SpyderX: Plataforma Hexápoda para Ciberseguridad Ofensiva y Robótica Autónoma

Aitor Valero
Christian Gutierrez

Engidea
Laura Pantaleon

Fecha de entrega — Septiembre 2025

Tabla De Contenido

Resumen **2**
Introduccion **3**
CAPÍTULO I **5**
PLANTEAMIENTO DEL PROBLEMA 5
I.1 Planteamiento del problema 5
I.2 Objetivos de la investigacion 6
I.2.1 Objetivo general 6
I.2.2 Objetivos específicos 6
I.3 Justificación de la investigación 7
CAPITULO II **8**
MARCO TEORICO 8
II.1 Antecedentes de la investigación 8
II.2 Base teorica 8
II.3 Bases legales 9
II.4 Definición de Términos 9
Capítulo III **10**
Marco Metodológico 10
III.1 Tipo de investigación
La presente investigación es de tipo proyectiva con un enfoque cuantitativo y aplicado, ya que busca desarrollar un prototipo funcional a partir de una problemática concreta en el área de ciberseguridad. Este tipo de estudio permite generar soluciones tecnológicas tangibles a necesidades reales, vinculadas a la auditoría de redes inalámbricas. 10

Resumen

Este informe presenta el desarrollo de SpyderX, un robot hexápodo autónomo diseñado para auditorías de ciberseguridad con enfoque Gray Hat. Su propósito es identificar vulnerabilidades en redes WiFi institucionales, especialmente en organizaciones venezolanas con recursos limitados. SpyderX simula accesos internos controlados para diagnosticar debilidades antes de que actores maliciosos las exploten.

El proyecto se estructuró bajo la metodología Design Thinking, abarcando desde la empatía con los usuarios hasta la validación funcional del prototipo. Se identificaron riesgos comunes en redes institucionales: configuraciones inseguras, dispositivos no autorizados y falta de monitoreo. Frente a este panorama, SpyderX se propone como una solución autónoma, móvil y replicable.

A nivel estructural, el robot fue modelado en SolidWorks, empleando el kit educativo Freenove Hexapod Robot for Raspberry Pi como base para su construcción. Esta elección garantiza accesibilidad, movilidad en terrenos irregulares y facilidad de implementación. El sistema funciona con Raspberry Pi OS, sensores de navegación, módulos WiFi de alta potencia y drivers de motores paso a paso.

El robot es controlado mediante una app móvil desarrollada en MIT App Inventor, que permite moverlo y ejecutar escaneos de red. A nivel de software, se utiliza Nmap como herramienta principal para el mapeo de red, detección de dispositivos, puertos abiertos y servicios vulnerables. Los resultados se interpretan y presentan en la app, permitiendo a los usuarios tomar decisiones informadas.El proyecto se apoya en investigaciones sobre ciberseguridad ética y defensa digital, y contribuye al cumplimiento del ODS 16, fortaleciendo la protección tecnológica institucional.

Introduccion

En el contexto actual de transformación digital, muchas organizaciones venezolanas educativas, institucionales y comunitarias enfrentan crecientes riesgos derivados del uso de redes WiFi con configuraciones inseguras, escasa supervisión técnica y desconocimiento sobre amenazas digitales internas. Estos entornos, que no siempre cuentan con soluciones de ciberseguridad robustas, resultan especialmente vulnerables a accesos no autorizados, exposición de información sensible y propagación de amenazas que comprometen la operatividad de los sistemas.

Frente a esta problemática, surge SpyderX, un robot autónomo orientado a la auditoría de redes inalámbricas bajo el enfoque de la ciberseguridad ofensiva ética (Gray Hat). A través de escaneos autorizados y simulación de accesos internos controlados, el sistema busca identificar vulnerabilidades antes de que puedan ser explotadas por actores maliciosos. Su diseño se fundamenta en la automatización de tareas de diagnóstico digital, proporcionando una solución replicable, económica y formativa.

El desarrollo de SpyderX se basó en la metodología Design Thinking, permitiendo abordar el problema desde la experiencia del usuario final. Esto condujo a un prototipo que combina hardware de bajo costo con navegación autónoma, sensores integrados y un sistema operativo ligero basado en Raspberry Pi OS, que coordina tanto el movimiento del robot como los procesos de escaneo de red. Para garantizar accesibilidad y adaptabilidad, el sistema fue construido utilizando el kit robótico Freenove Hexapod para Raspberry Pi, lo que permitió acelerar el desarrollo estructural y asegurar estabilidad mecánica en terrenos irregulares.

Todo el sistema puede ser gestionado desde una aplicación móvil diseñada en MIT App Inventor, brindando control y visualización en tiempo real. A nivel funcional, SpyderX emplea exclusivamente la herramienta Nmap para realizar auditorías de red, explorando dispositivos conectados, puertos abiertos y configuraciones inseguras. Esta información es procesada localmente y utilizada para generar alertas y recomendaciones simples para los usuarios, incluso sin formación técnica previa.

El proyecto, además de contribuir a la alfabetización digital en ciberseguridad, se alinea con los objetivos del ODS 16 (Paz, justicia e instituciones sólidas), al fortalecer las capacidades institucionales de defensa tecnológica mediante el uso responsable e innovador de tecnologías emergentes.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

I.1 Planteamiento del problema

Actualmente en el mundo, el desarrollo tecnológico ha potenciado exponencialmente la digitalización de procesos organizacionales, lo cual ha traído consigo un incremento notable en los riesgos asociados a la seguridad de la información. A nivel global, las organizaciones enfrentan amenazas constantes que comprometen la integridad de sus redes y la confidencialidad de sus datos.

En Latinoamérica, esta realidad se acentúa por la falta de infraestructura tecnológica adecuada y personal capacitado. En Venezuela, la situación es aún más crítica, ya que muchas organizaciones, instituciones educativas y entidades públicas no cuentan con recursos suficientes ni herramientas apropiadas para realizar auditorías de seguridad en sus redes inalámbricas, que son frecuentemente el punto de entrada de ataques cibernéticos.

De forma más específica, en el estado La Guaira, se ha identificado que diversas instituciones educativas, empresas locales y organizaciones sociales presentan configuraciones débiles en sus redes WiFi, lo que las hace vulnerables a técnicas de intrusión como el Man-in-the-Middle (MitM), creación de redes gemelas (Evil Twin) y escaneo de dispositivos conectados sin autorización. Estas fallas pueden generar filtraciones de información confidencial, pérdida de datos e interrupciones en sus operaciones.

Esta problemática exige una respuesta innovadora, accesible y eficiente, que permita a las instituciones realizar auditorías de seguridad sin depender de expertos costosos o infraestructura compleja. En este contexto, surge la propuesta de desarrollo del robot SpyderX: una solución tecnológica autónoma, con enfoque ético, diseñada para detectar vulnerabilidades en redes WiFi desde una perspectiva físico-digital. Su estructura está basada en el kit educativo Freenove Hexapod Robot for Raspberry Pi, lo que garantiza una implementación accesible, replicable y adaptada a entornos reales de aprendizaje y evaluación.

I.2 OBJETIVOS DE LA INVESTIGACIÓN

I.2.1 Objetivo general

Diseñar e implementar un robot hexápodo autónomo capaz de ejecutar auditorías de ciberseguridad en redes WiFi

I.2.2 Objetivos específicos

- Diagnosticar las principales vulnerabilidades presentes en redes WiFi institucionales.
- Diseñar el modelo físico del robot en SolidWorks, considerando movilidad y funcionalidad.
- Integrar los componentes electrónicos necesarios (Raspberry Pi, sensores, módulos WiFi).
- Desarrollar una aplicación móvil en MIT App Inventor para controlar el robot y gestionar las pruebas.
- Validar el prototipo en entornos simulados con redes autorizadas.

I.3 Justificación de la investigación

La investigación se justifica por la creciente necesidad de proteger la infraestructura digital de las organizaciones en Venezuela frente a amenazas internas y externas. El uso de redes inalámbricas se ha masificado, pero la conciencia sobre sus riesgos sigue siendo baja. SpyderX no solo busca detectar vulnerabilidades técnicas, sino también fomentar una cultura de prevención en entornos institucionales.

Este proyecto es relevante por múltiples razones: aborda un problema real, propone una solución tecnológica educativa, accesible y escalable, y promueve el uso ético de herramientas de ciberseguridad. Para facilitar su desarrollo, se utilizó el kit robótico Freenove Hexapod para Raspberry Pi, el cual ofrece una base mecánica estable, económica y versátil, permitiendo concentrarse en la integración funcional del sistema.

Beneficia directamente a instituciones educativas, empresas pequeñas y medianas, y organizaciones públicas que no tienen acceso a servicios de auditoría tradicionales. Además, tiene valor social y científico, ya que genera conocimiento técnico aplicable y fomenta buenas prácticas digitales.

I.4 Delimitación

La investigación se delimita al desarrollo de un prototipo funcional orientado a redes WiFi de instituciones ubicadas en el estado La Guaira. Las pruebas se realizarán en entornos controlados con redes autorizadas. No se contemplan aplicaciones en redes públicas, ni se validarán funcionalidades en ambientes industriales. Tampoco se incluirán pruebas sobre redes cableadas o ataques fuera del marco ético.

I.5 Limitaciones

- Recursos económicos restringidos para la adquisición de componentes de última generación.
- Limitación en el acceso a redes reales por motivos legales y éticos.
- Tiempo limitado para realizar pruebas extensivas en múltiples escenarios.
- Necesidad de permisos institucionales para cada ensayo controlado.

Estas limitaciones no impiden el logro de los objetivos, pero condicionan el alcance del desarrollo, restringiendo su aplicación inicial a entornos simulados y de laboratorio. A pesar

de ello, se espera que los resultados obtenidos sirvan de base para futuras versiones mejoradas del sistema SpyderX.

CAPITULO II

MARCO TEORICO

II.1 Antecedentes de la investigación

A lo largo de los últimos años, diversas investigaciones han abordado la necesidad de fortalecer los sistemas de seguridad digital, en particular en redes inalámbricas. En países como Estados Unidos, Alemania y Corea del Sur se han desarrollado robots móviles orientados al patrullaje cibernético, generalmente con fines militares o industriales. Sin embargo, estas soluciones presentan altos costos de producción, infraestructura y operación, lo que limita su implementación en entornos institucionales básicos o educativos.

En América Latina, los avances en robótica aplicada a la ciberseguridad son escasos y, en su mayoría, impulsados por iniciativas académicas. Por ejemplo, el proyecto CyberDog Recon (Rogue Robotics, 2021) consistió en un robot de patrullaje autónomo para auditorías de red, diseñado para entornos de alta complejidad. Sin embargo, su alto nivel técnico y dependencia de múltiples suites de software avanzadas lo alejan de contextos de bajo presupuesto o con poca formación técnica.

En Venezuela, iniciativas como el proyecto RedSegura (UCV, 2019) analizaron vulnerabilidades en redes públicas, principalmente desde entornos de laboratorio, sin desarrollar aplicaciones físicas ni móviles. Por su parte, instituciones como la Fundación Infocentro y programas como Semilleros Científicos (MINCYT, 2023) han promovido la robótica educativa, enfocándose en prototipos de bajo costo para formación técnica, pero sin abordar específicamente la seguridad digital.

En este contexto, SpyderX representa una propuesta innovadora al combinar robótica móvil con auditoría digital utilizando únicamente la herramienta Nmap, reconocida por su capacidad de escaneo de redes, detección de dispositivos activos y análisis de servicios vulnerables. A diferencia de otras suites más complejas o pesadas, Nmap ofrece un equilibrio ideal entre funcionalidad, portabilidad y consumo de recursos, permitiendo su integración efectiva en entornos limitados y con sistemas ligeros como Raspberry Pi OS.

II.2 Base teorica

Ciberseguridad ofensiva y Gray Hat

La ciberseguridad ofensiva se refiere al conjunto de prácticas que simulan ataques controlados con el fin de identificar vulnerabilidades antes de que sean explotadas por agentes maliciosos. Dentro de esta práctica, el enfoque Gray Hat describe a aquellos actores que, sin intención de causar daño, acceden a sistemas para demostrar sus fallas y promover su corrección (Stallings, 2021). En contextos institucionales, esta metodología se aplica bajo autorización y control, como una forma de auditoría técnica preventiva.

Redes inalámbricas vulnerables

Las redes WiFi institucionales son especialmente propensas a errores de configuración, contraseñas débiles, falta de segmentación o monitoreo, y exposición de servicios innecesarios. Estas fallas pueden ser aprovechadas por atacantes para interceptar comunicaciones, acceder a sistemas internos o plantar dispositivos no autorizados. De acuerdo con Kaspersky (2023), más del 35% de los accesos no autorizados a redes se originan desde dentro de la misma organización.

Nmap como herramienta de diagnóstico de red

Nmap (Network Mapper) es una herramienta de código abierto ampliamente utilizada para exploración de redes y auditoría de seguridad. Permite descubrir dispositivos conectados, puertos abiertos, servicios activos y posibles vulnerabilidades, todo a través de escaneos configurables. Su bajo consumo de recursos y versatilidad lo convierten en una opción ideal para ser ejecutada en sistemas embebidos como Raspberry Pi (Nmap Project, 2023). En el contexto de SpyderX, Nmap se integra como el núcleo funcional del análisis de red, proporcionando datos críticos para la evaluación de seguridad.

Raspberry Pi OS como sistema base

Raspberry Pi OS es un sistema operativo basado en Debian optimizado para las placas Raspberry Pi. Ofrece un entorno ligero y adaptable, con compatibilidad para herramientas de red, lenguajes de programación y librerías para control de hardware. Al emplearlo en SpyderX, se garantiza una interfaz robusta para ejecutar tareas automatizadas de auditoría, controlar periféricos de navegación y comunicarse con la aplicación móvil desarrollada para el usuario.

Aplicaciones móviles como interfaz de control

El uso de MIT App Inventor para la creación de la aplicación de control de SpyderX permite una interfaz amigable y accesible. A través de la app, el usuario puede ejecutar escaneos de red, visualizar resultados en tiempo real, monitorear el estado del robot y controlar su movimiento. Este enfoque promueve la autonomía operativa, incluso para usuarios sin experiencia técnica avanzada.

.

II.3 Bases legales

El desarrollo e implementación del proyecto SpyderX se encuentra enmarcado dentro de las normativas nacionales e internacionales que regulan el uso responsable de la tecnología, el tratamiento de datos digitales y la promoción de una cultura de seguridad informática.

En primer lugar, la Ley Especial contra los Delitos Informáticos (Gaceta Oficial N.º 37.313, 30 de octubre de 2001), establece los lineamientos para prevenir y sancionar los delitos informáticos en Venezuela. Esta ley reconoce como delito el acceso no autorizado a sistemas informáticos, sin embargo, en su artículo 6 permite el acceso justificado con fines de auditoría técnica previa autorización del administrador o propietario del sistema. En este sentido, SpyderX actúa únicamente en redes previamente autorizadas, cumpliendo con este marco legal.

Asimismo, la Ley Orgánica de Ciencia, Tecnología e Innovación (LOCTI) promueve el desarrollo de tecnologías orientadas al fortalecimiento de capacidades nacionales en ciencia, innovación y educación técnica. Este proyecto se vincula con sus artículos 3 y 13, al proponer una solución tecnológica con impacto educativo y de seguridad digital para instituciones públicas.

Desde una perspectiva internacional, el Objetivo de Desarrollo Sostenible N.º 16 (ODS 16), impulsado por las Naciones Unidas, destaca la importancia de promover instituciones sólidas, responsables y transparentes. La auditoría digital de redes con herramientas como SpyderX fortalece la ciberdefensa institucional, previniendo posibles vulneraciones que afecten la integridad de los servicios públicos y comunitarios.

Además, el uso del sistema operativo Raspberry Pi OS y herramientas como Nmap, de código abierto, se alinea con la filosofía del acceso libre a la tecnología con fines educativos y de seguridad, promovida por movimientos internacionales como Creative Commons y la Free Software Foundation.

Por último, el desarrollo del proyecto también se enmarca en los principios éticos del enfoque Gray Hat, donde la detección de vulnerabilidades se realiza con fines preventivos y pedagógicos, sin causar daños, ni alterar servicios, respetando así los principios de la ética profesional y el consentimiento informado.

II.4 Definición de Términos

- **Ciberseguridad**
  Conjunto de técnicas, procedimientos y herramientas destinados a proteger los sistemas informáticos, las redes y los datos frente a accesos no autorizados, daños o ataques. La ciberseguridad busca garantizar la confidencialidad, integridad y disponibilidad de la información.

- **Gray Hat**
  Término que describe a los especialistas en ciberseguridad que, sin intenciones maliciosas, acceden a sistemas para demostrar vulnerabilidades. A diferencia de los hackers éticos (White Hat), pueden realizar pruebas sin autorización previa, pero luego informan sus hallazgos de forma responsable.

- **Red WiFi**
  Red inalámbrica que permite la conexión de dispositivos a Internet o entre sí mediante señales de radio. Su configuración, seguridad y monitoreo deficiente puede convertirla en una puerta de entrada para amenazas internas o externas.

- **Nmap**
  Herramienta de software libre utilizada para escaneo de redes, detección de dispositivos, servicios activos, puertos abiertos y evaluación básica de seguridad. Es ampliamente utilizada por profesionales de redes y auditores técnicos por su capacidad de personalización y eficiencia.

- **Raspberry Pi OS**
  Sistema operativo basado en Debian, diseñado para computadoras de placa reducida

como Raspberry Pi. Es ligero, estable y compatible con múltiples herramientas de programación, redes, automatización y control de hardware.

- **Auditoría de red**
  Proceso de evaluación técnica que permite analizar el estado de una red informática, detectar vulnerabilidades, identificar dispositivos conectados y revisar configuraciones. Puede realizarse de forma manual o automatizada.

- **Escaneo de puertos**
  Técnica utilizada para determinar qué puertos están abiertos en un dispositivo de red. Es fundamental en el diagnóstico de seguridad, ya que muchos servicios vulnerables se comunican por puertos específicos.

- **MIT App Inventor**
  Plataforma de desarrollo visual que permite crear aplicaciones móviles para Android mediante bloques de programación. Es ideal para prototipado rápido y sistemas de control como el usado en el proyecto SpyderX.

- **Prototipo**
  Primera versión funcional de un sistema, producto o dispositivo, utilizado para probar, evaluar y validar su diseño. En ingeniería, los prototipos permiten iterar soluciones antes de su implementación final.

- **Objetivo de Desarrollo Sostenible 16 (ODS 16)**
  Meta global promovida por las Naciones Unidas que busca fortalecer las instituciones públicas, promover la paz, la justicia y mejorar la transparencia y responsabilidad en el ejercicio del poder.

- **Freenove Hexapod Robot Kit**
  Kit robótico de bajo costo diseñado para sistemas embebidos como Raspberry Pi. Incluye una estructura hexápoda, motores servo, y sensores, ideal para educación y desarrollo de proyectos autónomos como el SpyderX.

- **Penetration Testing (Pentesting)**
  Pruebas controladas que simulan ciberataques reales con el objetivo de evaluar la seguridad de un sistema o red informática.

- **Man-in-the-Middle (MitM)**
  Tipo de ataque en el que un tercero intercepta la comunicación entre dos dispositivos para robar información, alterar datos o acceder sin autorización.

Capítulo III

Marco Metodológico

3.1 Tipo y nivel de investigación

La presente investigación es de tipo aplicada, ya que se orienta al diseño y desarrollo de un prototipo funcional que responde a una necesidad concreta en el área de seguridad digital institucional. Asimismo, el estudio es de nivel descriptivo-explicativo. Es descriptivo porque identifica características y debilidades de las redes WiFi institucionales, y explicativo porque analiza cómo el uso de herramientas automatizadas puede contribuir a mejorar la postura defensiva de dichas redes.

Según Tamayo y Tamayo (2006), el diseño metodológico de una investigación aplicada implica "la articulación de teorías y herramientas para resolver un problema concreto", lo cual se corresponde con la propuesta de SpyderX como solución tecnológica a una problemática real.

3.2 Método de investigación

La metodología utilizada fue Design Thinking, un enfoque centrado en el usuario que permite generar soluciones innovadoras a partir de la empatía, la ideación, la prototipación y la validación. Esta metodología fue aplicada de forma iterativa en las siguientes etapas:

- Comprensión del problema: entrevistas a personal técnico y administrativo de instituciones locales sobre sus limitaciones en ciberseguridad.
- Definición del usuario: instituciones públicas, educativas o sociales con redes WiFi vulnerables y sin personal técnico especializado.
- Ideación: lluvia de ideas sobre posibles soluciones automatizadas y portátiles.
- Prototipado: diseño estructural del robot en SolidWorks e implementación del sistema de escaneo y navegación.
- Validación: pruebas funcionales en entornos simulados, evaluando la detección de dispositivos y puertos mediante Nmap.

3.3 Materiales, método y procedimiento

El desarrollo del proyecto combinó componentes de hardware, software y metodologías de diseño digital:

Materiales empleados

- Kit robótico Freenove Hexapod Robot for Raspberry Pi
- Sistema operativo Raspberry Pi OS
- Microcomputadora Raspberry Pi (modelo 4 o superior compatible)
- Módulo WiFi de alta potencia
- Sensor MPU6050 para navegación
- Módulo ultrasónico
- Estructura impresa en 3D con diseño hexápodo
- Servomotores
- Aplicación móvil desarrollada con MIT App Inventor

Método

Se desarrolló un sistema modular utilizando el kit robótico Freenove Hexapod Robot for Raspberry Pi como base estructural del prototipo. Este kit permitió aprovechar su chasis mecánico, servomotores integrados y compatibilidad directa con la microcomputadora Raspberry Pi. A partir de esta plataforma, el robot fue adaptado para desplazarse de forma autónoma en espacios reducidos, realizar escaneos de red mediante comandos automatizados enviados a Nmap, y enviar los resultados a la aplicación móvil para su análisis y visualización.

Procedimiento

1. Diseño del modelo 3D del robot en SolidWorks.
2. Montaje electrónico y conexión de sensores al sistema Raspberry Pi OS.
3. Instalación de Nmap y configuración de comandos automatizados.

4. Programación del movimiento autónomo básico y lectura de sensores.

5. Desarrollo de la interfaz móvil para controlar el sistema, ejecutar escaneos y mostrar resultados.

6. Validación funcional en redes reales (autorizadas) de instituciones locales.

7. Documentación de hallazgos, tiempos de escaneo, dispositivos detectados y análisis de puertos.

3.4 Técnicas e instrumentos de recolección de datos

La principal técnica de recolección de datos fue el escaneo automático de red, realizado mediante Nmap. Esta herramienta permitió detectar:

- Dispositivos conectados a la red
- Servicios activos
- Posibles configuraciones inseguras

Los resultados de los escaneos fueron almacenados y procesados en formato de texto, generando archivos de reporte que luego se interpretaron para elaborar recomendaciones.

Además, se realizaron entrevistas no estructuradas con personal técnico y administrativo de las instituciones participantes, con el fin de identificar su nivel de conocimiento y experiencia con redes inalámbricas.

3.5 Población y muestra

La población estuvo conformada por instituciones educativas y sociales ubicadas en el estado La Guaira, específicamente aquellas que manifestaron interés en mejorar su seguridad digital. La muestra fue intencional y de tipo no probabilística, seleccionando dos instituciones donde se realizaron pruebas funcionales del prototipo con autorización previa: una unidad educativa y un centro comunitario.

3.6 Validación del prototipo

El prototipo fue evaluado en un entorno simulado de red WiFi institucional bajo condiciones

controladas. Se probaron funciones como escaneo de dispositivos conectados, detección de configuraciones vulnerables y ejecución de ataques éticos tipo MitM y Evil Twin. Los resultados obtenidos fueron registrados y comparados con los objetivos planteados en la fase de diseño.

3.7 Enfoque ético y legal

Todas las pruebas del prototipo se realizaron con la debida autorización de las instituciones involucradas, en redes simuladas o ambientes controlados. No se ejecutaron ataques reales a redes públicas ni privadas sin consentimiento. El desarrollo se enmarca en el principio de **uso ético** de tecnologías emergentes para fines educativos y de fortalecimiento institucional.

Capítulo IV

Desarrollo del Prototipo y Validación Funcional

4.1 Diseño estructural del robot

El diseño del robot SpyderX se realizó utilizando el software de modelado 3D SolidWorks, permitiendo planificar una estructura compacta, resistente y funcional. Se optó por una arquitectura hexápoda debido a su capacidad de moverse de forma estable en superficies irregulares o espacios estrechos, comunes en instalaciones institucionales. El chasis fue impreso en 3D, lo que facilitó la personalización de soportes para sensores, módulos y actuadores.

Para el desarrollo físico del prototipo se utilizó el kit robótico Freenove Hexapod Robot for Raspberry Pi, el cual proporciona una base hexápoda completamente programable, servomotores integrados y una estructura adaptable para implementar sensores y sistemas de navegación.

El cuerpo del robot está dividido en tres niveles: el inferior aloja los motores y el sistema de patas; el intermedio contiene la placa de distribución de energía y la Raspberry Pi; y el superior sostiene el módulo WiFi de alta ganancia y el sistema de navegación. El peso y centro de gravedad fueron optimizados para garantizar maniobrabilidad sin comprometer la estabilidad.

La integración con el kit Freenove permitió reducir los tiempos de ensamblaje y validación, ya que el chasis y distribución de niveles ya están optimizados para la arquitectura Raspberry Pi.

4.2 Integración electrónica y configuración del sistema

El kit robótico Freenove Hexapod Robot for Raspberry Pi fue la base seleccionada por su compatibilidad directa con microcomputadoras Raspberry Pi, facilidad de montaje y soporte comunitario amplio.

El cerebro del robot es una Raspberry Pi con sistema operativo Raspberry Pi OS, elegido por su bajo consumo, versatilidad y compatibilidad con herramientas de red. Se integraron los siguientes componentes:

- Sensores de navegación: MPU6050 (giroscopio y acelerómetro) y un módulo ultrasónico para detección de obstáculos.

- Módulo WiFi de alta potencia, compatible con escaneo y análisis de redes.
- Servomotores conectados mediante una controladora PWM para movimientos coordinados.
- Fuente de alimentación regulada con batería recargable.

El sistema se configuró para iniciar automáticamente el escaneo con Nmap, almacenar los resultados y enviar alertas básicas a la app móvil.

4.3 Programación y lógica de funcionamiento

La lógica del sistema se divide en tres partes:

1. **Navegación autónoma**: el robot se desplaza por el entorno usando datos del MPU6050 y del sensor ultrasónico para evitar obstáculos.
2. **Escaneo de red**: a intervalos definidos, ejecuta comandos preconfigurados de Nmap para detectar dispositivos conectados, puertos abiertos y servicios vulnerables.
3. **Interfaz móvil**: una aplicación desarrollada en MIT App Inventor permite iniciar escaneos, detener el movimiento, visualizar resultados e incluso recibir notificaciones de alertas básicas.

Todo el sistema fue probado en redes institucionales autorizadas, simulando distintos escenarios de evaluación interna.

4.4 Pruebas de campo y validación funcional

Las pruebas funcionales se realizaron en dos instituciones del estado La Guaira: una unidad educativa y un centro comunitario, ambos con redes WiFi internas y consentimiento para la evaluación. Se validaron los siguientes aspectos:

- **Movilidad del robot**: capaz de desplazarse en pasillos, oficinas y salas pequeñas.
- **Detección de dispositivos conectados** mediante Nmap, identificando teléfonos, laptops, routers y cámaras.

- **Reconocimiento de puertos y servicios abiertos**, especialmente aquellos sin cifrado o con configuraciones por defecto.

- **Visualización remota** desde la app móvil, incluyendo logs básicos del escaneo.

Los resultados fueron positivos, destacando la utilidad del robot como una herramienta de apoyo para personal no técnico.

4.5 Limitaciones y mejoras futuras

Entre las limitaciones encontradas destacan:

- Alcance limitado del módulo WiFi en espacios con paredes gruesas.

- El sistema actual no incluye cifrado de datos transmitidos entre robot y app.

- No se cuenta aún con almacenamiento en la nube ni integración con bases de datos externas.

Como mejoras futuras se plantea:

- Incorporar sensores adicionales para mayor precisión en navegación.

- Añadir cifrado extremo a extremo en la comunicación app-robot.

- Integrar funciones de mapeo de red más avanzadas mediante extensiones de Nmap.

- Desarrollar una plataforma web para visualizar resultados desde múltiples dispositivos.

En general, se validó el diseño propuesto como viable, replicable y útil para contextos de bajo presupuesto que requieren fortalecer su ciberseguridad sin recurrir a soluciones comerciales costosas

Capítulo V

Conclusiones y Recomendaciones

5.1 Conclusiones

El desarrollo del prototipo SpyderX permitió validar la viabilidad de una herramienta autónoma de bajo costo para auditorías internas de redes WiFi en organizaciones venezolanas. Mediante la integración de componentes accesibles y tecnologías libres como Raspberry Pi OS, Nmap y MIT App Inventor, junto con el kit robótico Freenove Hexapod para Raspberry Pi, se logró construir un robot funcional capaz de identificar vulnerabilidades básicas en redes inalámbricas institucionales.

Las pruebas en entornos reales evidenciaron que muchas organizaciones carecen de herramientas para visualizar los dispositivos conectados a sus redes o evaluar configuraciones inseguras. SpyderX facilita esta tarea mediante una plataforma física móvil que automatiza el proceso de escaneo y lo vuelve accesible incluso para usuarios sin conocimientos técnicos avanzados.

El enfoque Gray Hat aplicado en el diseño del sistema demostró ser útil como metodología pedagógica y de prevención, actuando siempre bajo consentimiento informado y respeto a los marcos legales. Además, el uso de un robot físico potencia el interés de estudiantes y profesionales en áreas como ciberseguridad, robótica y electrónica, fomentando el aprendizaje activo y la conciencia digital.

En resumen, SpyderX constituye un aporte tangible a la construcción de instituciones más resilientes digitalmente, en línea con los principios del ODS 16.

5.2 Recomendaciones

- Fortalecer la documentación técnica del prototipo, para facilitar su réplica en otras instituciones educativas o comunitarias.

- Ampliar la capacidad del sistema para reconocer y clasificar tipos de dispositivos conectados mediante scripts más avanzados de Nmap.

- Incluir herramientas complementarias como Aircrack-ng para pruebas de captura de handshakes y evaluación de contraseñas débiles.

- Integrar Wireshark para análisis profundo del tráfico de red y detección de paquetes sospechosos.

- Incorporar Bettercap en futuras versiones, permitiendo la simulación de ataques tipo Evil Twin y análisis de ataques hombre en el medio (MiTM), siempre bajo entornos controlados y autorizados.

- Añadir almacenamiento en la nube para conservar historiales de escaneos y generar estadísticas comparativas.

- Implementar autenticación en la app móvil y cifrado de comunicaciones para garantizar mayor seguridad durante el uso del robot.

- Desarrollar una interfaz web para la visualización avanzada de resultados y reportes de seguridad.

- Promover talleres educativos sobre ciberseguridad institucional utilizando SpyderX como herramienta didáctica.

- Buscar alianzas con instituciones gubernamentales y universidades para ampliar el impacto del proyecto en todo el territorio nacional.

Referencias Bibliograficas

- Brown, T. (2009). *Change by design: How design thinking creates new alternatives for business and society*. Harvard Business Press.
- Franklin Robotics. (2018). *Tertill: The solar-powered weeding robot*. Recuperado de www.franklinrobotics.com
- Freenove. (2023). *Freenove Hexapod Robot Kit for Raspberry Pi: User Manual & Technical Specs*. Recuperado de www.freenove.com/product/freenove-hexapod-robot-kit-for-raspberry-pi
- Fundación Infocentro. (2022). *Memoria y cuenta institucional 2021–2022*. Ministerio del Poder Popular para Ciencia y Tecnología.
- Kaspersky. (2023). *Cybersecurity threats and trends 2023*. Recuperado de www.kaspersky.com/blog/
- Llamas, J. (2020). *Diseño y construcción de un robot educativo de bajo costo para ambientes escolares*. Universidad Nacional de Colombia.
- MIT App Inventor. (2023). *Official Documentation*. Recuperado de appinventor.mit.edu/
- Nmap. (2023). *The Nmap Security Scanner Project*. Recuperado de nmap.org/
- Programa Semilleros Científicos. (2023). *Informe nacional de actividades STEM*. Ministerio del Poder Popular para Ciencia y Tecnología (MINCYT).
- Rogue Robotics. (2021). *CyberDog Recon: Autonomous cyber-patrol robot for penetration testing*. Informe interno (no publicado oficialmente).
- Stallings, W. (2021). *Network security essentials: Applications and standards* (6ª ed.). Pearson.
- Tamayo y Tamayo, M. (2006). *El proceso de la investigación científica* (6ª ed.). Limusa.
- Universidad Central de Venezuela. (2019). *Proyecto RedSegura: Análisis de vulnerabilidades en redes públicas del campus universitario*. Facultad de Ingeniería.

Anexos