EL HERALDO
Fecha: 31/07/2025 Audiencia: 6.000 Sección: ACTUALIDAD
Vpe: $752.222 Tirada: 3.000 Frecuencia: DIARIO
Vpe pág: $1.850.000 Difusión: 3.000
Vpe portada: $1.850.000 Ocupación: 40,66%

¿Tus dispositivos te están espiando sin que lo sepas?

¿Dejarías que un extraño entrara a tu casa y escuchara tus conversaciones privadas? Probablemente no. Sin embargo, eso es exacta mente lo que podrías estar permitiendo cuando usas ciertos dispositivos inteligentes sin configurar adecuadamente su seguridad.

En los últimos años, el crecimiento sobre el uso de dispositivos inteligentes que nos ayudan a poder automatizar nuestros hogares ha ido en crecimiento. Si bien es cierto que este tipo de dispositivos tales como: asistentes de voz, focos inteligentes, cámaras de seguridad, enchufes, termostatos y cerradoras electrónicas entre otras, que son las más utilizadas, nos ayudan en gran manera a automatizar varias funciones de nuestro hogar, incluso permitiendo generar una percepción de seguridad mayor (si no me encuentro en mi hogar, se pueden encender las luces a distancia, generando la idea de que la casa no está desocupada), cabe formular la interrogante sobre si ¿esto tiene algún riesgo? Una mala gestión de estos dispositivos puede involucrar vulnerabilidades de seguridad, pérdida de privacidad, ciberataques, falla en rendimiento y consumo energético. Este tipo de vulnerabilidades se pueden presentar por faltas de actualizaciones en los dispositivos, exposición pública o ataques a la red wi-fi de la casa. Según un estudio de Kaspersky y de Palo Alto Network, cada 39 segundo se registra un intento de ataque a un dispositivo inteligente.

Frente a este panorama, no basta con llenar nuestros hogares de dispositivos inteligentes; es urgente aprender a usarlos con… inteligencia. La primera medida clave es cambiar las contraseñas predeterminadas apenas se instalan, optando por claves únicas y seguras. También es necesario mantener los dispositivos actualizados, ya que las actualizaciones no solo mejoran funciones, sino que corrigen vulnerabilidades que pueden ser explotadas por atacantes. Otra buena práctica es segmentar la red del hogar, creando una red Wi-Fi exclusiva para los dispositivos IoT, separada de

Edgardo Fuentes
Director Ingeniería en Ciberseguridad
UNAB

aquella donde se conectan computadores y teléfonos. Además, muchas funciones como el acceso remoto o el micrófono pueden desactivarse si no se usan habitualmente, reduciendo así la superficie de ataque. A la hora de comprar, es recomendable optar por marcas reconocidas que ofrezcan soporte y actualizaciones, y evitar dispositivos genéricos que no garantizan estándares básicos de seguridad. Finalmente, es vital que todos en el hogar, no solo quien configura el dispositivo, entiendan los riesgos básicos y participen activamente en la protección del entorno digital.

Vivimos en una época donde la tecnología se ha integrado de manera natural a nuestra vida doméstica, otorgándonos comodidad, eficiencia y sensación de control. Sin embargo, esa misma tecnología, si no se maneja con criterio y responsabilidad, puede convertirse en una puerta abierta al riesgo. La ciberseguridad en el hogar inteligente no es un lujo técnico ni un problema lejano: es una necesidad concreta y cotidiana. Así como cerramos la puerta con llave al salir de casa, debemos aprender a cerrar también nuestras puertas digitales. La clave está en la prevención, la educación y la conciencia: porque la seguridad de nuestros hogares ya no depende solo de muros físicos, sino también de las decisiones invisibles que tomamos cada día frente a un dispositivo conectado.