



VARIOS SON LOS DESAFÍOS

¿Estaremos seguros en un mundo ultraconectado?

En un mundo digital cada vez más interconectado, el paso de la quinta (5G) a la sexta (6G) generación de conectividad inalámbrica, promete revolucionar las comunicaciones móviles, pero también plantea dudas acerca de si los sistemas de ciberseguridad están preparados para protegernos de las amenazas que planteará este avance tecnológico.

EFE Internacional

Si la quinta generación de tecnología celular inalámbrica (5G), ahora en funcionamiento, ya ofrece un aumento y una mejora radicales en las velocidades de carga y descarga, consistencia, capacidad, eficacia y fiabilidad de las conexiones, respecto de las redes anteriores, la sexta generación (6G), hoy en desarrollo, promete generar una transformación aún más radical. "El avance hacia el 6G está plantean-

do una revolución en la conectividad global y llevando la interconexión de dispositivos a niveles insospechados", según explica Gema Ruiz, responsable de innovación en la firma de ingeniería de "software" Softtek (www.softtek.com).

Esta especialista destaca que, "ante la integración de billones de dispositivos electrónicos en tiempo real" (al instante), mediante esta tecnología emergente "las redes de comunicación serán más rápidas, eficientes y expansivas".



La conectividad 6G es la próxima generación de redes móviles, que irá reemplazando a la 5G, que ahora está operativa.

ENTRANDO EN LA ERA DE LA ULTRAONECTIVIDAD

Aun así, "este progreso tecnológico viene acompañado de una serie de desafíos, especialmente en el ámbito de la ciberseguridad", advierte.

"El avance hacia el 6G traerá enormes beneficios en la conectividad, pero es fundamental que las empresas y gobiernos trabajen conjuntamente para garantizar una protección robusta de los sistemas informáticos, programas, dispositivos, datos, activos digitales y personas, frente a los ciberataques y amenazas que puedan plantear esta nueva tecnología, según Ruiz, "Debemos estar preparados para desarrollar y aplicar soluciones de seguridad que no solo se adapten a un mundo ultra conectado, sino que evolucionen junto con esta nueva era tecnológica", enfatiza.

A medida que el mundo se aproxima al lanzamiento comercial del 6G, previsto para 2030, la creciente complejidad de las infraestructuras y la proliferación de puntos de acceso, aumentan las ciberamenazas, como consecuencia del aumento de la "superficie de ataque", es decir el conjunto de puntos de entrada, vías y vulnerabilidades que un atacante puede explotar para acceder a un sistema o red, según Softtek.

Señalan que la sexta generación de conectividad móvil pretende reducir aún más la latencia (retraso de milisegundos en la comunicación de datos a través de una red), en las conexiones e incrementar la velocidad de transmisión.

Softtek prevé que el 6G permitirá utilizar hologramas interactivos (imágenes tridimensionales proyectadas en el aire con las que se podrá interactuar)



El progreso tecnológico del 6G viene acompañado de una serie de desafíos, especialmente en el ámbito de la ciberseguridad.

y la Internet sensorial (la navegación por la Red permitirá también oler, saborear y tocar a distancias, a través de dispositivos especiales).

Gracias a que los sistemas que estarán conectados entre sí, el 6G también posibilitará la automatización avanzada (aplicación de inteligencia artificial, aprendizaje automático) y robots para automatizar procesos) y las ciudades inteligentes (zonas en las que utilizarán tecnologías digitales y se recopilarán datos a gran escala para mejorar la eficiencia y la calidad de vida), adelantan.

CINCO DESAFÍOS PARA LA CIBERSEGURIDAD GLOBAL

Los especialistas de Softtek han identificados cinco desafíos principales para la protección de las infraestructuras digitales, que plantearán la llegada del 6G que requerirán soluciones innovadoras y nuevos estándares globales para garantizar un entorno digital seguro.

Las organizaciones y compañías deberán investigar nuevas tecnologías e invertir en infraestructura, capacitación y desarrollo de otros modelos de ne-

gocio, para asegurar la privacidad y tener una ventaja competitiva en un mundo ultraconectado, aseguran.



ciberamenazas como consecuencia de su dependencia de redes conectadas.

SE EXPANDIRÁ LA "SUPERFICIE DE ATAQUE"

"La interconexión de cada vez más dispositivos está multiplicando los puntos de acceso, que los ciberdelincuentes pueden explotar para lanzar sus ataques" según estos expertos.

AUMENTAN LOS RIESGOS EN LAS INFRAESTRUCTURAS CRÍTICAS

Algunos sectores, vitales para garantizar la estabilidad y seguridad globales, como la salud, el transporte y la energía se pueden ver aún más expuestos a

EL CIFRADO SE VOLVERÁ MÁS VULNERABLE

La computación cuántica, que según el reporte de Softtek "2025 Digital Trends" (www.softtek.com/es/digital-trends-2025) está emergiendo como la próxima gran revolución tecnológica, podría debilitar los sistemas de cifrado actuales, convirtiéndose en un desafío crucial en la protección de datos confidenciales.

LAS REDES DE TELECOMUNICACIONES SERÁN MENOS SEGURAS

A raíz de la expansión de las redes

6G, se integrarán tanto infraestructuras terrestres como satelitales, en redes híbridas, lo cual aumentará la complejidad de las ciberamenazas, señalan.

SE NECESITARÁN NUEVOS ESTÁNDARES DE SEGURIDAD

A medida que los sistemas de la conectividad de sexta generación se desplieguen a nivel global, será esencial crear marcos regulatorios y estándares de seguridad internacionales para coordinar esfuerzos, evitar brechas en la protección de datos y garantizar que el diseño de las redes 6G se encamine a beneficiar a los usuarios finales y a ofrecer soluciones rentables para proveedores y operadores, concluye Softtek.

CONECTIVIDAD 5G Y COMPUTACIÓN CUÁNTICA: DOBLE RETO

"La conectividad 6G será mucho más rápida que la 5G, tendrá un menor tiempo de espera en la conexión y permitirá conectar billones de dispositivos al mismo tiempo. La computación cuántica es una nueva forma de procesar información que usa principios de la física cuántica", explica a EFE Doris Seedorf, directora ejecutiva (CEO) de Softtek, para España. Seedorf señala que "ambas tecnologías están avanzando rápidamente y, aunque ofrecen grandes beneficios, también representan nuevos desafíos para la seguridad digital".

"El 6G conectará muchos más dispositivos a la red, aumentando los puntos por donde los atacantes podrían entrar, mientras que la computación cuántica podría romper los actuales sistemas de seguridad, como los métodos de cifrado que protegen nuestras contraseñas o la información bancaria", advierte.

Por eso, "es crucial que trabajemos desde ahora en nuevas formas de proteger la información, para crear tecnologías de cifrado resistentes a la computación cuántica y reforzar la ciberseguridad en el nuevo entorno ultra conectado", concluye Seedorf.