

OUCH!

El Boletín Mensual de Concientización en Seguridad para ti

# Limpieza de primavera

## Resumen

¡Muchos de nosotros estamos ansiosos por la llegada de la primavera! Los paisajes comienzan a tomar forma, las flores empiezan a florecer y para muchos surge un deseo de limpieza de primavera. Si bien, puede ser fácil identificar la necesidad de purgar y ordenar, darse cuenta de la necesidad de organizarse digitalmente no es tan evidente. Te compartimos algunos rápidos consejos para tener tu vida digital en orden y establecer nuevos hábitos digitales:



**RESPALDOS:** Colocamos este paso al inicio porque, a la larga, es uno de los más importantes y es el paso que querrás tomar antes de pasar a los siguientes. No importa que tan seguro o a salvo estés, en algún momento, lo más probable es que necesites respaldos para recuperar tu información importante. Las razones pueden incluir: una falla en un disco duro, perder un dispositivo, e infectarte con malware como ransomware. Crear y programar respaldos automáticos asegura que puedas recuperar tu información más importante.



**BORRADO:** Elimina cualquier programa o aplicación que no utilices en tus dispositivos móviles y computadoras. Algunas aplicaciones requieren grandes cantidades de almacenamiento, pueden introducir nuevas vulnerabilidades e incluso ralentizar las cosas. Mientras menos aplicaciones tengas, más seguro serán tus sistemas e información. Muchos dispositivos te muestran cuánto tiempo ha pasado desde que utilizaste una aplicación; si han pasado más de unos pocos meses, ¡es probable que no la necesites!



**ACTUALIZA:** Actualiza todos los dispositivos y aplicaciones que tengas, y habilita la actualización automática siempre que sea posible. De esta forma, tus dispositivos y aplicaciones se mantendrán actualizados, y no solo asegurarás que se ejecuten más rápido, sino que también será mucho más difícil para cualquiera hackearlos.



**CONTRASEÑAS:** Revisa tus contraseñas. Si utilizas la misma contraseña para varias cuentas, cámbialas para que cada cuenta tenga una única contraseña. ¿No puedes recordar todas tus contraseñas únicas? Considera utilizar un gestor de contraseñas. Finalmente, habilita el doble factor de autenticación (2FA, por sus siglas en inglés) siempre que sea posible, especialmente para cualquier correo electrónico o cuentas financieras.



**CUENTAS FINANCIERAS:** Asegúrate de que tus cuentas bancarias, cuentas de tarjetas de crédito y cuentas de jubilación estén configuradas para alertarte cada vez que se realice una transacción, especialmente para compras grandes o transferencias de dinero. Cuanto antes detectes una actividad fraudulenta, de inmediato podrás detenerlas. Dependiendo del país en el que vives, el congelamiento de crédito puede ser una de las formas más efectivas de proteger tu identidad.



**NAVEGADOR:** Revisa todos y cada uno de los complementos instalados en tu navegador. Revisa la configuración de permisos; los complementos realmente necesitan acceso a tu ubicación, contraseñas o listas de contactos? Si ya no usas ciertos complementos, o si tienes inquietudes de privacidad sobre ellos, bórralos.



**REDES SOCIALES:** Comprueba tu presencia en línea y se el propietario. Revisa la configuración de privacidad y elimina las fotos y videos a los que ya no accedes o que no necesitas. También puedes buscarte en un motor de búsqueda y ver qué información hay sobre ti. Recuerda, está bien limitar la cantidad de información que compartes, e incluso con quién eliges compartirla.



**ESCRITORIO:** Limpia el cajón de tu escritorio, limpia todos los discos duros y USB viejos, y tal vez incluso destruye las notas adhesivas con demasiada información. Considera invertir en una destructora de documentos si no tienes alguna.



**CORREO:** Realiza una purga de archivos de correo electrónico, elimina lo que no necesitas y organiza lo que haces. ¡Presta especial atención a cualquier documento confidencial, como aquellos con tu fecha de nacimiento o número de seguro social, y quítalos de tu bandeja de entrada!

Si bien esto puede parecer una tarea desalentadora, puedes estar seguro de que tus dispositivos e información estarán mucho más protegidos. Si esto parece mucho que hacer, considera elegir solo unos pocos artículos, o intenta marcar uno por día o por semana. Cada pequeño paso ayuda mucho a protegerte.

## Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: <http://www.seguridad.unam.mx>

Síguelo en Twitter [@unamcert](https://twitter.com/unamcert)

## Editor invitado

**Katie Nickels** ([@LikeTheCoins](https://twitter.com/LikeTheCoins)) es Analista principal de inteligencia con Red Canary, así como instructora en el SANS de FOR578: Cyber Threat Intelligence. Ella ha trabajado en defensa de redes, respuesta a incidentes e inteligencia de amenazas cibernéticas durante más de una década.



## Recursos

¿Realizo respaldos?:

<http://www.sans.org/u/Z2Q>

Creando contraseñas simples:

<http://www.sans.org/u/Y63>

Búscate a ti mismo en línea:

<http://www.sans.org/u/ZVB>

Desechar tu dispositivo móvil:

<http://www.sans.org/u/ZVG>

OUCH! es publicado por SANS Security Awareness y distribuido bajo la [licencia Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Puedes distribuir y compartir este boletín, siempre y cuando no lo vendas o modifiques. Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Traductor: Céllica Martínez Aponte