Amenazas Invisibles: Una Revisión de Seguridad, Malware y Defensa en Sistemas Operativos

Castro Mamani Sebastian Adriano
Huamaní Vasquez Juan José
Yabar Carazas Melvin Jarred
Zela Flores Gabriel Frank Krisna
Escuela Profesional de Ingeniería de Software
Universidad La Salle

***Abstract*—En la actualidad, la seguridad informática se ha convertido en una preocupación constante debido al aumento de ataques cada vez más sofisticados, como el malware, el software de explotación y los ataques internos. Este artículo presenta una revisión de estudios recientes relacionados con los desafíos actuales en seguridad, especialmente aquellos que involucran el uso de inteligencia artificial y ataques adversariales en sistemas operativos. Se analiza cómo los atacantes logran evadir sistemas de detección mediante técnicas cada vez más complejas y cómo se están desarrollando defensas para contrarrestar estas amenazas. Además, se incluye un enfoque específico en el contexto peruano, considerando la realidad de las pequeñas y medianas empresas (PYMES) y su nivel de preparación frente a estos riesgos.**

***Index Terms*—Seguridad informática, malware, ataques adversariales, defensas, inteligencia artificial, sistemas operativos, PYMES, ISO 27001.**

I. Introducción

La seguridad en los sistemas informáticos se ha vuelto un pilar fundamental dentro del mundo tecnológico actual. A medida que las organizaciones y usuarios dependen cada vez más de la tecnología, también lo hacen los atacantes, quienes aprovechan vulnerabilidades en los sistemas para robar información, interrumpir servicios o causar daños económicos. En particular, el malware ha evolucionado considerablemente, adoptando formas más difíciles de detectar y utilizando técnicas que incluso engañan a sistemas de inteligencia artificial entrenados para identificar amenazas (Aryal et al., 2021; Ling et al., 2021).

Una de las preocupaciones más recientes en este campo es el uso de ataques adversariales: entradas diseñadas para confundir modelos de aprendizaje automático utilizados en la detección de amenazas. Este tipo de ataques ha sido estudiado tanto en entornos de Windows como en Android, mostrando que los sistemas de defensa todavía presentan muchas debilidades frente a estrategias nuevas y creativas por parte de los atacantes (He et al., 2023; Expert Systems with Applications, 2024).

En el caso del Perú, muchas pequeñas y medianas empresas aún carecen de políticas de seguridad sólidas. Esto se vuelve especialmente crítico cuando se considera que, al no tener estructuras robustas, son más vulnerables frente a ataques tanto internos como externos. Según un estudio realizado en Ayacucho, la implementación de un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001 podría marcar una diferencia significativa en la protección de los datos empresariales (Lima Loayza, 2024).

Este artículo busca ofrecer una revisión clara y actualizada sobre el panorama de la seguridad informática, centrándose en el comportamiento del malware, los ataques adversariales y las estrategias de defensa actuales. Además, se propone generar conciencia sobre la importancia de aplicar buenas prácticas de seguridad, tanto en grandes organizaciones como en contextos más cercanos como el peruano.

II. Método

Este artículo fue elaborado a partir de una revisión bibliográfica centrada en investigaciones publicadas entre los años 2021 y 2024. Se seleccionaron seis fuentes principales, incluyendo artículos científicos indexados en IEEE, arXiv, ScienceDirect y repositorios académicos como el de la Universidad Nacional de San Cristóbal de Huamanga (UNSCH).

Los criterios de selección fueron:

Actualidad (publicaciones de los últimos 5 años)

Relevancia directa con los subtemas: malware, ataques internos, software de explotación, defensas y seguridad en sistemas

Enfoque técnico y aplicado, especialmente en contextos reales y entornos operativos

También se consideró incluir una tesis nacional que aportara una visión local sobre la implementación de estándares de seguridad como ISO/IEC 27001 en empresas peruanas. Todas las referencias fueron analizadas en profundidad para identificar los hallazgos más importantes y así integrarlos de forma coherente en las secciones temáticas del desarrollo.

Esta metodología permite construir una visión actualizada y bien fundamentada sobre el estado de la seguridad informática, así como sobre los retos técnicos y organizacionales que implica.

III. Desarrollo y discusión

III-A. Conceptos, características, ventajas, desventajas e importancia

La seguridad informática es el conjunto de prácticas, técnicas, políticas y herramientas destinadas a proteger los sistemas de información frente a accesos no autorizados, alteraciones, destrucción o robo de datos. Esta protección se aplica tanto a nivel físico como lógico, abarcando desde la infraestructura de red hasta los algoritmos que corren sobre un sistema operativo.
Uno de los conceptos clave es el modelo de la tríada CIA (Confidencialidad, Integridad y Disponibilidad), que define los pilares fundamentales de la seguridad. Sin al menos uno de estos tres elementos, un sistema no puede considerarse seguro.

Características principales:

–Multinivel: La seguridad debe aplicarse en todos los niveles del sistema: hardware, software, redes, usuarios.
–Proactiva y reactiva: No solo se trata de responder a incidentes, sino de anticiparlos mediante monitoreo, auditoría y análisis de vulnerabilidades.
–Dinámica: Las amenazas evolucionan constantemente, lo que obliga a actualizar las estrategias de defensa con regularidad (Aryal et al., 2021).

Ventajas:

–Protección de la información crítica, tanto personal como empresarial.
–Prevención de pérdidas económicas debidas a ciberataques, como los causados por ransomware o malware.
–Cumplimiento normativo, especialmente en sectores regulados como el financiero o el de salud. –Mejora de la confianza del usuario, un factor clave en servicios digitales y plataformas en línea.

Desventajas:

–Costo de implementación: Implementar soluciones de seguridad avanzadas puede ser costoso, especialmente para pequeñas empresas (Lima Loayza, 2024).
–Complejidad técnica: Algunas herramientas requieren conocimientos especializados y personal capacitado.
–Impacto en el rendimiento: Ciertos sistemas de defensa pueden ralentizar procesos si no están bien optimizados.

La importancia de la seguridad en sistemas operativos radica en que estos son el núcleo que gestiona los recursos y controla el acceso a la información. Si un atacante logra comprometer el sistema operativo, tiene acceso potencial a todo lo que se ejecuta en él. Es por eso que hoy en día se implementan mecanismos como la autenticación de múltiples factores, las políticas de control de acceso, y las auditorías automáticas.

Además, con el auge de la inteligencia artificial y el aprendizaje automático, los atacantes han comenzado a desarrollar métodos para evadir los sistemas de detección tradicionales, utilizando técnicas como los ataques adversariales. Estos consisten en modificar archivos maliciosos apenas lo suficiente como para que no sean detectados por modelos entrenados, mientras siguen cumpliendo su función dañina (Ling et al., 2021).

Por ello, no solo basta con instalar un antivirus: se requiere una visión integral que incluya políticas claras, herramientas bien configuradas y personal capacitado. La seguridad informática no es un gasto, sino una inversión que previene problemas mayores en el futuro.

III-B. Software de explotación

El software de explotación (exploit) es un programa o fragmento de código que aprovecha una vulnerabilidad en un sistema operativo o aplicación para alterar su comportamiento normal. Estos exploits son utilizados con frecuencia para obtener acceso no autorizado, ejecutar código malicioso, robar información o comprometer la disponibilidad de servicios.

Existen diferentes tipos de exploits, dependiendo de la vulnerabilidad que aprovechan. Por ejemplo, algunos se enfocan en fallas de desbordamiento de búfer, mientras que otros atacan errores de configuración o servicios mal protegidos. En muchos casos, los atacantes automatizan estos procesos mediante kits de explotación (exploit kits), lo que facilita los ataques incluso para usuarios con pocos conocimientos técnicos.

Según Aryal et al. (2021), en los últimos años se ha observado un crecimiento en el uso de exploits diseñados para evadir modelos de aprendizaje automático usados en sistemas de detección de malware. Estos exploits son particularmente complejos porque no solo deben funcionar como un ataque, sino también engañar a los modelos inteligentes entrenados para reconocer patrones maliciosos. Ling et al. (2021) detallan cómo los ejecutables de Windows (archivos PE) pueden ser modificados sutilmente con código que no afecta su funcionamiento externo pero que logra pasar desapercibido para los antivirus o clasificadores automáticos. Esto convierte al software de explotación en una herramienta doblemente peligrosa: causa daño y evita ser detectada.

He et al. (2023) muestran cómo, en el caso de Android, los atacantes pueden modificar aplicaciones legítimas insertando exploits que manipulan el flujo de ejecución interno, logrando saltarse validaciones y ejecutando instrucciones maliciosas solo bajo ciertas condiciones. Esto es especialmente grave porque muchas aplicaciones en Android tienen permisos amplios por defecto. Además, la revisión realizada por Expert Systems with Applications (2024) indica que los ataques

adversariales utilizados en sistemas de seguridad basados en deep learning, como redes neuronales convolucionales o modelos transformers, pueden ser combinados con software de explotación para lanzar ataques altamente eficaces y difíciles de prevenir. El uso de exploits también plantea retos específicos en el contexto peruano. Muchas empresas pequeñas carecen de políticas de actualización de software, lo que deja abiertas vulnerabilidades conocidas por largos periodos de tiempo. Lima Loayza (2024) destaca que una de las prácticas más básicas pero también más olvidadas es la gestión adecuada de parches y actualizaciones, la cual podría prevenir muchos ataques basados en exploits.

En resumen, el software de explotación representa uno de los medios más efectivos que tienen los atacantes para comprometer sistemas. Su combinación con técnicas de evasión y manipulación de modelos de inteligencia artificial lo convierte en una amenaza crítica para la seguridad actual, tanto a nivel global como local.

III-C. Ataques internos

Los ataques internos son aquellos que provienen desde dentro de la organización o sistema, ya sea por parte de empleados, exempleados, contratistas o usuarios con acceso legítimo que utilizan sus privilegios para causar daño. Este tipo de amenaza es particularmente compleja, ya que los atacantes suelen tener conocimiento del entorno, credenciales válidas y acceso directo a información sensible.

A diferencia de los ataques externos, los internos no siempre requieren vulnerabilidades técnicas: basta con un mal uso intencional de los recursos disponibles. Por esta razón, se les considera una de las formas más peligrosas de amenaza para la seguridad informática.

Según el estudio de Lima Loayza (2024), muchas empresas peruanas, especialmente las PYMES, no cuentan con mecanismos de auditoría ni políticas de control de acceso definidas, lo que las hace vulnerables a este tipo de ataques. En varios casos estudiados, el acceso no supervisado a bases de datos y sistemas administrativos fue utilizado para filtrar información confidencial sin que existiera un sistema que alertara de este comportamiento.

La falta de segmentación de permisos y el uso de cuentas genéricas o compartidas también agrava el riesgo. Tal como lo destaca el artículo de IEEE COMST (2022), los ataques internos pueden combinarse con malware o exploits para escalar privilegios, borrar rastros o incluso instalar puertas traseras (backdoors) que permitan accesos futuros sin levantar sospechas.

En ambientes más sofisticados, como los estudiados por Aryal et al. (2021) y Ling et al. (2021), se ha visto que algunos ataques internos se valen de técnicas adversariales para modificar archivos o procesos sin ser detectados por los sistemas de defensa automatizados. Por ejemplo, un usuario interno con conocimientos de programación puede modificar un ejecutable legítimo con pequeñas variaciones para que realice acciones no autorizadas, sin ser detectado por antivirus o filtros basados en aprendizaje automático.

Además, en entornos móviles como Android, los ataques internos pueden tomar la forma de aplicaciones instaladas por usuarios con intenciones maliciosas o ingenuamente por empleados que no están informados sobre los riesgos. He et al. (2023) indican que muchas aplicaciones pueden actuar como “caballos de Troya”, recolectando información y enviándola sin consentimiento, aprovechando permisos otorgados durante la instalación.

La mitigación de este tipo de amenazas requiere un enfoque múltiple que incluya: políticas de mínimo privilegio, monitoreo constante de actividad, segmentación de redes, autenticación robusta y concientización del personal. Como se concluye en el artículo de Expert Systems with Applications (2024), ninguna herramienta por sí sola es suficiente si no se acompaña de una cultura de seguridad al interior de la organización.

En definitiva, los ataques internos son una amenaza real y silenciosa. Su detección y prevención deben formar parte central de cualquier estrategia de seguridad informática moderna.

III-D. Malware

El término malware proviene de “malicious software” (software malicioso) y hace referencia a cualquier tipo de programa diseñado con el propósito de dañar, interrumpir o acceder de forma no autorizada a un sistema. El malware puede tomar muchas formas: virus, gusanos, troyanos, spyware, ransomware, entre otros. En los últimos años, el uso de malware se ha sofisticado a tal punto que incluso puede evadir modelos de detección avanzados basados en inteligencia artificial.

De acuerdo con Aryal et al. (2021), los atacantes han comenzado a diseñar variantes de malware que son funcionalmente equivalentes a sus versiones originales, pero modificadas en su estructura para engañar a los sistemas de detección. Estos ataques se conocen como adversarial malware y representan un gran reto para los antivirus tradicionales y los modelos de aprendizaje automático.
Uno de los entornos más vulnerables al malware es el sistema operativo Windows, especialmente debido a su amplia distribución en ambientes empresariales y personales. Ling et al. (2021) señalan que los archivos ejecutables PE pueden ser alterados con técnicas como padding (agregado de bytes innecesarios), section injection (inyección en secciones) o code obfuscation (ofuscación del código), logrando que el malware pase desapercibido para los clasificadores de seguridad sin

perder su funcionalidad maliciosa. Por otro lado, en entornos móviles como Android, el malware también se ha convertido en una amenaza constante. He et al. (2023) demuestran cómo los atacantes pueden modificar aplicaciones legítimas o crear clones maliciosos que, al instalarse, actúan como troyanos recolectando información privada, enviando datos a servidores externos o activando funciones sin conocimiento del usuario. Muchas veces, este tipo de malware no requiere exploits complejos, sino simplemente permisos concedidos de forma imprudente.

TABLE I
TIPOS COMUNES DE MALWARE Y SUS COMPORTAMIENTOS

Tipo de malware	**Acciones típicas**	**Sistema afectado**
Troyano	Se oculta como app legítima y filtra información	Android, Windows
Ransomware	Encripta datos y exige rescate	Windows, Linux
Spyware	Monitorea actividades sin consentimiento	Windows, Android
Adversarial malware	Evita modelos de detección IA	Android, Windows

Fuente: Adaptado de Aryal et al. (2021), Ling et al. (2021), He et al. (2023).

Además, Expert Systems with Applications (2024) resalta que el malware moderno suele combinar varias técnicas a la vez: evasión, persistencia, polimorfismo, y técnicas adversariales. Esto significa que el malware puede cambiar su estructura con cada ejecución, resistir intentos de eliminación y atacar directamente los modelos de detección entrenados, haciendo mucho más difícil su identificación.

En el contexto nacional, Lima Loayza (2024) advierte que las pequeñas y medianas empresas del Perú son particularmente vulnerables al malware, debido a la falta de políticas de seguridad, uso de software pirata y ausencia de sistemas de respaldo. Esta situación permite que el malware no solo acceda a datos críticos, sino que también tenga efectos devastadores sobre la operación diaria de las empresas.

En resumen, el malware ha dejado de ser una simple molestia informática para convertirse en un arma digital compleja y estratégica. Su evolución actual requiere defensas inteligentes, monitoreo constante y, sobre todo, una cultura de prevención activa tanto en los usuarios como en las organizaciones.

III-E. Defensas

Frente a la creciente sofisticación de las amenazas cibernéticas, las estrategias de defensa han tenido que evolucionar más allá de las soluciones tradicionales como antivirus o firewalls. Actualmente, las defensas más efectivas combinan herramientas tecnológicas, prácticas organizacionales y modelos de inteligencia artificial para anticiparse a los ataques, detectarlos y contener su impacto.

Una de las técnicas más estudiadas en los últimos años es el uso de modelos de aprendizaje automático y redes neuronales para identificar patrones anómalos o archivos maliciosos. Sin embargo, como se ha mencionado en secciones anteriores, estos modelos pueden ser vulnerables a ataques adversariales diseñados para engañarlos. Por eso, han surgido diversas técnicas de defensa como el adversarial retraining, la regularización o el uso de redes robustas que resisten perturbaciones (Expert Systems with Applications, 2024).

TABLE II
COMPARATIVA DE MÉTODOS DE DEFENSA EN SISTEMAS OPERATIVOS

Método	**Ventaja principal**	**Limitación**
Antivirus tradicional	Fácil de implementar y mantener	Vulnerable a malware nuevo
Análisis de comportamiento	Detecta amenazas desconocidas	Requiere más recursos
Aprendizaje automático	Precisión adaptativa	Sensible a ataques adversariales
Sandboxing (Android)	Aísla procesos maliciosos	No previene instalación inicial

Fuente: Adaptado de Aryal et al. (2021), Ling et al. (2021), He et al. (2023), Li et al. (2024).

Según Aryal et al. (2021), uno de los enfoques más prometedores consiste en combinar modelos de detección clásicos (basados en firmas o reglas) con modelos de comportamiento que analizan cómo actúa un archivo en el sistema. Este enfoque híbrido permite identificar malware aunque haya sido modificado en su estructura para evadir un detector basado solo en firmas.

En sistemas operativos como Windows, las defensas incluyen la segmentación de memoria, las listas de control de acceso (ACLs), y la restricción de ejecución de programas no autorizados. Ling et al. (2021) proponen además mecanismos de validación de integridad para los ejecutables, y monitoreo de actividad en tiempo real para detectar procesos sospechosos incluso si no son detectados por el antivirus.

En entornos Android, las defensas se centran en la revisión de permisos, la detección de comportamientos anómalos en aplicaciones instaladas y la limitación del acceso a funciones críticas del sistema operativo. He et al. (2023) indican que muchas soluciones modernas también incluyen mecanismos de sandboxing (ejecución en entornos controlados) para minimizar los daños en caso de infección.

Desde un punto de vista organizacional, una de las defensas más importantes es la implementación de políticas de seguridad estructuradas. En su tesis, Lima Loayza (2024) demuestra que aplicar el estándar ISO/IEC 27001 permite a las PYMES establecer controles adecuados, reducir el riesgo de ataques internos y asegurar la disponibilidad de los datos.

Entre las prácticas más efectivas se encuentran:

- Establecer niveles de acceso diferenciados.
- Capacitar al personal en ciberseguridad.
- Realizar copias de seguridad regulares.
- Monitorear los sistemas de forma continua.

Finalmente, el artículo de IEEE COMST (2022) enfatiza que ningún sistema es 100 porciento seguro, por lo que es esencial implementar defensas en capas (modelo de defensa en profundidad), con múltiples barreras que puedan contener o ralentizar a un atacante en cada etapa del intento de intrusión.

En conclusión, las defensas actuales deben ser adaptativas, integradas y conscientes del contexto. No basta con una única herramienta o política: se requiere un enfoque completo que incluya tecnología, procesos y educación. Solo así se podrá estar un paso adelante frente a las amenazas cada vez más avanzadas del panorama digital actual.

III-F. Impacto económico de los ataques y la brecha en la preparación

Más allá de los aspectos técnicos, los ataques informáticos tienen un fuerte impacto económico y operativo para las organizaciones. Según IEEE COMST (2022), los costos globales relacionados con ciberataques superaron los 6 billones de dólares en 2021, y se estima que podrían alcanzar los 10 billones en 2025 si no se refuerzan las defensas.

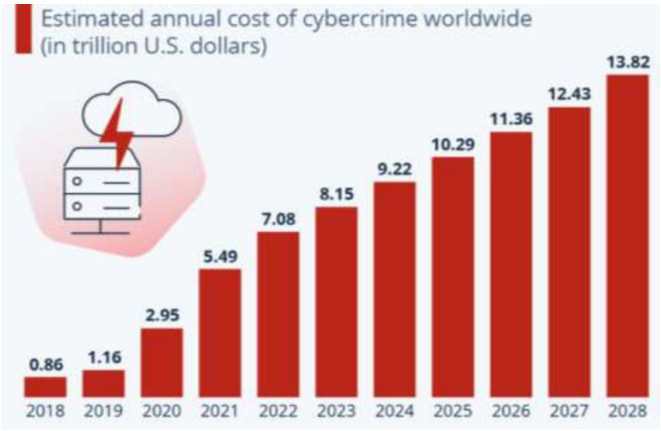

Fig. 1. Evolución del costo global del cibercrimen (2018–2028).

Esta cifra incluye costos por pérdida de datos, paralización de servicios, recuperación, multas regulatorias y pérdida de reputación.

Las pequeñas y medianas empresas (PYMES) son particularmente vulnerables. A diferencia de las grandes corporaciones, muchas no cuentan con personal técnico especializado ni con planes de respuesta ante incidentes. Lima Loayza (2024) documenta casos reales de empresas en Ayacucho que, tras sufrir ataques internos o infección por ransomware, enfrentaron interrupciones operativas de hasta dos semanas. Algunas incluso perdieron toda su base de datos por no contar con copias de seguridad adecuadas.

Un aspecto crítico es el tiempo de detección. Según He et al. (2023), los ataques dirigidos a sistemas Android mediante malware adversarial pueden permanecer ocultos durante semanas si no se implementan mecanismos de monitoreo continuo. Durante ese tiempo, se produce robo de información, uso indebido de recursos y daño progresivo al sistema.

Otro factor económico es el costo de las herramientas defensivas modernas. Aunque soluciones basadas en inteligencia artificial han demostrado ser eficaces, como lo indican Li et al. (2024), su implementación implica gastos en licencias, infraestructura y capacitación. Esto representa una barrera para muchas PYMES que operan con presupuestos limitados.

Además, existe un riesgo de dependencia tecnológica. Si una organización confía exclusivamente en soluciones automatizadas sin desarrollar una cultura de seguridad, corre el riesgo de no detectar comportamientos anómalos que escapen al alcance de las herramientas. Aryal et al. (2021) remarcan que ningún modelo es infalible, y que la supervisión humana sigue siendo clave para una defensa integral.

En resumen, los ataques informáticos no solo comprometen la seguridad técnica, sino que también afectan la estabilidad financiera y la viabilidad operativa de las organizaciones. Ignorar la inversión en seguridad puede salir mucho más caro a largo plazo que prepararse adecuadamente desde el principio.

TABLE III
IMPACTO ECONÓMICO ESTIMADO POR TIPO DE CIBERATAQUE

Tipo de ataque	**Costo promedio (USD)**	**Objetivo frecuente**
Ransomware	$120,000	PYMES, sector salud
Ataques internos	$85,000	Empresas sin auditoría
Adversarial malware	$140,000	Sistemas con IA
Phishing empresarial	$40,000	Organizaciones generales

Fuente: Adaptado de IEEE COMST (2022), Lima Loayza (2024), Aryal et al. (2021).

IV. CONCLUSIONES

La seguridad informática es un campo en constante evolución, impulsado tanto por el avance de la tecnología como por la creatividad de los atacantes. A lo largo de este artículo, se ha podido observar cómo las amenazas actuales —como el malware, los ataques internos y el software de

explotación— han adoptado formas más complejas, muchas veces difíciles de detectar por los métodos tradicionales.

El uso de técnicas de inteligencia artificial en los sistemas de defensa ha abierto nuevas posibilidades, pero también ha generado nuevos desafíos, como los ataques adversariales, que buscan explotar las debilidades de estos modelos. Como se ha demostrado en múltiples estudios (Aryal et al., 2021; Ling et al., 2021; He et al., 2023), estos ataques pueden modificar el comportamiento o la estructura de archivos maliciosos sin que pierdan su funcionalidad, logrando engañar a los detectores.

Además, quedó en evidencia que no solo hay que preocuparse por las amenazas externas, sino también por los riesgos internos, que suelen pasar desapercibidos pero pueden tener un gran impacto. La falta de controles, políticas y auditorías favorece este tipo de ataques, sobre todo en organizaciones pequeñas o con escasa cultura de seguridad, como es el caso de muchas PYMES peruanas (Lima Loayza, 2024).

Las defensas actuales deben ir más allá de los antivirus. Se requiere una combinación de herramientas tecnológicas, políticas claras y formación constante del personal. La implementación de estándares como ISO 27001, el uso de modelos híbridos de detección y la aplicación del enfoque de defensa en profundidad son algunas de las estrategias más efectivas para enfrentar las amenazas modernas (IEEE COMST, 2022; Expert Systems with Applications, 2024). Finalmente, este trabajo refuerza la importancia de ver la seguridad no solo como un componente técnico, sino también como una cuestión estratégica. Proteger nuestros sistemas no es solo responsabilidad de los ingenieros, sino de toda la organización, desde la dirección hasta los usuarios finales.

REFERENCES

[1] A. Aryal, M. Gupta y M. Abdelsalam, “A Survey on Adversarial Attacks for Malware Analysis,” ResearchGate, 2021. [Online]. Disponible en: https://www.researchgate.net/publication/356282100

[2] X. Ling, Z. Li, Z. Wang y Y. Zhang, “Adversarial Attacks against Windows PE Malware Detection: A Survey,” arXiv preprint arXiv:2112.12310, 2021. [Online]. Disponible en: https://arxiv.org/pdf/2112.12310

[3] P. He et al., “Defending against Adversarial Malware Attacks on Machine-Learning-based Android Malware Detection Systems,” arXiv:2303.16004, 2023. [Online]. Disponible en: https://arxiv.org/pdf/2303.16004

[4] J. Li et al., “Adversarial examples: A survey of attacks and defenses in deep-learning-based cybersecurity,” Expert Systems with Applications, vol. 231, 2024. [Online]. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S0957417423027252

[5] IEEE Communications Society, “A Survey of Adversarial Attack and Defense Methods for Malware,” IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2462–2492, 2022. doi: 10.1109/COMST.2022.3225137

[6] J. M. Lima Loayza, *Sistema de gestión de seguridad de la información según ISO/IEC 27001 para las PYMES del Perú*, Tesis, UNSCH, 2024. [Online]. Disponible en: https://repositorio.unsch.edu.pe/items/5c5b3faa-eb51-4bb9-8bee-0b47960edeff