¿TIENES UNA NUEVA PC, MAC O DISPOSITIVO MÓVIL?

A continuación, te indicamos cómo protegerlo y utilizarlo con seguridad.

Norton™ by Symantec

Introducción 02 »

Seis buenos hábitos para proteger tus dispositivos 04 »

Las principales amenazas en línea a evitar 06 »

Los smartphones también necesitan seguridad 08 »

12 » Protege tus nuevos dispositivos con la seguridad de Norton

Mantente informado con Norton 13 »

Tienes un dispositivo nuevo. ¡Felicidades!

Sabemos lo emocionante que es desenvolver y sacar tu nueva y brillante tecnología de ese elegante empaque. No puedes esperar para probar todas sus novedosas funciones y mostrárselas a tus amigos. Hay una alegría indescriptible que viene con cada nuevo dispositivo. Estás tan emocionado y feliz de tener un nuevo dispositivo que ni siquiera piensas en cómo mantenerlo así, no solo por fuera, sino también por dentro, donde se almacena lo más importante.

Es hora de sacudir esa euforia.

Te entendemos. Es difícil controlar esa euforia tecnológica, pero seamos conscientes de la protección del dispositivo y hagamos una promesa de asegurar tu nueva tecnología y todos los mensajes de correo electrónico, fotos y cuentas que serán parte de tu vida digital. Por supuesto, los ciberdelincuentes prefieren que no lo hagas, porque les encanta el acceso fácil a la información de las PCs, Macs, smartphones, y tablets desprotegidas.

¿Estás listo? Este eBook te brinda consejos simples sobre cómo mantener tu nuevo dispositivo protegido y cómo usarlo de forma segura en línea. **¡Comencemos!**

Cómo mantenerse más seguro que el resto

Si aún no has protegido tu dispositivo, no eres el único. Muchas personas no protegen sus dispositivos simplemente porque no creen que lo necesitan[1]. Sin embargo, eso no es para nada cierto. En el 2016, el reporte de Norton Cyber Security Insights reveló que 689 millones de personas en 21 países, experimentaron delitos cibernéticos en un período de un año. Solo en México, 22.4 millones de personas fueron víctimas[1].

En los Estados Unidos el 35% de las personas tiene por lo menos un dispositivo sin protección[1]. En el 2015, los hogares americanos tenían un promedio de 5.2 dispositivos conectados[2]. Esto significa que potencialmente 4 dispositivos por hogar no tienen ningún tipo de seguridad. No es de extrañar que el crimen cibernético esté en aumento.

De los que no protegieron sus dispositivos, el 27% dijo que no hacen nada "riesgoso" en línea por lo tanto no necesitan protección[1]. Cuando piensas en todo lo que hacemos en línea que implica información personal como: enviar correos electrónicos, hacer transacciones bancarias, compras y creación de cuentas y perfiles, todo comienza a parecer arriesgado. Pero aparte de no instalar un software de seguridad, algunas personas no están tomando ni siquiera los pasos básicos para proteger sus dispositivos y cuentas, como usar configuraciones de bloqueo automático y contraseñas.

Los resultados de la encuesta publicados en el Reporte Norton de Cyber Seguridad de 2016 demuestran que:

+ del 50%	**El 44%**	**Casi 1/3**
afirmó usar contraseñas seguras para cada cuenta	dijo que solo lo hacen cuando es requerido	compartirá esas contraseñas con otras personas

Conoce algunos buenos hábitos para diferenciarte de aquellos que se están arriesgando más por no proteger sus dispositivos.

6 buenos hábitos para proteger tus PCs, Macs, smartphones y tablets

1. **Instala un software de seguridad integral.** Elige un software de seguridad de Internet que proteja tu PC o Mac contra el malware, ransomware y virus de Día Cero. Las suites de seguridad más completas respaldarán y restaurarán tus archivos, e incluso protegerán los dispositivos móviles. Para dispositivos móviles en particular, elige un software de seguridad que pueda bloquearlos y limpiarlos remotamente si son robados o extraviados.

2. **Haz una copia de seguridad de tus datos.** Crea el hábito de realizar copias de seguridad regularmente de tu computadora portátil, tablet o smartphone en la nube o en un dispositivo de almacenamiento portátil. De lo contrario, si tu dispositivo se daña, se pierde o es robado, es posible que también pierdas tus números de contacto, fotos y videos valiosos, e importantes documentos financieros y de trabajo.

3. **Bloquea tu dispositivo con una contraseña/clave.** Por lo menos, siempre debes bloquear tu dispositivo para evitar que otras personas accedan a tus cuentas y perfiles en línea u otra información privada. Asegúrate de que tu contraseña sea fuerte usando por lo menos 8 caracteres, incluyendo letras mayúsculas y minúsculas, números y símbolos. Para mayor seguridad, elige una autenticación de dos factores para tus cuentas en línea, siempre que sea posible.

4. **Protege tu información personal.** Realiza transacciones solo en sitios web seguros. Asegúrate que las URL comiencen con HTTPS o muestren un símbolo de bloqueo o texto en verde lo que indica que son sitios seguros. Evita las estafas de phishing siendo cauteloso al hacer clic en vínculos en correos electrónicos, redes sociales, o textos. Ten cuidado con la información personal que divulgas en las redes sociales. Nunca envíes información personal, como números de tarjeta de crédito o de Seguro Social por correo electrónico, texto, mensaje instantáneo o a través de redes sociales, especialmente en sitios Wi-Fi públicos no seguros.

5. **Descarga aplicaciones de fuentes seguras.** Evita aplicaciones de sitios de terceros. Los sitios de aplicaciones más conocidos, como Google Play y el App Store de Apple, cuentan con políticas estrictas de envío y revisión de aplicaciones que garantizan que las aplicaciones son seguras y no son malware disfrazado. App Advisor, una función de Norton Mobile Security, te permite saber si una aplicación es segura o no, antes de descargarla.

6. **Desactiva Wi-Fi, Bluetooth y etiquetado geográfico.** Evita que tus dispositivos móviles se conecten a redes y dispositivos desconocidos desactivando Wi-Fi y Bluetooth cuando no los utilices. Desactiva la función de etiquetado geográfico en tu dispositivo, que identifica la ubicación donde se toman las fotos, lo que permite que alguien más rastree tus movimientos, si las fotos son publicadas en línea.

3 maneras fáciles de proteger tu nuevo dispositivo

Configura tu dispositivo para que se **bloquee automáticamente** cuando esté inactivo.

Activa las funciones de reconocimiento de huellas dactilares, como el **ID de toque**.

Crea una **contraseña segura** para cada dispositivo.

Las principales amenazas en línea a evitar

Método Hacker	Cómo Funciona	Dispositivos afectados
Malware	El malware es un software creado para hacer daño. Incluye virus informáticos, gusanos y Caballos de Troya. También incluye aplicaciones para dispositivos móviles, como las que ejecutan sistemas operativos para Android e iOS.	**Todos los dispositivos conectados a Internet**
Phishing	Las estafas de phishing intentan divulgar tu información personal haciéndose pasar por entidades legítimas como bancos, compañías de pago en línea o sitios de redes sociales. La mayoría de las personas no están muy seguras de diferenciar un correo electrónico real de un correo electrónico de phishing. Solo 4 de cada 10 lo están haciendo correctamente al verificar si el correo electrónico les pide tomar una acción comprometedora, como descargar archivos adjuntos o dar la información de inicio de sesión.[1]	**Todos los dispositivos conectados a Internet**
Estafas en las redes sociales	Los hackers usan ofertas falsas, la forma más común de ataques basados en las redes sociales, para robar información personal o infectar un dispositivo con malware. Los usuarios de las redes sociales son invitados a unirse a un evento falso, descargar una aplicación o música, o participar en un concurso. A menudo piden a los usuarios que brinden la información de inicio de sesión de su cuenta o que envíen un texto con un número telefónico.	**Todos los dispositivos conectados a Internet**
Robo de identidad	Los criminales usan estafas de phishing para engañarte, hacerte revelar información personal y así poder robar tu identidad. Los dispositivos extraviados o robados, o dispositivos viejos que no se limpian, también pueden darle a los ladrones lo que ellos necesitan.	**Todos los dispositivos conectados a Internet**
Ransomware/ crypto-ransomware	Ransomware es un malware que hace que tu computadora sea inutilizable a menos que pagues al hacker para desbloquearla. Crypto-ransomware es aún más desagradable porque encripta tus datos.	**Principalmente PCs, computadoras portátiles y también dispositivos móviles**
Wi-Fi Público	Los hackers explotan las redes Wi-Fi públicas no seguras para interceptar mensajes de correo electrónico, contraseñas, credenciales de inicio de sesión o cualquier otra información no encriptada. Algunos hackers hasta crean puntos de acceso falsos que tienen nombres aparentemente legítimos, como “el Wi-Fi oficial de un aeropuerto” para “espiar” todas tus actividades en línea y robar tu información personal.	**Dispositivos móviles que utilizas fuera de tu casa, como computadoras portátiles, notebooks, tablets y smartphones**

Cómo regalar (y limpiar) tu viejo dispositivo

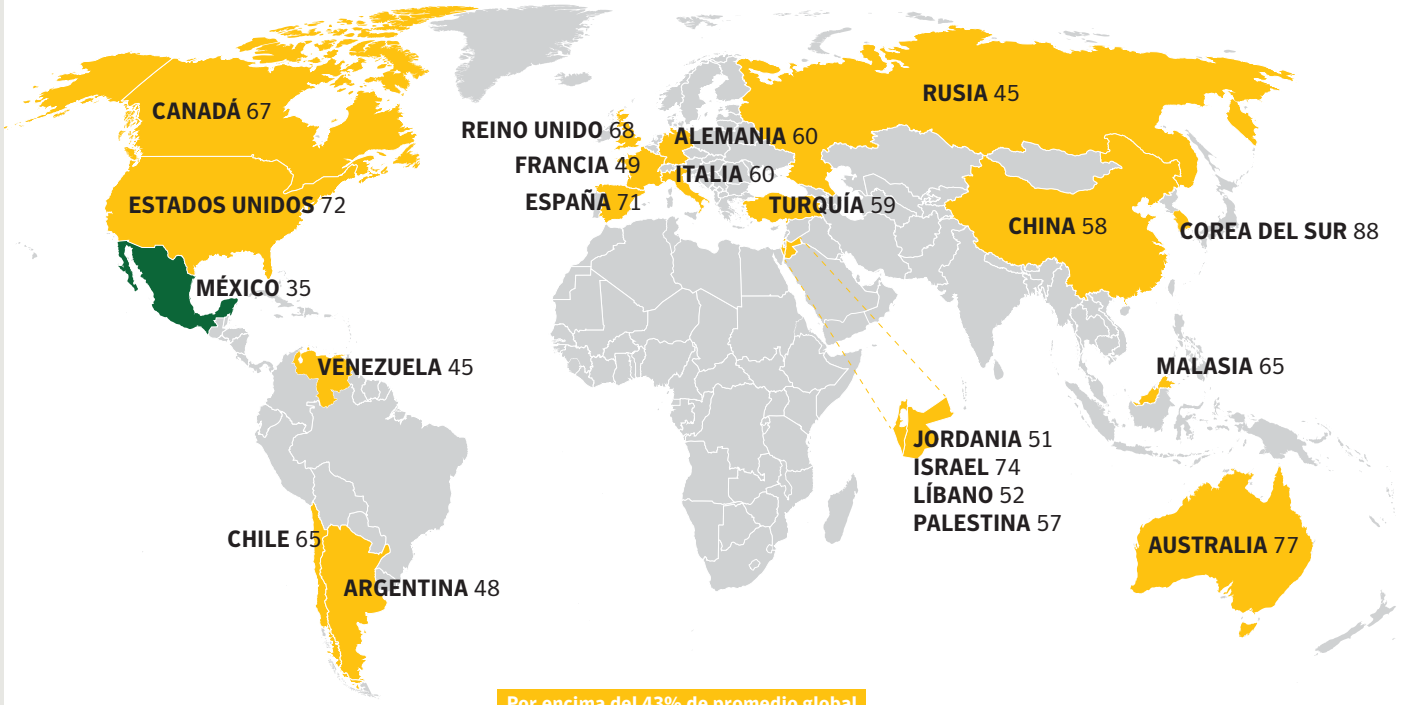
Si has tenido la suerte de comprar o recibir un nuevo dispositivo, quizás consideres regalar el viejo. Antes de hacerlo, asegúrate de no estar regalando también tu información personal. Deberás limpiar el dispositivo de cualquier contenido, incluidos los archivos personales, contraseñas guardadas o información de tarjetas de crédito almacenadas.

Teléfonos móviles o tablets. Limpia tu dispositivo restableciéndolo o restaurándolo a la programación de fábrica.

PCs, Macs, o computadoras portátiles. Limpia cualquier contenido reinstalando el sistema operativo.

Los smartphones son comunes en los Estados Unidos y Europa

(Porcentaje de adultos que afirman poseer un smartphone)



Adaptado del Pew Research Center "Encuesta sobre Actitudes Globales, Primavera 2015", Q71 y Q72.

Los smartphones también necesitan seguridad

El número de dispositivos móviles está creciendo a nivel mundial. Los smartphones en particular, se están convirtiendo en omnipresentes en muchas partes del mundo, inclusive en los Estados Unidos[3].

Los smartphones son el objetivo cada vez más atractivo para los delincuentes debido a la información que poseen y a su vulnerabilidad. Los ciberdelincuentes están diseñando ataques más sofisticados para robar datos personales valiosos o extorsionar a sus víctimas por dinero[4]. Ningún sistema operativo es totalmente seguro, tanto las plataformas Android como iOS han tenido un número creciente de ataques.

Peligros de las aplicaciones con malware

Las aplicaciones con malware pueden:

Seguir la ubicación de tu dispositivo

Desviar textos de tu banco

Recopilar información del dispositivo

Utilizar el micrófono y la cámara de tu dispositivo para monitorear tus actividades

Hacer compras con tu teléfono

Descargar e instalar aplicaciones y archivos

Robar tu información personal

Enviar mensajes a tus contactos

Entregar el control de tu dispositivo a un hacker

Los 5 consejos más importantes para compartir en #redessociales de forma más segura

Globalmente, los usuarios de Internet pasan casi dos horas al día en las redes sociales[5]. Si eres un "networker" social frecuente, es posible que no te des cuenta de que el exceso de compartir tanta información puede comprometer tu seguridad, o la de tu familia y amigos.
Sigue estos consejos para compartir en línea con mayor seguridad.

Revisa la configuración de privacidad en tus sitios de redes sociales. Aunque originalmente hayas definido tus actualizaciones para que solo sean vistas por personas a las que estás conectado, algunos sitios de redes sociales actualizan sus políticas y los usuarios no se dan cuenta de que tienen que optar por salir de algunas nuevas configuraciones de vista pública.

Acepta solo invitaciones para conectarte en línea con personas que conoces bien en la vida real. A menos que la información que compartes sea muy general, es más seguro aceptar invitaciones para conectarte solo con las personas que conoces.

No muestres los nombres de las personas de tu red. Las estafas de spear-phishing, se basan en la recopilación de información personal por parte de los cibercriminales para enviar correos electrónicos convincentes, aparentemente de personas conocidas por la víctima. El acceso a los nombres de tus contactos puede resultar en que tus amigos reciban emails falsos de alguien que se hace pasar por ti.

Publicar actualizaciones y anuncios de eventos que no son súper específicos. No des a conocer los lugares o momentos exactos de tus actividades y eventos. Guarda los detalles de los eventos especiales para las invitaciones privadas que envías a los invitados. De lo contrario, estarás anunciando cuando no estás o no estarás en casa. Recuérdalo antes de publicar, cuando estás de vacaciones.

Comparte, pero no abuses. Antes de hacer tus actualizaciones en línea, recuerda que debes ser cuidadoso. No seas culpable de DI—demasiada información. La información que decides compartir puede ser compartida por tus contactos en sus redes. Al final, una vez que tu información está en Internet, ya no tienes control sobre quién puede verla.

¿Por qué desconfiar de los sitios Wi-Fi públicos?

El Wi-Fi público puede ser conveniente, pero rara vez es seguro. Los hackers pueden “espiar” tus contactos no seguros y robar información personal, como contraseñas y números de tarjetas de crédito. Aprende cómo mantenerte seguro en sitios Wi-Fi públicos.

Qué no hacer:

- Permitir que tu dispositivo se conecte automáticamente a redes Wi-Fi
- Dejar tu Wi-Fi o Bluetooth activados si no los usas
- Acceder a los sitios web que contienen tu información confidencial, tales como cuentas bancarias o de salud
- Iniciar una sesión en una red que no está protegida por contraseña

Qué hacer:

- Desactivar el uso compartido de archivos
- Visita solo los sitios con HTTPS
- Cerrar la sesión de las cuentas y perfiles al terminar de usarlos
- Usa un VPN. Norton WiFi Privacy crea una red privada virtual que encripta toda tu información en un Wi-Fi público, haciendo que tu conexión pública sea privada

Cómo diferencias los sitios Wi-Fi seguros de los no seguros

Protege tus dispositivos con la mejor seguridad de Norton

Tu nuevo dispositivo merece una seguridad galardonada[6]. Protege todos tus dispositivos y experimenta un nuevo sentido de seguridad con los productos Norton, que reciben regularmente las máximas calificaciones en pruebas de la industria.

Norton Security Standard ofrece una protección completa para tu PC o Mac. **Conoce más**

Norton Security Deluxe protege hasta cinco dispositivos, Incluyendo PCs, Macs, Androids y dispositivos iOS, con protección en tiempo real contra amenazas existentes y emergentes. Protege contra virus, spyware, malware y otros ataques en línea. **Conoce más**

Norton Security Premium cubre hasta 10 dispositivos y añade protección para tus archivos y documentos importantes contra amenazas tales como fallas de disco duro y ransomware. Puedes hacer copia de seguridad y encriptar automáticamente hasta 25 GB de datos de tu PC a nuestro almacenamiento seguro en la nube. **Conoce más**

Norton WiFi Privacy es una aplicación VPN que protege cualquier conexión Wi-Fi convirtiéndola en una red privada virtual para encriptar toda la información que entra y sale de tu dispositivo. Norton WiFi Privacy previene que los hackers "espíen" tu información privada cuando estás usando Wi-Fi público. **Conoce más**

Norton Mobile Security protege tus smartphones y tablets Android y iOS contra amenazas digitales como aplicaciones arriesgadas, mientras que también ofrece controles para proteger tu privacidad en línea. Si tu dispositivo móvil se pierde o es robado, Norton Mobile Security te permite recuperar la información y bloquear o limpiar tu dispositivo de forma remota. **Conoce más**

Norton Safe Search asegura que los sitios que visitas sean seguros y legítimos, no de phishing o fraudulentos. Convenientemente libre y siempre activo, Norton Safe Search es un entorno de búsqueda desarrollado con enfoque en la seguridad en línea. **Conoce más**

Norton Safe Web es un servicio gratuito de clasificación de sitios web aplicable a: Google, Yahoo, Bing y Ask.com que usa la barra Norton instalada en tu PC. Con Norton Safe Web puedes saber qué tan seguro es cada sitio. **Conoce más**

Norton Identity Safe es un administrador de contraseñas gratuito que hace que el inicio de sesión en tus sitios favoritos sea más fácil y seguro. Mantiene tus contraseñas sincronizadas en diferentes computadoras, navegadores y dispositivos móviles, con tus contraseñas almacenadas en una bóveda segura basada en la nube, a la que solo tú puedes acceder. **Conoce más**

Norton Family Premier es un software de control parental que ayuda a tus hijos a explorar, aprender y disfrutar de su mundo conectado de forma segura. Conoce de un vistazo cuándo y dónde tus hijos pasan su tiempo en línea. **Conoce más**

Norton Identity Protection Elite protege todo lo que has construido proporcionando un monitoreo extenso, alertas y servicios de restauración para mantener tu identidad segura. Si tu identidad fue comprometida, un equipo de expertos en restauración de identidad basado en los Estados Unidos trabajará contigo hasta que el problema sea resuelto. **Conoce más**

Para conocer más formas de cómo proteger tus dispositivos: "Cómo configurar y proteger tu nueva tecnología"

Seguridad galardonada

PC EDITORS' CHOICE™ PCMAG.COM

Mantente informado con Norton

Para obtener consejos sobre cómo proteger tus dispositivos y otros problemas de seguridad en línea, lee los artículos en el Blog de Protección de Norton y las actualizaciones de respuesta rápida de las últimas amenazas en Seguridad Cubierta por Norton.

Sigue a Norton

[1] Norton, "Norton Cyber Security Insights Report 2016," Octubre de 2016. https://us.norton.com/cyber-security-insights-2016

[2] Ericsson, "North America Ericsson Mobility Report," Noviembre de 2015. www.ericsson.com/mobility-report

[3] Pew Research Center, "Spring 2015 Global Attitudes Survey," Febrero 23 de 2016. http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/

[4] Symantec, "Internet Security Threat Report 2016," Abril de 2016. https://www.symantec.com/security-center/threat-report

[5] Statista, "Average daily time spent on social media worldwide 2012-2016", Septiembre de 2016. https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/

[6] Hasta 2016, PC Magazine ha otorgado el Premio Editors' Choice a los productos de seguridad Norton 39 veces desde 2001, más veces que cualquier competidor. Entre los recientes ganadores de los premios Editors' Choice se incluyen Norton Security Premium (otorgado el 25 de agosto de 2016 y el 27 de octubre de 2015) y Norton Family Premier (otorgado el 19 de octubre de 2015).