Información General del Semillero de Investigación	
Facultad: **Ciencias Naturales e Ingeniería FCNI**	
Programa académico: **Ingeniería de Telecomunicaciones**	Grupo(s) de Investigación: **GNET**
Nombre del semillero – Siglas **Semillero de investigación en Sistemas de Telecomunicaciones - SISTEL**	
Líneas de Investigación: **Sistemas de transmisión y recepción**	

Áreas del saber *			
	1. Agronomía veterinaria y afines		5. Ciencias sociales y humanas
	2. Bellas artes		6. Economía, administración, contaduría y afines
	3. Ciencias de la educación		7. Matemáticas y ciencias naturales
	4. Ciencias de la salud	x	8. Ingenierías, arquitectura, urbanismo y afines

Al diligenciar este documento autorizo a UNIDADES TECNOLÓGICAS DE SANTANDER, ubicada en Calle de los Estudiantes 9-82 Ciudadela Real de Minas y con teléfono de contacto 6076917700, para que recolecte, almacene, use, circule y/o suprima mis datos personales. Lo anterior para dar cumplimiento a las finalidades incorporadas en la Política de Tratamiento de Información disponible en www.uts.edu.co, la cual declaro conocer y saber que en esta se especifican cuáles datos son sensibles. Así mismo, conozco que como titular me asisten los derechos a conocer, actualizar, rectificar y suprimir mis datos y revocar la autorización. Igualmente declaro que poseo autorización, de los otros titulares de datos que suministro, para que UNIDADES TECNOLÓGICAS DE SANTANDER les dé tratamiento conforme a las finalidades consignadas en la Política.

Información del Docente Líder

Nombre	Documento	Correo electrónico
Johan Leandro Téllez Garzón	1101753049	jtellez@correo.uts.edu.co

Información de los Autores

Nombre	Documento	Correo electrónico
Naren Alejandro Velandia Paredes	1005150595	navelandia@uts.edu.co
Daniel Hernando Almeida Lizarazo	1005256688	adaniel@uts.edu.co

Proyecto

1. Título del proyecto: Análisis de seguridad en tecnologías inalámbricas mediante el dispositivo Flipper Zero	MODALIDAD DEL PROYECTO **			
	PA	PI	TI	Otra. ¿Cuál?
			x	
	Fecha de terminación del proyecto:			17/02/2025

2. Resumen del trabajo:

La presente investigación se enfoca en el análisis de vulnerabilidades en dispositivos que utilizan tecnologías inalámbricas como RFID, NFC, Bluetooth y Sub-GHz, mediante pruebas controladas de penetración con el dispositivo Flipper Zero. La investigación se enmarca en un enfoque ético - técnico con el objetivo de determinar el riesgo y proponer contramedidas de mitigación que puedan aplicarse en entornos del mundo real.

Metodología centrada en revisión de la literatura bibliográfica, análisis de vulnerabilidades de tecnologías inalámbricas mencionadas anteriormente y pruebas de laboratorio controladas con Flipper Zero con aplicación de herramientas de código abierto en delineamiento de capacidad complementaria. Se realizó la simulación de ataques mediante clonación de tarjetas, suplantación de dispositivos y reproducción de la señal mediante registro del resultado alcanzado bajo escenarios seguros.

Los resultados evidencian vulnerabilidades críticas en dispositivos de uso masivo en Colombia, particularmente en sistemas inalámbricos institucionales, residenciales y automotrices. El análisis identificó protocolos de obsoletos aún en uso, incompatibilidades con estándares actualizados de seguridad y configuraciones inadecuados por parte de técnicos e usuarios finales. Como medidas de mitigación, se recomienda la migración a protocolos seguros, capacitación en configuraciones adecuada y actualización de firmware en dispositivos vulnerables. Adicionalmente, los resultados sustentan la urgencia de que los fabricantes para integrar protocolos actualizado que garanticen la compatibilidad con estándares modernos de seguridad.

La investigación muestra que dispositivos accesibles como Flipper Zero se pueden utilizar para fortalecer la ciberseguridad mediante pruebas éticas. La investigación contribuye al aprendizaje académico y profesional en la especialidad de telecomunicaciones, arraigándose la creación de ingenieros especialistas en seguridad digital. También contribuye a la seguridad tecnológica de la sociedad mediante la identificación y mitigación de amenazas existentes en infraestructuras inalámbricas.

El estudio valida la efectividad de esta herramienta para el uso de análisis de seguridad y evidencia la necesidad urgente de actualizar protocolos en dispositivos de uso masivo.

3. Objetivo general y objetivos específicos:

Analizar la seguridad de dispositivos en comunicaciones inalámbricas mediante el desarrollo de pruebas de vulnerabilidad con Flipper Zero, integrando herramientas de código abierto y programación personalizada para verificar la susceptibilidad de tecnologías como RFID, NFC, Bluetooth y Sub-GHz, y proponer estrategias orientadas a la mitigación de riesgos.

- Analizar vulnerabilidades en dispositivos de comunicaciones inalámbricas que emplean tecnologías como RFID, NFC y Bluetooth.
- Desarrollar pruebas de seguridad controladas utilizando Flipper Zero para evaluar la efectividad de ataques como repetición de señales RF, clonación de tarjetas y suplantación de dispositivos Bluetooth.
- Integrar herramientas de código abierto con el Flipper Zero mediante programación, con el fin de potenciar su capacidad de análisis y ataque en dispositivos inalámbricos.
- Proponer estrategias orientadas a la mitigación de riesgos en dispositivos inalámbricos, considerando configuraciones seguras, cifrado y autenticación reforzada.

4. Análisis de resultados:

Análisis de la Encuesta

Los resultados de la encuesta muestran una percepción generalizada de riesgo frente a la interceptación de información en dispositivos electrónicos. Una parte significativa de los participantes manifestó preocupación por la posibilidad de que sus datos sean copiados o robados mediante ataques inalámbricos, lo que confirma la relevancia del estudio y del Flipper Zero como herramienta de demostración.

La muestra estuvo compuesta principalmente por personas entre 26 y 35 años (53,6 %) y con un nivel avanzado de conocimiento tecnológico (64,3 %). Esto aporta validez al análisis, pues las opiniones provienen de usuarios con un entendimiento relativamente profundo de las tecnologías evaluadas.

En relación con los controles remotos vehiculares, la mayoría de los encuestados considera que la señal no es completamente segura, e incluso muchos han contemplado la posibilidad de que alguien pueda abrir su vehículo sin autorización. Esto evidencia desconfianza hacia las tecnologías de radiofrecuencia de uso cotidiano, alineándose con las capacidades del Flipper Zero para replicar señales vulnerables.

Respecto a los pagos NFC, predominó la neutralidad o el desacuerdo frente a sentirse seguros utilizando estas tarjetas. La preocupación por el robo de datos bancarios sin contacto sigue siendo alta, lo cual indica que las tecnologías de proximidad aún generan incertidumbre y deben ser analizadas desde una perspectiva de seguridad.

En cuanto al uso de redes WiFi públicas, los participantes reconocen los riesgos, pero aun así las utilizan con frecuencia. Aunque desconfían de introducir contraseñas en estos entornos, su comportamiento refleja una contradicción que puede ser aprovechada por atacantes mediante técnicas de interceptación o suplantación.

Finalmente, en el ámbito de Bluetooth, se observó que muchos usuarios mantienen esta tecnología activada permanentemente o la utilizan con frecuencia sin aplicar buenas prácticas de seguridad. Esto incrementa la superficie de ataque y facilita intentos de spoofing o saturación.

Evaluación de Capacidades Sub-GHz con Firmware de Fábrica

Las pruebas en la banda Sub-GHz permitieron evaluar la capacidad del Flipper Zero para observar, capturar y retransmitir señales de dispositivos de acceso y alarmas vehiculares.

En el Vehículo 1 (Suzuki Swift), los intentos de clonación fueron infructuosos. Este resultado sugiere el uso de rolling codes, mecanismo que invalida cualquier señal repetida y protege el sistema frente a ataques de repetición.

En contraste, en el Vehículo 2 (Toyota Hilux) se logró capturar y retransmitir con éxito las señales de apertura y cierre utilizando una frecuencia de 433.92 MHz con modulación AM650. Esto demuestra que el sistema es vulnerable a ataques básicos, incluso usando únicamente la antena interna del Flipper.

El análisis indica que mientras algunos fabricantes implementan medidas robustas, otros continúan utilizando sistemas que pueden comprometer la seguridad del usuario frente a equipos de bajo costo y fácil acceso.

Evaluación de Capacidades Bluetooth y Resultados en Dispositivos

Las pruebas de Bluetooth spoofing consistieron en emular múltiples periféricos inexistentes para generar un exceso de solicitudes de conexión en distintos dispositivos.

Los resultados fueron contundentes:

- El iPhone se reinició por saturación.
- El equipo Windows presentó una ralentización severa y consumo alto de recursos, lo cual sugiere que un ataque similar en un entorno empresarial (p. ej., Windows Server) podría comprometer la estabilidad del servicio.
- El Samsung Android mostró lags considerables.
- En MacOS, aunque no hubo reinicio, sí se observaron molestias por notificaciones constantes.

Las pruebas confirman que los ataques de saturación Bluetooth pueden generar afectaciones reales en el rendimiento de equipos modernos, lo que expone una vulnerabilidad relevante en escenarios donde se confía en esta tecnología para comunicaciones o sincronización de dispositivos.

Evaluación de Capacidades NFC

Se realizaron pruebas con tarjetas bancarias colombianas y tarjetas de control de acceso Hikvision y ZKTeco. Ninguna de ellas pudo ser clonada ni leída de forma adecuada.

En el caso de las tarjetas bancarias, las pruebas con diferentes tipos de modulación (ASK y PSK) tampoco permitieron identificar protocolos o formatos, lo que sugiere la implementación de estándares propietarios o mecanismos avanzados de protección. Esto demuestra un alto nivel de seguridad en sistemas de pago NFC.

De igual forma, las tarjetas de acceso corporativo no respondieron a los intentos del Flipper Zero, lo que indica que el dispositivo, con su firmware estándar, no cuenta con la capacidad técnica necesaria para vulnerar este tipo de credenciales.

En síntesis, las tecnologías NFC evaluadas presentan barreras sólidas frente a ataques de clonación con dispositivos de propósito general como el Flipper Zero.

Evaluación BAD USB

Las pruebas BADUSB representan la sección donde se identificó el mayor nivel de riesgo. Todas las pruebas se realizaron mediante el uso de payloads en lenguaje DuckyScript, aprovechando la capacidad del Flipper Zero para actuar como un teclado HID.

Prueba 1: Script de prueba “Hola Mundo”

Sirvió para demostrar la estructura básica de un payload, la forma en que el dispositivo interactúa con Windows y el funcionamiento general del módulo BadUSB. Aunque simple, validó que la ejecución automática de comandos es inmediata y no requiere interacción del usuario.

Prueba 2: Extracción automática de configuración de red

El payload ejecutó ipconfig, copió la salida y la pegó en Notepad. Esta prueba evidenció que un ataque sencillo puede obtener información sensible sin alertar al usuario y sin generar notificaciones visibles. Refuerza la importancia del control de dispositivos USB y del uso de soluciones EDR.

Prueba 3: Apertura automatizada de navegador mediante PowerShell

Esta prueba demostró cómo un script puede abrir aplicaciones, ejecutar comandos avanzados y acceder a URL específicas sin intervención del usuario. Esto implica que un atacante podría dirigir al sistema hacia páginas maliciosas o descargar contenido peligroso de forma automatizada.

Prueba 4: Automatización HID para creación de usuarios

Se utilizó firmware UNLSHD-082 para corregir errores de escritura en los payloads y se ejecutó un script que:

- Abrió la consola con privilegios.
- Creó un nuevo usuario.
- Lo añadió al grupo de administradores.
- Confirmó los cambios tanto por consola como por la interfaz gráfica.

Esta prueba es la más crítica, ya que demuestra cómo un atacante podría conseguir persistencia y escalamiento de privilegios en cuestión de segundos, únicamente conectando un dispositivo HID no autorizado.

5. Conclusiones:

El análisis de tecnologías inalámbricas mediante el Flipper Zero evidenció que, pese a los avances en seguridad, la superficie de ataque sigue siendo amplia cuando no existen configuraciones adecuadas ni prácticas de protección sólidas. Las pruebas en entornos controlados demostraron vulnerabilidades en redes Wi-Fi —especialmente por la obtención de PMKID—, en sistemas RFID con implementaciones débiles y en la explotación de puertos USB mediante ataques BadUSB. Esto confirma que la seguridad no depende solo de la tecnología en sí, sino del uso responsable, la configuración correcta y la gestión continua de los riesgos.

En redes Wi-Fi, se comprobó que la efectividad de WPA, WPA2 y WPA3 está condicionada por la robustez de las contraseñas y el mantenimiento de los equipos. Los protocolos más recientes ofrecen mejoras, pero las credenciales débiles siguen permitiendo ataques de fuerza bruta, evidenciando que la seguridad debe valorarse tanto por el diseño criptográfico como por la conducta del usuario.

En RFID se identificaron fallas relevantes en sistemas de baja frecuencia y en soluciones sin cifrado o autenticación fuerte. La clonación continúa siendo viable cuando no se implementan controles avanzados, y la falta de estandarización entre fabricantes incrementa los riesgos. El estudio reafirma que la protección efectiva requiere combinar mecanismos físicos, lógicos y una gestión integral.

Los ataques BadUSB demostraron nuevamente su vigencia como vector de amenaza, ya que permiten ejecutar comandos automatizados en segundos. Aunque los antivirus y políticas de seguridad influyeron en las pruebas, fue evidente que la

mitigación requiere un modelo de defensa multicapa que incluya controles de hardware, administración de dispositivos y capacitación del usuario.

De forma transversal, se concluye que ninguna tecnología es completamente segura: el nivel de riesgo depende de su implementación, actualización y del nivel de conciencia de quienes la utilizan. La seguridad, por tanto, es un proceso dinámico que involucra a fabricantes, organizaciones y usuarios.

El proyecto también reveló limitaciones técnicas y legales, como incompatibilidades entre equipos y la necesidad de entornos controlados para pruebas éticas. Superar estas dificultades reafirmó la importancia de la planificación rigurosa y la documentación en auditorías de seguridad.

Finalmente, se destaca que la ciberseguridad trasciende lo técnico e incorpora dimensiones éticas, legales y sociales. En instituciones y hogares, la adopción de contraseñas robustas, autenticación multifactor, actualizaciones periódicas y precaución frente a dispositivos externos son medidas esenciales. Asimismo, los desarrolladores deben integrar la seguridad desde el diseño mediante cifrado por defecto, autenticación fuerte y actualizaciones continuas.

.

6. Recomendaciones:

Los resultados del estudio sugieren que futuras investigaciones deberían ampliar el uso del Flipper Zero mediante módulos y antenas externas adecuadamente calibradas, ya que estos elementos influyen directamente en la precisión de las pruebas Sub-GHz, RFID y NFC. Para asegurar resultados replicables, se recomienda establecer estándares técnicos previos e incluir dispositivos de distintos fabricantes que permitan una evaluación más completa.

En cuanto a la metodología, se propone mantener los ensayos en entornos controlados, pero complementarlos con simulaciones que reflejen situaciones reales de uso. También se resalta la importancia de una documentación rigurosa y del almacenamiento seguro de evidencias digitales para mejorar la trazabilidad y la reproducibilidad de futuros estudios.

A nivel práctico, se enfatiza la necesidad de fortalecer la protección de dispositivos inalámbricos mediante contraseñas robustas, autenticación adicional y cifrado moderno, así como promover programas de formación en seguridad para instituciones y usuarios domésticos. Finalmente, se recomienda que los fabricantes adopten protocolos de seguridad más estrictos, actualicen firmware con mayor frecuencia y reduzcan funciones vulnerables, con el fin de disminuir la superficie de ataque. El proyecto concluye con un llamado a la industria, la academia y los usuarios a mantener una postura ética y preventiva frente a los riesgos emergentes de las tecnologías inalámbricas.

7. Bibliografía:

llatif, H., Ariyarathna, V., Madanayake, A., & Jornet, J. M. (2024). A Real-time Software-defined Radio Platform for Sub-Terahertz Communication Systems. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3473615

to, N., & Solano, A. (2025). Fortaleza digital: estrategias para blindar infraestructuras contra ciberataques. *Encuentro Internacional de Educación En Ingeniería*, 1–7. https://doi.org/10.26507/PAPER.4344

dia, B. (2025, October 1). *Bucaramanga avanza en tecnología, desarrollo e innovación a través de las TIC*. Https://Www.Bucaramanga.Gov.Co/Noticias/Bucaramanga-Avanza-En-Tecnologia-Desarrollo-e-Innovacion-a-Traves-de-Las-Tic/. https://www.bucaramanga.gov.co/noticias/bucaramanga-avanza-en-tecnologia-desarrollo-e-innovacion-a-traves-de-las-tic/

ıtani, A. H., & Iftikhar, M. (2013). TCP / IP Attacks , Defenses and Security Tools. *Proceedings - IEEE Symposium on Security and Privacy*, *1*(10), 42–47. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.686.1616&rep=rep1&type=pdf

ıioli, D. (2021a). BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses. *CCS 2023 - Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 636–650. https://doi.org/10.1145/3576915.3623066

hioli, D. (2021b). BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses. *CCS 2023 - Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 636–650. https://doi.org/10.1145/3576915.3623066

riya. (2025). *Bluetooth Flaws Allow Hackers to Eavesdrop via Headphones and Earbuds*. https://cyberpress.org/bluetooth-flaws-headphones-earbuds/?utm_source=chatgpt.com

kens, B., Penne, R., & Weyn, M. (2018). Realistic Indoor Radio Propagation for Sub-GHz Communication. *Sensors 2018, Vol. 18, Page 1788*, *18*(6), 1788. https://doi.org/10.3390/S18061788

eau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *Proceedings - IEEE Symposium on Security and Privacy*, 553–567. https://doi.org/10.1109/SP.2012.44

Y., & Zhu, D. (2019). Trustworthy and profit: A new value-based neighbor selection method in recommender systems under shilling attacks. *Decision Support Systems*, *124*. https://doi.org/10.1016/j.dss.2019.113112

Tech. (2024). *Gallery | Your SubGHz Replay Attack Gadget For RF Hacking | Hackaday.io*. https://hackaday.io/project/196709/gallery?utm_source=chatgpt.com#cb4e1c0f7eca531643f587df4b5b51b6

Eric., Krutz, R. L. ., & Conley, J. W. . (2009). *Network security bible*. 891.

nado, J. M., Kim, B.-G., Iglesias, C. A., Lee, I., Ren, F., Mehmood, R., Abu Al-Haija, Q., & Alsulami, A. A. (2022). Detection of Fake Replay Attack Signals on Remote Keyless Controlled Vehicles Using Pre-Trained Deep Neural Network. *Electronics 2022, Vol. 11, Page 3376*, *11*(20), 3376. https://doi.org/10.3390/ELECTRONICS11203376

well J. David, & Creswell and John W. (2018). Research Design Qualitative, Quantitative, and Mixed Methods Approaches. *Sage*, 1–304.

A., & Stolfo, S. J. (2010). A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan. *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 97–106. https://doi.org/10.1145/1920261.1920276

, G., Kush, ashwani, Kumar, B., & Bhushan, B. (2010). Future Trends in Wireless World. *CSI Communications*, *34*, 21–23.

rio, A., Buckley, J., Barton, J., Newberry, R., Rodencal, M., Dunlop, G., & O'Flynn, B. (2017). Potential of Sub-GHz Wireless for Future IoT Wearables and Design of Compact 915 MHz Antenna. *Sensors 2018, Vol. 18, Page 22*, *18*(1), 22. https://doi.org/10.3390/S18010022

stituto Nacional de Ciberseguridad. (2024, April 24). *Los incidentes de ciberseguridad de 2023, gestionados por INCIBE, aumentan en un 24% respecto al año anterior | INCIBE | INCIBE*. Incibe. https://www.incibe.es/incibe/sala-de-prensa/los-incidentes-de-ciberseguridad-de-2023-gestionados-por-incibe-aumentan-en

ández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M., & Castedo, L. (2017). Reverse engineering and security evaluation of commercial tags for RFID-based IoT applications. *Sensors (Switzerland)*, *17*(1). https://doi.org/10.3390/S17010028

ández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M., & Castedo, L. (2024). Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications. *Sensors (Switzerland)*, *17*(1). https://doi.org/10.3390/s17010028

nzeller, K. (2010). RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication, third edition. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition*, 1–1065. https://doi.org/10.1002/9780470665121

er. (2025, March 1). *Flipper Zero — Portable Multi-tool Device for Geeks*. FlipperZero. https://flipperzero.one/

n, T. (2009). *Electric Power Transmission System Engineering Analysis and Design*. www.mepcafe.com

lin, D. (2023, November 2). *This tiny device is sending updated iPhones into a never-ending DoS loop - Ars Technica*. Https://Arstechnica.Com/Security/2023/11/Flipper-Zero-Gadget-That-Doses-Iphones-Takes-Once-Esoteric-Attacks-Mainstream/. https://arstechnica.com/security/2023/11/flipper-zero-gadget-that-doses-iphones-takes-once-esoteric-attacks-mainstream/

i, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/J.FUTURE.2013.01.010

a, C., & Varshney, G. (2022). An Improved Authentication Scheme for BLE Devices with no I/O Capabilities. *ArXiv Preprint*.

, A., Oufaska, K., Yassini, K. El, Boulmalf, M., & Bouya, M. (2022). Systematic Mapping Study on RFID Technology. *IEEE Access*, *10*, 6363–6380. https://doi.org/10.1109/ACCESS.2022.3140475

covici, N., & Christodoulou, C. (2002). Wireless communications and networking: An overview. *IEEE Antennas and Propagation Magazine*, *44*(1), 185–193. https://doi.org/10.1109/74.997963

., Li, K., & Huang, S. (2021). Energy-efficient and Secure Data Transmission in BLE-based Wearable Networks. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3089894

der, M. F., & Yun, Z. (2002). Propagation prediction models for wireless communication systems. *IEEE Transactions on Microwave Theory and Techniques*, *50*(3), 662–673. https://doi.org/10.1109/22.989951

31000: Risk Management – Guidelines. (2018).

EC 27001: Information Security, Cybersecurity and Privacy Protection – Requirements. (2022).

EC 27032: Guidelines for Cybersecurity. (2021).

K., Choi, W., & Lee, D. H. (2020). Hold the Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft. *27th Annual Network and Distributed System Security Symposium, NDSS 2020*. https://doi.org/10.14722/ndss.2020.23107

lczyk, M. (2023, December 8). *Leading european penetration testing company*. Securitum. https://www.securitum.com/hacking_the_invisible.html

ughlin, S., Podkuiko, D., Miadzvezhanka, S., Delozier, A., & McDaniel, P. (2010). Multi-vendor penetration testing in the advanced metering infrastructure. *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 107–116. https://doi.org/10.1145/1920261.1920277

. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

andards, N. I., & Technology. (2022). *Cybersecurity Framework (CSF) 2.0 Draft*.

H., Zero, F., & Uusitalo, M. (2024). *RF Hacking Lab Development: HackRF One and Flipper Zero*. http://www.theseus.fi/handle/10024/869150

, R., Martin, R., & Mishra, S. (2024). Unveiling exploitation potential: a comparative analysis of flipper zero and rubber ducky. *Issues in Information Systems*, *25*(2), 84–95. https://doi.org/10.48009/2_IIS_2024_107

an, A., Karras, D. A., Kumar, J., Sánchez-Chero, M., Mogollón Taboada, M. M., & Altamirano, G. C. (2022). An Internet of Things (IoT) Based Block Chain Technology to Enhance the Quality of Supply Chain Management (SCM). *Mathematical Problems in Engineering*, *2022*. https://doi.org/10.1155/2022/9679050

, R., & Pillitteri, V. (2024). *Protecting controlled unclassified information in nonfederal systems and organizations*. https://doi.org/10.6028/NIST.SP.800-171R3

ieri, R. H. (2015). *Metodología_de_la_investigación*.

so, S., & Beaty, H. W. (2018). Standard Handbook for Electrical Engineers. In S. Santoso & H. W. Beaty (Eds.), *Standard Handbook for Electrical Engineers*. McGraw-Hill Education. https://www.accessengineeringlibrary.com/content/book/9781259642586

yeva, Y., & Chan, H. C. B. (2023). A survey on indoor positioning security and privacy. *Computers and Security*, *131*. https://doi.org/10.1016/j.cose.2023.103293

ab, M., Marouf, S., & Hudel, C. (2011). ROAuth: Recommendation based open authorization. *SOUPS 2011 - Proceedings of the 7th Symposium on Usable Privacy and Security*. https://doi.org/10.1145/2078827.2078842

, H., Huang, Q., Chen, Y., Huang, H., & Wang, Y. (2023). Research on Insulation Structure Optimization of Autotransformer Winding. *2023 IEEE Sustainable Power and Energy Conference, ISPEC 2023*. https://doi.org/10.1109/ISPEC58282.2023.10403029

ngs, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.

Y., Lin, C., & Zhou, F. (2024). BLEGuard: Detecting and Preventing Relay Attacks in Bluetooth Low Energy Communication. *Computers & Security*. https://doi.org/10.1016/j.cose.2024.103202

anns, J., Classen, J., Rohrbach, F., & Hollick, M. (2020). *Firmware Insider: Bluetooth Randomness is Mostly Random*. http://arxiv.org/abs/2006.16921

ıa, F. D. S. (2017). *POWER ELECTRONICS Converters, Applications, and Design THIRD EDITION*. https://www.academia.edu/40906425/POWER_ELECTRONICS_Converters_Applications_and_Design_THIRD_EDITION

, R. (2004). Enabling ubiquitous sensing with RFID. *Computer*, *37*(4), 84–86. https://doi.org/10.1109/MC.2004.1297315

nan, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.

.

8. Anexos:

Corresponde a las evidencias de realización y resultados de proyecto y a las herramientas desarrolladas y/o utilizadas en su ejecución.

*** Organización para la Cooperación y Desarrollo Económico (OCDE)**
**** PA: Proyecto de Aula; PI: Proyecto Integrador; TI: Trabajo de Investigación**