LITORALPRESS

Fecha: 26-12-2023
Medio: Hoy x Hoy
Supl. : Hoy X Hoy
Tipo: Noticia general
Título: Cuatro aspectos en que hay que fijarse si se desea comprar una cámara de seguridad para el hogar

Pág. : 6
Cm2: 705,3
VPE: $ 1.578.528

Tiraje: 82.574
Lectoría: 251.974
Favorabilidad: No Definida

Cuatro aspectos en que hay que fijarse si se desea comprar una cámara de seguridad para el hogar

Con una percepción de inseguridad al alza, cada vez más familias se equipan con implementos de vigilancia. Sin embargo, es necesario tener claros los elementos en los que hay que fijarse y los que deben evitarse a la hora de elegir un dispositivo.

Ignacio Silva

SHUTTERSTOCK

El mercado de la seguridad familiar ha experimentado un alza ante el temor a la delincuencia que aqueja al país.

Cuando se hizo pública hace menos de un mes, hubo un dato de la Encuesta Nacional Urbana de Seguridad Ciudadana (Enusc) 2023 que fue replicado por medios de Chile y el extranjero.

El sondeo reveló que la percepción de inseguridad en Chile había alcanzado el 90,6%, la cifra más alta en 10 años. Los resultados del estudio coinciden además con los obtenidos por otras encuestas como la de la Fundación Paz Ciudadana, que en octubre dio a conocer que el temor de la población chilena a sufrir un delito había llegado al 30,5%, su peak desde 2000.

Entre otras cosas, el contexto ha llevado a parte de la población a adquirir implementos asociados a la seguridad. Uno de los más populares son las cámaras de vigilancia, a pesar de que los expertos indican que puede tratarse de un artefacto que no se asocia directamente a la prevención del delito.

"Instalar una cámara de seguridad en estos días es muy importante pero es un mecanismo post-mortem, o sea, después de que ocurrió el suceso sirven como registro de actividades o de prueba. Las cámaras permiten reconocimiento de los delincuentes, prueba de los sucesos que ocurren y también identificación para tribunales", advierte Iván Llanos, académico de la Escuela de Ingeniería en Ciberseguridad de la Universidad de Las Américas (UDLA).

Pese a esto, el especialista no duda en recomendar el uso de cámaras de seguridad, aunque comenta que hay que fijarse en ciertos detalles antes de adquirir un dispositivo.

> "Instalar una cámara de seguridad en estos días es muy importante pero es un mecanismo post-mortem, o sea, después de que ocurrió el suceso sirven como registro de actividades o de prueba."
>
> IVÁN LLANOS
> ACADÉMICO UDLA

"Lo primero es que sean certificadas, para garantizar el correcto uso y funcionamiento de las mismas, así como cumplir con los estándares de calidad. Segundo, la resolución y calidad. No mirar si es 4K o 1080 de resolución, sino verificar in situ una prueba de la calidad de grabado y foto. La mayoría de pruebas desechadas en tribunales son por mala calidad", alerta el docente. "Tercero, el ángulo de visión que tienen para poder cubrir toda el área de interés. También debe contar con audio, sensor de movimiento y visión nocturna, porque es fundamental para captar intrusiones de forma adecuada", agrega.

Según el especialista, una cámara de buena calidad y que cumpla con todas esas condiciones se puede encontrar en el mercado por valores que fluctúan entre los $40.000 y los $100.000.

"Las opciones más económicas fallan en lo indicado previamente. Los modelos chinos muchas veces carecen de certificaciones y pueden fallar, quemarse o tener fallas electricas. Marcas como Xiaomi, TP-Link, Hikvision que estén certificadas dan una buena cobertura para ámbito particular", agrega Llanos.

HACKERS

El uso extendido de las cámaras de vigilancia también ha creado nuevos riesgos. Así lo asegura David González, especialista en seguridad informática del Laboratorio de ESET Latinoamérica, quien advierte que es posible que sean intervenidas por hackers.

> "Lamentablemente sí es posible hackearlas, aunque depende mucho de las habilidades del ciberdelincuente, el fabricante y configuraciones que haya dejado el usuario por defecto."
>
> DAVID GONZÁLEZ
> ESET LATINOAMÉRICA

"Lamentablemente sí que es posible hackearlas, aunque depende mucho de las habilidades del ciberdelincuente, el fabricante y configuraciones que haya dejado el usuario por defecto. Con la llegada del Internet de las Cosas miles de electrodomésticos, sistemas de climatización, energía, agua y seguridad incrementaron su uso, pero esto trajo consigo un mayor riesgo para la privacidad o la seguridad si no son bien configurados y esto es aprovechado por los ciberdelincuentes", advierte.

El especialista explica que los hackers acceden a las cámaras empleando diversas técnicas. Entre las más habituales se encuentran el aprovechamiento de contraseñas preestablecidas por el fabricante y que no fueron cambiadas por el usuario, la búsqueda en una web específica que muestra las unidades con problemas de seguridad y el uso de un exploit o software malicioso.

"Vulnerar las cámaras de seguridad, indistintamente que sean de hogares o entornos de trabajo, por parte de los ciberdelincuentes, tiene como objetivos el espionaje, obtención de información confidencial, el sabotaje o incluso acceder a redes más amplias de donde están ubicadas. La motivación puede variar dependiendo de los intereses del ciberdelincuente, que van desde la obtención de información hasta la realización de actividades ilegales", agrega González.

Para evitar ser víctima de ciberdelincuentes, el especialista recomienda asegurarse de que las grabaciones se almacenen de manera segura y cumpliendo con las normativas de protección de datos, además de revisar periódicamente el hardware y software. "También es importante cambiar las credenciales de fábrica, buscar modelos que permitan habilitar un segundo factor de autenticación, activar las funciones de seguridad y utilizar una conexión por VPN para cuando necesite ingresar a la cámara al momento de revisar la transmisión de video en tiempo real. Esto para mantener el equipo con el que está visualizando seguro", concluye.