UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

Prevención y resiliencia sobre infraestructuras críticas y su impacto en planificaciones I+D+i en ciberseguridad

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: IVÁN DANIEL MEDINA ASTUDILLO

TUTOR: JOE LLERENA IZQUIERDO

Guayaquil – Ecuador

2022

2

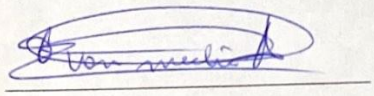
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Iván Daniel Medina Astudillo con documento de identificación N° 0927546739 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 23 de septiembre del año 2022

Atentamente,



Iván Daniel Medina Astudillo
0927546739

3

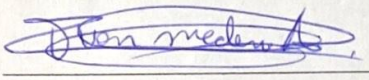
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Iván Daniel Medina Astudillo con documento de identificación N° 0927546739, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: "Prevención y resiliencia sobre infraestructuras críticas y su impacto en planificaciones I+D+i en ciberseguridad", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 23 de septiembre del año 2022

Atentamente,



Iván Daniel Medina Astudillo
0927546739

4

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Prevención y resiliencia sobre infraestructuras críticas y su impacto en planificaciones I+D+i en ciberseguridad, realizado por Iván Daniel Medina Astudillo con documento de identificación N° 0927546739, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 23 de septiembre del año 2022

Atentamente,

Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Dedico este trabajo a Dios por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mi madre, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar nuestras diferencias de opiniones. A mi padre, a pesar de nuestra distancia física, siento que estás conmigo siempre y aunque nos faltaron muchas cosas por vivir juntos, sé que este momento hubiera sido tan especial para ti como lo es para mí.

A mis hermano Eduardo y Ariel que siempre me brindaron sus palabras de aliento cuando todo parecía difícil.

A mi Esposa Ámbar quien con su paciencia y cariño ha sido una pieza fundamental durante todo este proceso de aprendizaje.

Pero sobre todo deseo hacer una mención especial para mi hijo Leonel porque cuando creí que mi sueño de terminar mi carrera universitaria había terminado él llegó y se volvió mi inspiración, mi motor.

A toda mi familia que me acompañó en esta etapa, aportando a mi formación tanto profesional y como ser humano.

AGRADECIMIENTO

Primero quiero agradecer a las personas que se han involucrado en la realización de este trabajo, sin embargo merecen reconocimiento especial mi Madre y mi Padre que con su esfuerzo y dedicación me ayudaron a culminar mi carrera universitaria y me dieron el apoyo suficiente para no decaer cuando todo parecía complicado e imposible.

Así mismo, agradezco infinitamente a mis Hermanos que con sus palabras me hacían sentir orgulloso de lo que soy y de lo que les puedo enseñar. Ojala algún día yo me convierta en se fuerza para que puedan seguir avanzando en su camino.

Debo agradecer a la universidad y de manera especial y sincera al Ing. Joe Frand Llerena Izquierdo por aceptarme para realizar este artículo bajo su dirección. Su apoyo y confianza en mi trabajo y su capacidad para guiar mis ideas ha sido un aporte invaluable, no solamente en el desarrollo de esta tesis, sino también en mi formación como investigador. Las ideas propias, siempre enmarcadas en su orientación y rigurosidad, han sido la clave del buen trabajo que hemos realizado juntos, el cual no se puede concebir sin su siempre oportuna participación. Le agradezco también el haberme facilitado siempre los medios suficientes para llevar a cabo todas las actividades propuestas durante el desarrollo de este artículo.

RESUMEN

Es notorio el aumento de los ciberataques en los últimos años, esto genera un gran impulso en ciberseguridad para proteger la infraestructura, sistemas informáticos y activos digitales de las organizaciones, las vulnerabilidades, riesgos y amenazas en la seguridad involucran un alto grado de responsabilidad financiera, informática, de reputación y organizacional. El objetivo general es proponer un modelo de planificación I+D+i en ciberseguridad para contrarrestar la problemática hacia las áreas críticas, atentados terroristas, atentados cibernéticos y ataques híbridos mediante índices de impacto. Entre los resultados se obtuvo: enfoques, técnicas utilizadas, ataques realizados, tipos de propuestas y tipos de herramientas, además se propone un modelo general de ciberseguridad basado en artículos científicos, entre los 20 artículos seleccionados en la revisión sistemática, 11 documentos tienen nivel de incidencia e impacto medio o alto, es decir 55% son aplicables a nuestra realidad ecuatoriana. Se concluye que la ciberseguridad es necesaria modelar y aplicar en organizaciones u hogares para minimizar el impacto negativo de los posibles ataques.

Palabras claves: Ciberseguridad, Ciberataques, Seguridad de Información, I+D+i.

ABSTRACT

The increase in cyberattacks in recent years is notorious, this generates a great impulse in cybersecurity to protect the infrastructure, computer systems and digital assets of organizations, vulnerabilities, risks and threats in security involve a high degree of financial, it, reputation and organizational responsibility. The general objective is to propose an R&D&I planning model in cybersecurity to counteract the problems towards critical areas, terrorist attacks, cyber attacks and hybrid attacks through impact indices. Among the results were obtained: approaches, techniques used, attacks carried out, types of proposals and types of tools, in addition a general model of cybersecurity based on scientific articles is proposed, among the 20 articles selected in the systematic review, 11 documents have a medium or high level of incidence and impact, that is, 55% are applicable to our Ecuadorian reality. It is concluded that cybersecurity is necessary to model and apply in organizations or homes to minimize the negative impact of possible attacks.

Key words: Cybersecurity, Cyberattacks, Information Security, R+D+i.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN 10
2. REVISIÓN DE LITERATURA 12
3. METODOLOGÍA 14
4. RESULTADOS 16
4.1. Identificar diferentes tipos de ataques críticos para establecer una categorización del tipo de soporte correcto mediante una revisión de literatura. 16
4.2. Diseñar un modelo de sistemas óptimos para determinar el tipo de ataque y vulnerabilidad mediante una contrastación de trabajos relevantes. 18
4.3. Evaluar el trabajo de investigación para definir una planificación I+D+i en ciberseguridad en áreas críticas mediante una tabla de incidencia y de nivel de impacto. 20
5. DISCUSIÓN 21
6. CONCLUSIÓN 22
REFERENCIAS 23

1. INTRODUCCIÓN

Hoy, los sistemas o estructuras de agua, salud, energía, educación y otros están conectados con infraestructuras cibernéticas, las aplicaciones y equipos cibernéticos gestionan el flujo de información para controlar las redes de servicios de manera eficiente y económica, y algunas redes son más inteligentes (Salazar Guzmán, 2021)(Soto Eras, 2021)(Carvajal Nagua & Solano Cedeño, 2021); las redes físicas y cibernéticas son integradas, es decir, si existe una interrupción en la capa informática-cibernética también se afectada la capa física; generalmente las infraestructuras utilizan firewall u otra clase de defensas para minimizar los ataques maliciosos; los ataques maliciosos se dividen en: Ataque de inyección de datos falsos, Ataque de inyección de comando falso, y Ataque de denegación de servicio distribuido (Zhang et al., 2020)(Pérez González, 2021).

Por otra parte, las personas, empresa o gobiernos ofrecen servicios de varios tipos o características por medio de Internet, los servicios ofrecen bienestar y celeridad a los clientes; si los servicios dejan de funcionar por varios minutos entonces causan malestar y desconfianza en los clientes, al momento existen amenazas relacionadas a los protocolos de Internet (Rios et al., 2022)(Reinoso Ordóñez, 2021)(Falconi Tamayo, 2021). Otro ataque fuerte es phishing que está dirigido a personas de áreas estratégicas, y que obtienen información importante de empresas privadas o públicas (Lee et al., 2021)(Barberán Vizueta & Chela Criollo, 2021). Por otra parte, existen los dispositivos IoT que se utilizan en muchas áreas y carecen de seguridad o tienen seguridad limitada, por ejemplo algunos dispositivos IoT tienen clave, usuario y contraseña anticipados y no son cambiables; esta clase de métodos inseguros son explotados para obtener control, los ataques cibernéticos están en aumento debido al aumento en la cantidad de dispositivos IoT inseguros (Hussain et al., 2021)(Mora-Alvarado & Llerena-Izquierdo, 2022). Los ataques de Denegación de Servicio sencillo y distribuido son las grandes amenazas que se asientan sobre cualquier entornos de red como Internet de las Cosas, Cloud Computing y 5G, de acuerdo a un informe de ataques la denegación de servicios aumentó del año 2019 al año 2020 en 300% (Yungaicela-Naula et al., 2021).

La I+D+i aprovecha la bonanza de las tecnologías actuales, ayuda a transformar muchas áreas en las organizaciones, y en ciberseguridad protege las infraestructuras e información como motor de las empresas o corporaciones; la información digital está extendida en muchos lugares y dispositivos conectados, los procesos y personas comparten información en línea, y además

existen los problemas de los ataques cibernéticos dirigidos a los datos, servicios, sistemas informáticos, software general, y dispositivos; algunos ataques comunes son los fraudes cibernéticos, malware, denegación de servicios, falsificaciones digitales, las filtraciones de software, filtraciones de datos, entre otros; algunos objetos digitales son audio, bases de datos, imágenes, software, videos y páginas web que se extienden a través de Internet en ritmo muy avanzado, los ataques cibernéticos intentan corromper la capa de seguridad para explotar toda clase de vulnerabilidades (Iwendi et al., 2020)(Robles Balaz, 2021).

La Confidencialidad, Integridad y Disponibilidad (Confidentiality, Integrity, Availability) de los datos obtenidos en cualquier entorno afectan en forma positiva la vida de los ciudadanos, las grandes cantidades de datos obtenidos por sistemas o dispositivos están conectados a redes e Internet, se reconoce que esto es una puerta abierta para que personas o programas ilegítimos amenacen vidas y perjudiquen infraestructuras (Álava Morán, 2021)(Narváez Picón, 2021); la seguridad es importante en los procesos de Autenticación, Autorización y Responsabilidad (Authentication, Authorization, Accounting) que responden la consistencia de la información, la Seguridad Cibernética salvaguarda el ciberespacio contra los ataques cibernéticos que pueden hacer afectaciones negativas en las redes, servicios o información (Guaranda Lara, 2021)(Llerena et al., 2021); los ataques cibernéticos ponen en riesgo las capacidades de los sistemas o infraestructuras que brindar servicios a las personas, el aumento de aplicaciones informáticas aumenta la posibilidad romper la privacidad de los ciudadanos (Tacuri López, 2021)(Rosero Tejada, 2021), se afirma que uno de los principales problemas en seguridad es la falta de estándares de seguridad comunes, por esta razón los programas o personas ilegítimas pueden interferir en la información y en los servicios (Elsaeidy et al., 2021)(Toala Indio, 2021).

El objetivo general es proponer un modelo de planificación I+D+i en ciberseguridad para contrarrestar la problemática hacia las áreas críticas, atentados terroristas, atentados cibernéticos y ataques híbridos mediante índices de impacto.

Los objetivos específicos son:

Identificar diferentes tipos de ataques críticos para establecer una categorización del tipo de soporte correcto mediante una revisión de literatura.

Diseñar un modelo de sistemas óptimos para determinar el tipo de ataque y vulnerabilidad mediante una contrastación de trabajos relevantes.

Evaluar el trabajo de investigación para definir una planificación I+D+i en ciberseguridad en áreas críticas mediante una tabla de incidencia y de nivel de impacto.

2. REVISIÓN DE LITERATURA

En (Huang et al., 2020) realizan un modelo de ataque de denegación de servicios sobre una red IoT y proponen como ventaja el costo cero de administración, sigiloso y robusto, pensado para pruebas de ataques distribuidos con pocos recursos; los autores afirman que el modelo es óptimo en su estrategia de ataque de acuerdo al impacto y relacionado a la estrategia de ataque (Vera Navas, 2021)(Orozco Bonilla, 2021).

En (Trabelsi et al., 2019) se concentra en el ataque de denegación de firewall que trata de sobrecargar los procesadores de un firewall, realizaron pruebas en tres diferentes firewall, analizaron las mitigaciones de ataques existentes en los dispositivos, como detección, eficacia; además presentaron y simularon un mecanismo para mitigar un ataque mediante reglas de rechazo con variación de tiempos y basados en las estadísticas de ataque (Rodríguez Pesantes, 2021).

En (Zhang et al., 2020) analizaron un ataque a un sistema cibernético para afectar a la red física, y comprobaron los múltiples accesos a la red, realizaron alteraciones y corte del servicio; para contrarrestar los ataque, los autores analizaron los patrones de secuencias de ataque e implementan una estrategia de exploración hacia los ataques (Coello Ochoa, 2021); los autores afirman que el patrón es representativo, disminuye las secuencias de ataques, tiene buen rendimiento y precisión, además la configuración de software ayuda en mitigar el riesgo en las aplicaciones (Moncayo Ronquillo, 2021).

En (Dehghani et al., 2021) se realizaron simulaciones para detectar datos falsos en forma confiable, precisa y rápida en varios tipos de ataque; el método procesa las señales digitales en un módulo anti-ataque cibernético y mantiene buen rendimiento, el modelo que detecta los ciberataques en línea se ejecuta en un hardware experimental (Sánchez Guzmán, 2021).

En (Yungaicela-Naula et al., 2021) utilizaron algoritmos de Inteligencia Artificial para implementar ataques de denegación de acceso en las capa de transporte y capa de aplicación, en los experimentos obtuvieron una precisión de 99% (Escalante Quimis, 2021)(Muñoz Campuzano, 2021).

En (Elsaeidy et al., 2021) realizaron un modelo basado en Inteligencia Artificial para detectar ataques como denegación de acceso y repetición, el modelo se evalúa con conjuntos de datos para simular los ataques; el modelo tiene una tasa precisión del 98%, el modelo tiene capa de entrada, capa estricta, capa neural y capa salida, además esta propuesto para una ciudad inteligente (Holguín Mendoza, 2021)(Ponce Larreategui, 2021)(Miranda Jiménez, 2021).

En (Wang et al., 2021) analizaron un modelo de ataques y defensas que ejecuta inundación de enlaces, desde el punto de vista defensivo se infiere en desconectar los enlaces identificados por el atacante; también analizan el tráfico para minimizar los ataques de inundación; los autores deducen que la ingeniería de tráfico minimiza la congestión generada por los ataques de inundación, existe un gran desafío en los enlaces importantes para conocer la red a desconectar, debido a que la obstrucción de un enlace obstruye otras redes de aplicaciones informáticas o infraestructuras (Morán Maldonado, 2021)(Guaigua Bucheli, 2021)(Aguirre Sánchez, 2021).

3. METODOLOGÍA

Para realizar el primer objetivo: “Identificar diferentes tipos de ataques críticos para establecer una categorización del tipo de soporte correcto mediante una revisión de literatura”, se realiza una revisión sistemática basada en los pasos de (Osorio-Carlozama & Llerena-Izquierdo, 2022)(Alvarado-Salazar & Llerena-Izquierdo, 2022), como son: a) Preguntas de investigación, b) Búsqueda de información relevante, c) Entorno en el que se relaciona, d) Selección de datos útiles, e) Muestra de información en gráficos, g) Planificación del estudio, h) Resultados de los datos seleccionados. Luego se tabulan los artículos científicos en una hoja de cálculo para obtener las respuestas en gráficos y sean entendibles. La selección final de los artículos es 20 documentos, ver Fig. 1.

Las preguntas de investigación son la guía para conocer ataques críticos y la categorización, se analizan artículos científicos. Las preguntas son: (P1): ¿Qué enfoques tienen las investigaciones? (P2): ¿Qué técnicas se utilizan para controlar los ataques? (P3): ¿Cuáles son los ataques realizados? (P4): ¿Qué proponen los artículos para mitigar los ataques? (P5): ¿Qué tipos de herramientas se proponen?

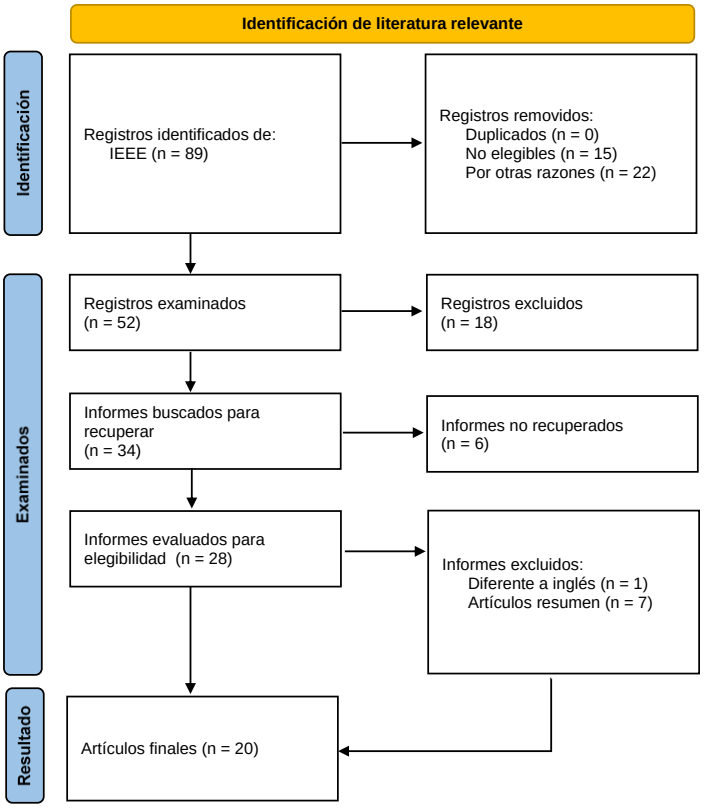


Figura 1. Flujo PRISMA del proceso de investigación

La tabla 1 representa los artículos luego de la identificación de la literatura.

Tabla 1. Artículos seleccionados

Año	Artículo
2019	(Trabelsi et al., 2019)
2020	(Huang et al., 2020), (Zhang et al., 2020), (Melih Tas et al., 2020), (Bhardwaj et al., 2020), (Iwendi et al., 2020), (Dong & Sarem, 2020), (Yoon et al., 2020), (Alamri & Thayananthan, 2020)
2021	(Hussain et al., 2021), (Han et al., 2021), (Lee et al., 2021), (Dehghani et al., 2021), (Yungaicela-Naula et al., 2021), (Elsaeidy et al., 2021), (Wang et al., 2021)
2022	(Rios et al., 2022), (D. Kwon et al., 2022), (Li et al., 2022), (Taherian-Fard et al., 2022)

Fuente: Autor.

Para realizar el segundo objetivo: “Diseñar un modelo de sistemas óptimos para determinar el tipo de ataque y vulnerabilidad mediante una contrastación de trabajos relevantes”, se propone un modelo en forma gráfica y descriptiva para mejor entendimiento, basados en los artículos científicos seleccionados en el primer objetivo.

Para realizar el tercer objetivo: “Evaluar el trabajo de investigación para definir una planificación I+D+i en ciberseguridad en áreas críticas mediante una tabla de incidencia y de nivel de impacto”, se presenta una tabla con los artículos científicos y las preguntas de investigación y una puntación para conocer la incidencia en la seguridad.

4. RESULTADOS

4.1. Identificar diferentes tipos de ataques críticos para establecer una categorización del tipo de soporte correcto mediante una revisión de literatura.

En este resultado se responden las preguntas de investigación basados en 20 artículos seleccionados mediante la revisión sistemática.

(P1): ¿Qué enfoques tienen las investigaciones?

El 20% se centra en prevenir los ataques, el 28% se centra el mitigar los ataques, y el 58% se centran en detectar los ataques, ver Fig. 2. Por otra parte, el 40% detectan y mitigan los ataques.

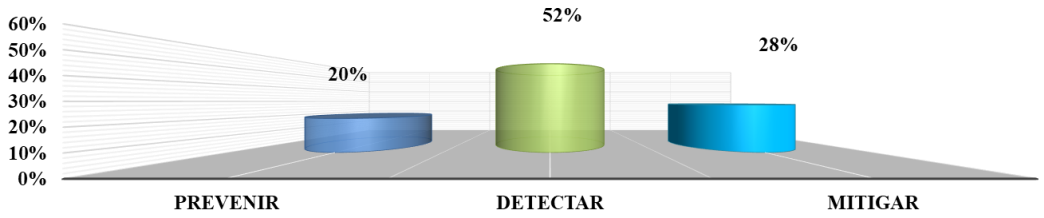


Figura 2. Enfoques

(P2): ¿Qué técnicas se utilizan para controlar los ataques?

El 4% utiliza algún lenguaje de programación, el 13% utiliza el dispositivo firewall, el 33% utiliza Inteligencia Artificial, y el 50% utiliza algoritmo de acuerdo a sus necesidades, ver Fig. 3. Por otra parte, el 15% utilizan Inteligencia Artificial y algoritmos para minimizar los ataques.

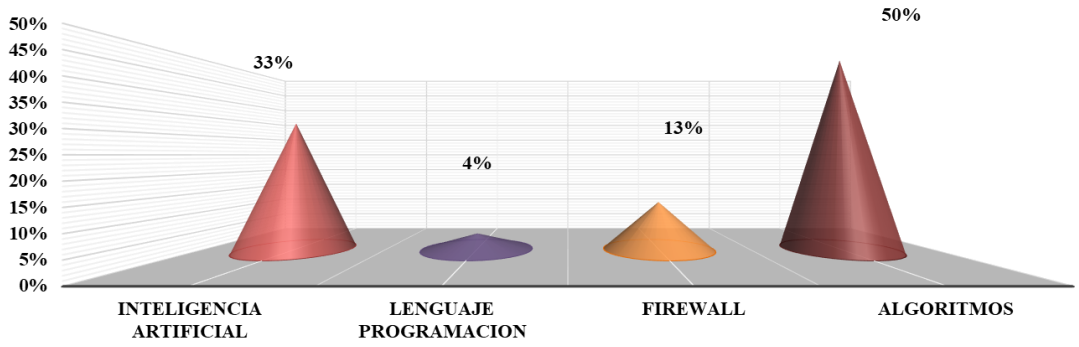


Figura 3. Técnicas

(P3): ¿Cuáles son los ataques realizados?

El 4% son phishing, el 4% son ataques de inyección de datos, 4% son ataques de repetición, 4% son ataques de inundación de enlaces, el 9% son ataques de red, el 9% son ataques a canales de comunicación, 14% son ataques dirigidos a aplicaciones informáticas, el 52% son ataques de denegación de acceso, ver Fig. 4. Por otra parte, solo artículo mitiga el ataque de denegación

de acceso junto a repetición, y otro artículo mitiga el ataque de red junto al ataque de denegación de acceso.

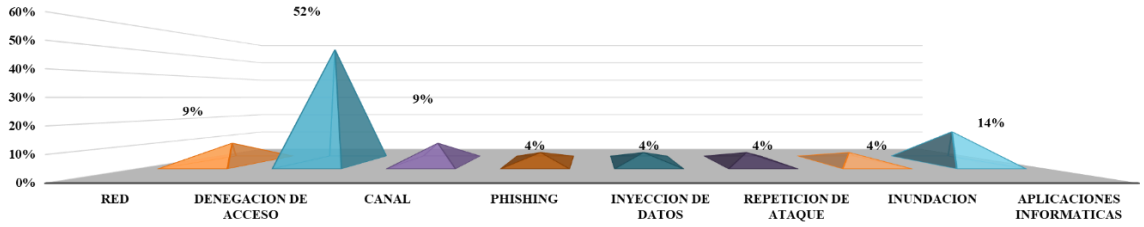


Figura 4. Ataques

(P4): ¿Qué proponen los artículos para mitigar los ataques?

Los artículos proponen revisión de modelos en 11%, desarrollo del modelo en 27%, y diseño de modelos contra ataques en 62%, ver Fig. 5. Por otra parte, el 25% de los artículos proponen el diseño y desarrollo de las propuestas.

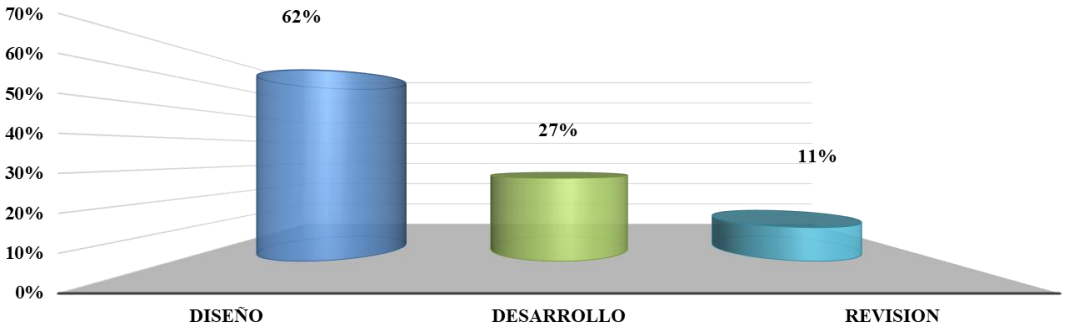


Figura 5. Ataques

(P5): ¿Qué tipos de herramientas se proponen?

En los artículos 10% son métodos, 15% son sistemas de ataques para mejorar los modelos, 31% son sistemas de defensa para mitigar los ataques, y 44% se realizaron simulaciones o experimentos de los modelos propuestos, ver Fig. 6. Por otra parte, el 25% de los artículos realizaron experimentos de los sistemas de ataques. Por otra parte, el 55% de los artículos realizaron experimentos de los sistemas de defensa. Por otra parte, el 10% de los artículos realizaron experimentos de los sistemas de ataques y sistemas de defensa.

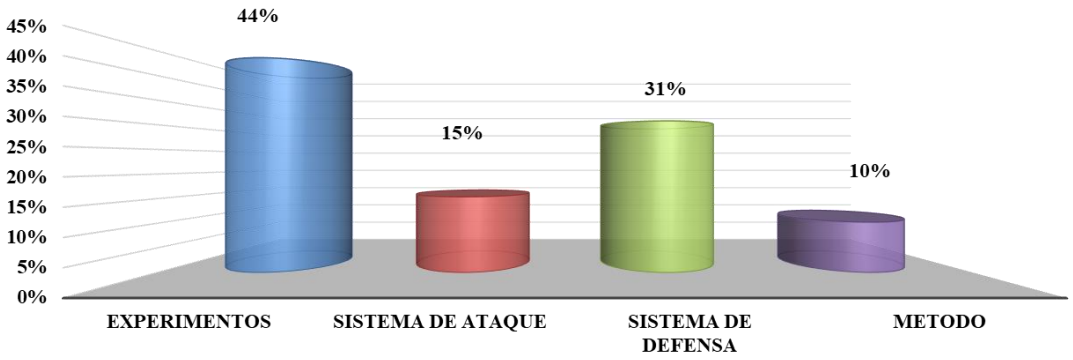


Figura 6. Ataques

4.2. Diseñar un modelo de sistemas óptimos para determinar el tipo de ataque y vulnerabilidad mediante una contrastación de trabajos relevantes.

Proponemos un modelo de ciberseguridad general para minimizar las Vulnerabilidades, Riesgos y Amenazas, ver Fig. 7, se presenta cíclico porque el modelo debe estar en continua actualización de acuerdo con nuevos tipos de ataques, está basado en investigaciones obtenidas del primer resultado y relacionadas a ataques, además está relacionado con otros trabajos relevantes sobre ciberseguridad, ver tabla 2. Esos trabajos se basaron en políticas, aplicaron estándares o utilizaron herramientas para aplicar ciberseguridad.

Tabla 2. Artículos sobre ciberseguridad

	Artículo
Políticas	(Sabillón, 2019), (Cujabante Villamil et al., 2020), (Vargas Borbúa et al., 2019)
Estándares	(Lapeña, 2020), (Chulde & Défaz, 2021), (Hamdani et al., 2021)
Herramientas	(Ben Fredj et al., 2020), (Bazlur Rashid et al., 2022), (Jahromi et al., 2021), (Hajny et al., 2021), (Deng et al., 2021), (T. Kwon et al., 2020)

Fuente: Autor

Las fases del modelo propuesto son:

a) Definir políticas: Esta fase trata de mantener la Confidencialidad, Integridad y Disponibilidad de la información en las organizaciones y asegurar la continuidad de las operaciones internas y externas, aquí se definen los objetivos, alcances, compromisos, roles, responsabilidades, políticas generales, políticas específicas, excepciones y comunicación de las políticas.

b) Inventario de activos físicos y digitales: En esta fase se debe realizar y actualizar los activos de la organización, inventariar activos físicos como servidores, switch, computadores, rack, centrales de comunicación, periféricos de energía, entre otros; inventariar activos digitales

como bases de datos, sistemas informáticos, sistemas operativos, software de gestión, manuales, entre otros.

c) Realizar enfoques: Esta fase se definen los enfoques como prevenir, mitigar, detectar, bloqueos, restricciones, entre otros; la organización puede aplicar uno o varios.

d) Adoptar técnica y estándares: En esta fase se toman técnicas como contingencia, recuperaciones, buenas prácticas, entre otros; adema se toman estándares como Cobit e ISO 27001.

e) Identificar ataque: En esta fase se debe tener una lista actualizada de los ataques con sus posibles soluciones y medidas para contrarrestar la presencia del ataque, al momento de identificar el ataque es menos complicado ejecutar las medidas de acuerdo al inventario de ataques.

f) Identificar vulnerabilidad: En esta fase es necesario realizar un inventario de las Vulnerabilidades, Riesgos y Amenazas de la organización con respecto a los sistemas informáticos, infraestructura e información, esto es útil para determinar fortalezas y debilidades ante los posibles ataques.

g) Utilizar herramientas: De acuerdo a las políticas, técnicas, estándares y vulnerabilidades de la organización se debe adquirir herramientas para prevenir o mitigar los posibles ataques, por ejemplo en hardware puede ser firewall y en software puede ser antivirus.

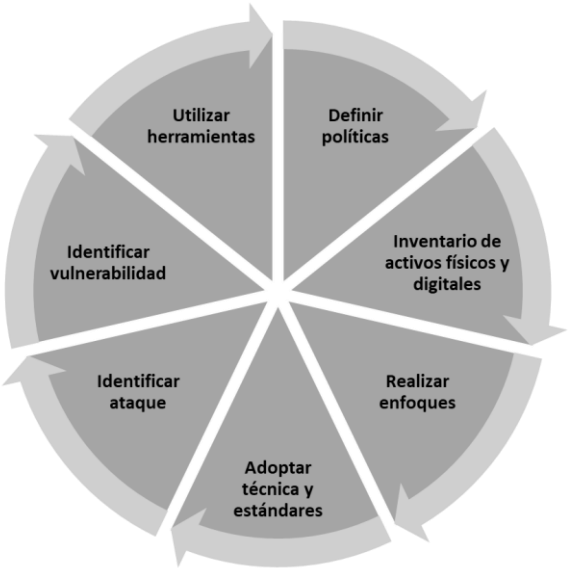


Figura 7. Modelo de sistemas

4.3. Evaluar el trabajo de investigación para definir una planificación I+D+i en ciberseguridad en áreas críticas mediante una tabla de incidencia y de nivel de impacto.

Para la evaluación se presenta en una tabla los artículos científicos, se asignó un punto a cada columna que cumple el artículo, se suma en forma horizontal cada artículo, el nivel incidencia puede ser bajo-medio-alto, el Nivel Bajo es el puntaje menor e igual a 6 puntos que lo tienen el 45% de los (9) artículos, el Nivel Medio es puntaje 7 u 8 que lo tienen otro 45% de los (9) artículos, el Nivel Alto es puntaje 9 que lo tienen el 10% de los (2) artículos. Son buenos niveles de incidencia e impacto los artículos que se encuentran en nivel medio o alto es decir 55% u 11 documentos, ver Fig. 8.

		ENFOQUE			TECNICAS				ATAQUES									PROPUESTA			HERRAMIENTAS					
ITEM	ARTICULO	PREVENIR	DETECTAR	MITIGAR	INTELIGENCIA ARTIFICIAL	LENGUAJE PROGRAMACION	FIREWALL	ALGORITMOS	RED	DENEGACION DE ACCESO	CANAL	PHISHING	INYECCION DE DATOS	REPETICION DE ATAQUE	INUNDACION	APLICACIONES INFORMATICAS		DISEÑO	DESARROLLO	REVISION	EXPERIMENTOS	SISTEMA DE ATAQUE	SISTEMA DE DEFENSA	METODO	PUNTOS	INCIDENCIA
1	(Hussain et al., 2021)	x	x		x				x									x			x	x			7	MEDIO
2	(Rios et al., 2022)		x	x		x				x										x			x		6	BAJO
3	(Trabelsi et al., 2019)		x	x			x			x									x		x		x		7	MEDIO
4	(Han et al., 2021)	x			x						x								x		x		x		6	BAJO
5	(Huang et al., 2020)		x					x		x								x				x			5	BAJO
6	(Lee et al., 2021)		x	x			x					x								x				x	6	BAJO
7	(Zhang et al., 2020)		x	x				x		x								x			x			x	7	MEDIO
8	(Dehghani et al., 2021)		x	x				x					x					x	x		x			x	8	MEDIO
9	(Melih Tas et al., 2020)		x	x				x		x								x	x		x		x		8	MEDIO
10	(Yungaicela-Naula et al., 2021)		x	x	x					x								x			x		x		7	MEDIO
11	(Elsaeidy et al., 2021)		x		x			x		x				x				x			x		x		8	MEDIO
12	(Wang et al., 2021)		x	x				x							x			x		x	x	x	x		9	ALTO
13	(Bhardwaj et al., 2020)		x		x			x		x								x			x			x	7	BAJO
14	(Kwon et al., 2022)		x		x			x			x							x			x	x			7	BAJO
15	(Li et al., 2022)	x						x								x		x	x		x	x			7	BAJO
16	(Iwendi et al., 2020)	x						x								x		x	x		x		x		7	BAJO
17	(Dong & Sarem, 2020)		x		x			x		x						x		x			x	x	x		9	ALTO
18	(Yoon et al., 2020)	x					x		x	x								x			x		x		7	MEDIO
19	(Alamri & Thayananthan, 2020)	x						x		x								x	x		x		x		7	MEDIO
20	(Taherian-Fard et al., 2022)		x		x					x								x			x		x		6	BAJO
		6	15	8	8	1	3	12	2	12	2	1	1	1	1	3	0	16	7	3	17	6	12	4	7.05	
			29					24								23				26				39	PROM	

Figura 8. Nivel de incidencia

5. DISCUSIÓN

Después de la revisión de la literatura, esta investigación analizó 20 artículos científicos para responder las preguntas de investigación, por esa razón presentó en forma detallada los descubrimientos en enfoques, técnicas utilizadas, ataques realizados, tipos de propuestas y tipos de herramientas.

Existe variedad de soluciones para mitigar los ataques, las soluciones son en hardware o software, otras proponen utilizar Inteligencia Artificial para conocer el comportamiento de los usuarios o infiltrados.

El modelo propuesto en esta investigación es general, no está basado un solo estándar o herramienta, sería interesante realizar otra investigación apegado a un estándar como Cobit o ISO 27000 o NIST u otros, aunque seleccionar un estándar requiere de una metodología.

No se evaluaron los modelos encontrados en los artículos científicos, pero se adoptaron características para lograr un modelo generalizado, pensamos que el modelo propuesto es útil en organizaciones pequeñas y medianas para la implementación y evaluación de la ciberseguridad interna o externa.

Como trabajo futuro se propone la evaluación de modelos de ciberseguridad para un sector específico de la industria.

6. CONCLUSIÓN

La variedad de ataques cibernéticos impulsa a diseñar e implementar variedad de modelos en ciberseguridad, los modelos trabajan sobre áreas como redes, infraestructura o información, no es posible cubrir todo en un solo modelo. El conocimiento sobre ciberataques y ciberseguridad son muy amplios es necesario aplicar un modelo sobre cada área.

Las nuevas profesiones en Tecnologías de Información ofrecen variedad de especialidades para mejorar el conocimiento y experiencia en seguridad informática, se resalta que los modelos de ciberseguridad deben evolucionar de acuerdo con los ciberataques.

El modelo generalizado que se propone en esta investigación puede variar en su contenido creado por la organización, porque las organizaciones utilizan estándares, herramientas, hardware o software de acuerdo con sus necesidades o presupuestos. Entre los 20 documentos, 11 tienen nivel de incidencia e impacto medio o alto, es decir 55% son aplicables a nuestra realidad ecuatoriana.

REFERENCIAS

Aguirre Sánchez, M. J. (2021). *Tecnologías de Seguridad en Bases de Datos: Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20566

Alamri, H. A., & Thayananthan, V. (2020). Bandwidth control mechanism and extreme gradient boosting algorithm for protecting software-defined networks against DDoS attacks. *IEEE Access*, *8*, 194269–194288. https://doi.org/10.1109/ACCESS.2020.3033942

Álava Morán, N. S. (2021). *Metodologías y técnicas analíticas de aprendizaje en la educación superior: un mapeo sistemático*.

Alvarado-Salazar, R., & Llerena-Izquierdo, J. (2022). Revisión de la literatura sobre el uso de Inteligencia Artificial enfocada a la atención de la discapacidad visual (Literature review on the use of Artificial Intelligence focused on visual impairment care). *Revista de Ciencias de La Ingeniería de La Universidad Técnica Estatal de Quevedo*, *5*, 10–21.

Barberán Vizueta, M. S., & Chela Criollo, J. K. (2021). *Prótesis impresas en 3D y aplicativo móvil de geolocalización: Caso de Estudio Novus Spem*. https://dspace.ups.edu.ec/handle/123456789/20293

Bazlur Rashid, A. N. M., Ahmed, M., Sikos, L. F., & Haskell-Dowland, P. (2022). Anomaly Detection in Cybersecurity Datasets via Cooperative Co-evolution-based Feature Selection. *ACM Transactions on Management Information Systems*, *13*(3). https://doi.org/10.1145/3495165

Ben Fredj, O., Mihoub, A., Krichen, M., Cheikhrouhou, O., & Derhab, A. (2020). CyberSecurity Attack Prediction: A Deep Learning Approach. *ACM International Conference Proceeding Series*, 0–5. https://doi.org/10.1145/3433174.3433614

Bhardwaj, A., Mangat, V., & Vig, R. (2020). Hyperband Tuned Deep Neural Network With Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud. *IEEE Access*, *8*, 181916–181929. https://doi.org/10.1109/ACCESS.2020.3028690

Carvajal Nagua, K. A., & Solano Cedeño, C. S. (2021). *Desarrollo de una Aplicación Web para el Control de citas y manejo de historial médico en la Unidad Médica Family care de la ciudad de Guayaquil*. https://dspace.ups.edu.ec/handle/123456789/20905

Chulde, L., & Défaz, H. (2021). Diseño del Modelo de Ciberseguridad IADI para el Sistema de Gestión Académica Ignug del Instituto Superior Tecnológico Yavirac. *Ecuadorian Science Journal*, *5*(3), 272–292. https://doi.org/10.46480/esj.5.3.160

Coello Ochoa, I. N. (2021). *Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos*. http://dspace.ups.edu.ec/handle/123456789/20738

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, *18*(30), 357–377. https://doi.org/10.21830/19006586.588

Dehghani, M., Ghiasi, M., Niknam, T., Kavousi-Fard, A., Tajik, E., Padmanaban, S., & Aliev, H. (2021). Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack. *IEEE Access*, *9*, 16488–16507. https://doi.org/10.1109/ACCESS.2021.3051300

Deng, Y., Zeng, Z., & Huang, D. (2021). NeoCyberKG: Enhancing Cybersecurity Laboratories with a Machine Learning-enabled Knowledge Graph. *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*, 310–316. https://doi.org/10.1145/3430665.3456378

Dong, S., & Sarem, M. (2020). DDoS Attack Detection Method Based on Improved KNN with

the Degree of DDoS Attack in Software-Defined Networks. *IEEE Access*, *8*, 5039–5048. https://doi.org/10.1109/ACCESS.2019.2963077

Elsaeidy, A. A., Jamalipour, A., & Munasinghe, K. S. (2021). A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City. *IEEE Access*, *9*, 154864–154875. https://doi.org/10.1109/ACCESS.2021.3128701

Escalante Quimis, O. A. (2021). *Prototipo de sistema de seguridad de base de datos en organizaciones públicas para mitigar ataques cibernéticos en Latinoamérica*. http://dspace.ups.edu.ec/handle/123456789/20576

Falconi Tamayo, L. F. (2021). *Desarrollo e implementación de una aplicación Web para la Gestión de Boletería de Vilaró Microteatro Restaurante*. https://dspace.ups.edu.ec/handle/123456789/20292

Guaigua Bucheli, C. J. (2021). *Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático*. https://dspace.ups.edu.ec/handle/123456789/20319

Guaranda Lara, S. N. (2021). *Modelo de gestión para el alineamiento de estrategias corporativas en pymes mediante las tecnologías de la información y comunicación*. http://dspace.ups.edu.ec/handle/123456789/20911

Hajny, J., Ricci, S., Piesarskas, E., & Sikora, M. (2021). Cybersecurity Curricula Designer. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3465481.3469183

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. Bin, Amjad, M. F., Malik, J., Murtaza, M. H., Atiquzzaman, M., & Khan, A. W. (2021). Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons. *ACM Computing Surveys*, *54*(3), 1–36.

Han, J., Lee, T., Kwon, J., Lee, J., Kim, I. J., Cho, J., Han, D. G., & Sim, B. Y. (2021). Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-Based Profiling. *IEEE Access*, *9*, 166283–166292. https://doi.org/10.1109/ACCESS.2021.3135600

Holguín Mendoza, J. D. (2021). *Categorización de protocolos de seguridad en criptomonedas para mitigar ataques informáticos: una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20915

Huang, K., Yang, L.-X., Yang, X., Xiang, Y., & Tang, Y. Y. (2020). A Low-Cost Distributed Denial-of-Service Attack Architecture. *IEEE Access*, *8*, 42111–42119. https://doi.org/10.1109/ACCESS.2020.2977112

Hussain, F., Abbas, S. G., Pires, I. M., Tanveer, S., Fayyaz, U. U., Garcia, N. M., Shah, G. A., & Shahzad, F. (2021). A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks. *IEEE Access*, *9*, 163412–163430. https://doi.org/10.1109/ACCESS.2021.3131014

Iwendi, C., Jalil, Z., Javed, A. R., Reddy G., T., Kaluri, R., Srivastava, G., & Jo, O. (2020). KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against Cyber-Attacks. *IEEE Access*, *8*, 72650–72660. https://doi.org/10.1109/ACCESS.2020.2988160

Jahromi, M. Z., Jahromi, A. A., Kundur, D., Sanner, S., & Kassouf, M. (2021). Data analytics for cybersecurity enhancement of transformer protection. *ACM SIGEnergy Energy Informatics Review*, *1*(1), 12–19. https://doi.org/10.1145/3508467.3508469

Kwon, D., Hong, S., & Kim, H. (2022). Optimizing Implementations of Non-Profiled Deep Learning-Based Side-Channel Attacks. *IEEE Access*, *10*, 5957–5967. https://doi.org/10.1109/ACCESS.2022.3140446

Kwon, T., Shin, I., Kim, K., Song, J., & Lee, J. (2020). Integrated Visual Analytics Approach

against Multivariate Cybersecurity Attack. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3399715.3399944

Lapeña, A. P. (2020). *Capítulo tercero Ciberseguridad , geopolítica y energía*. 159–196.

Lee, J., Lee, Y., Lee, D., Kwon, H., & Shin, D. (2021). Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3084897

Li, N., Han, Q., Zhang, Y., Li, C., He, Y., Liu, H., & Mao, Z. (2022). Standardization Workflow Technology of Software Testing Processes and Its Application to SRGM on RSA Timing Attack Tasks. *IEEE Access*, *10*(June). https://doi.org/10.1109/ACCESS.2022.3196934

Llerena, J., Alava-Moran, N., & Zamora-Galindo, J. (2021). Learning analytics for student academic tracking, a comparison between Analytics Graphs and Edwiser Reports. *2021 Second International Conference on Information Systems and Software Technologies (ICI2ST)*, 101–107. https://doi.org/10.1109/ICI2ST51859.2021.00022

Melih Tas, I., Unsalver, B. G., & Baktir, S. (2020). A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism. *IEEE Access*, *8*, 112574–112584. https://doi.org/10.1109/ACCESS.2020.3001688

Miranda Jiménez, J. N. (2021). *Mapeo sistemático de metodologías de Seguridad de la Información para el control de la gestión de riesgos informáticos*. http://dspace.ups.edu.ec/handle/123456789/20966

Moncayo Ronquillo, K. C. (2021). *Seguridades de la información bases de datos distribuidas: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21701

Mora-Alvarado, M., & Llerena-Izquierdo, J. (2022). Mobile Application of Registry Information for Urban Planning Context with Augmented Reality and QR Codes. *International Conference on Smart Technologies, Systems and Applications*, 30–43. https://doi.org/https://doi.org/10.1007/978-3-030-99170-8_3

Morán Maldonado, N. M. (2021). *Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática*. http://dspace.ups.edu.ec/handle/123456789/20243

Muñoz Campuzano, P. S. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20932

Narváez Picón, E. A. (2021). *Las tecnologías de la información y comunicación orientadas a la calidad del servicio en la gestión empresarial: una revisión sistemática*. https://dspace.ups.edu.ec/handle/123456789/20929

Orozco Bonilla, C. A. (2021). *Estrategias algorítmicas orientadas a la ciberseguridad: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/20933

Osorio-Carlozama, J., & Llerena-Izquierdo, J. (2022). Utility of Computer Hardware Recycling Technique for University Learning: A Systematic Review. *International Conference on Computer Science, Electronics and Industrial Engineering (CSEI)*, 175–189. https://doi.org/https://doi.org/10.1007/978-3-030-97719-1_10

Pérez González, R. F. (2021). *Softwares de penetración utilizados por los piratas informáticos: Una revisión sistemática (2015-2020).*

Ponce Larreategui, J. G. (2021). *Indicadores de compromiso (IOC) para detección de amenazas en la seguridad informática con enfoque en el código malicioso*. http://dspace.ups.edu.ec/handle/123456789/20937

Reinoso Ordóñez, L. A. (2021). *Desarrollo de sistema informático para la gestión de pagos de cuotas de los residentes de la Urbanización Belo Horizonte*. https://dspace.ups.edu.ec/handle/123456789/20332

Rios, V. D. M., Inacio, P. R. M., Magoni, D., & Freire, M. M. (2022). Detection and Mitigation of Low-Rate Denial-of-Service Attacks: A Survey. *IEEE Access*, *10*(June), 76648–76668. https://doi.org/10.1109/ACCESS.2022.3191430

Robles Balaz, G. J. (2021). *Desarrollo de la aplicación web para el registro de matrículas y gestión de conducta e incidencias en la Escuela José Martí*. http://dspace.ups.edu.ec/handle/123456789/20951

Rodríguez Pesantes, R. P. (2021). *Seguridad en dispositivos IOT en Organizaciones de América Latina*. http://dspace.ups.edu.ec/handle/123456789/20970

Rosero Tejada, L. F. (2021). *El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21699

Sabillón, R. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *32*, 33–48. https://doi.org/10.17013/risti.32.33-48

Salazar Guzmán, B. J. (2021). *Desarrollo de una aplicación bajo android para el control y monitoreo de unidades vehiculares en la empresa TCPLUMESAL SA*.

Sánchez Guzmán, C. O. (2021). *Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad*. https://dspace.ups.edu.ec/handle/123456789/20321

Soto Eras, W. M. (2021). *Desarrollo del portal web de la fundación nuestra Señora del Cisne para la gestión de servicios en el Cantón Durán*. http://dspace.ups.edu.ec/handle/123456789/20947

Tacuri López, I. L. (2021). *Acoso por medio de las tecnologías en las redes sociales durante tiempos de pandemia en Ecuador, una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20242

Taherian-Fard, E., Niknam, T., Sahebi, R., Javidsharifi, M., Kavousi-Fard, A., & Aghaei, J. (2022). A Software Defined Networking Architecture for DDoS-Attack in the storage of Multi-Microgrids. *IEEE Access*, *10*(July), 83802–83812. https://doi.org/10.1109/ACCESS.2022.3197283

Toala Indio, Y. I. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio*. http://dspace.ups.edu.ec/handle/123456789/20942

Trabelsi, Z., Zeidan, S., & Hayawi, K. (2019). Denial of Firewalling Attacks (DoF): The Case Study of the Emerging BlackNurse Attack. *IEEE Access*, *7*, 61596–61609. https://doi.org/10.1109/ACCESS.2019.2915792

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2019). Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, *20*, 31. https://doi.org/10.17141/urvio.20.2017.2571

Vera Navas, N. A. (2021). *Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales*. http://dspace.ups.edu.ec/handle/123456789/20949

Wang, X., Ma, X., Peng, J., Li, J., Xue, L., Hu, W., & Feng, L. (2021). On Modeling Link Flooding Attacks and Defenses. *IEEE Access*, *9*, 159198–159217. https://doi.org/10.1109/ACCESS.2021.3131503

Yoon, S., Cho, J. H., Kim, D. S., Moore, T. J., Free-Nelson, F., & Lim, H. (2020). Attack Graph-Based Moving Target Defense in Software-Defined Networks. *IEEE Transactions on Network and Service Management*, *17*(3), 1653–1668. https://doi.org/10.1109/TNSM.2020.2987085

Yungaicela-Naula, N. M., Vargas-Rosales, C., & Perez-Diaz, J. A. (2021). SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning. *IEEE Access*, *9*, 108495–108512. https://doi.org/10.1109/ACCESS.2021.3101650

Zhang, Z., Huang, S., Liu, F., & Mei, S. (2020). Pattern Analysis of Topological Attacks in Cyber-Physical Power Systems Considering Cascading Outages. *IEEE Access*, *8*, 134257–134267. https://doi.org/10.1109/ACCESS.2020.3006555