Las herramientas para blindar tus dispositivos ante los delincuentes. Hay un buen número de imprescindibles: 'cleaners', bloqueadores, cortafuegos...

ILUSTRACIÓN **ADOBE STOCK**

J. C. CASTILLO

La ciberseguridad es la asignatura pendiente de muchos ciudadanos y empresas, lo que constituye un problema en una sociedad hiperconectada como la nuestra. Raro es el dispositivo particular o corporativo que no tiene ya acceso a internet, lo que brinda tantas oportunidades como amenazas. Los datos que almacenamos en discos duros, teléfonos móviles, ordenadores o servidores pueden quedar expuestos si no somos lo suficientemente precavidos.

Solo en 2024, el Instituto Nacional de Ciberseguridad (Incibe) gestionó 97.348 incidentes de este tipo. Supone un aumento del 16,6% respecto al ejercicio anterior. Las infecciones por 'malware' y los fraudes online fueron las principales amenazas (con 42.136 y 21.571 casos identificados respectivamente). El organismo detectó, además, cerca de 200.000 sistemas vulnerables, es decir, susceptibles de ser explotados por los ciberdelincuentes.

En términos globales, el cibercrimen ha dejado pérdidas superiores a los 10.500 millones de dólares durante el año que acabamos de despedir. De ahí la importancia de recurrir a las llamadas 'herramientas de seguridad', programas y aplicaciones cuyo fin es prevenir, detectar y ofrecer soluciones a las principales tretas cibernéticas. La Oficina de Seguridad del Internauta (OSI) nos recomienda un buen número. Toma nota.

Detección de virus

Los antivirus o 'cleaners' son quizás las herramientas más conocidas. Detectan y eliminan cualquier 'software' malicioso a la mínima sospecha de infección, y muchas son gratuitas. 'Microsoft Defender' forma parte de Windows, por ejemplo, pero también son muy utilizados 'AVG Antivirus', 'Malwarebytes Antimalware' o 'Avast Antivirus'. Por su parte, los analizadores de URL y archivos ('URLVoid', 'Kaspersky QR Scanner', 'Virus Total'...) permiten comprobar la seguridad de un ejecutable o una página web antes de que hagamos clic.

Protección de cuentas

En este apartado encontramos las aplicaciones de autenticación de doble factor ('Microsoft Authenticator', 'Google Authenticator'..., diseñadas para que nuestra seguridad no dependa exclusivamente de una contraseña); y los gestores de contraseñas ('KeepassXC', 'Keeper'), que generan claves aleatorias en un mismo lugar, lo que las hace más seguras y evita que tengamos que recordarlas.

Refuerzo de conexiones

Las aplicaciones de Red Privada Virtual o VPN ('Tunnel Bear', 'NordVPN', 'HIDE.me'...) permiten establecer conexiones seguras cuando nos dispongamos a intercambiar información sensible; y los cortafuegos ('Netguard' o los propios 'firewalls' de MacOS y Windows) previenen los accesos no autorizados a nuestros dispositivos. También resultan útiles los programas de análisis de tráfico ('WiFiman', 'Fing'), que identifican al momento todos los dispositivos conectados a nuestra red, además de la información que viaja por ella, lo que facilita la detección de intrusos.

Navegación segura

Los expertos del Incibe recomiendan usar navegadores centrados en la seguridad ('Brave', 'Tor', Comodo Dragon') y buscadores que no recopilen datos personales ni los compartan con terceros, como 'Yandex', 'Qwant' o 'DuckDuckGo'. Tampoco está de más instalar un bloqueador de publicidad para surcar la red sin molestas intromisiones (algunas potencialmente peligrosas si nos da por hacer clic). 'AdGuard', 'Stands Adblocker' o 'uBlock Origin' se encuentran en español y son gratuitos.

Salvaguarda de información

Las herramientas de cifrado permiten proteger archivos sensibles de forma que nadie pueda abrirlos sin autorización. Las encontramos tanto integradas en nuestro sistema operativo ('FireVault' en MacOS y 'EFS' en Windows) como independientes y gratuitas ('Cryptomator', 'VeraCrypt'). Además, los programas de borrado seguro ('Utilidad de discos' para MacOS, 'Shreddit - Data Eraser') garantizan que no quede rastro de la información almacenada en aquellos dispositivos que vayamos a reciclar o revender.

Monitorización de recursos

Una de las señales de que nuestro equipo ha sido infectado con un virus es que, de repente, funcione más lento de lo habitual. Algo que puede detectarse fácilmente con los llamados programas de monitorización de recursos, también capaces de «corregir errores básicos y eliminar funciones obsoletas», explica la OSI. Pueden servirnos el 'Administrador de tareas de Windows' o el 'Monitor de Actividad de macOS', pero también se encuentran opciones como 'Process Explorer' o 'CPU X'.

Bloqueadores

En última instancia encontramos los bloqueadores de aplicaciones y llamadas. Si queremos impedir el libre acceso a determinadas apps (como WhatsApp o Instagram) en el móvil, algunas soluciones independientes de los sistemas operativos son 'Bloqueo de Aplicaciones xLock' o 'AppBlock'. Y si pretendemos librarnos de las molestas llamadas de spam (que persisten pese a los cambios en la normativa implementados por el Gobierno), 'Truecaller', 'Call Control' o 'Hiya' son capaces de identificarlas y bloquearlas para que no caigamos en las estafas que esconden.

El Incibe apela igualmente a ser previsores realizando copias de seguridad, instalando programas de recuperación de archivos y activando la geolocalización del smartphone, 'tablet' u ordenador para facilitar su recuperación si nos lo sustraen. Todo ello al tiempo que recuerda algo fundamental: tan importante es instalar estas herramientas de seguridad como configurarlas correctamente.