Minerva Journal
ISSN-E: 2697-3650 Vol.5, Issue N°15, (pp. 22-31)

Artículo de investigación https://doi.org/10.47460/minerva.v5i15.171

# Estrategias proactivas para mitigar los riesgos emergentes de ciberseguridad en dispositivos IoT para hogares inteligentes

Kevin García Pérez*
https://orcid.org/0009-0006-16632258
kevin.garciaperez@upse.edu.ec
Universidad Estatal Península de Santa Elena
Salinas-Ecuador

Oscar Apolinario Arzube
https://orcid.org/0000-0003-4059-9516
papolinario@upse.edu.ec
Universidad Estatal Península de Santa Elena
Salinas-Ecuador

*Autor de correspondencia: kevin.garciaperez@upse.edu.ec

Recibido (12/07/2024), Aceptado (21/08/2024)

**Resumen:** En este trabajo se propusieron estrategias para mitigar los riesgos emergentes en dispositivos inteligentes de Internet de las Cosas (IoT) en hogares. Con el aumento significativo de estos dispositivos, la ciberseguridad se convirtió en una preocupación primordial. Por lo tanto, este estudio se centró en identificar posibles riesgos y vulnerabilidades, mediante el uso de encuestas para evaluar las prácticas de seguridad actuales, el conocimiento acerca de las medidas de protección entre otros aspectos relacionados con la ciberseguridad. A partir de estos resultados, se realizaron recomendaciones para los usuarios, con el objetivo de fortalecer la seguridad en sus dispositivos IoT, y promover buenas prácticas para crear un entorno doméstico más seguro y protegido contra posibles amenazas cibernéticas.

**Palabras clave:** ciberseguridad, internet de las cosas, hogares inteligentes, estrategias.

## Proactive strategies to mitigate emerging cybersecurity risks in IoT devices for smart homes

**Abstract.-** This work proposes strategies to mitigate emerging risks in smart Internet of Things (IoT) devices within homes. With the significant increase in these devices, cybersecurity became a primary concern. Therefore, this study focused on identifying potential risks and vulnerabilities, using surveys to assess current security practices and knowledge about protective measures among other aspects related to cybersecurity. Based on these results, recommendations were made for users, to strengthen security in their IoT devices and promote good practices to create a safer and more protected home environment against possible cyber threats.

**Keywords:** cybersecurity, internet of things, smart homes, strategies.

## I. INTRODUCCIÓN

En la actualidad el internet de las cosas (IoT) ha transformado la manera en la que interactuamos con nuestro entorno, siendo un hecho el incremento del uso de dispositivos conectados a internet en diversos campos, como hogares inteligentes, ciudades inteligentes e industrias. No obstante, la expansión de estos dispositivos también ha originado una serie de desafíos de ciberseguridad que requieren atención inmediata. La ciberseguridad en los dispositivos IoT se ha convertido en una preocupación crítica. Debido a su auge, están expuestos a una serie de amenazas que pueden comprometer tanto la privacidad como la seguridad de los usuarios [1]. Las vulnerabilidades en estos dispositivos pueden ser explotadas por atacantes para acceder a redes privadas, robar datos personales, incluso controlar dispositivos de manera remota [2].

El uso de IoT es cada vez más frecuente en los hogares, ya que pueden estar presentes desde un pequeño enchufe inteligente, hasta electrodomésticos conectados mediante internet [3]. Estos pueden ser blanco fácil de algún ciberataque, por lo cual, es crucial mantener la seguridad en este tipo de dispositivos utilizados en hogares inteligentes [4]. En este trabajo se analiza la falta de estrategias proactivas y efectivas para mitigar los riesgos emergentes asociados con la ciberseguridad en dispositivos IoT para hogares inteligentes. A pesar de los avances en tecnología y la creciente conciencia sobre la seguridad, los ataques a estos dispositivos siguen siendo comunes, lo que pone en evidencia la necesidad de enfoques más robustos y anticipados.

El presente trabajo se estructura de la siguiente manera: La sección 1, incluye la introducción, ofrece un contexto del estudio, y establece los objetivos de investigación, la sección 2 pertenece al desarrollo, donde se ofrece una revisión de la literatura, los riesgos y vulnerabilidades asociados. La sección 3 es la metodología, donde se detalla el enfoque y las técnicas utilizadas, principalmente para recolectar datos mediante encuestas, En los resultados se analizan los hallazgos obtenidos. Finalmente, la sección de conclusiones, resume los descubrimientos del estudio y ofrece recomendaciones para mitigar los riesgos.

## II. DESARROLLO

El Internet de las cosas (IoT), es una red de dispositivos interconectados a través de internet, que permite la comunicación entre los dispositivos y la nube. Estos se encuentran presentes en nuestro entorno, y van desde simples equipos inteligentes en los hogares, hasta aquellos utilizados en las grandes industrias [5]. En el contexto de hogares, el término “Smart Home” hace referencia a una casa equipada con tecnologías que permiten la automatización y control remoto de diversos aspectos en un entorno doméstico mediante un ordenador o smartphone, y una de sus características principales es que conectan a internet [6]. Existen varios dispositivos inteligentes para el hogar [7]. En la tabla 1 se muestran junto a sus características.

**Tabla 1.** Tipos de Dispositivos inteligentes para el hogar.

| DISPOSITIVOS | CARACTERÍSTICAS PRINCIPALES |
|---|---|
| Asistentes virtuales | - Interacción conversacional<br>- Automatización de tareas<br>- Capacidad de procesamiento de lenguaje natural reconocimiento de voz |
| Iluminación inteligente | - Control remoto<br>- Eficiencia energética<br>- Ajuste de intensidad de brillo y color |
| Termostatos inteligentes | - Automatización<br>- Ahorro energético<br>- Programación de horarios |
| Detectores y sensores | - Detección de movimiento<br>- Detección de humo<br>- Sensores de puertas y ventanas |
| Cámaras de seguridad inteligente | - Conectividad Wifi<br>- Detección de sonido y movimiento<br>- Resolución 4K / FULLHD / HD, visión nocturna, audio |
| Electrodomésticos inteligentes | - Control mediante apps<br>- Monitoreo y notificaciones<br>- Integración con asistentes virtuales, funciones especiales |
| Enchufes y regletas inteligentes | - Control de energía<br>- Programación remota, monitoreo de consumo energético<br>- Protección contra sobrecargas de voltaje |
| Wereables | - Monitoreo de salud, de estrés y actividad física<br>- Notificaciones en tiempo real y GPS integrado<br>- Pagos móviles |

La ciberseguridad es fundamental para la protección los sistemas informáticos, bases de datos, redes, de posibles ciberataques y accesos no autorizados con el fin de salvaguardar la información [8]. Dentro de este ámbito la seguridad de la información juega un papel importante, basándose en la confidencialidad, integridad y disponibilidad [9]. Sin embargo, estos principios mencionados, pueden verse amenazados por los diversos ciberataques existentes, ya que poseen técnicas para infiltrarse y afectar la seguridad de la información [10]. En la Tabla 2 se resumen los ciberataques más comunes, su impacto, sus objetivos y consecuencias.

**Tabla 2.** Tipos de Ataque.

| Tipos de Ataques | Impacto | Objetivo principal | Consecuencias |
|---|---|---|---|
| Ransomware | ALTO | Encriptar datos | - Bloquear acceso a los datos<br>- Pago por rescate |
| Phishing | ALTO | Obtener información confidencial | - Accesos no autorizados a cuentas financieras<br>- Robo de identidad |
| Inyección SQL | ALTO | Acceder a las bases de datos | - Acceso a datos sensibles<br>- Modificación o eliminación de datos. |
| Cross – Site – Scripting (XSS) | MEDIO | Inyectar Scripts en sitios web | - Suplantación de identidad<br>- Robo de cookies |
| Denegación de Servicio Distribuida (DDoS) | MEDIO | Sobrecargar servicios | - Interrupción de los servicios<br>- Daño a la reputación |
| Adware | BAJO | Mostrar publicidad no deseada | - Afectar el rendimiento del sistema<br>- Exposición a malware |

El panorama de ciberseguridad actual reveló la prevalencia de diversos tipos de ataques. El phishing es uno de los ataques más utilizados, representando el 36% de todos los ataques de ingeniería social, junto al Ransomware con alrededor del 24% de las amenazas dirigidas a industrias. Los ataques a sitios web, como la inyección SQL y XSS, comprenden un 25%. Por otra parte, la denegación de servicio distribuida DDoS comprenden aproximadamente el 5% de incidentes [11]. Por último, el malware (programa maligno) Adware, que afecta con un 35% de los dispositivos móviles [12].

El fortalecimiento de las medidas de seguridad de los dispositivos IoT en la actualidad, es importante debido a sus vulnerabilidades, y a su presencia en áreas muy importantes, cómo son las empresas, hogares, y la industria 4.0 [13]. En este contexto, Flores [14] propuso la creación de taxonomía experimental basada en código abierto para los sistemas de detección y prevención de intrusos (IDS/IPS) para identificar vulnerabilidades, optimizar su rendimiento y adaptar soluciones a las amenazas emergentes. Los riesgos asociados a la privacidad que tienen los dispositivos IoT, demuestran que las principales vulnerabilidades incluyen, autenticaciones débiles, acceso a los datos sin seguridad, y redes Wi-Fi inseguras [15], de ahí se destaca la importancia de implementar tecnologías avanzadas, para mejorar la seguridad la seguridad de los dispositivos en los hogares inteligentes [16]. Tapia [17] utilizando encuestas analizó la relación entre las habilidades y el uso de dispositivos IoT en los hogares, dicho análisis fue relevante para comprender el nivel de familiaridad de las personas con la adopción de estas tecnologías. Según Calle [18] en su estudio, realizó un análisis de vulnerabilidades a cámaras IP domésticas, demostrando que a pesar de que los fabricantes utilizan configuraciones predeterminadas de seguridad, existen debilidades asociadas con la configuración del usuario, esto evidencia la necesidad de fortalecer los conocimientos en ciberseguridad.

## III. METODOLOGÍA

Para abordar el tema de estrategias proactivas para mitigar los riesgos emergentes de ciberseguridad en dispositivos IoT para hogares inteligentes, se utilizó una metodología cuantitativa. El método de recolección de información consistió en encuestas dirigidas a un público conformado por profesionales del área de tecnología y ciberseguridad, estudiantes universitarios y usuarios que utilizan dispositivos IoT en sus hogares. Para el presente estudio, se ha considerado información proporcionada por el Instituto Nacional de Estadísticas y Censos (INEC) en su último censo realizado en el año 2022, acerca del número de hogares que poseen conexión a internet en la provincia de Santa Elena - Ecuador, obteniendo un total de 52.219 hogares conectados, distribuidos en tres cantones. Santa Elena cuenta con 22.665 hogares, La Libertad con 16.871 hogares, y Salinas con 12.683 hogares. La ecuación (1) se utilizó para el cálculo de la muestra:

$$n = \frac{N*Z^2*p*q}{e^2*(N-1)+Z^2*p*q} \qquad (1)$$

Los tamaños calculados corresponden a la muestra del número de encuestados por cantón, obteniendo un total de 202 encuestas. Las mismas que abordaron temas relevantes referentes a la ciberseguridad en los dispositivos IoT. La distribución de la encuesta se realizó en el Cantón de Santa Elena con 74 encuestas, Cantón La Libertad 51 encuestas, Cantón de Salinas 77 encuestas. La encuesta fue validada por expertos y estuvo compuesta por los criterios descritos en la tabla 3. Se observa que los criterios incluyen datos demográficos y el uso de aplicativos tecnológicos, así como el conocimiento en el uso de estos dispositivos. Todos estos con el fin de ubicar y contextualizar el problema de estudio y poder definir futuras estrategias de mejora.

**Tabla 3.** Características de la encuesta aplicada.

| Objetivo según criterio | Aporte al tema de investigación | Categoría de evaluación |
|---|---|---|
| Conocer la ubicación geográfica de los encuestados. | Proporciona contexto sobre la distribución geográfica de los participantes. | Información demográfica |
| Determinar la distribución de edades de los participantes. | Ayuda a segmentar la muestra según rangos de edad y evaluar si la edad influye en la seguridad IoT. | Información demográfica |
| Identificar los dispositivos IoT presentes en los hogares. | Permite comprender el nivel de adopción de dispositivos IoT y su diversidad en los hogares. | Adopción de tecnología IoT |
| Medir la experiencia de uso de dispositivos IoT. | Ofrece datos sobre la experiencia de los usuarios con dispositivos IoT. | Experiencia de uso |
| Conocer el proveedor de servicios de internet. | Brinda información sobre la infraestructura de red que los participantes utilizan. | Infraestructura de red |
| Evaluar la frecuencia de actualización del software en dispositivos IoT. | Permite evaluar las prácticas de mantenimiento y seguridad en los dispositivos IoT. | Mantenimiento de dispositivos |
| Identificar las medidas de seguridad aplicadas en el uso de dispositivos IoT. | Contribuye a identificar las estrategias de seguridad más comunes. | Medidas de seguridad |
| Medir el nivel de conocimiento de las mejores prácticas de seguridad. | Proporciona un panorama del nivel de conocimiento de los usuarios sobre seguridad IoT. | Conocimiento en ciberseguridad |
| Determinar la percepción de preocupación por la seguridad en IoT. | Mide la conciencia y percepción de riesgo relacionada con la seguridad IoT. | Percepción de seguridad |
| Identificar los riesgos percibidos en los dispositivos IoT. | Ayuda a entender las amenazas que los usuarios consideran más importantes en IoT. | Riesgos percibidos |
| Conocer las fuentes de información utilizadas para temas de seguridad IoT. | Aporta información sobre la búsqueda de recursos educativos en temas de seguridad IoT. | Fuentes de información |
| Determinar la incidencia de problemas de seguridad o ciberataques. | Proporciona evidencia sobre la frecuencia de ciberataques en dispositivos IoT domésticos. | Incidentes de seguridad |
| Identificar los recursos que los usuarios consideran necesarios para mejorar la seguridad IoT. | Ayuda a identificar necesidades de recursos educativos o soporte técnico en seguridad IoT. | Recursos necesarios |
| Conocer las prácticas de protección de red para asegurar dispositivos inteligentes. | Ofrece datos sobre las prácticas de seguridad de la red doméstica. | Medidas de protección de red |

## IV. RESULTADOS

A. Hallazgos encontrados en la aplicación de encuestas

En la Fig. 1, se muestran las medidas de seguridad que los encuestados aplican a sus dispositivos IoT en el hogar, siendo la práctica más utilizada el cambio de contraseñas predeterminadas, entre otras medidas que también son relevantes Esto indica una buena implementación de seguridad básica, sin embargo, es necesario fomentar el uso de prácticas de seguridad más avanzadas para la protección de los dispositivos IoT.

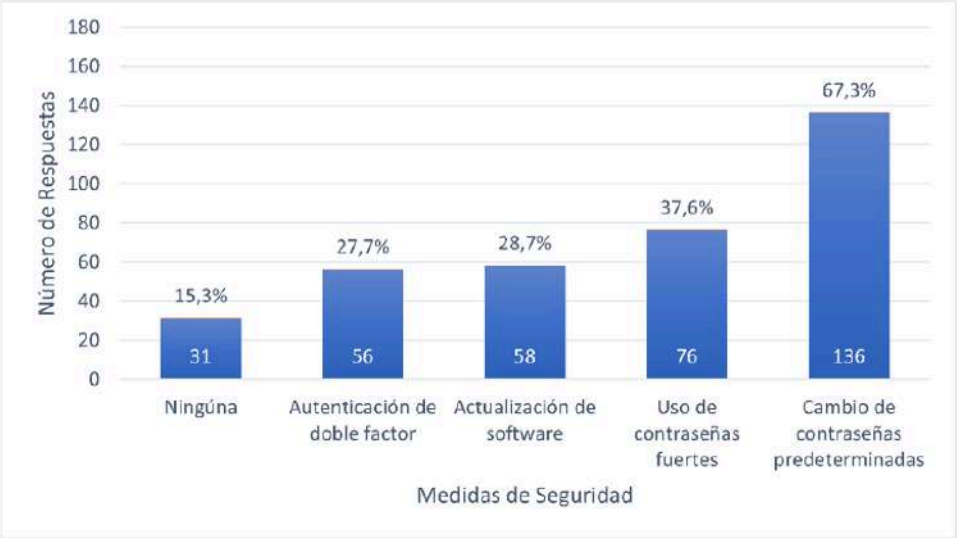


**Fig 1.** Medidas de seguridad aplicadas en dispositivos inteligentes IoT en los hogares.

Por otra parte, se consultó acerca del nivel de preocupación de los riesgos de seguridad en los dispositivos inteligentes IoT. Los resultados mostrados en la Fig. 2 reflejan que los usuarios tienen una alta percepción de los riesgos, lo que podría incentivar la adopción de nuevas prácticas de seguridad.

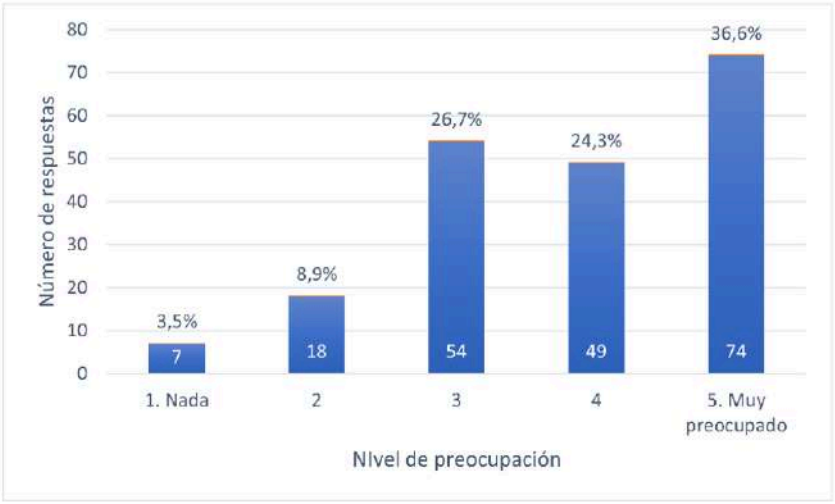


**Fig 2.** Nivel de preocupación de los riesgos de seguridad en los dispositivos inteligentes IoT en los hogares.

Y como último punto, los resultados de la Fig. 3 reflejan una combinación de enfoques básicos de seguridad en redes Wi-Fi, con una alta adopción de prácticas como el cambio de contraseña regular, y el uso de cifrado WPA2/WPA3, no obstante, se sugiere un refuerzo adicional acerca de prácticas de seguridad más robustas para una mejor protección de las redes inalámbricas Wi-Fi, ya que estas redes son el medio por el cual los dispositivos IoT comparten información.

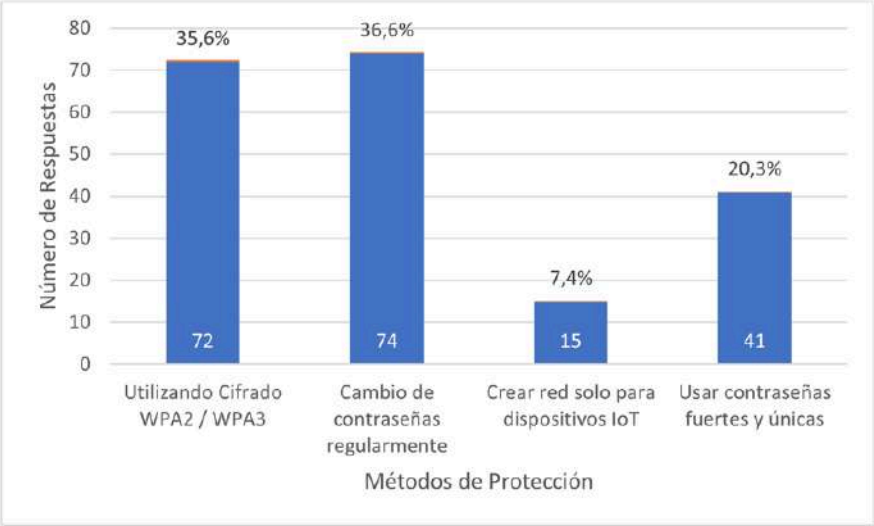


**Fig 3.** Medidas de protección para mantener la seguridad en los dispositivos inteligentes IoT en los hogares.

B. Propuestas para fortalecer la protección digital en el hogar

Estos resultados permiten proponen ciertas estrategias guía para fortalecer la seguridad en dispositivos IoT en los hogares, y proteger a los usuarios contra posibles amenazas cibernéticas (Fig. 4). Además, permitirán mitigar los riesgos de los dispositivos IoT en hogares distribuidas por grupo.


**Fig 4.** Medidas fundamentales de seguridad.

En la figura 4 se muestran algunas características que se deben considerar para mejorar la protección cibernética en el hogar, entre ellas se pueden mencionar las siguientes:

- Utilizar contraseñas seguras: Se recomienda emplear contraseñas complejas que combinen caracteres especiales, letras y números tanto en la red Wi-Fi como en los dispositivos, reduciendo así el riesgo de accesos indebidos.

- Cambiar contraseñas predeterminadas: Las contraseñas que vienen de fábrica suelen ser fáciles de descifrar por los atacantes, por lo que es fundamental modificarlas cuanto antes.
- Actualizar constantemente el software: Mantener el software de los dispositivos al día garantiza que se cuente con los últimos parches de seguridad, lo que ayuda a protegerlos de vulnerabilidades. Es importante asegurarse de que las actualizaciones provengan del proveedor oficial del dispositivo o del sistema.
- Desactivar funciones no utilizadas: Deshabilitar las características innecesarias en los dispositivos reduce la superficie de ataque, disminuyendo así las posibilidades de un ciberataque.

Este conjunto de medidas forma un pilar esencial para mantener la seguridad digital en entornos personales y profesionales. Sin embargo, otro factor importante que muchas veces se pasa por alto en los hogares es la protección de redes wifi (fig. 5), donde se pueden aplicar las siguientes acciones:

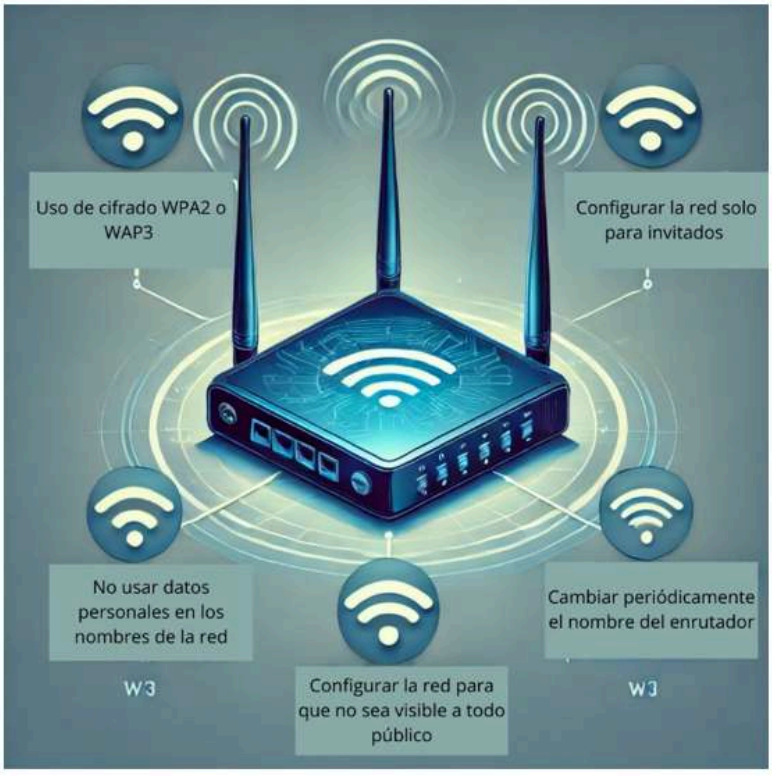


**Fig 5.** Acciones para la protección en redes wifi.

Como se puede apreciar en la figura 5, una de las acciones que contribuyen al mejoramiento de la seguridad en las redes wifi es el uso de cifrado WPA2 o WAP3 que sirven para proteger la red Wi-Fi y la información que se transmite por ella. Además, es importante configurar la red solo para invitados, esta configuración desde el enrutador minimizaría el riesgo de ataques por malware, o de accesos no autorizados a dispositivos. Así como cambiar periódicamente el nombre del enrutador, para dificultar la identificación de la red, en este caso es recomendable cambiarlo sin develar algún dato personal. Otros factores de seguridad en el hogar incluyen estrategias avanzadas de seguridad, como implementar autenticación multifactor (MFA) para adicionar una capa de seguridad extra, pidiendo múltiples formas de verificación previas para acceder a dispositivos o cuentas. Así mismo, es importante la educación y capacitación en ciberseguridad, como también adquirir conocimientos continuos acerca de ciberseguridad para mantenerse informados y conocer las mejores prácticas para prevenir y actuar ante amenazas emergentes. Sin descuidar el monitoreo y la utilización de herramientas para identificar y actuar rápidamente ante cualquier actividad sospechosa.

## CONCLUSIONES

A medida que más hogares utilicen dispositivos digitales, más son las probabilidades de tener riesgos de seguridad. Por lo tanto, resulta necesario promover la concientización y la educación en el ámbito de ciberseguridad, de tal manera que puedan implementarse buenas prácticas de seguridad, evitando ser víctimas de algún tipo de ciberataque.

Las sociedades modernas son cada vez más propensas a sufrir situaciones digitales, y por ello, la capacitación y preparación en estos temas, ya no es algo exclusivo de los ingenieros informáticas y áreas afines, sino que es una necesidad en todos los sectores de la población, donde el uso de la tecnología se ha hecho parte de los hogares y de la vida común.

A medida que crece el uso de dispositivos digitales en los hogares, también aumenta la cantidad de información personal y financiera que se transmite a través de redes, lo que eleva las probabilidades de ataques cibernéticos. Desde dispositivos inteligentes conectados a internet hasta la simple conexión de una computadora portátil, cada punto de acceso a una red representa una posible vulnerabilidad. Por esta razón, es vital que las personas comprendan los riesgos asociados y adopten medidas preventivas, como el uso de contraseñas seguras y el cifrado adecuado, para proteger sus redes y dispositivos.

Además de implementar buenas prácticas de seguridad, es crucial que las familias y los individuos mantengan una actitud proactiva respecto a la educación en ciberseguridad. La protección de datos personales y el resguardo de la privacidad en línea son aspectos que deben aprenderse desde edades tempranas, para así formar una cultura de seguridad digital sólida. Programas de formación en este ámbito pueden ayudar a que las personas identifiquen amenazas comunes, como correos de phishing o software malicioso, y sepan cómo actuar frente a ellas.

En una era donde la digitalización está presente en casi todos los aspectos de la vida cotidiana, la seguridad en línea se ha vuelto una responsabilidad compartida. No solo es deber de los expertos en tecnología proteger sistemas y redes, sino que cada usuario, independientemente de su campo profesional, debe ser consciente de los peligros que existen en el ciberespacio y tomar medidas activas para minimizarlos. La ciberseguridad es un desafío global, y cuanto más se expanda el conocimiento y la implementación de buenas prácticas, mejor preparados estaremos para enfrentar futuras amenazas.

## REFERENCIAS

[1] J. S. Rueda Rueda, “El reto del desarrollo seguro de aplicaciones IoT en un mercado acelerado”, Revista Ingenio, vol. 18, núm. 1, 2021, doi: 10.22463/2011642x.2667.
[2] D. Cárdenas-Quintero, E. Ropero-Silva, K. Puerto-López, K. Sanchez-Mojica, S. Castro-Casadiego, y J. Ramirez-Mateus, “Vulnerabilidad en la seguridad del internet de las cosas”, Mundo FESC, vol. 10, núm. 19, pp. 162–179, ene. 2020, doi: 10.61799/2216-0388.542.
[3] J. E. Mendoza Padilla y M. A. Marín Mendoza, “Prototipo de Smart Home automatizado con IoT”, Investigación e Innovación en Ingenierías, vol. 8, núm. 2, 2020, doi: 10.17081/invinno.8.2.3771.
[4] A. C. Morales Suárez, S. S. Díaz Ávila, y M. Á. Leguizamón Páez, “Mecanismos de seguridad en el internet de las cosas”, Revista vínculos, vol. 16, núm. 2, 2019, doi: 10.14483/2322939x.15758.
[5] L. M. Amaya Fariño, A. Tumbaco Reyes, E. Roca Quirumbay, T. Villón González, B. Mendoza Morán, y Á. Reyes Quimís, “El IoT aplicado a la Domótica”, Revista Científica y Tecnológica UPSE, vol. 7, núm. 1, pp. 21–28, jun. 2020, doi: 10.26423/rctu.v7i1.490.
[6] D. S. Ramirez Supe, E. de las M. Zurita Meza, y F. J. Galora Silva, “Analizando Internet de las Cosas y la nube informática”, REVISTA ODIGOS, vol. 3, núm. 1, 2022, doi: 10.35290/ro.v3n1.2022.535.

[7] T. A. Coleti, O. A. Mahmoud, V. H. Sotti, A. L. A. Menolli, M. Morandini, y R. Balancieri, "Equipamentos para Smart Home: O que eles querem saber sobre nós?", 2023. doi: 10.5753/wics.2023.230083.
[8] F. S. Capeta Mondoñedo, C. M. Franco Del Carpio, y H. O. Villafuerte Barreto, "Ciberseguridad y su relación con la empleabilidad para egresados de Ingeniería de Sistemas en una Universidad Pública", Revista de Climatología, vol. 23, 2023, doi: 10.59427/rcli/2023/v23cs.1510-1519.
[9] G. R. De La Cruz Rodríguez, R. A. Méndez Fernández, y A. C. Mendoza De Los Santos, "Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática", Innovación y Software, vol. 4, núm. 1, 2023, doi: 10.48168/innosoft.s11.a79.
[10] "¿Qué es un ciberataque y los tipos de ataques en la red? | Fortinet". Consultado: el 11 de agosto de 2024. [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks.
[11] Verizon, "Verizon DBIR 2023 Data Breach Investigations Report", Consultado: el 31 de agosto de 2024. [En línea]. Disponible en: https://www.verizon.com/about/news/2023-data-breach-investigations-report.
[12] "Cuáles son las vulnerabilidades más relevantes detectadas en 2023". Consultado: el 31 de agosto de 2024. [En línea]. Disponible en: https://www.welivesecurity.com/es/seguridad-corporativa/vulnerabilidades-mas-relevantes-2023/
[13] L. F. Gélvez-Rodríguez y L. M. Santos-Jaimes, "Internet de las Cosas: una revisión sobre los retos de seguridad y sus contramedidas", Revista Ingenio, vol. 17, núm. 1, 2020, doi: 10.22463/2011642x.2370.
[14] J. C. Gómez Castaño, N. J. Castaño Pérez, y L. C. Correa Ortiz, "Sistemas de detección y prevención de intrusos", Ciencia e Ingeniería Neogranadina, vol. 33, núm. 1, 2023, doi: 10.18359/rcin.6534.
[15] A. Flórez Gutiérrez, A. Paola Gordillo, y L. A. Roa H, "Vulnerabilidad de la información en los dispositivos domésticos inteligentes del hogar", Elementos, ISSN-e 2248-5252, Vol. 7, No. 1, 2022, vol. 7, núm. 1, p. 8, 2022, doi: 10.15765/E.V7I1.
[16] D. Ordoñez-Camacho, "Reduciendo la brecha de seguridad del IoT con una arquitectura de microservicios basada en TLS y OAuth2", Ingenius, núm. 25, 2020, doi: 10.17163/ings.n25.2021.09.
[17] A. Calvopiña, F. Tapia, y L. Tello-Oquendo, "Uso del asistente virtual Alexa como herramienta de interacción para el monitoreo de clima en hogares inteligentes por medio de Raspberry Pi y DarkSky API", 2020, doi: 10.17013/risti.36.102-115.
[18] J. F. Calle Sarmiento y J. P. Cuenca Tapia, "Plan de mitigación de riesgos ante vulnerabilidades y amenazas presentes en un dispositivo IoT", ConcienciaDigital, vol. 6, núm. 4.2, 2023, doi: 10.33262/concienciadigital.v6i4.2.2773.

## LOS AUTORES

**Kevin García Pérez** es Ingeniero en Tecnologías de la Información, graduado en la Universidad Estatal Península de Santa Elena y actualmente estudiante de la Maestría de Ciberseguridad en la misma institución.

**Oscar Apolinario Arzube** es un científico con doctorado en Informática y amplia experiencia en telecomunicaciones. Especializado en ontología, web semántica y machine learning, ha publicado en revistas de alto impacto y ha liderado proyectos ágiles. Posee habilidades en programación y bases de datos.