Cinco soluciones para mantener el celular seguro si ya no recibe más actualizaciones

La vida útil de los celulares suele estar marcada por el ciclo de actualizaciones que reciben, un factor que impacta de manera directa en la protección, el desempeño y la compatibilidad del equipo.

Aunque los fabricantes han mejorado en los últimos años la entrega de parches y mejoras, la obsolescencia llega inevitablemente para millones de usuarios: el dispositivo ya no recibe actualizaciones de sistema ni de seguridad y queda expuesto a diversas amenazas, reseña Infobae.

No obstante, existen modos efectivos para mantener la seguridad y sacar provecho de un teléfono antiguo.

Cómo mantener seguro el celular si ya no hay actualizaciones

– Realizar copias de seguridad de manera habitual

Uno de los principales riesgos de usar un dispositivo sin soporte oficial radica en la posible pérdida de datos, ya sea por un fallo, un ataque o la necesidad de restaurar el equipo. Por este motivo, realizar copias de seguridad frecuentes adquiere un papel central.

Guardar la información en la nube, mediante servicios como Google Drive, iCloud u otros, permite a los usuarios recuperar con facilidad contactos, fotos, videos y documentos personales ante cualquier contingencia. Quienes prefieran opciones fuera de línea pueden valerse de discos duros externos o memorias USB, aunque se recomienda verificar siempre la integridad de estos respaldos y actualizarlos cada cierto tiempo.

– Mantener actualizadas todas las aplicaciones instaladas

Aunque el sistema operativo deje de recibir actualizaciones, es frecuente que muchas de las aplicaciones disponibles en el celular sigan renovándose a través de las tiendas oficiales como Google Play Store o App Store. Esta dinámica es clave, ya que los desarrolladores corrigen fallas de seguridad, mejoran la compatibilidad y agregan nuevas funciones en estas continuas revisiones.

Se recomienda revisar periódicamente la lista de apps instaladas y verificar si existen nuevas versiones para descargar. Activar la opción de actualizaciones automáticas garantiza que las aplicaciones importantes, como navegadores, mensajeros o sistemas de autenticación, estén protegidas ante amenazas emergentes.

Sin embargo, es conveniente eliminar aplicaciones obsoletas, no actualizadas o sospechosas, puesto que, al no recibir soporte, podrían convertirse en una vía de ingreso para cualquier software malicioso.

– Priorizar la seguridad al instalar aplicaciones y navegar

La recomendación de descargar aplicaciones únicamente desde los repositorios oficiales cobra vital importancia en celulares que ya no cuentan con parches de seguridad. Las tiendas como Google Play Store o App Store filtran una gran cantidad de amenazas y reducen significativamente el riesgo de instalar software malicioso.

Evitar la instalación de archivos APK de fuentes desconocidas, así como mantenerse alerta frente a enlaces incluidos en correos electrónicos, mensajes SMS o cualquier otro tipo de comunicación sospechosa. Tampoco conviene seguir instrucciones poco claras para “mejorar el rendimiento” del móvil a través de páginas no verificadas.

Este enfoque de máxima precaución debe aplicarse a toda interacción digital: documentos adjuntos, archivos descargados, redes WiFi abiertas y cualquier canal de acceso externo.

– Instalar apps de seguridad y maximizar buenas prácticas

La utilización de aplicaciones de seguridad puede suplir, al menos en parte, la ausencia de parches oficiales. Los antivirus para móviles, tanto en versiones gratuitas como pagas, realizan análisis periódicos de archivos y alertan sobre posibles amenazas. Entre sus funciones más útiles figuran la detección de troyanos, spyware y aplicaciones no autorizadas.

Además de estas herramientas, resulta esencial reforzar las prácticas personales de protección: elegir contraseñas robustas y distintas para cada servicio, activar la autenticación de dos factores cuando sea posible, y mantener los accesos a servicios bancarios y redes sociales bien resguardados. La autenticación en doble paso, por ejemplo, ofrece una lámina de seguridad adicional frente al robo de datos y accesos indeseados.

– Considerar alternativas como las Custom ROM o evaluar el recambio

Para quienes utilizan Android, una opción relevante consiste en instalar una Custom ROM. Se trata de versiones personalizadas del sistema operativo, mantenidas por comunidades de desarrolladores independientes que actualizan y refuerzan la seguridad de equipos desatendidos por los fabricantes originales.

Proyectos como LineageOS, GrapheneOS o crDroid permiten adaptar móviles antiguos con nuevas certificaciones de seguridad y funcionalidades. Si bien el proceso de instalación requiere cierto grado de conocimiento técnico y puede resultar complejo para el usuario promedio, termina extendiendo la vida útil del dispositivo y permitiendo su uso diario con garantías superiores.

Quienes usen iOS, por su parte, disponen de medidas más restrictivas, ya que Apple no permite modificar el sistema operativo. En ese caso, reforzar contraseñas, desinstalar apps no oficiales y adoptar el doble factor de autenticación son los pasos esenciales.

Con información de VF