP). A continuación, se indican algunos aspectos que deben tenerse en cuenta:

- ¿El software o el servicio interactúa directamente con Internet? Muchas empresas trasladan sus aplicaciones de correo electrónico y de gestión de relaciones con los clientes (CRM) a la nube, ya que son aplicaciones de misión crítica cuyos servidores tradicionalmente necesitan mucho mantenimiento y cuidado. En la actualidad, la mayoría de las empresas también obtiene su software empresarial básico (es decir, procesamiento de texto, hojas de cálculo, contabilidad) a través de una suscripción SaaS.
- ¿Hasta qué punto resultará difícil o generará interrupciones? Algunas funciones son mucho más fáciles de migrar que otras. Por ejemplo, trasladar su correo electrónico o su almacenamiento de archivos a la nube es sencillo. Sin embargo, trasladar sistemas como los de nóminas o de contabilidad que implican una gran cantidad de datos históricos puede ser mucho más complejo.
- ¿Cuáles son los costes relativos? Si se comparan los costes entre usar la nube y hacerlo usted mismo, no olvide contar también con el tiempo y los gastos de hacerlo en las instalaciones. No es solo el coste del hardware y el software: tenga en cuenta el tiempo para configurar, actualizar, mantener y solucionar problemas en su sistema.
- Evalúe los aspectos de seguridad mejorados que aporta usar la nube. Piense en las posibles interrupciones en su negocio, así como en la pérdida de la información, sobre todo su información más valiosa.

¿Cómo afectará el cambio a la nube a nuestro flujo de trabajo actual y qué deben hacer nuestros empleados?

La respuesta a esta pregunta dependerá de lo que transfiera a la nube. Trasladar el correo electrónico a la nube normalmente produce muy pocos cambios, mientras que transferir el software de contabilidad a la nube podría suponer una gran interrupción que requiere gestionar los cambios para los usuarios y la organización.

¿Cuál es el impacto del uso de la nube, si lo hay, en la forma de interactuar con mis proveedores y clientes?

La respuesta simple es que depende. Las empresas utilizan la nube para lograr diferentes objetivos en proyectos muy diversos. Sin embargo, pasar a la nube a menudo libera tiempo y dinero que invertiría en recursos de TI (servidores, redes, etc.). En la mayoría de los casos, el uso de la nube hará que sea más fácil y seguro transferir o compartir información con sus clientes y proveedores.