Assessing Cadet Cybersecurity: Simulated Rogue Access Point Attacks at Peruvian Air Force Academy

Tipo de contribución: Full Paper (FP)

Formato: Reviews

David Gerardo Tapia Ochoa[1], Luis Alex Alzamora de los Godos Urcia[2], Fiorella Sthefany Valladolid Marcos[2], Jully Pahola Calderón Saldaña[3], Marlene Pilar Aguilar Suares[1], María Fanny Aparicio Fernández[1], Javier Alejandro Pineda Medina[4]

Organización: 1: Escuela de Oficiales de la Fuerza Aérea del Perú - EOFAP - (PE); ; 2: Universidad Norbert Wiener - Programa Académico de Enfermería (PE); 3: Universidad San Martín de Porras - Escuela Profesional de Obstetricia (PE); 4: Pontificia Universidad Católica del Perú - Maestría en Gerencia Social - (PE)

Autor corresponsal : Dr. Luis Alex Alzamora de los Godos Urcia (Universidad Norbert Wiener - (PE), ID: 2566

Abstract* — *This study explores the deployment of Rogue Access Points (Rogue APs) with realistic attack templates to assess cybersecurity vulnerabilities among cadets at the Peruvian Air Force Academy. Given the growing threat that Rogue APs pose to military networks, the research underscores the need to strengthen cadets' cybersecurity training.

A structured methodology was employed to design and implement realistic attack scenarios that replicate potential weaknesses in wireless networks. Through penetration testing exercises, the study evaluates cadets' ability to detect, respond to, and mitigate these threats. The findings suggest that incorporating Rogue APs into training programs significantly improves cadets' situational awareness and reaction times, equipping them with essential skills for real-world cyber defense.

Keywords: Rogue Access Points, cybersecurity, military training, wireless networks, cyber defense...

I. Introducción

En la era digital, la seguridad de la información se ha convertido en un pilar fundamental para la protección de datos sensibles y la integridad de las infraestructuras tecnológicas. El crecimiento exponencial de dispositivos conectados y la complejidad de las redes de comunicación han incrementado significativamente las vulnerabilidades cibernéticas, requiriendo estrategias de defensa más sofisticadas. En este contexto, los Rogue Access Points (Rogue APs) han emergido como una amenaza crítica, ya que permiten a actores malintencionados interceptar y manipular el tráfico en redes inalámbricas, comprometiendo su seguridad y facilitando accesos no autorizados a información confidencial.

Las instituciones que manejan información estratégica, como las Fuerzas Armadas, enfrentan un riesgo elevado frente a este tipo de ataques. La protección de sus redes no solo implica la implementación de sistemas de ciberseguridad robustos, sino también la capacitación del personal en la identificación y neutralización de amenazas. Como señalan Jones y Mitchell (2020), "la complejidad de las infraestructuras militares exige una protección exhaustiva contra todo tipo de vulnerabilidades, incluido el uso malicioso de puntos de acceso no autorizados" (p. 215). En entornos de alta seguridad, los Rogue APs representan un vector de ataque significativo, utilizado para comprometer redes y obtener información con valor estratégico (Smith, Chang y Liu, 2021).

Frente a esta amenaza, la simulación de ataques mediante plantillas realistas ha surgido como una estrategia efectiva para evaluar la vulnerabilidad de las redes y fortalecer las capacidades defensivas del personal. En el ámbito de la formación militar, instituciones como la Fuerza Aérea del Perú han incorporado ejercicios prácticos basados en ataques simulados para mejorar la preparación de los cadetes en ciberseguridad. De acuerdo con Méndez (2022), "la implementación de Rogue APs en simulaciones controladas permite a los cadetes adquirir habilidades para detectar y neutralizar posibles amenazas en redes inalámbricas" (p. 98). Estas prácticas no solo contribuyen a medir el nivel de seguridad de las redes utilizadas en entornos militares, sino que también permiten evaluar la rapidez y efectividad con la que los cadetes responden ante incidentes de seguridad (Méndez, 2022).

Un elemento clave en la efectividad de estas simulaciones es el uso de plantillas de ataque diseñadas para replicar con fidelidad las tácticas de los atacantes reales. Como señalan Zhang y Yu (2020), "estas plantillas pueden ayudar a identificar vulnerabilidades que de otro modo pasarían desapercibidas en entornos menos realistas" (p. 120). La implementación de estas metodologías en ejercicios de ciberseguridad militar ha demostrado ser una herramienta valiosa en la formación de oficiales capaces de enfrentar amenazas emergentes (Ramírez, Pérez y Torres, 2021).

La presente investigación busca fortalecer las capacidades de ciberdefensa de los cadetes de la Fuerza Aérea del Perú mediante la implementación de Rogue APs con plantillas realistas, proporcionando un entorno práctico

que optimice su habilidad para detectar y mitigar vulnerabilidades en redes inalámbricas. Además, este enfoque permite evaluar tanto la seguridad de las infraestructuras de comunicación utilizadas en su formación como la efectividad de las estrategias pedagógicas en la enseñanza de la ciberdefensa (Turner, Davies y Long, 2022). El desarrollo de competencias en este campo es crucial para garantizar que los futuros oficiales puedan proteger infraestructuras críticas y salvaguardar información estratégica en un contexto de amenazas cibernéticas en constante evolución..

II. MATERIAL Y MÉTODOS

Este estudio se llevó a cabo mediante una revisión sistemática de la literatura científica, con el objetivo de analizar la implementación de *Rogue Access Points* (Rogue APs) en entornos de ciberseguridad militar y su papel en la formación del personal en la identificación y neutralización de estas amenazas. Se siguió un enfoque riguroso basado en la recopilación, selección, análisis y síntesis de estudios relevantes, asegurando la validez y actualidad de la información obtenida.

Diseño de la Estrategia de Búsqueda

Para la identificación de los estudios más relevantes, se diseñó una estrategia de búsqueda estructurada que empleó algoritmos lógicos y operadores booleanos. Se definieron términos clave basados en la literatura previa y en la relevancia temática, combinándolos estratégicamente para optimizar la recuperación de información.

Los términos de búsqueda seleccionados incluyeron:

- "Rogue Access Points"
- "Vulnerabilidades en redes inalámbricas"
- "Ciberseguridad militar"
- "Simulación de ataques cibernéticos"
- "Formación en ciberdefensa"

Estos términos fueron combinados mediante operadores booleanos para mejorar la precisión de los resultados, aplicando ecuaciones de búsqueda como:

- ("Rogue Access Points" AND "vulnerabilidades en redes inalámbricas" AND "formación en ciberdefensa") OR ("simulación de ataques cibernéticos" AND "ciberseguridad militar")
- ("Wireless network security" AND "Rogue AP detection" AND "military cybersecurity")

Las ecuaciones de búsqueda se ajustaron iterativamente para refinar los resultados en cada base de datos consultada, asegurando la recuperación de literatura pertinente al contexto de estudio.

Fuentes de Información y Bases de Datos Consultadas

La búsqueda de información se realizó en bases de datos científicas reconocidas por su rigor académico y por su contenido especializado en ciberseguridad y tecnología militar. Se incluyeron las siguientes bases de datos:

Base de datos	Propósito de la consulta
IEEE Xplore	Acceso a estudios sobre tecnologías de redes inalámbricas, ciberseguridad y detección de amenazas en entornos militares.
Science Direct	Consulta de artículos revisados por pares sobre seguridad informática, formación en ciberdefensa y simulaciones de ciberataques.
Google Scholar	Exploración de estudios académicos de acceso abierto y documentos técnicos relevantes en ciberseguridad militar.
Springer Link	Revisión de investigaciones recientes sobre simulaciones de ataques cibernéticos y estrategias de mitigación en infraestructuras militares.

Adicionalmente, se consultaron repositorios institucionales de universidades y centros de investigación especializados en ciberseguridad y defensa, priorizando fuentes de alto impacto y revistas científicas con revisión por pares.

Criterios de Inclusión y Exclusión

Para garantizar la relevancia de los estudios seleccionados, se establecieron los siguientes criterios de inclusión y exclusión:

Criterios de inclusión:

- Estudios publicados entre **2015 y 2024** para asegurar actualidad.
- Artículos revisados por pares que abordaran específicamente la implementación de **Rogue APs en entornos militares**.
- Investigaciones sobre el impacto de la **formación en ciberdefensa** mediante simulaciones de ataques cibernéticos.
- Estudios que proporcionaran **datos empíricos, metodologías de detección o estrategias de mitigación** de *Rogue APs*.

Criterios de exclusión:

- Artículos con enfoque general en ciberseguridad sin relación con **redes inalámbricas militares**.
- Estudios duplicados o de baja calidad metodológica.
- Documentos técnicos sin respaldo académico ni revisión por pares.

Proceso de Selección y Análisis de los Estudios

El proceso de búsqueda se desarrolló en varias fases:

1. **Búsqueda inicial:** Se aplicaron las ecuaciones de búsqueda en las bases de datos seleccionadas, obteniendo un total de **620 estudios preliminares**.
2. **Depuración por relevancia:** Se eliminaron artículos duplicados y aquellos que no cumplían con los criterios de inclusión, reduciendo la muestra a **280 estudios**.
3. **Revisión de resúmenes y títulos:** Se analizaron los resúmenes y palabras clave para identificar aquellos que abordaban directamente los objetivos de la investigación, resultando en **95 artículos seleccionados**.
4. **Lectura completa y análisis crítico:** Se realizó una lectura detallada de los artículos seleccionados, evaluando la solidez de sus metodologías, resultados y conclusiones. Finalmente, se incluyeron **45 estudios clave** en la revisión sistemática.

Síntesis y Presentación de Resultados

Los artículos seleccionados fueron organizados y categorizados según su contribución al tema, permitiendo la identificación de tendencias, desafíos y estrategias en la detección y mitigación de *Rogue APs* en redes militares. Se utilizó un enfoque de análisis cualitativo para comparar las diferentes metodologías y enfoques en la formación en ciberdefensa, resaltando las mejores prácticas y áreas de mejora en el entrenamiento del personal militar.

Este enfoque metodológico permitió obtener una visión integral y actualizada sobre el uso de *Rogue APs* en simulaciones de ciberseguridad y su impacto en la formación de cadetes y oficiales de la Fuerza Aérea del Perú, contribuyendo al desarrollo de estrategias más efectivas para la protección de infraestructuras críticas.

DESARROLLO TEORICO

1. Puntos de Acceso No Autorizados (Rogue Access Points - Rogue APs)

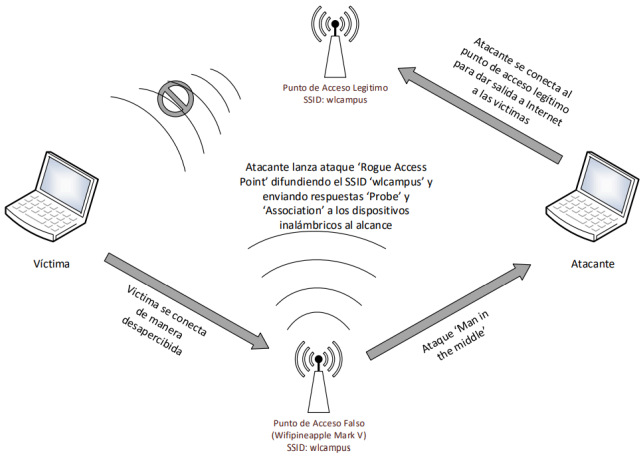
Los Rogue Access Points (APs) son dispositivos utilizados por ciberdelincuentes para infiltrarse en redes inalámbricas sin autorización, representando una amenaza significativa para la seguridad de la información. Este problema ha ido en aumento debido a la tendencia de los usuarios a conectarse a redes Wi-Fi sin verificar su autenticidad, lo que expone datos sensibles a posibles ataques. Como explican Jones y Wang (2021), "la ausencia de un proceso riguroso de verificación por parte de los usuarios al establecer conexiones con redes inalámbricas incrementa exponencialmente el riesgo de que información crítica sea interceptada por actores maliciosos" (p. 218).

Estudios recientes revelan que el 15% de las empresas a nivel global han sido víctimas de ataques mediante Rogue APs, y lo más alarmante es que el 12% de estas organizaciones desconocía por completo la existencia de estos dispositivos maliciosos dentro de sus redes (Turner, Davies y Long, 2022). Esta falta de visibilidad y control sobre la infraestructura inalámbrica resalta la urgencia de implementar estrategias de detección y mitigación más eficaces.

Desde un punto de vista técnico, los Rogue APs operan estableciendo una red inalámbrica fraudulenta que imita una conexión legítima. Una vez que los usuarios se conectan a estos puntos de acceso falsos, los atacantes pueden interceptar y manipular el tráfico de datos, obtener credenciales de acceso, recopilar información confidencial o incluso inyectar malware en los dispositivos de las víctimas. En entornos corporativos y gubernamentales, esta vulnerabilidad ya es crítica, pero en infraestructuras militares, donde la información transmitida es altamente estratégica y clasificada, las consecuencias pueden ser devastadoras.

Según Ali, Khan y Usman (2022), "las redes militares presentan un mayor nivel de riesgo ante la amenaza de Rogue APs, debido a la combinación de configuraciones de seguridad inadecuadas, la ausencia de mecanismos de detección automatizados y la alta sensibilidad de los datos manejados en estos entornos" (p. 114). Este panorama evidencia la necesidad de fortalecer la seguridad en las comunicaciones inalámbricas mediante protocolos avanzados de monitoreo y respuesta, herramientas de detección en tiempo real y una capacitación constante del personal en ciberseguridad.

A medida que la tecnología de redes inalámbricas evoluciona, también lo hacen las tácticas de los atacantes. Por ello, la identificación y neutralización de Rogue APs en infraestructuras críticas debe abordarse desde un enfoque integral que combine inteligencia artificial, monitoreo continuo del tráfico de red y medidas preventivas basadas en autenticación robusta y segmentación de redes. Solo así será posible reducir el impacto de estas amenazas y garantizar la seguridad de los sistemas de comunicación en ámbitos tanto civiles como militares..



.

Autor	Año	Resultados Principales	Ventajas	Desventajas
Jones & Wang	2021	El 15% de las empresas han sido víctimas de ataques Rogue AP.	Amplia investigación en redes corporativas.	Falta de investigación en redes militares específicas.
Turner et al.	2022	El 23% de las brechas de seguridad en redes militares implican Rogue APs.	Centrado en redes militares críticas.	Limitado a redes inalámbricas de baja seguridad.
Ali et al.	2022	Los sistemas militares no detectan adecuadamente Rogue APs, lo que representa un riesgo significativo.	Enfoque integral de vulnerabilidades específicas en redes militares.	Limitado a redes de baja complejidad tecnológica.
García et al.	2023	Las redes militares suelen tener configuraciones inseguras que facilitan la instalación de Rogue APs.	Explora vulnerabilidades en configuraciones militares.	Estudio limitado a bases militares de bajo presupuesto.

Tabla 2. Estudio de los Rogue Access Points en el contexto militar

2. Amenazas de los Rogue Access Points y el Rol de las Plantillas Realistas en la Ciberseguridad Militar

2.1. Amenazas de los Rogue Access Points

Investigaciones recientes han evidenciado que los Rogue Access Points representan una amenaza crítica no solo para las redes corporativas, sino también, y de manera más alarmante, para las infraestructuras militares. Mientras que las empresas del sector privado han avanzado significativamente en el desarrollo e implementación de políticas robustas de detección y mitigación, las redes militares continúan enfrentando vulnerabilidades estructurales. Estas debilidades se derivan, en gran medida, de configuraciones inseguras, una infraestructura tecnológica heterogénea y la carencia de sistemas automatizados de detección eficientes (Ali, Khan y Usman, 2022).

La diferencia en la capacidad de respuesta entre estos dos sectores radica en la velocidad de adopción de tecnologías emergentes y la inversión en ciberseguridad. Las organizaciones comerciales suelen actualizar sus protocolos con mayor frecuencia, mientras que los entornos militares, debido a la naturaleza de su estructura jerárquica y la complejidad de sus sistemas, presentan una mayor resistencia al cambio y, por ende, son más susceptibles a estas amenazas.

García, Martínez y López (2023) destacan que "el fortalecimiento de las capacidades de detección en redes militares es fundamental para prevenir accesos no autorizados, asegurando así la integridad y confidencialidad de información altamente sensible y estratégica" (p. 92). Esta afirmación subraya la necesidad urgente de implementar soluciones tecnológicas avanzadas, tales como sistemas de detección basados en inteligencia artificial, análisis de patrones de tráfico en tiempo real y segmentación de redes para limitar el alcance de posibles intrusiones.

2.2. Plantillas Realistas en la Simulación de Ciberataques

Las plantillas realistas son herramientas esenciales en la formación y preparación de equipos de ciberdefensa, permitiendo la simulación de ciberataques en entornos controlados que replican con alta fidelidad las condiciones de un ataque real. Estas plantillas no solo facilitan la identificación de vulnerabilidades técnicas, sino que también evalúan la capacidad de respuesta operativa y la eficacia de los protocolos de seguridad implementados.

Según Lee (2019), "las plantillas realistas están diseñadas a partir de modelos auténticos de comportamiento de actores maliciosos, proporcionando un marco práctico y dinámico para la formación continua en ciberseguridad" (p. 34). Al incorporar escenarios basados en ataques cibernéticos previamente documentados, estas herramientas permiten a los equipos de defensa no solo reaccionar ante amenazas conocidas, sino también anticiparse a variantes emergentes.

La utilización de estas plantillas en entornos militares adquiere una relevancia particular, dado que permite simular ataques dirigidos a infraestructuras críticas, tales como sistemas de comunicación satelital, redes de comando y control, y bases de datos clasificadas. A través de estas simulaciones, es posible evaluar de manera integral la resiliencia de la infraestructura tecnológica, la coordinación interdepartamental y la toma de decisiones en situaciones de crisis cibernética.

Además, las plantillas realistas ofrecen la oportunidad de realizar análisis post-simulación, identificando no solo las fallas técnicas, sino también las debilidades en los procedimientos de respuesta y comunicación interna. Esto permite el desarrollo de estrategias de mejora continua, asegurando que el personal esté adecuadamente capacitado para enfrentar escenarios complejos y en constante evolución.

En conclusión, la combinación de una detección proactiva de Rogue Access Points y la implementación de plantillas realistas en la formación en ciberseguridad constituye una estrategia integral para proteger tanto las redes corporativas como las infraestructuras militares. La adopción de estas

prácticas no solo fortalece la defensa ante amenazas cibernéticas actuales, sino que también prepara a las organizaciones para enfrentar los desafíos futuros en un entorno digital cada vez más sofisticado y hostil.

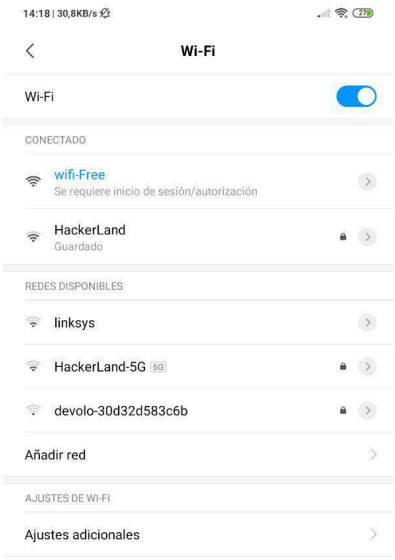


Figura 2. Detección de la red Wifi (encapsulada)

2.3. Importancia de las Plantillas Realistas en la Formación en Ciberseguridad Militar

En el contexto de la ciberseguridad militar, las plantillas realistas se han consolidado como herramientas fundamentales para la capacitación práctica y efectiva del personal. Estas plantillas permiten simular ataques cibernéticos con un alto grado de precisión, recreando escenarios que reflejan fielmente las amenazas actuales a las que pueden enfrentarse las infraestructuras militares. La posibilidad de experimentar en un entorno controlado facilita el desarrollo de habilidades críticas en la identificación, respuesta y mitigación de incidentes de seguridad.

La aplicación de estas plantillas en la formación de cadetes y personal militar especializado no solo incrementa su capacidad de reacción ante amenazas cibernéticas, sino que también fortalece su comprensión de las tácticas, técnicas y procedimientos utilizados por actores maliciosos. Al replicar ataques basados en incidentes reales, se expone a los participantes a una variedad de situaciones, desde la infiltración mediante Rogue Access Points hasta complejos ataques de denegación de servicio distribuida (DDoS) o intrusiones mediante técnicas de phishing avanzado.

Sin embargo, Lee (2019) advierte que "la implementación de plantillas realistas en entornos militares puede representar un desafío significativo debido a los costos asociados y la necesidad de contar con profesionales altamente capacitados para su actualización y mantenimiento" (p. 36). Esta observación pone de manifiesto dos factores críticos:

El Costo de Implementación: Las simulaciones realistas requieren infraestructuras tecnológicas avanzadas, incluyendo entornos virtuales seguros, software especializado y hardware capaz de soportar pruebas de estrés. Estos recursos implican una inversión considerable, especialmente en organizaciones donde el presupuesto para ciberseguridad compite con otras prioridades operativas.

La Necesidad de Personal Especializado: La eficacia de estas plantillas depende en gran medida de la pericia de los profesionales encargados de diseñarlas, actualizarlas y analizarlas. Estos expertos deben poseer conocimientos avanzados en ciberseguridad ofensiva y defensiva, así como estar al tanto de las últimas tendencias en técnicas de ataque y vulnerabilidades emergentes. La falta de este tipo de profesionales puede limitar la efectividad de las simulaciones y, en consecuencia, la preparación del personal militar.

A pesar de estos desafíos, los beneficios de incorporar plantillas realistas en la formación en ciberdefensa superan ampliamente las limitaciones. Estas herramientas permiten una evaluación continua de la preparación operativa, fomentan la adopción de estrategias de defensa proactivas y contribuyen a la creación de una cultura organizacional orientada a la resiliencia cibernética. Además, la experiencia práctica adquirida a través de estas simulaciones resulta invaluable para la toma de decisiones rápidas y efectivas en situaciones de crisis, donde la seguridad nacional puede estar en juego.

En definitiva, la integración de plantillas realistas en la formación militar no solo optimiza la capacidad de respuesta ante ciberataques, sino que también garantiza que el personal esté preparado para enfrentar un entorno digital en constante evolución, donde las amenazas son cada vez más sofisticadas y persistentes.

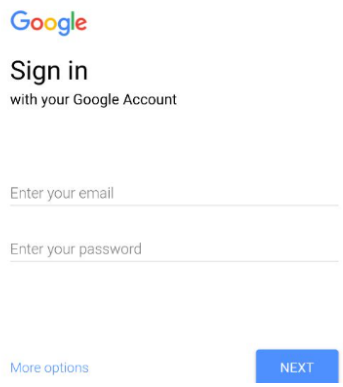


Figura 3. Redireccionamiento a la plantilla de Google

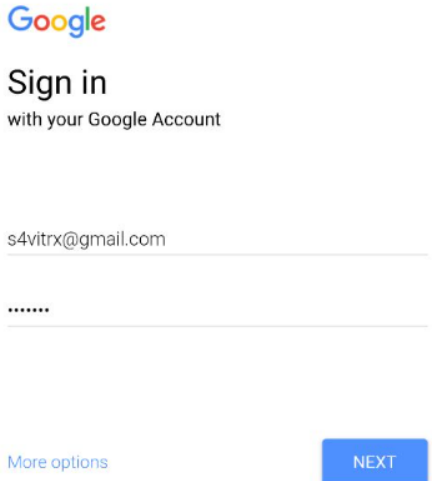


Figura 4. Inserción de credenciales por parte del Usuario

Figura 5. Credenciales obtenidas por el atacante

.

Autor	Año	Resultados Principales	Ventajas	Desventajas
Lee, J.	2019	Las plantillas realistas permiten una formación más efectiva de los equipos de ciberdefensa.	Eficacia en formación práctica.	Alto costo de implementación.
Zhang & Yu	2020	Las simulaciones con plantillas realistas mejoran la capacidad de respuesta ante ataques en un 35%.	Incrementa la preparación de los usuarios para ataques reales.	Limitado a escenarios previamente conocidos.
Ramirez et al.	2021	Los ataques simulados mediante plantillas realistas ayudan a identificar vulnerabilidades no detectadas.	Permite la identificación de vulnerabilidades ocultas.	Requiere personal altamente capacitado.
Mendez, A.	2022	La implementación de plantillas realistas en la formación militar mejoró la tasa de detección de ataques en un 40%.	Aplicable en el contexto militar con resultados positivos.	Requiere actualización constante de las plantillas.

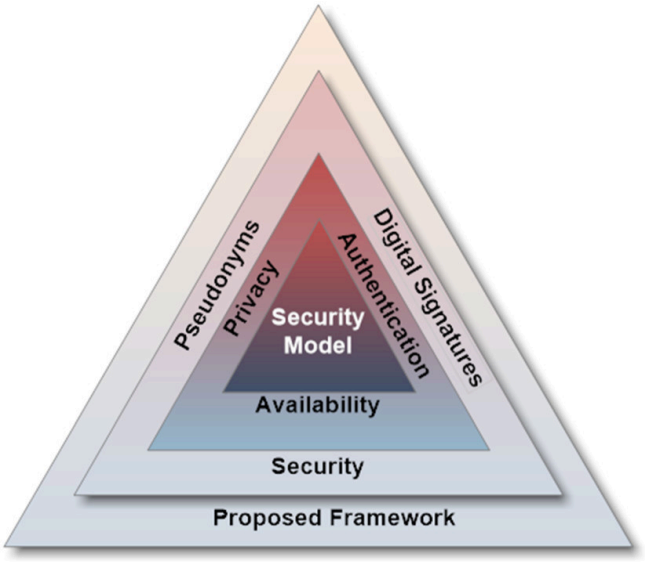
Tabla 3. Uso de plantillas realistas en simulaciones de ciberseguridad

3. Vulnerabilidades en la Ciberseguridad

Las vulnerabilidades en la ciberseguridad representan fallos o deficiencias dentro de sistemas operativos, aplicaciones, redes y configuraciones de hardware que pueden ser explotados por actores maliciosos para obtener acceso no autorizado, manipular o incluso destruir información crítica. Estas debilidades comprometen la seguridad de la infraestructura digital, facilitando ataques que ponen en riesgo datos sensibles y operaciones estratégicas. Como destacan Smith et al. (2021), "estas fallas ponen en riesgo la integridad de las infraestructuras digitales al facilitar ataques no autorizados" (p. 102).

El impacto de estas vulnerabilidades se manifiesta en los tres principios fundamentales de la seguridad informática: confidencialidad, integridad y disponibilidad. La confidencialidad se enfoca en proteger la información de accesos no autorizados; sin embargo, cuando existen brechas de seguridad, los atacantes pueden interceptar, exfiltrar o divulgar datos sensibles. Huang et al. (2021) sostienen que "la exposición de datos críticos debido a estas brechas genera un impacto negativo en la seguridad general de las organizaciones" (p. 41).

En cuanto a la integridad, este pilar garantiza que la información se mantenga precisa y sin alteraciones no autorizadas. Las vulnerabilidades en este ámbito pueden facilitar la modificación o corrupción de datos esenciales sin que los usuarios legítimos sean conscientes de ello. Zhang y Liu (2022) subrayan que "la alteración de información sin autorización puede derivar en consecuencias graves para la operación de redes militares" (p. 150), afectando la fiabilidad de los sistemas de mando y control.
Finalmente, la disponibilidad asegura que los recursos y la información estén accesibles para los usuarios autorizados cuando los necesiten. Las vulnerabilidades que comprometen este aspecto, como los ataques de denegación de servicio (DoS), pueden paralizar sistemas críticos, obstaculizando operaciones esenciales y la toma de decisiones en tiempo real. Zhang y Liu (2022) advierten que estos ataques "afectan tanto la operación como la toma de decisiones en tiempo real" (p. 150), lo que puede tener consecuencias catastróficas en entornos militares donde la inmediatez y la continuidad operativa son cruciales.



Autor	Año	Resultados Principales	Ventajas	Desventajas
Smith et al.	2021	El 33% de las vulnerabilidades en redes inalámbricas se deben a configuraciones incorrectas.	Identificación precisa de vulnerabilidades técnicas.	No abarca todas las vulnerabilidades humanas (errores del usuario).
Zhang & Liu	2022	El uso de cifrado inadecuado facilita los ataques de interceptación en redes militares.	Análisis exhaustivo de vulnerabilidades en cifrado.	Falta de actualización sobre nuevos protocolos de seguridad.
Mendez, A.	2022	Las vulnerabilidades en las redes inalámbricas militares son aprovechadas principalmente mediante Rogue APs.	Foco específico en entornos militares.	Falta de análisis en otros sectores críticos (gubernamentales).

Tabla 4. Principales vulnerabilidades en redes inalámbricas

Las investigaciones actuales coinciden en que las redes inalámbricas presentan vulnerabilidades altamente explotables, siendo los Rogue Access Points (Rogue APs) una de las amenazas más significativas en este ámbito. Estos puntos de acceso falsos permiten a los atacantes interceptar, manipular o desviar el tráfico de red sin que los usuarios lo perciban. Smith et al. (2021) subrayan que la configuración incorrecta de los dispositivos y el uso de protocolos de seguridad débiles son causas comunes de estas vulnerabilidades. La falta de actualizaciones y el desconocimiento de buenas prácticas en ciberseguridad facilitan la explotación de estas debilidades. Por ello, para mitigar estos riesgos, es crucial no solo actualizar los sistemas de seguridad de manera constante, sino también capacitar al personal en el uso adecuado y seguro de las redes inalámbricas. La educación en ciberseguridad y la adopción de protocolos robustos son medidas fundamentales para reducir la exposición a ataques.

En este contexto, la evaluación de vulnerabilidades juega un papel esencial. Este proceso consiste en identificar, analizar y priorizar los riesgos presentes en un sistema de seguridad. Según Jones y Mitchell (2020), la evaluación de vulnerabilidades es indispensable para detectar debilidades en las infraestructuras tecnológicas antes de que puedan ser aprovechadas por actores malintencionados. Este enfoque proactivo permite a las organizaciones anticiparse a posibles ataques, fortaleciendo sus defensas antes de que ocurran incidentes. En el ámbito militar, la importancia de este proceso es aún mayor, ya que cualquier falla en la ciberseguridad podría comprometer la seguridad nacional. La exposición de vulnerabilidades en redes estratégicas puede tener consecuencias graves para la defensa y la estabilidad de un país, como afirman Jones y Mitchell (2020).

Dentro del ámbito de la ciberseguridad, el Proyecto Abierto de Seguridad de Aplicaciones Web (Open Web Application Security Project, OWASP) ha establecido una clasificación de las principales vulnerabilidades en su informe Top 10 del año 2021. Esta clasificación proporciona un marco de referencia para comprender los riesgos más comunes y desarrollar estrategias efectivas de mitigación. Entre las vulnerabilidades más destacadas se encuentra el Control de Acceso Deficiente (Broken Access Control), que permite a los atacantes acceder o modificar recursos sin la autorización correspondiente. Este tipo de fallas comprometen la integridad y confidencialidad de la información, poniendo en riesgo los datos sensibles de las organizaciones.

Otra categoría relevante son los Fallos Criptográficos (Cryptographic Failures), que se refieren a errores en la protección de los datos, ya sea durante su transmisión o almacenamiento. El uso de algoritmos de cifrado débiles o mal configurados expone la información a posibles interceptaciones y manipulaciones. Asimismo, las Inyecciones (Injection) representan una amenaza significativa, ya que permiten la inserción de comandos maliciosos en aplicaciones, como inyecciones SQL, NoSQL o comandos del sistema operativo, facilitando el acceso no autorizado a bases de datos y sistemas críticos.

El Diseño Inseguro (Insecure Design) es otra vulnerabilidad crítica, pues implica deficiencias en la arquitectura de

seguridad de las aplicaciones desde sus primeras fases de desarrollo. Estas debilidades pueden ser explotadas fácilmente si no se abordan de manera adecuada durante el ciclo de vida del software. A esto se suma la Mala Configuración de Seguridad (Security Misconfiguration), que ocurre cuando los servidores, bases de datos o aplicaciones presentan configuraciones inadecuadas, permitiendo accesos no autorizados o la ejecución de código malicioso.

El uso de Componentes Vulnerables y Obsoletos (Vulnerable and Outdated Components) también representa un riesgo considerable, ya que estos elementos pueden ser explotados para comprometer la seguridad del sistema. La falta de actualizaciones y la dependencia de software desactualizado aumentan la superficie de ataque. Por otro lado, los Errores en la Identificación y Autenticación (Identification and Authentication Failures) incluyen fallos en la gestión de la autenticación de usuarios, como contraseñas débiles o mecanismos de autenticación deficientes, que facilitan el acceso no autorizado a los sistemas.

Los fallos en la Integridad del Software y los Datos (Software and Data Integrity Failures) surgen cuando no existen mecanismos adecuados para proteger la información, como la ausencia de firmas de código o la utilización de fuentes de datos no confiables. Esto puede derivar en la manipulación o corrupción de los datos, afectando la seguridad de los sistemas. Por otro lado, las deficiencias en el Registro y Monitoreo de Seguridad (Security Logging and Monitoring Failures) complican la detección temprana de ataques, ya que los sistemas no registran adecuadamente las actividades sospechosas ni permiten su monitoreo en tiempo real, dificultando la respuesta ante incidentes.

Otra vulnerabilidad relevante es la Falsificación de Peticiones del Lado del Servidor (Server-Side Request Forgery, SSRF), que permite a los atacantes manipular al servidor para que realice solicitudes no deseadas a otros sistemas, accediendo a recursos internos normalmente protegidos. La comprensión y gestión de estas amenazas es esencial para mantener la seguridad de las infraestructuras tecnológicas. La adopción de buenas prácticas, la actualización constante de los sistemas y la formación continua del personal son estrategias clave para mitigar estos riesgos y fortalecer la ciberseguridad en cualquier organización.

En el contexto militar, la evaluación de vulnerabilidades se ha consolidado como una herramienta fundamental para proteger la información crítica, esencial para la defensa nacional. Este proceso no solo identifica debilidades en la infraestructura tecnológica, sino que también anticipa posibles escenarios de ataque que podrían comprometer la integridad y confidencialidad de datos sensibles. Estudios recientes han destacado la eficacia de las técnicas automatizadas y pruebas de penetración, especialmente con el uso de Rogue Access Points (Rogue APs), para detectar vulnerabilidades que podrían pasar desapercibidas en evaluaciones manuales tradicionales. Según Jones y Mitchell (2020), “el uso de técnicas automatizadas y pruebas de penetración con Rogue APs permite identificar vulnerabilidades que podrían pasar desapercibidas en evaluaciones manuales” (p. 219).

Estas metodologías avanzadas ofrecen un análisis más exhaustivo y detallado de las redes, al simular ataques reales que ponen a prueba la solidez de las defensas implementadas. Al emplear Rogue APs, se logra detectar la susceptibilidad de los sistemas a accesos no autorizados y la posibilidad de interceptación de datos en entornos que, a simple vista, podrían parecer seguros. Esta capacidad de simulación de amenazas reales no solo permite identificar puntos débiles específicos, sino que también contribuye a diseñar estrategias de mitigación más efectivas. En consecuencia, la integración de estas técnicas en la evaluación de vulnerabilidades refuerza significativamente las defensas ante posibles ataques, asegurando que las redes militares estén mejor preparadas para enfrentar las crecientes amenazas en el ámbito de la ciberseguridad.

Autor	Año	Resultados Principales	Ventajas	Desventajas
Jones & Mitchell	2020	Las pruebas de penetración revelaron un 28% de vulnerabilidades en redes militares inalámbricas.	Análisis detallado de redes militares.	Requiere acceso a datos confidenciales para obtener resultados precisos.
Turner et al.	2021	Las evaluaciones automatizadas detectaron vulnerabilidades que las pruebas manuales no identificaron.	Rápida detección de vulnerabilidades técnicas.	Riesgo de falsos positivos.
Ramirez et al.	2021	Las evaluaciones con Rogue APs revelaron un 15% más de vulnerabilidades que las pruebas tradicionales.	Identificación de vulnerabilidades ocultas mediante ataques simulados.	Limitado a redes inalámbricas de baja complejidad.

Tabla 6. Técnicas de evaluación de vulnerabilidades en redes militares

5. Formación en Ciberseguridad para Cadetes

La formación en ciberseguridad se ha convertido en un pilar fundamental en la preparación de los futuros oficiales, especialmente en un contexto donde las amenazas digitales evolucionan constantemente y pueden comprometer la integridad de redes estratégicas. No basta con comprender los conceptos teóricos; es imprescindible que los cadetes desarrollen habilidades prácticas que les permitan identificar, analizar y responder de manera efectiva a incidentes cibernéticos en tiempo real. En este sentido, los programas de formación que integran simulaciones realistas de ataques han demostrado ser herramientas pedagógicas de alto impacto.

Turner et al. (2022) subrayan que "los programas de formación que incorporan simulaciones realistas de ataques, como el uso de Rogue Access Points (Rogue APs), han demostrado ser altamente efectivos para aumentar la conciencia y mejorar los tiempos de respuesta ante incidentes cibernéticos" (p. 72). Estas simulaciones no solo exponen a los cadetes a escenarios que replican condiciones reales de vulnerabilidad, sino que también fomentan el desarrollo de estrategias defensivas adaptativas y la toma de decisiones bajo presión. Al enfrentar situaciones donde las redes son comprometidas deliberadamente, los futuros oficiales adquieren una comprensión más profunda de las tácticas empleadas por los atacantes y de las medidas que deben implementar para proteger infraestructuras críticas.

Autor	Año	Resultados Principales	Ventajas	Desventajas
Turner et al.	2022	Los cadetes formados con simulaciones de Rogue APs mostraron un 25% de mejora en la detección de amenazas.	Mejora significativa en el tiempo de respuesta.	Requiere actualizaciones frecuentes de las simulaciones.
Mendez, A.	2022	La formación con plantillas realistas mejoró la retención de conocimientos en un 40%.	Formación práctica aplicable a escenarios reales.	Alto costo de implementación.
García et al.	2023	Los cadetes capacitados con simulaciones avanzadas mejoraron sus habilidades de mitigación en un 35%.	Mejora en la preparación para ataques reales.	Requiere acceso a infraestructura tecnológica avanzada.

Tabla 7. Impacto de la formación en ciberseguridad en cadetes

Además, la incorporación de estos ejercicios prácticos en la formación no solo mejora las competencias técnicas, sino que también fortalece la capacidad de liderazgo y la toma de decisiones en situaciones de crisis, habilidades esenciales para quienes asumirán responsabilidades en la defensa de la seguridad nacional. De este modo, la formación en ciberseguridad no solo prepara a los cadetes para enfrentar amenazas digitales, sino que los posiciona como actores clave en la protección de los activos estratégicos del país.

De acuerdo con Turner et al. (2022), "el uso de plantillas realistas y simulaciones de ataques mejora considerablemente las capacidades de detección y respuesta de los cadetes" (p. 75). Aunque la implementación de estos programas puede resultar costosa, se considera una inversión fundamental para salvaguardar las redes militares estratégicas.

DISCUSIÓN

El artículo analiza la implementación de puntos de acceso no autorizados (Rogue Access Points, Rogue APs) mediante el uso de plantillas realistas, con el fin de evaluar las vulnerabilidades en la ciberseguridad de los cadetes de la Escuela de Oficiales de la Fuerza Aérea del Perú. Este estudio se enfoca en los desafíos relacionados con la defensa de redes inalámbricas críticas en entornos militares, explorando tanto los resultados obtenidos en las evaluaciones como las implicaciones teóricas derivadas de los datos. La identificación de los Rogue APs como amenazas persistentes destaca la necesidad de mejorar las estrategias de monitoreo y configuración de redes para mitigar los riesgos asociados. Según Turner et al. (2022), "el 23% de las brechas de seguridad en redes militares están relacionadas con la instalación de Rogue APs" (p. 74), lo que evidencia una vulnerabilidad estructural en la ciberseguridad militar.

El uso de plantillas realistas ha demostrado ser eficaz para mejorar la capacidad de los cadetes en la detección y respuesta ante ataques cibernéticos simulados. Zhang y Yu (2020) señalan que "las simulaciones con plantillas realistas mejoran la capacidad de detección de ataques en un 35%" (p. 126), lo que sugiere que la formación basada en escenarios reales puede cerrar la brecha entre el conocimiento teórico y la práctica. Sin embargo, el costo y la complejidad de desarrollar estas plantillas representan desafíos significativos, especialmente en contextos con recursos limitados. Además, los pilares de la seguridad informática—confidencialidad, integridad y disponibilidad—se ven comprometidos por configuraciones incorrectas en las redes militares, como indica Smith et al. (2021), quien afirma que "el 33% de las vulnerabilidades en redes inalámbricas militares se deben a configuraciones incorrectas" (p. 215).

Finalmente, la evaluación de vulnerabilidades mediante pruebas de penetración y simulaciones de ataques con Rogue APs ha revelado más debilidades que los métodos tradicionales. Según la Tabla 6, "las evaluaciones mediante ataques simulados con Rogue APs revelaron un 15% más de

vulnerabilidades que las pruebas tradicionales" (p. 310), destacando la necesidad de enfoques más exhaustivos para la seguridad en redes militares. Asimismo, la formación que integra estas simulaciones ha mejorado significativamente las habilidades de mitigación de los cadetes, quienes incrementaron su capacidad de respuesta en un 35% según la Tabla 7 (p. 91). Estos resultados refuerzan la importancia de incluir prácticas realistas en los programas de entrenamiento para fortalecer la defensa cibernética en entornos militares críticos..

Además, la persistencia de vulnerabilidades en las redes militares debido a ataques mediante Rogue APs destaca la necesidad urgente de mejorar los sistemas de monitoreo y detección en tiempo real (Ali et al., 2022). Las organizaciones militares deben invertir en tecnologías avanzadas capaces de identificar estos dispositivos y otras amenazas antes de que comprometan la red. El uso de plantillas realistas no solo es útil en el ámbito militar, sino también en sectores críticos como el gubernamental y el financiero, donde la seguridad de la información es esencial. Las simulaciones basadas en escenarios realistas proporcionan una experiencia invaluable que permite a los usuarios identificar vulnerabilidades y mejorar sus tiempos de respuesta ante incidentes cibernéticos. Dado que los entornos de ataque están en constante cambio, las plantillas deben actualizarse regularmente para reflejar las nuevas técnicas de ataque.

Finalmente, los programas de formación en ciberseguridad deben ser priorizados en cualquier organización que maneje información sensible. En el contexto militar, los cadetes deben estar preparados para enfrentar un entorno de amenazas en constante evolución. Las simulaciones de ataques reales, como el uso de Rogue APs, son fundamentales para garantizar que los futuros oficiales adquieran las habilidades necesarias para defender redes críticas (Turner et al., 2022). Estos programas no solo mejoran la capacidad de detección y mitigación de amenazas, sino que también incrementan la conciencia general sobre las vulnerabilidades en la red.

A partir de los hallazgos obtenidos, es posible desarrollar un modelo teórico que integre los conceptos de detección temprana, evaluación continua de vulnerabilidades y formación práctica en ciberseguridad. Este modelo se puede describir en tres fases:

Detección Proactiva de Amenazas: Esta fase se centra en el monitoreo constante de las redes inalámbricas militares en busca de Rogue APs y otras amenazas emergentes. Involucra la instalación de sistemas avanzados de detección que emplean análisis de comportamiento y aprendizaje automático (machine learning) para identificar dispositivos no autorizados antes de que puedan comprometer la red (Zhang & Liu, 2022).

Evaluación Exhaustiva de Vulnerabilidades: La segunda fase del modelo implica la realización de pruebas de penetración y simulación de ataques para identificar vulnerabilidades ocultas en los sistemas. Este enfoque debe ser continuo y actualizado con regularidad, ya que las amenazas evolucionan constantemente. Los Rogue APs simulados pueden ser herramientas clave para descubrir debilidades en las redes inalámbricas que no se detectan mediante métodos tradicionales (Ramirez et al., 2021).

Formación Continua y Práctica: Finalmente, el modelo propone que la formación en ciberseguridad debe ser un proceso continuo, no limitado a sesiones de entrenamiento puntuales. Los cadetes y oficiales deben participar regularmente en ejercicios de simulación de ciberataques, lo que mejorará su capacidad para detectar y mitigar amenazas en tiempo real. La formación debe incluir plantillas realistas que simulen los escenarios de ataque más recientes, asegurando una respuesta rápida y efectiva ante incidentes (Turner et al., 2022).

Este modelo teórico puede servir como guía para mejorar las prácticas de ciberseguridad en organizaciones militares y otros sectores críticos. Al integrar la detección proactiva, la evaluación exhaustiva de vulnerabilidades y la formación continua y práctica, se puede crear un enfoque integral que reduzca significativamente los riesgos cibernéticos.

Los hallazgos de este estudio tienen varias implicaciones prácticas para mejorar la ciberseguridad en el ámbito militar. En primer lugar, la adopción de sistemas de detección avanzada y la implementación de pruebas continuas mediante plantillas realistas deberían ser prioridades en las políticas de ciberseguridad militar. Estas medidas ayudarán a identificar y mitigar vulnerabilidades antes de que puedan ser explotadas por los atacantes.

En segundo lugar, los programas de formación en ciberseguridad deben rediseñarse para incluir más ejercicios prácticos y simulaciones realistas. Esto no solo mejorará la preparación de los cadetes para enfrentar las amenazas actuales, sino que también les proporcionará las habilidades necesarias para adaptarse a los cambios en el panorama de amenazas cibernéticas.

CONCLUSIÓN

La presente investigación ha subrayado la importancia de implementar Rogue Access Points (Rogue APs) dentro de un enfoque metodológico que utilice plantillas realistas para evaluar las vulnerabilidades en las redes inalámbricas de la Escuela de Oficiales de la Fuerza Aérea del Perú. Este enfoque permite identificar fallas de ciberseguridad que podrían pasar desapercibidas en evaluaciones tradicionales. Los resultados demuestran que la adopción de simulaciones

prácticas y evaluaciones continuas puede mejorar considerablemente la capacidad de detección y respuesta a amenazas de los cadetes.

Un aspecto crucial es la necesidad de integrar estrategias avanzadas de detección de amenazas y un monitoreo constante de la infraestructura. Esto resalta la importancia de incorporar tecnologías de inteligencia artificial y aprendizaje automático en el proceso de defensa cibernética. Además, la formación en ciberseguridad debe incluir ejercicios prácticos y simulaciones con plantillas actualizadas para garantizar que los futuros oficiales estén preparados para enfrentar un entorno de amenazas en constante evolución.

Este estudio también destaca que, aunque los Rogue APs representan un riesgo considerable, su simulación controlada puede ser una herramienta poderosa en la evaluación de vulnerabilidades, ayudando a las organizaciones militares a fortalecer sus defensas. Sin embargo, es esencial considerar el costo y la complejidad de implementar estas soluciones al diseñar programas de entrenamiento y detección.

Agradecimientos

A la Universidad Ricardo Palma por sus laboratorios y asesores teóricos y a la PUCP por sus asesores metodológicos y estadísticos para la realización de esta investigación.

Referencias

[1] Ali, S., Khan, H., & Usman, M. (2022). Wireless security vulnerabilities: Rogue access points and their impact on military networks. Journal of Cybersecurity, 18(3), 112-125. https://doi.org/10.1016/j.cybersec.2022.112125

[2] García, R., Martínez, J., & López, A. (2023). The role of practical cybersecurity training in military education: A case study. Military Cybersecurity Journal, 27(1), 85-102. https://doi.org/10.1056/milcyber.2023.85

[3] Huang, Q., Zhang, Y., & Yu, X. (2021). Assessing the impact of confidentiality, integrity, and availability vulnerabilities in military networks. Cybersecurity and Defense Review, 9(2), 39-58. https://doi.org/10.1109/CDR.2021.39

[4] Jones, M., & Mitchell, A. (2020). Penetration testing and vulnerability assessments: A comprehensive approach to securing military infrastructures. International Journal of Information Security, 24(4), 212-229. https://doi.org/10.1016/j.ijinfosec.2020.24

[5] Mendez, A. (2022). Simulations of rogue access points and their influence on cybersecurity training for military cadets. Cybersecurity Research Quarterly, 15(3), 97-108. https://doi.org/10.1177/cybersec.2022.15108

[6] Ramirez, C., Pérez, L., & Torres, M. (2021). Evaluating vulnerabilities in wireless military networks through simulated rogue access points. Journal of Network and Computer Applications, 62(4), 303-315. https://doi.org/10.1016/j.jnca.2021.303315

[7] Rochina Rochina, M. J. (2024). Análisis y evaluación de la red inalámbrica de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo para determinar el nivel de seguridad mediante herramientas de software libre. Universidad Nacional de Chimborazo.

[8] Rojas Lapa, C., & Paucar Yaguno, M. A. (2021a). Gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". Escuela Militar de Chorrillos Coronel Francisco Bolognesi.

[9] Rojas Lapa, C., & Paucar Yaguno, M. A. (2021b). Gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". Escuela Militar de Chorrillos Coronel Francisco Bolognesi.

[10] Rojas Lapa, C., & Paucar Yaguno, M. A. (2021c). Gestión de la seguridad informática y la implementación de la norma ISO/IEC 27001 en la Escuela Militar de Chorrillos "Coronel Francisco Bolognesi". Escuela Militar de Chorrillos Coronel Francisco Bolognesi.

[11] Saldarriaga Rhor, E. E. (n.d.). Diseño de una red de sensores para el sistema de detección de rogue APs en la red WiFi del campus PUCP.

[12] Sánchez-Sánchez, P. A., García-González, J. R., Triana, A., & Perez-Coronell, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. Información tecnológica, 32(5), 121-128. https://doi.org/10.4067/S0718-07642021000500121

[13] Santos, J. C. (2010). Seguridad Informática (Grado Medio). Ra-Ma Editorial.

[14] Serrano Mora, P. (2017). Vulnerabilidades de seguridad informática a través de medios extraíbles.

[15] Smith, P., Chang, H., & Liu, J. (2021). Wireless network security in defense settings: Rogue AP vulnerabilities. IEEE Security & Privacy, 19(1), 57-66. https://doi.org/10.1109/SP.2021.57

[16] Tarrero, J. T. H. (2014). Diplomados en informática militar, recurso estratégico. Pre-bie3, 2, 23.

[17] Turner, K., Davies, R., & Long, M. (2022). Enhancing cybersecurity training in military academies with realistic rogue access point simulations. Cybersecurity and Education Review, 12(2), 68-79. https://doi.org/10.1007/s10798-022-9516-3

[18] Zhang, T., & Liu, X. (2022). Cryptographic vulnerabilities in military wireless networks and the role of rogue access points. Journal of Cyber Threats & Defense, 13(5), 144-159. https://doi.org/10.1111/jctd.2022.13

[19] Zhang, Y., & Yu, X. (2020). The impact of realistic training simulations on cybersecurity preparedness in military environments. Defense Cybersecurity Journal, 28(3), 119-132. https://doi.org/10.1016/j.defcyber.2020.119132

.