LITORALPRESS

Fecha: 24-06-2026 **Visitas:** 3.396 **Favorabilidad:** ☐ No Definida
Fuente: Los Andes Online
Título: **Cuando la tecnología envejece, la seguridad se debilita**

Link: https://www.losandesonline.cl/noticias/62146/cuando-la-tecnologia-envejece-la-seguridad-se-debilita.html

Por Edgardo Fuentes Cáceres – Director Ingeniería en Ciberseguridad, UNAB Opinión Cuando la tecnología envejece, la seguridad se debilita Por Edgardo Fuentes Cáceres – Director Ingeniería en Ciberseguridad, UNAB Tuitea Comparte Imprimir Más Noticias Reproducción asistida Desertificación y sequía, un desafío de cuenca La recaudación silenciosa Un Estado fatigado Los niños perdidos de Chile: una vergüenza que exige justicia Resiliencia en transporte e infraestructura En un mundo donde la tecnología avanza rápidamente, es común pensar que cambiar de celular, computador o dispositivo es solo una cuestión de tener algo más rápido o moderno. Sin embargo, hay un aspecto mucho más importante que muchas veces pasa desapercibido: la seguridad.

El reciente descubrimiento de una vulnerabilidad en chips de Qualcomm vuelve a poner este tema sobre la mesa, demostrando que los riesgos no siempre están en las aplicaciones o en internet, sino también en componentes internos de los equipos que usamos a diario. Este problema no afecta solo a un tipo de dispositivo ni a una marca en particular. Al contrario, está presente en millones de equipos que han estado en uso durante años. Hablamos de teléfonos móviles, tablets, routers de internet, equipos industriales conectados e incluso sistemas instalados en vehículos. Es decir, no se trata solo de algo que impacte a personas en su vida cotidiana, sino también a empresas y organizaciones que dependen de esta tecnología para funcionar.

Ahora bien, ¿qué hace que esta vulnerabilidad sea tan relevante? Para entenderlo sin entrar en complejidades técnicas, basta saber que está ubicada en una especie de “parte básica” del dispositivo, que se encarga de que el equipo pueda encenderse y funcionar correctamente desde el primer momento. Si esa parte presenta un problema, un atacante podría intervenir el dispositivo desde muy adentro, logrando acceso a información o incluso controlándolo. Eso sí, hay un punto importante que ayuda a poner el riesgo en contexto: no es un ataque que se pueda hacer a distancia fácilmente. En la mayoría de los casos, requiere que alguien tenga acceso físico al equipo, por ejemplo, conectándolo a un computador mediante un cable o manipulándolo directamente. Y es aquí donde aparece un tema clave que muchas veces se subestima: la seguridad física. Aunque el ataque no sea remoto, sigue siendo posible en situaciones bastante comunes. Por ejemplo, cuando dejamos un teléfono sin supervisión, cuando lo enviamos a reparación, cuando usamos un cargador desconocido o cuando lo conectamos en lugares públicos. En esos momentos, el equipo puede quedar expuesto sin que lo notemos.

Por eso, más allá de soluciones técnicas, hay acciones simples que marcan la diferencia, como evitar cargar dispositivos en puertos USB públicos, no perderlos de vista, utilizar mecanismos de bloqueo y proteger la información que contienen. En entornos laborales, además, es clave llevar un control claro de los equipos y de quién tiene acceso a ellos. A partir de este escenario, surge una reflexión más profunda. Muchos de los dispositivos afectados por este tipo de problemas tienen varios años en el mercado y, en muchos casos, ya no reciben actualizaciones de seguridad. Esto significa que, aunque exista una vulnerabilidad, simplemente no habrá solución disponible para esos equipos. Aquí es donde cambia la forma de ver la renovación tecnológica. No se trata solo de tener lo último o de mejorar el desempeño, sino de reducir los riesgos. Un dispositivo antiguo no solo es más lento o limitado, también puede ser más vulnerable, porque sus sistemas de protección ya no están al día. Renovar un equipo, entonces, debe entenderse como una medida preventiva. Significa utilizar tecnología que aún cuenta con soporte, que recibe actualizaciones y que incorpora mejoras en seguridad. Es una forma de proteger tanto la información personal como los datos de una organización. En cuanto a los plazos recomendables, no existe una regla única, pero sí orientaciones claras. Para usuarios personales, cambiar de dispositivo cada tres a cinco años suele ser adecuado, especialmente cuando dejan de recibir actualizaciones. En empresas, donde el riesgo es mayor, lo recomendable es un recambio cada tres o cuatro años. En el caso de equipos críticos o industriales, estos plazos pueden ser incluso más cortos o depender directamente del soporte que entregue el fabricante. Mantener equipos antiguos puede parecer una forma de ahorrar, pero en la práctica puede generar problemas mayores. Un dispositivo sin soporte puede transformarse en el punto más débil de una red, facilitando el acceso a información o provocando fallas que afecten el funcionamiento completo de un sistema. En definitiva, lo que deja este caso no es solo una preocupación puntual, sino una enseñanza más amplia. La seguridad no depende únicamente de lo que vemos o usamos directamente, sino también de la base tecnológica que sostiene nuestros dispositivos. Renovar tecnología no es un lujo, es una forma de cuidarnos en un entorno donde los riesgos evolucionan constantemente. Porque al final, no se trata solo de tener algo nuevo, sino de evitar quedar vulnerables por seguir dependiendo de lo antiguo.