VERSIÓN EN ESPAÑOL
UNAM CERT
OUCH! | Junio 2012
Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN



# Usando la nube de manera segura

## EDITOR INVITADO

James Tarala es el editor invitado para esta edición. Es Instructor Senior del SANS Institute y Director de Consultoría de Enclave Security. Además, es autor de numerosos cursos del SANS, incluyendo SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls y del SANS Audit 407: Foundations of Auditing Information Systems, así como de otros más.

## RESUMEN

Los servicios en la nube son una poderosa tecnología que muchas personas y organizaciones están adoptando. El cómputo en la nube no es más que hacer uso de los servicios de un proveedor para almacenar y administrar datos por ti. La razón por la que llamamos a este servicio "la nube" es porque nunca sabes con precisión donde está alojada tu información físicamente, pues está siendo atendida por la "nube". Algunos ejemplos de cómputo en la nube son la creación de documentos en Google Docs, compartir archivos vía Dropbox, crear tu propio servidor en Amazon Elastic Compute Cloud o almacenar tu música y fotos en iCloud de Apple, estos servicios en línea tienen el potencial de hacerte mucho más productivo. Sin embargo, los beneficios vienen acompañados de riesgos. En este boletín examinamos estos problemas y la forma en que puedes proteger tu información.

## Seleccionando un proveedor en la nube

La nube no es buena ni mala, es una herramienta para utilizarla tanto en el trabajo como en casa, sin embargo, al hacerlo entregas la disponibilidad y la seguridad de tus datos privados a extraños. Por tal razón debes asegurarte que cumplan tus requerimientos. Considera las siguientes preguntas cuando busques proveedores de la nube.

1. **Soporte.** Si tienes un problema, ¿cómo responde el soporte ofrecido por la compañía? Si tus datos son críticos, podrías requerir soporte telefónico o por correo electrónico. Si la compañía no proporciona ese soporte, ¿en su página web existen foros públicos o una sección de Preguntas Frecuentes (FAQ)?
2. **Respaldos.** ¿La compañía respalda tus datos? Si es así, ¿qué es exactamente lo que respalda, con qué frecuencia y por cuánto tiempo se conservan los respaldos? Si por accidente borras archivos, ¿puedes recuperarlos?, si es así, ¿cómo?
3. **Privacidad. El proveedor de la nube** ¿A quién permite acceder a tus datos? ¿Solo tú tienes acceso o también sus empleados y socios externos?
4. **Seguridad.** ¿Cómo se transfieren los datos de tu computadora o dispositivo a la nube? ¿La conexión es protegida a través de cifrado? ¿Cómo son

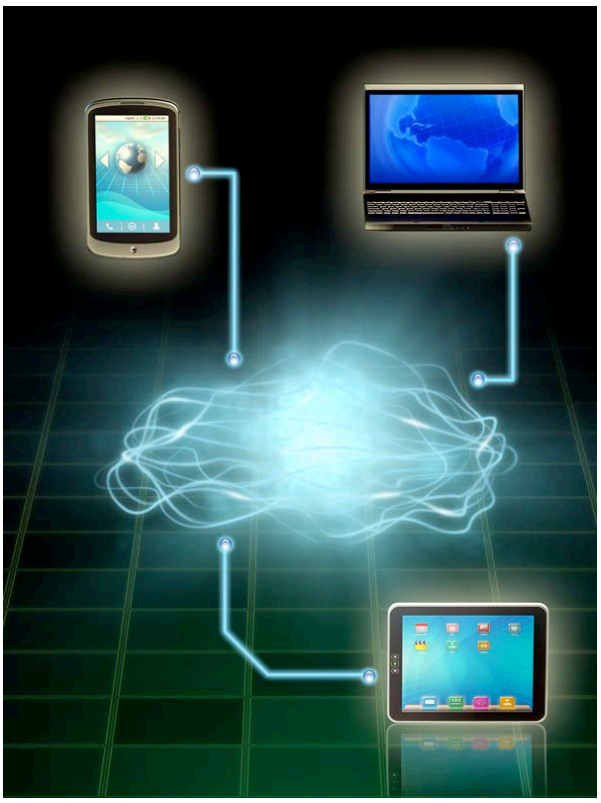
# Usando la nube de manera segura

almacenados tus datos en la nube?, una vez más, ¿están cifrados? ¿Quién puede descifrar tus datos?

## Acceso seguro

Una vez que hayas seleccionado una compañía (o compañías) para almacenar tus datos en la nube, el siguiente paso es asegurarte de usar sus servicios adecuadamente. La forma en que accedes y compartes tus datos, a menudo puede generar un impacto mucho mayor en la seguridad de los mismos, más que cualquier otro factor. Algunos pasos clave que puedes tomar para proteger tu información son:

1. **Autenticación**: Utiliza frases robustas y largas para autenticarte con tu proveedor en la Nube. Esto te protege contra ciberatacantes que intentan simplemente adivinar tu contraseña. Si tu proveedor ofrece dos factores de autenticación (a veces llamado verificación de dos pasos), te recomendamos que lo uses.
2. **Compartir**: La nube hace que sea muy sencillo compartir datos, ten cuidado de no compartir accidentalmente datos de más con otros usuarios, ya que involuntariamente puedes hacer que tu información esté disponible para todos. La mejor manera de protegerte es realizando las configuraciones necesarias para que de manera predeterminada no los compartas con nadie. Solo permite que gente específica (o grupos de personas) accedan a ciertos archivos o carpetas, considerando únicamente lo que necesitan saber.
3. **Configuraciones**: Conocer y comprender las configuraciones de seguridad que ofrece tu proveedor de la nube. Si proporcionas control total a alguien más, ¿puede compartir a su vez tus datos con terceros sin tu conocimiento o consentimiento? ¿Puedes eliminar completamente tus datos de los sistemas del proveedor de la nube, una vez que ya no necesites el servicio?
4. **Antivirus:** Asegúrate que la última versión del programa antivirus esté instalada en tu equipo o en cualquier otra máquina que utilices para compartir tus datos. Si un archivo que compartes es infectado, otras computadoras que acceden al mismo archivo podrían infectarse también.
5. **Cifrado:** ¿Cómo cifra tus datos el proveedor? ¿El servicio controla las llaves o lo haces tú? Una opción de seguridad más robusta consiste en cifrar tu información privada localmente antes de almacenarla en la nube. Estos pasos extra protegen tu información aún si tu proveedor de la nube es comprometido.
6. **Respaldos**: Incluso si tu proveedor respalda tus datos, considera hacer por tu cuenta respaldos



**El cómputo en la nube tiene el potencial de ahorrarte dinero y hacerte más productivo, pero sé cuidadoso al almacenar y compartir tu información**

# Usando la nube de manera segura

locales regularmente y de forma programada. Esto no solo protege tus datos si el proveedor sale del negocio o es dado de baja, sino que también será más sencillo recuperar grandes cantidades de información desde tu respaldo local en vez de descargarlos de la nube.

7. **Términos de servicio**: Lee el Acuerdo de Niveles de Servicio (SLA) o el Acuerdo de Licencia de Usuario Final (EULA) antes de inscribirte en un servicio. Considera otras opciones de proveedores si existen términos en el contrato que no entiendas o que te preocupen.
8. **Organización de los datos**: No almacenes información de tu empresa en la nube sin antes tener el permiso correspondiente de un supervisor. Almacenar los datos de tu organización en la nube, podría no solo violar políticas de tu organización sino que también podría violar leyes estatales y federales, exponiéndote a ti y a tu organización a repercusiones legales.

## Síntesis

La nube no es buena ni mala, es simplemente una herramienta que puedes utilizar. Los pasos clave para protegerte consisten en escoger un proveedor de la nube que cumpla con tus requerimientos de uso y seguridad, además de tomar medidas para proteger la forma en que tú y otros acceden y comparten tus datos.

## RECURSOS

Algunos de los enlaces mostrados a continuación se redujeron para mejorar la legibilidad a través del servicio TinyURL. Con el fin de mitigar problemas de seguridad, OUCH! Siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino solicitando permiso antes de abrirlo.

Cloud Security Alliance (CSA):
https://cloudsecurityalliance.org

Términos comunes de seguridad:
http://preview.tinyurl.com/6qpm9q4

Revista .Seguridad Cultura de prevención para TI:
http://preview.tinyurl.com/revista-unamcert

Tip del día SANS Security:
http://preview.tinyurl.com/6s2wrkp

Consejos UNAM-CERT:
http://preview.tinyurl.com/consejos-unamcert

## MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en http://www.securingthehuman.org

## VERSIÓN EN ESPAÑOL

UNAM-CERT, equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país.

Sitio web http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert



*Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner*
*Versión en español a cargo de UNAM-CERT: Iván Alvarado, Pablo Lorenzana, Célica Martínez, Jazmín López, Dante Ramírez*