OUCH! Agosto 2021

El Boletín Mensual de Concientización en Seguridad para ti

# Usando la nube de forma segura

## Resumen

Seguramente has escuchado un concepto llamado la "nube". Esto significa utilizar un proveedor de servicios en Internet para almacenar y administrar tus datos. Los ejemplos incluyen crear documentos en Google Docs, acceder al correo electrónico en Microsoft O365, compartir archivos a través de Dropbox o almacenar sus imágenes en iCloud de Apple. Si bien accedes y sincronizas tus datos desde múltiples dispositivos en cualquier parte del mundo y compartes tu información con quien deseas, a menudo no sabes ni puedes controlar dónde se almacenan físicamente tus datos.

## Seleccionar un proveedor de nube

Los servicios en la nube no son buenos ni malos. Son herramientas para hacer las cosas. Sin embargo, cuando utilizas estos servicios, esencialmente estás entregando tus datos privados a extraños, esperando que los mantengan seguros y disponibles. Como tal, deseas estar seguro de que estás eligiendo sabiamente a tu proveedor de servicios. Sobre la información relacionada con el trabajo, consulta con tu jefe si puedes usar los servicios en la nube y cuáles están autorizados. Si estás considerando utilizar servicios en la nube para uso personal, considera lo siguiente:

1. **Confianza:** ¿Puedes confiar en el proveedor de nube? ¿Es una empresa pública y con buena reputación que es utilizada por millones de personas, o es una empresa pequeña y desconocida con sede en un país del que nunca has oído hablar?
2. **Soporte**¿Qué tan fácil es obtener ayuda o obtener una respuesta a una pregunta? ¿Hay un número de teléfono al que puedas llamar o una dirección de correo electrónico en la que puedas contactar? ¿Hay otras opciones de soporte, como foros públicos o preguntas frecuentes en su sitio web?
3. **Simplicidad**: ¿Qué tan sencillo es utilizar el servicio? Cuanto más complejo sea el servicio, más probabilidades habrá de que cometas errores y expongas o pierdas accidentalmente tu información. Utiliza un proveedor en la nube que le resulte fácil de entender, configurar y usar.
4. **Seguridad**: ¿Cómo llegarán tus datos desde tu computadora al servicio en la nube? ¿La conexión está cifrada? ¿Cómo se almacenan tus datos? ¿Están cifrados, y si es así, quién puede descifrar tus datos? A medida que migras tus datos, recuerda que la seguridad es una responsabilidad compartida entre tú y el proveedor.
5. **Compatibilidad:**¿El proveedor de servicios es compatible con todos los dispositivos y sistemas operativos que usas o planeas usar?

6. **Términos del servicio**: Tómate un momento para revisar los Términos del servicio (a menudo son sorprendentemente fáciles de leer). ¿Bajo las leyes de qué país opera el proveedor de servicios? Presta especial atención a los derechos que cede a su proveedor de servicios.

## Asegurar tus datos

El siguiente paso es asegurarte de utilizar correctamente tus servicios en la nube. La forma en que accedes y compartes tus datos a menudo puede tener un mayor impacto en su seguridad que cualquier otra cosa. Algunos pasos clave que puedes tomar incluyen:

1. **Autenticación**:Utiliza una contraseña única y segura para proteger tu cuenta en la nube. Si tu proveedor de nube ofrece verificación en dos pasos, te recomendamos encarecidamente que la habilites.
2. **Compartir archivos / carpetas**: Los proveedores de nube facilitan el intercambio de datos, a veces de forma muy simple. Puede ser muy fácil compartir accidentalmente tu información públicamente. Protégete permitiendo que solo personas específicas (o grupos de personas) accedan a archivos o carpetas específicos. Cuando alguien ya no necesite acceso, elimínalo. Tu proveedor de nube debe proporcionar una manera fácil de rastrear quién tiene acceso a tus archivos y carpetas.
3. **Configuraciones**: Comprenda la configuración de seguridad que ofrece su proveedor de nube. Por ejemplo, si compartes imágenes, archivos o una carpeta con otra persona, ¿pueden compartir tus datos con otras personas sin tu conocimiento?
4. **Renovación**: No olvides renovar tu suscripción o podrías perder el acceso a tus datos.

## Editor invitado

Tameika Reed (@womeninlinux), Fundadora de Women in Linux. Lidera iniciativas con un enfoque en explorar carreras en infraestructura, ciberseguridad, DevSecOps y liderazgo. Ella organiza una reunión semanal con temas que van desde Infraestructura hasta Blockchain. Ha hablado en OSCon, LISA, Seagl y HashiConf EU.

## Recursos

Ingeniería social: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Creando contraseñas simples: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Gestores de contraseñas: https://www.sans.org/newsletters/ouch/password-managers/
El Poder de actualizar:https://www.sans.org/newsletters/ouch/the-power-of-updating

**Traducido para la comunidad por:** Célica Martínez Aponte, UNAM-CERT