UNIVERSIDAD TECNOLÓGICA ECOTEC

FACULTAD DE DERECHO Y GOBERNABILIDAD

TÍTULO DEL TRABAJO:

Análisis de la vulnerabilidad de información en el sistema de control aduanero y aplicación de estrategias de mitigación a la práctica de hackeo en las redes informáticas aduaneras.

Línea de Investigación:

Proyecto de investigación.

Modalidad de Investigación:

Gestión de las relaciones jurídicas.

CARRERA:

Derecho con énfasis en derecho tributario y empresarial.

Derecho con énfasis en derecho en ciencias penales y criminalística.

Título a Obtener:

Abogado.

AUTORES:

Alvarado Cochea Harvy Jared

Bucaram Ramírez Maximiliano Daniel

TUTOR:

Fabian Orellana Batallas.

Samborondón – Ecuador

2024

Certificado de aprobación.

ANEXO No. 9

PROCESO DE TITULACIÓN
CERTIFICADO DE APROBACIÓN DEL TUTOR

Samborondón, 11 de agosto de 2024.

Magíster.
Ab. Andrés Madero Mgtr.
Decano(a) de la Facultad.
Derecho y Gobernabilidad.
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **Análisis de la vulnerabilidad de información en el sistema de control aduanero y aplicación de estrategias de mitigación a la práctica de hackeo en las redes informáticas aduaneras.** Fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, por lo que se autoriza al estudiante: **ALVARADO COCHEA HARVY JARED y BUCARAM RAMIREZ MAXIMILIANO DANIEL,** para que proceda con la presentación oral del mismo.

ATENTAMENTE,

FABIAN ERNESTO ORELLANA BATALLAS

Firmado digitalmente por FABIAN ERNESTO ORELLANA BATALLAS
DN: cn=FABIAN ERNESTO ORELLANA BATALLAS gn=FABIAN ERNESTO c=EC
Motivo:Soy el autor de este documento
Ubicación:
Fecha:2024-08-12 21:22+02:00

Firma

Mgtr. Fabian Orellana Batallas.
Tutor(a)

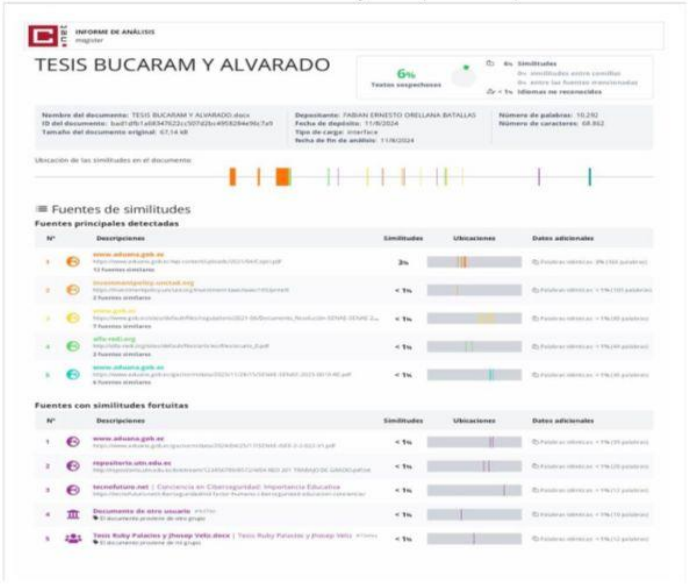
Certificado de porcentaje de coincidencias.

Universidad Ecotec

ANEXO No. 10

PROCESO DE TITULACIÓN
CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS
DEL TRABAJO DE TITULACIÓN

Habiendo sido revisado el trabajo de titulación TITULADO: **ANÁLISIS DE LA VULNERABILIDAD DE INFORMACIÓN EN EL SISTEMA DE CONTROL ADUANERO Y APLICACIÓN DE ESTRATEGIAS DE MITIGACIÓN A LA PRÁCTICA DE HACKEO EN LAS REDES INFORMÁTICAS ADUANERAS**. Elaborado por **HARVY JARED ALVARADO COCHEA y MAXIMILIANO DANIEL BUCARAM RAMIREZ** fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del (6%) mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del documento. Adicional se adjunta print de pantalla de dicho resultado.



ATENTAMENTE,

FABIAN ERNESTO ORELLANA BATALLAS

Firmado digitalmente porFABIAN ERNESTO ORELLANA BATALLAS
DN: cn=FABIAN ERNESTO ORELLANA BATALLAS gn=FABIAN ERNESTO c=EC
Motivo:Soy el autor de este documento
Ubicación:
Fecha:2024-08-12 21:23+02:00

Firma
Mgtr/ PhD.. Fabian Orellana Batallas.
Tutor(a)

Agradecimiento.

En primer lugar, agradezco a Dios, por su infinita bondad. De manera especial agradezco a mi familia, a mis padres por creer en mí por su amor incondicional y por ser mi mayor fuente de inspiración y apoyo. A mi hermana y mi pareja sentimental

por su apoyo constante, por su paciencia y por acompañarme en cada paso de este camino. Sin duda han sido una fuente inagotable de motivación.

Harvy Jared Alvarado Cochea.

Agradezco profundamente a mi esposa, por su paciencia, amor y constante apoyo durante todo este proceso. Su comprensión y aliento han sido esenciales para superar los desafíos de esta investigación.

Maximiliano Daniel Bucaram Ramírez.

Dedicatoria.

Dedico este trabajo a mi familia. A mis padres por enseñarme el valor del esfuerzo y la perseverancia. A mi hermana y mi pareja sentimental, por compartir este camino conmigo. Este logro es tanto mío como de ustedes, Gracias.

Harvy Jared Alvarado Cochea.

Dedicó este trabajo a mi esposa, por su amor, comprensión y constante apoyo durante todo este proceso. Su paciencia y aliento han sido esenciales para superar los desafíos de esta investigación. A mis padres, por su amor y enseñanzas que me han guiado a lo largo de mi vida. Agradecemos de corazón a todas aquellas personas que, de una manera u otra, han formado parte de esta etapa de nuestras vidas. Este logro es tanto nuestro como de ustedes.

Maximiliano Daniel Bucaram Ramírez.

Índice de contenidos

Resumen

El control aduanero y la lucha contra los ataques de piratas informáticos son aspectos esenciales de la gestión de medios y la vigilancia del comercio internacional. La Aduana es una unidad gubernamental que desempeña un papel crucial en la regulación y seguimiento del movimiento de mercancías a nivel nacional e internacional. Por lo tanto, el objetivo principal de este estudio es analizar las estrategias implementadas por esta entidad gubernamental para proteger la seguridad nacional, proteger la economía y prevenir actividades ilegales como el contrabando u otras actividades similares para proteger su plataforma de los piratas informáticos. A través de una metodología cualitativa basándose en la observación natural de las prácticas existentes, tal como se describen en fuentes secundarias y mediante entrevistas con personal clave involucrado en la gestión de las tecnologías de la información en aduanas. Se obtiene como resultado que en la aduna, a pesar de la existencia de delitos informáticos, la ciberseguridad previamente establecida en el servicio aduanero ha sido capaz de proteger la información y asegurar el perímetro digital de la organización. Podemos destacar que los muros cuentan con una infraestructura TI (Tecnologías de la Información) que es capaz de hacer frente a las diversas dificultades que se presentan. Lo que permitió concluir que es fundamental establecer requisitos de seguridad adecuados para proteger los activos de información utilizados por los empleados de la organización en el desempeño de diversas tareas para que el trabajo diario pueda realizarse con el objetivo de alcanzar las metas de la organización.

Palabras claves: Tecnología, control, aduana, hackeo.

Abstract.

Customs control and combating hacker attacks are essential aspects of media management and international trade surveillance. Customs is a government unit that plays a crucial role in regulating and monitoring the movement of goods nationally and internationally. Therefore, the main objective of this study is to analyze the strategies implemented by this government entity to protect national security, protect the economy and prevent illegal activities such as smuggling or other similar activities to protect its platform from hackers. Through a qualitative methodology based on natural observation of existing practices, as described in secondary sources and through interviews with key personnel involved in the management of information technologies in customs. The result is that in customs, despite the existence of computer crimes, the cybersecurity previously established in the customs service has been capable of protecting information and securing the digital perimeter of the organization. We can highlight that the walls have an IT (Information Technology) infrastructure that is capable of dealing with the various difficulties that arise. Which allowed us to conclude that it is essential to establish adequate security requirements to protect the information assets used by the organization's employees in the performance of various tasks so that daily work can be carried out with the objective of achieving the organization's goals.

Keywords: Technology, control, customs, hacking

1. Introducción

1.1. Contexto histórico social del objeto de estudio

El control aduanero y la lucha contra el hackeo son aspectos fundamentales en la gestión de fronteras y seguimiento del comercio internacional. La Aduana es una unidad gubernamental que desempeña un papel crucial en la regulación y seguimiento del movimiento de mercancías a nivel nacional e internacional. Por lo tanto, el objetivo principal de este estudio es analizar las estrategias implementadas por esta entidad gubernamental para proteger la seguridad nacional, proteger la economía y prevenir actividades ilegales como el contrabando u otras actividades similares para proteger su plataforma de los piratas informáticos.

En este estudio, el control aduanero se considera como un conjunto de reglas y procedimientos establecidos por las autoridades gubernamentales para verificar y controlar el movimiento de mercancías a través de las fronteras. Éste es el asiento de esta investigación, y sus características generales incluyen el examen de mercancías, la determinación de derechos, la imposición de impuestos y la aplicación de normas comerciales.

1.2. Antecedentes

Guerrero (2021), describe un estudio realizado en Ecuador para comprender el control aduanero y el impacto en la administración aduanera en el Carchi, que apuntó directamente a establecer mejor comprensión del tema. Todo esto a través de un método cualitativo, mediante una revisión documental y entrevistas que muestran que hay 35 casos en los que los bienes se importan sin aprobación previa de la región donde se encuentran, y los mismos se importan al país sin aprobación previa, lo que permite inferir que son ilegales. Como resultado también se han registrado un total de 15,983 registros de incautaciones de bienes importados ilegalmente, a través del trabajo conjunto con diversas estructuras y organizaciones establecidas por el

gobierno; Asimismo, también se puede encontrar que, al finalizar todos los procesos, las cosas encontradas son trasladadas a otras áreas que convienen para donar, subastar o destruir el material, todo con una incidencia del 46%. Por lo tanto, se concluye que el descontrol aduanero en el territorio afecta paulatinamente a sus habitantes y su economía, debido a que los materiales que llegan al territorio no pagan impuestos.

Aylas y Alcalá (2022) realizaron un trabajo sobre delitos aduaneros en el puerto del Callao para comprender cómo las aduanas gestionan y desarrollan controles para limitar las actividades ilícitas en el puerto. Se trata de un estudio básico, no experimental y transversal. Las herramientas y técnicas para recopilar información de muestras son los cuestionarios y las encuestas. La muestra es realizada por la Autoridad Aduanera. Los resultados revelaron que los controles propuestos se desarrollaron utilizando estrategias que generaron con éxito beneficios por $5,059 millones en 8 años. Destacando como estrategia utilizada la capacitación del personal para reforzar los procesos y acciones a tomar ante una situación de acciones ilícitas. Se concluyó que todas las medidas tomadas por las autoridades portuarias han permitido reducir los delitos y el uso de la tecnología ha permitido realizar controles más simples y efectivos en los casos en que es necesario revisar contenedores, y finalmente, capacitación. Lo que ha permitido trabajar de manera más eficiente, si bien es indudable que las actividades ilícitas no han sido erradicadas y continúa amenazando la salud pública, afectando los ingresos del gobierno y socavando la moral, la Aduana está haciendo todo lo posible para implementar estos cambios.

En 2018, durante la serie de conferencias del Instituto de Física (Institute of Physics et al., 2019) publicaron un artículo en el que realizaron un análisis de vulnerabilidad en los sitios web de tres empresas en Indonesia. Estas empresas, posteriormente, decidieron fortalecer su seguridad. Las herramientas utilizadas en este análisis fueron Zenmap, Nikto, OWASP DirBuster y ViSQL. Las vulnerabilidades detectadas incluyeron puertos abiertos, seguimiento HTTP activo, seguimiento entre sitios, errores XSS, listado de directorios no encontrados e inyección SQL. La solución

recomendada para mejorar la seguridad fue asegurar el sitio mediante el uso de acceso HTTPS y corregir los métodos de los scripts.

En febrero de 2018 se presentó un trabajo de grado en la Universidad Nacional Abierta y a Distancia –UNAD, por Rincón y Albarracín (2019), estos plantearon un trabajo de grado que analizaba y evaluaba la seguridad informática de sitios web publicados en hosting gratuito. Una organización responsable de descubrir y remediar vulnerabilidades y riesgos de la información. Esta investigación utilizó las herramientas Owasp, Skipfish y Sucuri y encontró algunas vulnerabilidades de seguridad de la información en sitios web que son vulnerables a ataques de hackeo. La página contenía uno o más archivos de secuencias de comandos de un dominio de terceros y el sitio no habilitaba la protección XSS contra ataques de secuencias de comandos entre sitios, y el contenido y el código de la página se podían copiar fácilmente.

1.3. Planteamiento del problema.

La sociedad ha logrado sobrevivir a tiempos difíciles, superar obstáculos, problemas, enfermedades y otras situaciones similares, con el único objetivo de garantizar una alta calidad de vida, por lo que se ve obligada a crear procesos y sistemas que permitan a todos los integrantes de la sociedad disfrutar de los mismos derechos e intereses; Algunos de los sistemas existentes incluyen la creación de estructuras gubernamentales para proteger los derechos y ser responsables de generar ingresos para cerrar brechas, garantizar buenos servicios y atención de calidad, y crear una organización descentralizada que permita la acción comunitaria. Dar a conocer los derechos y obligaciones de todos de conformidad con las políticas y leyes aplicables.

Sin embargo, también existen algunos ciudadanos que tienen pensamientos y comportamientos personales que solo se preocupan por intereses individuales, sin importar si dichos intereses muchas veces perjudican al resto de la sociedad y al país, estos comportamientos incluyen: ciberataques, hackeos, contrabando, tráfico de drogas, tráfico de armas, lavado de dinero, y otros

similares. Un buen ejemplo es el Ecuador, que puede tener políticas y regulaciones que prohíben las actividades anteriores, pero a pesar de prohibir estas actividades, el país todavía tiene falencias que permite el cometimiento de dichos delitos, por ejemplo, los delitos informáticos que últimamente han incrementado y perjudicado a la sociedad ecuatoriana, aumentando el nivel de incertidumbre en las actividades bancarias, en temas de aduana como importación y exportación, entre otras (Celis, 2020).

Una de las razones del auge de estas actividades ilegales es que la globalización permite que bienes, cultura, servicios, costumbres, valores, entre otros, interactúen y se comuniquen en este intercambio que se da, permitiendo este tipo de invasión cibernética en las importaciones y exportaciones, por eso los países tratan de proteger a los ciudadanos a través de restricciones aduaneras que permitan no sólo el registro y la razón por la cual los bienes están sujetos a impuestos, sino que promuevan estrategias que fundamente el correcto tránsito del comercio internacional (Ramos et al., 2023).

Además, a nivel nacional los delitos informáticos a lo largo de los años ha sido uno de los problemas que ha afectado negativamente a la economía del país, por lo que el gobierno ha querido tomar medidas para erradicar el cometimiento de este delito, pero este planteamiento que realizó es muy ambiguo. Convirtiéndose en algunas de las consecuencias negativas del comportamiento ciudadano, que trae consigo en el caso de las aduanas menores retornos de los recursos económicos, mercados sujetos a desequilibrios y mayores riesgos. Por ende, se plantea esta pregunta problemática a través de esta investigación:

¿Cómo reducir la vulnerabilidad de información en el sistema de control aduanero ante el ataque informático, y cómo aplicar estrategias de mitigación para prevenir y mitigar actividades ilícitas?

1.4. Los objetivos del trabajo de Integración curricular.

General

Evaluar el impacto de los delitos informáticos en el sistema de control aduanero, con el fin de proponer estrategias de mitigación para prevenir y combatir actividades ilícitas relacionadas.

Específicos

- Analizar el impacto generado por los delitos informáticos relacionados al sistema de control aduanero.
- Identificar la relación existente entre la vulnerabilidad en el sistema de control aduanero y las prácticas de mitigación anti - hackeo en las redes informáticas
- Proponer un modelo conceptual y un plan de estrategias para robustecer el sistema de informático aduanero.

1.5. Justificación

El desarrollo de la sociedad ha puesto la globalización como tema de vanguardia frente a todos los procesos a nivel empresarial ya sea de carácter privado o gubernamental. Por ello, la ciberseguridad cobra importancia, tomando medidas preventivas para proteger los sistemas informáticos a fin de evitar delitos informáticos, que en este caso pueden causar pérdidas económicas, e incidir en el sistema gubernamental nacional. Frente a lo cual, la seguridad de la información en equipos técnicos y sistemas online tiene poca importancia organizativa, por ende, es de vital relevancia describir las estrategias en materia de vulnerabilidad que aún no se han implementado y las necesidades de establecer los controles de seguridad de la red para garantizar la disponibilidad, confidencialidad e integridad de la información.

Por lo cual, las aduanas necesitan proteger los equipos técnicos y los sistemas de información, lo que genera preocupación y exige acciones preventivas y correctivas contra las amenazas a la ciberseguridad. En este sentido, el análisis de vulnerabilidad de control aduanero y aplicación de estrategias de mitigación a la práctica de delitos informáticos en el sistema de control informático aduanero se desarrolla para marcar el inicio de la implementación de la seguridad de la información en la organización, durante el proceso también se consideraron pruebas de ética y una revisión de los documentos de política de seguridad propuestos.

Frente a lo cual, será posible recopilar información sobre las variables y así obtener nuevos conocimientos que puedan informar sobre las mismas a diferentes investigadores que podrán realizar nuevas investigaciones en el futuro. Por ende, con base en los resultados de la investigación se podrán sacar conclusiones y recomendaciones, las cuales permitirán reducir problemas y hacer más prácticos y eficientes los procesos investigativos futuros. También se puede entender a través de la investigación la relación de vulnerabilidad entre el control aduanero y los delitos informáticos, se realizará utilizando una variedad de instrumentos que ayudarán a obtener datos de las muestras de manera eficiente, precisa y confiable, además de utilizar instrumentos para obtener una visión más concisa y personal de cada tema.

2. Revisión de la literatura

2.1. Seguridad cibernética anti- hackeo

La ciberseguridad destinada a prevenir el hackeo se define como parte del conjunto de herramientas y procedimientos utilizados para proteger toda la información procesada y generada mediante computadoras, redes, dispositivos móviles y sistemas electrónicos (Díaz, 2020).

2.1.1. Elementos de la seguridad cibernética anti- hackeo

Los tres elementos básicos de la seguridad de la red son: confidencialidad, integridad y disponibilidad.

El primer elemento es la confidencialidad, que tiene la propiedad de que la información no será divulgada ni accedida por procesos, personas o entidades no autorizados. Esta a su vez se desprende de dos elementos los cuales parten de la accesibilidad, que es una de las características de disponibilidad y usabilidad cuando lo requiere un organismo autorizado (Kosévich, 2019).

Estos elementos incluyen delitos informáticos y delitos cibernéticos, que son actividades ilegales que no están autorizadas e impiden el procesamiento de datos en sistemas informáticos y el desarrollo del ciberespacio utilizando tecnologías de Internet (Donoso, 2022).

2.2.3. Tipos de Hackeo

Los ciberdelincuentes pueden utilizar una gran cantidad de agentes maliciosos para obtener acceso ilegal a los sistemas informáticos, los más habituales y comunes son:

- **Malware**

Este proceso sólo puede ser realizado por Hackeratacantes que comprendan los distintos protocolos existentes como: Icmp, Tcp/Ip y Udp y sus limitaciones. Por lo tanto, pueden realizar acciones como aumentar la carga en cada sistema, bloquear la comunicación del remitente con el destinatario, paralizar la red, direccionar paquetes IP con destinatarios falsos, generalmente virus, troyanos, spyware, ransomware, adware y botnets, entre otros (Zabalo, 2019).

- **Phishing o suplantación de identidad**

Es un programa malicioso enviado a una víctima o usuario por correo electrónico que parece provenir de una empresa, banco u otra organización legítima que solicita información personal o confidencial. En muchos casos, estos correos electrónicos contienen enlaces a sitios web preparados por ciberdelincuentes. Estos ataques se utilizan a menudo para engañar a las personas para que entreguen su información bancaria, de crédito, de débito u otra información personal (Leyva, 2021).

- **Ataque de Inyección SQL**

Se trata de un ataque que utiliza código malicioso con lenguajes de programación de consultas que están estructurados y utilizados para comunicarse con bases de datos en servidores que almacenan información importante sobre servicios y sitios web con el fin de obtener secretos, datos de clientes y control, lo que suele ocurrir en los bancos, aduanas y usuario de procesamiento, contraseña, número de cuenta bancaria, tarjeta de crédito, entre otros (Garzón et al., 2024).

- **Ataque de denegación de servicio**

Este tipo se puede ejecutar en muchas computadoras al mismo tiempo y puede inundar un sistema informático o un sitio web con tráfico, sobrecargando servidores y redes, impidiendo que las solicitudes se cumplan y sean legítimas, haciéndolas inválidas y bloqueando negocios,

dejándolos sin cómo responder a las solicitudes de los usuarios o publicar contenido en una página web (Donoso, 2022).

2.2. Hackeo, amenazas y ataques a servidores

Un hackeo o una amenaza lógica es un software o código que afecta o daña nuestros sistemas de alguna manera y está diseñado deliberadamente para hacerlo, por ende, se tiene:

• Herramientas de seguridad: existen herramientas que pueden detectar y corregir errores del sistema, pero también se pueden utilizar para detectar los mismos errores y utilizarlos para atacarlos. Scareware, que es un falso antivirus o antispyware.

• Puertas traseras o backdoors: Los programadores insertan atajos de acceso o administración, en ocasiones con un nivel de seguridad menor.

• Virus: secuencia de código que se inserta en un archivo ejecutable (llamado host) para que el virus también se ejecute cuando se ejecuta el archivo. Detrás de la palabra virus se esconde todo un concepto llamado malware. Instrucciones del programa para que parezcan realizar la tarea esperada por el usuario, pero en realidad realiza funciones ocultas sin el conocimiento del usuario, donde por lo general está comprometiendo la seguridad (Rutz, 2021).

• Bunnies o Spam: Programas que no sirven para nada y simplemente se repiten hasta que el número de copias consume recursos del sistema ya sea en la memoria, procesador, disco, entre otros, provocando un ataque de denegación de servicio. Transmisión de información en violación de las políticas de seguridad del sistema; ya sea por el equipo y su configuración. Con esta información, pueden descubrir vulnerabilidades y puntos de entrada (Rodríguez, 2022).

• Spoofing: un atacante oculta su verdadera identidad y se hace pasar por otro usuario o computadora. A menudo se utiliza para enmascarar la dirección real de un ataque o para eludir

los sistemas de control de acceso basados en la dirección IP de origen. Los ataques de suplantación de identidad son la modificación de paquetes de datos existentes y la creación de nuevos paquetes de datos en una red con el objetivo de falsificar la identidad de un elemento de transmisión de mensajes (Garcés et al., 2022).

• Secuestro de sesión: en un atacante de este tipo se utiliza un programa para simular el comportamiento de un cliente o servidor, o intercepta paquetes de información en una red que puede verlos y modificarlos a voluntad. Como resultado, el servidor o cliente piensa que se está comunicando con una computadora legítima, cuando en realidad es la computadora del hacker, que para todos los efectos parece ser el destino real. A menudo se utiliza para obtener información de autenticación y datos confidenciales. Este tipo de ataques también se denominan ataques de intermediario (Oltra y Ibáñez, 2019).

• Denegación de servicio (DoS): este atacante intenta negar a los usuarios legítimos el acceso a un servidor o servicio de red, inundando la red con tráfico falsificado y consumiendo todo el ancho de banda y los recursos. Vale la pena enfatizar que una gran cantidad de ataques de este tipo se denominan denegación de servicio distribuido (DDoS), donde varios sistemas se coordinan para llevar a cabo ataques simultáneos contra un objetivo específico (Obando et al., 2022).

2.3. Riesgo Informático.

Los riesgos informáticos pueden describirse como debilidades en los sistemas de información que deben ser detectadas y controladas porque estas debilidades pueden dañar la información o los procesos. Hoy en día, el sistema de calidad de las empresas debería describir el proceso cibernético y su mejora, incluyendo una evaluación de riesgos para cada uno (Zabalo, 2019).

Por ende, los sistemas de calidad se convierten en detectores de riesgos que recopilan y controlan información sobre los mismos. Un riesgo informático puede tener un impacto fuerte o

leve dependiendo de su ubicación y de si se puede detectar a tiempo. Por ejemplo, deshabilitar el firewall de un sistema debido a circunstancias especiales puede provocar una intrusión de entidades externas, lo que resulta en hackeo o fuga de información y grandes pérdidas (Torre, 2023).

2.4. Control aduanero.

En el artículo 37 de COPCI establece que las personas y medios de transporte que ingresen o salgan de una ZEDE, así como los límites, puntos de acceso y de salida de las zonas especiales de desarrollo económico deberán estar sometidos a la vigilancia de la administración aduanera. El control aduanero podrá efectuarse previo al ingreso, durante la permanencia de las mercancías en la zona o con posterioridad a su salida Los procedimientos que para el control establezca la administración aduanera, no constituirán obstáculo para el flujo de los procesos productivos de las actividades que se desarrollen en las ZEDE; y deberán ser simplificados para el ingreso y salida de mercancías en estos territorios (COPCI, 2010).

Además, el control aduanero es una de las funciones del Servicio Nacional de Aduanas del Ecuador. Sin control aduanero, estas no pueden ejercer sus facultades y cumplir con las normas que permiten el movimiento de mercancías entre países. Por ello, la Organización Mundial de Aduanas define el control aduanero como medidas tomadas para garantizar el cumplimiento de las leyes y reglamentos de los cuales las aduanas son responsables (Rodríguez, 2022).

Por ende, para llevar a cabo las funciones descritas, la autoridad aduanera deberá cumplir con las normas aduaneras, así como con los contratos, convenios y normas especiales que permitan el ejercicio de sus facultades.

Según la Organización Mundial de Aduanas (OMA) este un organismo que brinda servicios, incluida la aplicación de la legislación aduanera, la recaudación de derechos e impuestos sobre

mercancías importadas y exportadas y la aplicación de otros servicios. leyes y regulaciones, normas de exportación, transporte o almacenamiento. Esto incluye varias medidas aplicables para asegurar el cumplimiento de las normas de competencia en la administración aduanera, así como medidas aplicables a las operaciones de comercio exterior y a los controles de las entidades involucradas. serán necesarios para alcanzar los objetivos de la agencia y se llevarán a cabo de forma selectiva utilizando medios técnicos, equipos de inspección y métodos de gestión de riesgos para lograr los máximos resultados mediante un trabajo administrativo optimizado (Oltra y Ibáñez, 2019).

En contexto, las funciones de supervisión desempeñadas por el servicio de aduanas, que se realizan mediante el denominado sistema de control aduanero, no son más que una serie de actividades de las autoridades de esta índole, como la inspección de las mercancías, el muestreo, la verificación de los datos contenidos y la información sobre la carga, en la declaración de aduana, entre otros. Por ello, su autenticidad está comprobada por las cuentas y otros registros de los usuarios de la aduana, inspeccionando vehículos, mercancías y equipajes y realizando investigaciones. Diversas estrategias exhaustivas que permite a la Aduana tomar cualquier medida que pueda imaginar para garantizar que se lleven a cabo sus controles (Mosquera, 2021).

2.4.1. Ámbito de aplicación

En el artículo 103 del COPCI determina que por ámbito de aplicación se tiene que este regula las relaciones jurídicas entre el Estado y las personas naturales o jurídicas que realizan actividades directa o indirectamente relacionadas con el tráfico internacional de mercancías. Para efectos aduaneros, se entiende por mercancía a todos los bienes muebles de naturaleza corporal (COPCI, 2010).

2.4.2. Control aduanero anterior, concurrente y posterior

Esto parte de reglamentos sobre la duración del control aduanero. Para este efecto, la normativa aduanera establece que los controles realizados inician con el proceso de nacionalización o desde el momento de la presentación de la declaración aduanera. De acuerdo con regulación y normativa de cada país (Guerra, 2020).

2.5. Funciones de aduanas

Aylas y Alcalá (2022) señalan que las funciones de las aduanas son incrementar el patrimonio cultural del país en términos económicos, por lo que intentan proteger los intereses de las empresas privadas y hacer justo el comercio de todos los bienes. El objetivo principal del control aduanero es prevenir la formación de más comerciantes informales y el incumplimiento de las políticas y regulaciones nacionales. El resultado de realizar estas funciones es que se pueden generar enormes ingresos tributarios.

2.5.1 Obligaciones del control aduanero

La Aduana está sujeta a la ley general y tiene los siguientes dos puntos: primero, debe garantizar la entrada y salida de mercancías dentro de un área determinada, y segundo, debe monitorear toda la información de las mercancías con el objetivo de: reducir las actividades ilegales (Oltra y Ibáñez, 2019).

2.5.2. Acciones de control aduanero

Entre las actividades que realiza el control aduanero, Rodríguez (2022) planteó que estas actividades se basan en relaciones de inspección constituidas por la responsabilidad que realizan las personas cuando pretenden ingresar mercancías a la aduana. Las acciones realizadas son

efectuadas por los responsables de velar por la legalidad de las mercancías, esto permite conocer de la existencia de estos controles de la siguiente manera:

- Para estos efectos el Servicio Nacional de Aduana del Ecuador podrá solicitar información a las demás instituciones del sector y empresas públicos respecto de las personas que operen en el tráfico internacional de mercancías. Para la información requerida por el Servicio Nacional de Aduana del Ecuador no habrá reserva ni sigilo que le sea oponible. Cuando una de las dos instituciones así lo requiera, el control posterior se podrá realizar mediante acciones coordinadas entre el Servicio Nacional de Aduana del Ecuador y el Servicio de Rentas Internas.
- En caso de que como resultado del control concurrente se determinen errores en una declaración aduanera aceptada, que den lugar a diferencias a favor del sujeto activo, se emitirá una liquidación complementaria. Las liquidaciones complementarias se podrán hacer hasta antes del pago de los tributos, en caso contrario se someterá el trámite a control posterior. En las mismas condiciones, y siempre que no exista presunción fundada de delito, se podrán admitir correcciones a la declaración aduanera y sus documentos de soporte, excepto en los casos que establezca la normativa aduanera dictada para el efecto.
- En todo caso de correcciones a una declaración aduanera el Servicio Nacional de Aduana del Ecuador conservará un registro de la información inicialmente transmitida o presentada, de todos los cambios que se efectúen y las servidoras o servidores públicos que intervinieren en dicho proceso (COPCI, 2010).

2.6. El Delito Informático y su realidad procesal en el Ecuador

Desde que en 1999 se discutió el proyecto de ley del Ecuador sobre comercio electrónico, mensajes de datos y firma electrónica, el tema se ha popularizado con diversos cursos,

seminarios y conferencias. También se formó un comité para discutir la ley y brindar información de organismos directamente interesados en este tema como CONATEL, Autoridad Reguladora Bancaria, Cámara de Comercio, entre otros, que consideran el comercio telemático como una buena oportunidad de negocio, denotando que el país ha entrado en el período de auge de la llamada nueva economía (Torre, 2023).

Por ende, cuando se propuso esta ley por primera vez, tenía varios vacíos que se fueron mejorando con el tiempo, uno de los cuales fue la parte penal de la ley, porque las violaciones a esta ley son los llamados delitos informáticos, y como se les conoce, ser un castigo con base en las disposiciones del código penal, comprendiendo que esta situación es un tanto forzada si consideramos que el mencionado código penal con los últimos avances en tecnologías informáticas y de procesamiento remoto, se han vuelto inútil para mantener a las empresas de procesamiento remoto a salvo de posibles ataques de ciberdelincuencia. (Mosquera, 2021). Además de presentar criterios muy ambiguos en temas relacionado a los delitos informáticos, por lo que deja vacíos al momento de abordar, regular o sancionar este delito en el país.

Finalmente, en abril de 2002, después de largas discusiones, los destacados representantes aprobaron el texto final de la Ley de Comercio Electrónico, Información de Datos y Firma Electrónica y luego reformaron el Código Penal, que aclaró el llamado delito informático. Según la constitución de la república se denomina Juicio Prejudicial y Penal. Esto está de acuerdo con el artículo 33 del Código de Procedimiento Penal, que establece que el examen de un caso público es responsabilidad exclusiva del fiscal (Samaniego, 2024).

De lo anterior se puede concluir que el responsable del proceso penal y de la investigación preliminar y procesal de los hechos considerados delictivos en el nuevo sistema de persecución penal es el fiscal. Por lo tanto, el fiscal debe tomar la iniciativa en la investigación de tales violaciones informáticas, que llevará a cabo de conformidad con el artículo 208 del Código

Procesal Penal y sus órganos subsidiarios, dentro de los cuales destacan la policía judicial, quienes deben realizar investigaciones de delitos públicos y privados bajo la dirección y control del Ministerio Público, por lo que los resultados de las referidas investigaciones se incluirán ya sea por el fiscal o investigaciones preliminares, todo lo cual forma parte de los elementos de aseguramiento que posteriormente ayudarán a los representantes del Ministerio de Estado a expresar las opiniones correspondientes (Ojeda et al., 2020).

El problema que señalan actualmente las autoridades que están llamadas a perseguir posibles infracciones informáticas es la falta de preparación del Estado y de la Policía Judicial en cuanto a procedimientos técnicos, en parte por la falta de infraestructura. Los fiscales y la policía que dirigen la investigación también carecen de todos los demás medios técnicos necesarios para procesar los llamados delitos informáticos, dado que la policía no cuenta con unidades especializadas como el FBI en Estados Unidos; que cuenta con una unidad de delitos informáticos o en España la Guardia Nacional cuenta con unidades especiales para ayudar en esta misión (Guerra, 2020).

Por otro lado, la función judicial de jueces y magistrados tampoco está preparada para abordar estas cuestiones, ya que, las leyes tipifican los delitos con una actitud tradicional y con la globalización actual es más tedioso legislar dada la demanda diaria y el crecimiento evidente a nivel tecnológico. Por ende, los delitos que por su estructura tipifican no pueden incluirse en estos nuevos delitos que utilizan las tecnologías de la información como medio o como fin. Por lo tanto, la policía y los departamentos gubernamentales deben crear unidades de investigación para abordar los problemas de ciberdelincuencia transfronterizos, así como a nivel nacional (Barrio, 2019).

Además, estas estructuras también pueden servir como base para la cooperación internacional formal o la cooperación informal basada en redes transnacionales de confianza entre organismos

encargados de hacer cumplir la ley. Esto se puede lograr mediante la aplicación de leyes de comercio electrónico, firmas electrónicas e informes de datos. La cooperación multilateral en grupos de trabajo multinacionales puede resultar especialmente útil, y ya hay ejemplos de cooperación internacional que resultan muy eficaces. De hecho, la colaboración puede conducir a la imitación y a un mayor éxito (Conal, 2023).

En los últimos años, con el desarrollo de la tecnología digital, ha surgido una nueva generación de delincuentes que exponen a gobiernos, empresas privadas, gubernamentales e individuos a estos peligros (Díaz, 2020).

Por lo tanto, no sólo existe la necesidad de leyes e instrumentos eficaces y compatibles que permitan a los países cooperar idealmente en la lucha contra los delitos informáticos, sino también una necesidad en cuanto a temas de tecnología e infraestructura y recursos humanos para hacer frente a esta nueva forma de delincuencia transnacional.

3. Metodología del Proceso de Investigación

3.1. Enfoque de la investigación

Este estudio adopta un enfoque cualitativo, dada la naturaleza del fenómeno bajo investigación: la evaluación de la vulnerabilidad en las redes informáticas aduaneras y la aplicación de estrategias de mitigación ante prácticas de delitos informáticos. Los datos fueron recopilados a través de un proceso inductivo, durante el cual se observaron y analizaron los fenómenos sin manipular directamente las variables, conforme a los principios establecidos por Arias (2021), quien sostiene que en los modelos inductivos las variables son observadas y no alteradas.

Este enfoque permite una comprensión profunda de las dinámicas de seguridad informática dentro del contexto aduanero, basándose en la observación natural de las prácticas existentes, tal como se describen en fuentes secundarias y mediante entrevistas con personal clave involucrado en la gestión de las tecnologías informáticas en aduanas, además de abogados especializados en derecho penal, tributario y aduanero. Este método es esencial para captar la realidad tal como es percibida y vivida por aquellos dentro del sistema, facilitando un análisis detallado de cómo las políticas y prácticas actuales influyen y configuran la seguridad operacional.

Adicionalmente, se utilizan entrevistas semi-estructuradas para recopilar datos cualitativos, lo que proporciona libertad para explorar en profundidad las actitudes, percepciones y experiencias del personal y de profesionales del derecho. Esta técnica es complementada con la revisión de documentación relevante, como manuales de operación, informes de seguridad y protocolos de respuesta ante incidentes, que ayudan a construir un marco de análisis más robusto.

La integración de métodos cualitativos con el análisis documental facilita la triangulación de datos, mejorando la validez de los hallazgos al comparar múltiples perspectivas sobre los mismos

fenómenos. Esta sinergia entre técnicas inductivas y revisiones sistemáticas permite una comprensión integral de los mecanismos de vulnerabilidad y defensa dentro de las redes informáticas aduaneras.

Según Sampieri (2018), este enfoque no solo permite describir y contextualizar el comportamiento y las actitudes sino también desarrollar un entendimiento teórico que puede prever y explicar los comportamientos y las respuestas institucionales ante amenazas cibernéticas. Así, el estudio cualitativo aquí propuesto no solo identifica las prácticas existentes, sino que también sugiere posibles mejoras y estrategias basadas en los datos recogidos, apuntando hacia recomendaciones prácticas y políticas para fortalecer la seguridad de la información aduanera.

3.2. Alcance de Investigación

El alcance de esta investigación es de carácter descriptivo, exploratorio y explicativo dado que a nivel exploratorio esta indagación se realiza para analizar los problemas de vulnerabilidad y posibles hackeos en las redes informáticas de las aduanas, existen pocos antecedentes o datos similares antes de la investigación, por lo que se deben investigar todos los temas relacionados con el desarrollo.

Por ende, a nivel descriptivo y explicativo se tiene que este medio se enfoca en los sujetos de investigación en este caso el personal de la Dirección Nacional de Mejora Continua y Tecnología de la Información, que labora en las instalaciones de la aduana en su entorno natural y en la realidad cotidiana y abogados profesionales y especializados en temas penales y aduaneros.

Por lo tanto, este estudio es esencialmente un diseño de literatura descriptivo transversal que permite clasificar los datos obtenidos en descriptivo y explicativo donde se revisó las variables específicas durante el estudio del problema. Por lo tanto, el alcance de la investigación será

transversal y basado en categorías, conceptos, eventos, contextos y perspectivas expresadas por diferentes autores y sus diferentes opiniones y conclusiones, incluidas aquellas que ocurren sin la intervención del investigador o cambios en las variables y conclusiones del estudio.

Asimismo, este estudio se centra en este fenómeno con el fin de conocer desde una perspectiva no experimental el impacto de la vulnerabilidad en la seguridad informática frente a los posibles hackeos en las redes informáticas de aduana. Según Cohen y Gómez (2021), la investigación no experimental no implica cambios en factores o variables, sino que todos los análisis se basan en datos reales y derivados de la realidad.

3.3. Delimitación de la investigación.

La investigación se desarrollará durante un período de cuatro meses, concentrándose geográficamente en la ciudad de Guayaquil, Ecuador. Este marco temporal y espacial está diseñado para proporcionar un contexto intensivo y focalizado que permita una inmersión profunda en el entorno específico de las aduanas locales, donde se evaluarán las prácticas de seguridad de la información.

3.4. Población y muestra de la investigación

Población

La población de este estudio incluye a todos los individuos que interactúan en la Dirección Nacional de Mejora Continua y Tecnología de la Información y Analistas aduaneros que son abogados especializados de las aduanas de Guayaquil, así mismo es un abogado especializado en derecho penal. Este grupo está bien posicionado para proporcionar información detallada sobre las vulnerabilidades, falta de tipicidad, medidas de seguridad en la infraestructura de tecnologías informáticas, dado su conocimiento y experiencia directa en el manejo de dichos sistemas. Según Alonso (2019), es crucial definir el conjunto de elementos (universo) cuyas

propiedades se desean explorar, lo que en este caso se relaciona con las interacciones cotidianas con la tecnología y la seguridad informática en el contexto aduanero.

Muestra

La muestra de este estudio está compuesta por el personal de la Dirección de Mejora Continua y Tecnología de la Información de la aduana de Guayaquil, que asciende a dos individuos. Estos profesionales han sido seleccionados debido a su involucramiento directo y sus roles específicos dentro del marco organizacional y operacional de la aduana, lo que les proporciona una perspectiva única sobre los desafíos y las prácticas de seguridad actuales. Además de analistas jurídicos como abogados especializados en derecho aduanero y derecho penal.

Hernández y Batista (2006) destacan que una muestra debe representar adecuadamente las características del universo de estudio, lo cual se asegura en este enfoque dado que la muestra incluye a todos los integrantes relevantes del departamento.

3.5. Métodos empleados.

En este estudio se utilizaron entrevistas semiestructuradas como principal técnica de recolección de datos, enfocándose en el personal del departamento de la Dirección Nacional de Mejore Continua y Tecnología de la Información de la Aduana de Guayaquil, además de analistas jurídicos. Este método fue seleccionado debido a su eficacia para explorar en profundidad las percepciones y experiencias del personal sobre la seguridad de la información dentro de su entorno laboral.

Entrevista al jefe del Departamento de la Dirección Nacional de Mejora Continua y Tecnología de la Información Ingeniero David Chaug.

La entrevista al jefe de este departamento fue fundamental para obtener una comprensión exhaustiva de la gestión de la seguridad de la información en la organización. Como líder del equipo, el jefe tiene una visión integral y detallada del diseño, implementación y evaluación de las medidas de seguridad que protegen los sistemas informáticos de la aduana. Esta entrevista proporcionó resultados valiosos sobre los desafíos, las estrategias y las políticas actuales en materia de seguridad.

Entrevistas con Otros Empleados del Departamento Ing. Patty Blum y analista jurídico Abg. Diego Polit Rivas.

Además, se realizaron entrevistas con otros miembros del equipo, quienes aportan conocimientos técnicos y operativos sobre la configuración diaria y la operación de los sistemas de seguridad. Estas entrevistas fueron esenciales para corroborar y complementar la información proporcionada por el jefe del departamento, ofreciendo una visión más diversa y representativa de las prácticas de seguridad actuales. Este enfoque permite captar distintos niveles de experiencia y perspectiva dentro del mismo departamento, enriqueciendo la calidad y profundidad de los datos recogidos.

Justificación de la Metodología

La elección de entrevistas semi-estructuradas se justifica por la flexibilidad que ofrecen, permitiendo que el entrevistador y los entrevistados profundicen en temas específicos que surjan durante la conversación. Esto es particularmente útil en contextos donde los aspectos técnicos y operativos de los sistemas son complejos y multifacéticos. Además, esta técnica facilita la exploración de aspectos no anticipados al inicio de la investigación, ajustándose a la naturaleza dinámica para abordar temas tecnológicos y legales.

3.6. Procesamiento y análisis de la información.

El análisis de datos en esta investigación fue esencialmente cualitativo, enfocado en profundizar en la comprensión de las prácticas de seguridad de la información en el departamento de la Dirección Nacional de Mejora Continua y Tecnología de la Información de la Aduana de Guayaquil. Este proceso comenzó con una extensa recopilación documental, diseñada para fundamentar el marco teórico del estudio. Se revisaron publicaciones académicas, informes técnicos, resoluciones del SENAE y documentos internos relacionados con las prácticas de seguridad de la información, lo que permitió establecer una base sólida de conocimiento previo sobre el tema.

3.6.1. Recopilación Documental

La recopilación documental involucró la sistematización de información procedente de diversas fuentes autorizadas, lo que facilitó la identificación de tendencias, patrones y brechas en el campo de la ciberseguridad aduanera. Este proceso no solo ayudó a contextualizar la investigación dentro del espectro más amplio de la seguridad informática sino también a definir las áreas clave que requerían exploración detallada mediante entrevistas y análisis directo.

3.6.2. Entrevistas

Las entrevistas semi-estructuradas con el personal del departamento de informática constituyeron la segunda fase de la recopilación de datos. Estas entrevistas fueron diseñadas para complementar los hallazgos de la recopilación documental, proporcionando información detallada sobre las herramientas tecnológicas y el análisis de leyes penales y aduaneras. Cada entrevista fue transcrita y analizada meticulosamente para identificar declaraciones clave que reflejaran las perspectivas de los empleados sobre la efectividad, deficiencias y áreas de mejora de las estrategias de seguridad actuales.

3.6.3. Análisis de Datos

El análisis de los datos recopilados se realizó a través de un enfoque inductivo, donde los patrones emergentes fueron identificados y categorizados para formular conclusiones fundamentales sobre el estado de la seguridad de la información en la aduana. Este análisis fue fundamental para discernir las causas subyacentes de las vulnerabilidades detectadas y para proponer recomendaciones basadas en evidencias concretas. Se utilizó codificación abierta para desglosar las transcripciones de las entrevistas en unidades de información que fueron posteriormente agrupadas en temas mayores.

3.6.4. Presentación de Información

La información obtenida fue sistematizada y presentada de manera que permitiera una fácil interpretación y comparación de datos. Los resultados se organizaron temáticamente en torno a las áreas de interés identificadas inicialmente en el marco teórico, y se utilizaron citas directas de las entrevistas para ilustrar puntos clave, siguiendo prácticas éticas de confidencialidad y anonimato de los participantes.

4. Análisis de Resultados de la investigación

4.1. Presentación de resultados.

Tabla 1. Entrevista ejecutada al jefe de la Dirección Nacional de Mejora Continua y Tecnologías de la Información Ing. David Chaug.

Entrevistado	Jefe de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.
Preguntas	**Opiniones**
¿En la actualidad la organización cuenta con políticas o normas para la seguridad en el sistema de control aduanero?	Si. En este momento la organización cuenta con unas políticas de control interno la cual se presenta para el personal nuevo, en reclutamiento y se les recuerdan dichas normas cada mes.
¿Cómo se encuentra actualmente estructurada la red?	La estructura, esta parte desde dos perspectivas el ingreso y salida de mercancía. Así como la procedencia y destino de dicha mercancía, es allí de donde parte la red, en chequeo, cifrado, puesta en sistema, entre otros.
¿Describa los equipos de gestión de seguridad o Software con los que actualmente cuenta la organización?	La organización cuenta con un sistema de seguridad para proteger no solo la mercancía que llega a las instalaciones, si no los datos sobre los cuales se reposa dicha mercancía.
¿Qué software es utilizado para el servidor de control aduanero?	Es un software de sistema, de base de datos. El cual es capaz de resguardar y proteger todos los datos que ingresa el personal en el desarrollo de sus actividades.
¿Tiene conocimiento de algún ataque que se haya realizado al servidor de comunicaciones?	Hasta el momento y durante mi gestión no he tenido ningún reporte de ataque que haya tenido peso. Si ha existido intentos de hackeo, pero han sido solventados inmediatamente.
¿Ha existido la conexión de usuarios no autorizados a través de redes privadas?	Hasta el momento ha ocurrido intento sede conexión y hasta manejo del sistema desde fuentes o mecanismos externos. Los mismos han sido vistos a tiempos y atacados con los diversos mecanismos.

4.1.2. Entrevistas con Empleado del Departamento de la Dirección Nacional de Mejora Continua y Tecnologías de la Información.

Tabla 2. Entrevista al empleado analista Ing. Patty Blum.

Entrevistado	Otro empleado del Dpto. Bajo supervisión
Preguntas	**Opiniones**
¿En la actualidad la organización cuenta con políticas o normas para la seguridad en el sistema de control aduanero?	SI. Dichas normas las evaluamos todos los meses.
¿Cómo se encuentra actualmente estructurada la red?	La red desde el control interno hasta el manejo correcto de usuarios y claves
¿Describa los equipos de gestión de seguridad o Software con los que actualmente cuenta la organización?	En la actualidad se utilizan Servidores proxy y almacenamientos de respaldo.
¿Qué software es utilizado para el servidor de control aduanero?	El más utilizado es el de sistema que abarca todo lo relacionado a bases de datos y cubre la extensión del soporte de la información y demás baches de las plataformas.
¿Tiene conocimiento de algún ataque que se haya realizado al servidor de comunicaciones?	En mi experiencia laboral hasta el momento no he visto un ataque que afecte las relaciones de entrada y salida de mercancía.

4.1.2.2 Entrevista a Abogado especializado en derecho aduanero y derecho penal Abg. Diego Polit Rivas.

Entrevistado	Abogado.
Preguntas	**Opiniones**
En ecuador los delitos informáticos no estas tipificados ni regulados ¿Qué elementos se deberían considerar para lograr agregar al Código Orgánico Integral Penal (COIP) este tipo de delitos?	Los delitos informáticos deben tener los mismos elementos que otros delitos: nombre, sujeto activo, sujeto pasivo, acción, bien jurídico protegido, partes objetiva y subjetiva, y pena. Además, es importante considerar la voluntariedad, ya que muchas personas aceptan anuncios sin leerlos y ceden datos personales. En estos casos, la responsabilidad es de quien no cuida su información, no de quien promueve estos acuerdos
Frente a la situación actual que vive el país ¿considera necesario realizar reformas y tipificar los delitos informáticos?	Más allá de la situación actual en Ecuador, la necesidad de incluir los delitos informáticos en el Código Orgánico Integral Penal surge del avance tecnológico. El derecho penal existe para regular y contener delitos que vulneren bienes jurídicos protegidos, no solo los más comunes.

	Aunque en Ecuador los delitos informáticos pueden no estar tipificados, sí lo están en otros países. Por ello, es esencial tipificar estos delitos, ya que pueden cometerse fácilmente desde la comodidad de una casa.
¿Conoce de algún caso real donde la falta de tipicidad de estos delitos informáticos haya sido un problema de vulnerabilidad del sistema de control aduanero?	Los delitos informáticos son un tema importante, especialmente cuando se relacionan con el control aduanero. La aduana gestiona mercancías y recauda impuestos sobre importaciones y exportaciones, actuando como un filtro entre lo nacional e internacional. Por eso, es esencial contar con métodos efectivos de seguridad. Sin embargo, la falta de tipificación específica de estos delitos puede permitir que se utilicen figuras legales o principios como "nullum crimen, nulla poena sine lege" (no hay crimen ni pena sin ley) para evitar el enjuiciamiento de estos delitos.
Frente a la creciente de los delitos informáticos ¿Cómo se ve afectado el sistema de control aduanero?	Aunque el Código Orgánico Integral Penal contempla ciertos delitos informáticos, no abarca aquellos que pueden afectar directamente al sistema de control aduanero. Es crucial incluir delitos como estafas, robo de datos, sabotajes informáticos e incluso phishing, ya que pueden causar grandes perjuicios en este ámbito tan importante.
¿Existen acuerdo de cooperación con otras instituciones o internacional para combatir los delitos informáticos en temas de aduanas?	La Interpol juega un papel crucial en la lucha contra los delitos, incluidos los ciberdelitos relacionados con las aduanas. Utiliza el intercambio de información y la coordinación de operaciones entre países, proporcionando plataformas para que las autoridades colaboren de manera más efectiva.

Todo lo expuesto anteriormente deja ver que la seguridad en el sistema de información aduanera se refiere a cualquier actividad, proceso, tecnología o política que está diseñada para proteger los recursos digitales de cualesquiera amenazas a la confidencialidad y la disponibilidad de los datos suministrados. Tanto así que el principal objetivo de estos es proteger los datos, sistemas y dispositivos almacenados evitando los ataques maliciosos y que un tercero pueda acceder a la

red interna de computadoras u otros dispositivos. El personal dejo ver que todas estas políticas hasta el momento han garantizado que la información que entre y salga del dispositivo se mantenga únicamente entre el dispositivo y su destinatario, permanece confidencial y se mantiene alejada de terceros.

5. Discusión de resultados.

Desde nuestra perspectiva, la seguridad de la infraestructura del sistema de control aduanero es un tema crítico en el ámbito de la tecnología de la información. En un mundo cada vez más digital y conectado, los sistemas y redes informáticas aduaneras son esenciales para el funcionamiento eficiente de organizaciones y gobiernos a nivel global. Sin embargo, esta interconexión trae consigo numerosos desafíos en términos de ciberseguridad, vulnerabilidad de la información y hackeos. En nuestro estudio, hemos evidenciado los desafíos que enfrentan las estrategias de protección de la infraestructura de red informática aduanera, donde las amenazas a la red se vuelven cada vez más complejas y plantean desafíos constantes para su protección.

Es evidente para nosotros que es necesario aumentar la conciencia sobre la seguridad y capacitar a los empleados en prácticas de seguridad para prevenir posibles vulneraciones del sistema de información aduanero. Consideramos que este es uno de los pilares importantes para mitigar estas amenazas. En este contexto, creemos que es esencial implementar un enfoque de seguridad integral que incluya medidas tanto preventivas como reactivas. No solo es crucial el uso de tecnología avanzada, sino también el desarrollo y la implementación de una política de seguridad sólida. Además, la colaboración entre departamentos y el intercambio de inteligencia sobre amenazas pueden mejorar aún más la protección de la infraestructura.

Para nosotros, tiene sentido la implementación de estrategias de seguridad basadas en prácticas de mitigación anti-hackeo. Esto incluye la verificación de la identidad y el acceso de cada usuario y dispositivo, independientemente de su ubicación en la red. Además, es crucial que las políticas de seguridad se monitoreen y actualicen continuamente a medida que evolucionan las amenazas, manteniéndose a la vanguardia de la tecnología y su crecimiento. La rápida adopción de medios virtuales crea desafíos para la gestión y la visibilidad de la infraestructura de red, y la distribución de activos y datos en entornos virtuales y de nube requiere soluciones de seguridad

especializadas, como herramientas de segmentación definida por software que permitan la gestión unificada de amenazas. También consideramos fundamental garantizar que los proveedores de servicios en la nube mantengan altos estándares de seguridad y establecer políticas de seguridad coherentes en todos los entornos de las redes virtuales.

En cuanto a los aspectos normativos, creemos que es crucial que los delitos informáticos se agreguen explícitamente al Código Orgánico Integral Penal (COIP) para mitigar su actividad en el país. Estos delitos afectan la capacidad de las autoridades aduaneras para detectarlos y prevenirlos. Aunque el COIP menciona los delitos informáticos, consideramos que su redacción es ambigua y presenta lagunas legales, lo que facilita la proliferación de estos delitos y afecta la seguridad y la economía del país.

Por ende, pensamos que la aplicación adecuada y eficaz de leyes y políticas de gestión de seguridad y riesgos ante la vulnerabilidad de la información en el sistema de control aduanero garantiza que existan los procedimientos necesarios para reducir o eliminar amenazas que puedan afectar la información y otros activos críticos de hardware y software. La implementación de una adecuada práctica de gestión anti-hackeo en las redes informáticas aduaneras, junto con políticas y leyes vigentes, reduce significativamente el riesgo. Permite la identificación temprana de posibles amenazas y la implementación de medidas preventivas para reducir su impacto y prevenir su ocurrencia. Esta combinación de medidas no solo protege la infraestructura, sino que también asegura la integridad de los datos aduaneros, contribuyendo a la eficiencia y seguridad de las operaciones aduaneras en un entorno cada vez más digital.

En resumen, consideramos que la ciberseguridad en el sistema de control aduanero requiere un enfoque integral y multidisciplinario, que aborde tanto las necesidades técnicas como normativas. Solo así se podrá garantizar un entorno seguro y confiable para las operaciones aduaneras y, por ende, para la economía y la seguridad del país.

6. Conclusiones

A nivel de análisis de la vulnerabilidad de la información en el sistema de control aduanero en la práctica de delitos informáticos, a fin de establecer la aplicación de estrategias de mitigación se puede concluir que es fundamental establecer requisitos de seguridad adecuados para proteger los activos de información utilizados por los empleados de la organización en el desempeño de diversas tareas para que el trabajo diario pueda realizarse con el objetivo de alcanzar las metas de la entidad. La reforma y aplicación de leyes en dichas normas vigentes permitirán controlar temas de vulnerabilidades, amenazas y peligros asociados con cada propiedad, como se desarrolló en el cuerpo de esta investigación, punto que ha demostrado ser fundamental para gestionar adecuadamente los riesgos inherentes.

Frente a los objetivos específicos se tiene que, se reconoce que implementar o tipificar los delitos informáticos en el Código Orgánico Integral Penal, puede hacer una gran diferencia ante el cometimiento de este delito y así reducir la vulnerabilidad de cada activo de información, minimizando riesgos inherentes en la entidad del Servicio Nacional de Aduanas del Ecuador. A su vez, creando políticas reflejándose en sistemas legales de otros países como base para poder regular estos delitos en el país.

En cuanto a identificar la relación existente entre la vulnerabilidad en el sistema de control aduanero y las prácticas de mitigación anti - hackeo en las redes informáticas, se concluye que es necesario proteger los recursos críticos de una organización que requiere implementar estrategias efectivas para prevenir y mitigar las amenazas a la seguridad y garantizar el cumplimiento y regulaciones. Al proteger la integridad, la confidencialidad y la disponibilidad de los activos de información, se puede garantizar que la entidad pueda continuar operando y alcanzar sus objetivos comerciales. Por ello, proponer políticas y recomendaciones para fortalecer el sistema de información aduanera, es necesario, pues se requiere aplicar medidas

de seguridad para garantizar que no se interrumpa la continuidad del proceso, teniendo en cuenta la integridad, confidencialidad y disponibilidad de los activos de información, de modo que las actividades en las que participa la entidad no se vean comprometidas.

Frente a proponer un marco de políticas y recomendaciones para robustecer el sistema de información aduanero, se concluye que ciertamente en cuanto a temas de seguridad de la información la prevención es muy importante porque permite desarrollar planes y estrategias para afrontar situaciones imprevistas, garantizar el cumplimiento del sistema de control aduanero y proteger los activos de dicha entidad.

7. Recomendaciones/Propuesta

Se debe dar mayor prioridad al sistema de control aduanero, ya que presenta información identificada como de alto riesgo en la práctica de delitos informáticos. Este aspecto es crucial, ya que su impacto podría tener consecuencias financieras o de reputación negativa para la entidad gubernamental si no se toman las precauciones adecuadas.

A continuación, proponemos el siguiente modelo conceptuales como estrategia de mitigación fundamentales que se deben implementar en el sistema de control aduanero para mejorar los estándares de seguridad y garantizar la disponibilidad, integridad y confidencialidad de la información. Si bien el proceso puede variar, el resultado final es siempre el mismo: identificar y corregir vulnerabilidades para mejorar la seguridad de los sistemas y redes. Para mantener la seguridad de la información, es importante recordar que la continua actualización e integración de tecnologías puede crear nuevas amenazas, lo que significa que los riesgos asociados con los activos de información de la organización también cambiarán. Por lo tanto, es esencial que todas las actualizaciones de estas funciones se basen en revisiones de seguridad definidas por el proyecto para garantizar que la información esté adecuadamente protegida.

De esta manera, se fortalecerá la capacidad institucional para enfrentar los desafíos que representan los delitos informáticos, garantizando un entorno más seguro y controlado tanto para el comercio como para la ciudadanía en general.

Por ende, dado el creciente impacto de los delitos informáticos en las operaciones económicas y de seguridad del país, es necesario incorporar herramientas metodológicas que ayuden a la prevención y mitigación frente al cometimiento de delitos informáticos que afectan las operaciones aduaneras, representan una amenaza significativa para la economía y la seguridad nacional.

Tabla 1. Criterios de vulnerabilidad según la severidad.

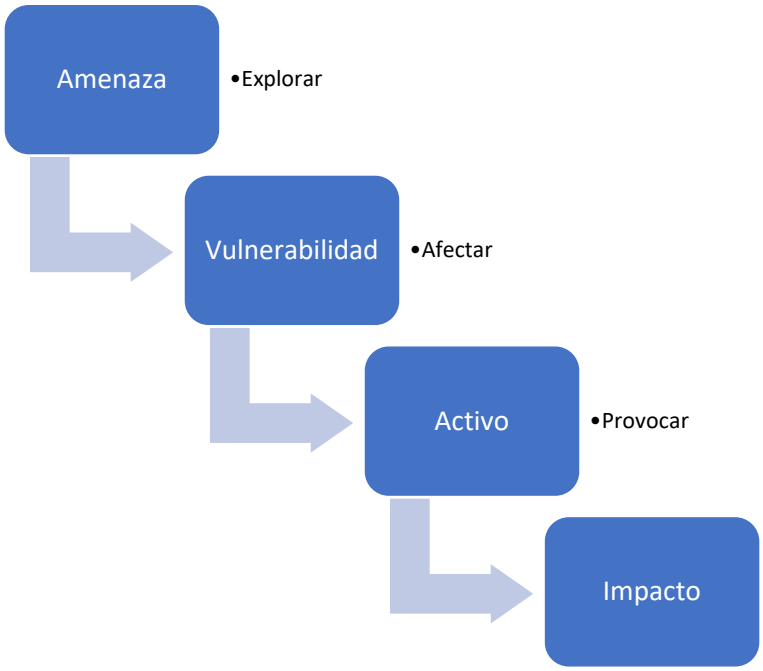
CLASIFICACIÓN	DESCRIPCIÓN
Crítica	Vulnerabilidades que reflejan exposiciones no comunes, Pero que en realidad comprometen el objetivo empresarial, reflejando un riesgo efectivo para la confidencialidad, integridad y disponibilidad de la información.
Alta	Vulnerabilidades que pueden representar un riesgo de explotación para la confidencialidad, integridad y disponibilidad de la información objetivo.
Media	Una vulnerabilidad que plantea un riesgo bajo de explotar la confidencialidad, integridad o disponibilidad de la información. Aun cuando la vulnerabilidad es baja, puede permite activar y desactivar el acceso.
Baja	No existen vulnerabilidades que representen un riesgo de explotación para la confidencialidad, integridad o disponibilidad de la información.
Informativa	Esto no se considera una vulnerabilidad, sino información importante sobre el servicio que se analiza.

Nota. La tabla muestra los criterios vulnerables que forman parte de la medición del nivel de riesgo. Fuente: (Villacres, 2021)

- Posteriormente a esto es necesario la definición del impacto, reconociendo que este se refiere a la forma en que una amenaza explota la vulnerabilidad de un activo del sistema de control aduanero y normalmente se mide por el grado de deterioro del activo. Las pruebas de penetración implican varios pasos para completar el proceso, aunque cada paso requiere el consentimiento del supervisor para comenzar. Por ende, se debe

determinar el nivel de amenaza que es un peligro eminente del hackeo que puede explotar en consecuencia financieras y de reputación. El nivel de vulnerabilidad el cual se enfrentó el sistema y su afección, seguido del activo que se vio comprometido y que puede provocar el impacto evidente en la acción negativa hacia la estrategia de mitigación.

Figura 1. Determinación de los puntos para establecer el impacto



Nota. La imagen muestra los niveles en medición del impacto. Fuente: (Villacres, 2021).

- Por ende, es necesario establecer fases que controlen el impacto ante la posible vulneración de la información en el sistema de control aduanero. Estas fases se utilizan normalmente de la siguiente manera:
  i. Fase de identificación. En esta fase inicial se definen los objetivos y se recopilan los datos requeridos para la auditoría, como los nombres de los activos de información de la organización, direcciones de correo electrónico, diagramas de red y direcciones IP.

ii. Fase de investigación. Se utiliza la información recopilada en el paso anterior para buscar posibles vectores de ataque, incluido el escaneo de puertos, servicios y versiones. Luego se examinan las vulnerabilidades para determinar el tipo de ataque.
iii. Fase de conteo. El objetivo de esta fase es encontrar información sobre datos del usuario, nombres de dispositivos, servicios de red, etc.
iv. Fase de acceso. Esta fase aprovecha las vulnerabilidades descubiertas en la fase anterior para obtener acceso al sistema.
v. Fase de presentación de informes. En la etapa final, se deja en claro para modo de aprendizaje y que no vuelva a ocurrir, las vulnerabilidades descubiertas y cómo fueron explotadas para poder tomar las mejores decisiones de seguridad en el futuro.

Si bien el proceso puede variar, el resultado final es siempre el mismo: identificar y corregir vulnerabilidades para mejorar la seguridad de los sistemas y redes. Para mantener la seguridad de la información, es importante recordar que la continua actualización e integración de tecnologías puede crear nuevas amenazas, lo que significa que los riesgos asociados con los activos de información de la organización también cambiarán. Por lo tanto, es importante que todas las actualizaciones de estas funciones se basen en revisiones de seguridad definidas por el proyecto para garantizar que la información esté adecuadamente protegida.

Por ende, como resultado de este modelo conceptual se presentan las siguientes estrategias de mitigación:

1. Mejorar la seguridad de la información de la entidad, lo que requiere implementar un proceso de gestión de vulnerabilidades para prevenir o mitigar nuevas vulnerabilidades que puedan surgir en el futuro. Estas herramientas pueden reducir el acceso no autorizado a los sistemas informáticos, bloquear puertos que albergan servicios críticos y hacer túneles de conexiones.

2. Realizar auditorías trimestralmente para que la organización pueda identificar potenciales vulnerabilidades y riesgos y así tomar acciones oportunas para prevenir daños o errores en el sistema de información.

3. Realizar informes periódicos para que la organización pueda actualizar datos sobre su estado, como informes con una jerarquía de vulnerabilidades en su sistema de red.

4. Implementar soluciones de seguridad basadas en la nube y cifrar datos en reposo y en tránsito es eficaz.

5. Desarrollar políticas de seguridad específicas.

6. Realizar evaluaciones de riesgos y proporcionar notificaciones adecuadas en cada caso.

7. Mantenerse al tanto de las regulaciones cambiantes y ajustar continuamente sus estrategias de retención. La clave para superar estos desafíos es implementar un sólido programa de gestión de seguridad de la información.

8. Evaluación periódica de la eficacia de las medidas de protección de la información, lo que ayudará a garantizar la continuidad de la entidad gubernamental y la seguridad de los activos críticos de la organización.

Beneficios de la aplicación de estrategias de mitigación

- Mantener la integridad de los datos.
- Mejora la imagen de la empresa.
- Productividad incrementada
- Evita gastos inesperados
- Mayor robustez y precisión de los datos.
- Esto conduce a la implementación de estrategias de conservación, cumplimiento de normas y estándares y dotación de personal profesional.

- Juega un papel importante en el cumplimiento de las regulaciones y estándares relacionados con la protección de datos. Esto incluye la detección temprana de posibles vulnerabilidades de seguridad, la evaluación de riesgos y la implementación de acciones correctivas para minimizar los efectos adversos.
- Proporciona un nivel crítico de protección contra posibles intrusos.

Por ende, contar con seguridad digital frente a la vulnerabilidad de la información en el sistema de control aduanero es importante porque este medio incluye todo lo relacionado con la protección de la información confidencial, información biométrica, información personal, software, compras y banca en línea, sistemas de TI gubernamentales y otras partes de la vida moderna que dependen de computadoras y otros dispositivos a fines.

Costos de ejecución

Descripción	**Monto**
Costos operativos	
Administración de Servidores	400$
Energía eléctrica de centro de datos	760$
Sistemas de respaldo	400$
Generadores	190$
Climatización	600$
Sistema contraincendios	300$
Capacitación al personal	200$
Subtotal	2.850$
Inversión	
Servidores Windows	550$
Data center virtual	480$
Enlaces delicados	80$

Subtotal	1.110$
Total	3960$

Recursos necesarios

1. Recursos físicos

- Personal
- Procesamiento
- Políticas de seguridad Robusta
- Tecnología
- ISO 27001
- Consulta a expertos

6. Recursos digitales

- Cifrado de nube
- Sistema de detección de riesgo
- Firewalls
- Antimalware
- Controles de acceso
- Uso de VPN
- Certificados SSL/TLS

Bibliografía

Alonso, J. (2019). *Metodología.* https://books.google.es/books?hl=es&lr=&id=-oeoyEHAwGIC&oi=fnd&pg=PA5&dq=Libros+de+metodologia&ots=NrgIxc09By&sig=KCR4R0KeIYq3-yY8r70DBdz5TqA#v=onepage&q=Libros%20de%20metodologia&f=false

Arias, J. (2021). *Diseño y metodología de la investigación.* http://repositorio.concytec.gob.pe/handle/20.500.12390/2260

Aylas, A., & Alcala de la Cruz, B. (2022). *El control de las aduanas en el delito de contrabando del Puerto del Callao.* https://repositorio.autonoma.edu.pe/handle/20.500.13067/1776

Barrio, S. (2019). *Nuevas tendencias en la gestión de riesgos del control interno.* https://asocex.es/wp-content/uploads/2019/06/Revista-Auditoria-Publica-n%C2%BA-73.-pag-43-a-51.pdf

Bekerman, U. (2020). *La gestión de riesgos cibernéticos en la Union Europea.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3636178

Bernal, J., Zorrilla, F., Rosales, N., Bailón, M., & Palacios, M. (2022). *Proceso de seguridad para evitar la infiltración de inyección SQL (SQL INJECTION).* https://revistas.milpaalta.tecnm.mx/index.php/IPSUMTEC/article/view/99

Catani, M. L. (2020). *Gestión de riesgos cibernéticos.* https://sedici.unlp.edu.ar/handle/10915/163322

Celis, D. (2020). *Corrupción en las aduanas, .* https://www.elfinanciero.com.mx/opinion/dario-celis/corrupcion-en-lasaduanas/

Cohaila, O. (2023). *Plan Estratégico para la Gestión de la Seguridad de la Información y la Ciberseguridad en la compañía de seguros SECREX.* https://repositorio.epnewman.edu.pe/handle/20.500.12892/870

Cohen, N., & Gomez, G. (2021). *Metodología de la investigación, ¿para qué?* https://biblioteca.clacso.edu.ar/clacso/se/20190823024606/Metodologia_para_que.pdf

Conal, C. (2023). *Ciberseguridad y Derecho penal.* https://portalciencia.ull.es/documentos/658b280e3c24c35ca4329a53?lang=en

Conal, I. (2020). *Ciberseguridad y Derecho penal.* https://books.google.es/books?hl=es&lr=&id=bu-mEAAAQBAJ&oi=fnd&pg=PT4&dq=Aspectos+cient%C3%ADficos+y+tecnol%C3%B3gicos+de+la+ciberseguridad&ots=MNqLsdA_zi&sig=y8C05R0QsoYQ5ly1lRqzqkwHq9o#v=onepage&q&f=false

COPCI, R. O.-d.-2. (2010). *CODIGO ORGANICO DE LA PRODUCCION, COMERCIO E INVERSIONES, COPCI.* https://www.gob.ec/sites/default/files/regulations/2020-04/CODIGO%20ORGANICO%20DE%20LA%20PRODUCCION%2C%20COMERCIO%20E%20INVERSIONES%20COPCI.pdf

Díaz, J. (2020). *Seguridad cibernética.* https://www.researchgate.net/profile/Juan-Diaz-Aparicio/publication/369790664_Seguridad_cibernetica/links/642cceab20f25554da0bd3eb/Seguridad-cibernetica.pdf

Donoso, M. C. (2022). *¿Cuán importante es la seguridad cibernética para lograr la seguridad hídrica?* https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S2215-38962022000100284

Garcés, L., Benjumea, M., Bernal, O., Valencia, A., & Saavedra, L. (2022). *Tendencias investigativas en el uso de tecnologías de Big Data en sistemas de ciberseguridad.* https://www.proquest.com/openview/67f6e1eb563ceb5ee29ce615722b6abc/1?pq-origsite=gscholar&cbl=1006393

García, G. (2019). *Contratación de la póliza de Ciberriesgos, tratamiento del siniestro y la importancia del reaseguro.* https://diposit.ub.edu/dspace/handle/2445/144759

Garzón, C., Navas, C., Illicachi, A., Espinoza, R., & Estrella, G. (2024). *Análisis de los Ataques de Ingeniería cibernética en Ecuador.* https://ciencialatina.org/index.php/cienciala/article/view/9777

Guaña, E., Sánchez, A., Chérrez, P., Chulde, L., Jaramillo, P., & Pillajo, C. (2022). *Ataques informáticos más comunes en el mundo digitalizado.* https://dspace.itsjapon.edu.ec/jspui/handle/123456789/3445

Guerra, V. (2020). *El papel de la Policía Fiscal y Aduanera para contrarrestar el contrabando a través de las plataformas digitales.* https://repository.unimilitar.edu.co/handle/10654/37101

Guerrero, J. (2021). *El control aduanero en la provincia del Carchi y el impacto en los delitos contra la administración aduanera.* http://repositorio.upec.edu.ec/handle/123456789/1076?mode=full

Jimeno, J. (2019). *Derecho de daños tecnológicos, ciberseguridad.* https://www.torrossa.com/it/resources/an/4513199

Kirton, J. (2021). *Propuesta de instrumento de evaluación de la aplicabilidad del marco de trabajo de Cyber Kill Chain, para el establecimiento de estrategias de seguridad de la información .* http://20.55.226.204/handle/123456789/351

Kosévich, E. (2019). *Estrategias de seguridad cibernética en los países de américa latina.* https://www.researchgate.net/profile/Ekaterina-Kosevich/publication/340419950_Cyber_Security_Strategies_of_Latin_America_Countries/links/5eac0008a6fdcc70509e07c7/Cyber-Security-Strategies-of-Latin-America-Countries.pdf

Leyva, A. (2021). *Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano.* https://dialnet.unirioja.es/servlet/articulo?codigo=7926828

Marín, M. (2023). *Análisis de las Vulnerabilidades Tecnológicas, a Nivel de Personal e Infraestructura, en la Empresa Sonda Costa Rica, a partir del Segundo Cuatrimestre del Año 2023.* https://repositorio.ulatina.ac.cr/bitstream/20.500.12411/2704/1/TFG_Ulatina_Marianela_Marin_Masis_201201096245.pdf

Monterroso, E., & Muñoz, A. (2019). *Inteligencia artificial y riesgos cibernéticos.* https://produccioncientifica.ucm.es/documentos/61989a2d49d6133331f42b3d

Mosquera, S. O. (2021). *Experiencias de seguridad cibernética en países europeos y latinoamericanos. Apuntes hacia la defensa nacional.* https://dialnet.unirioja.es/servlet/articulo?codigo=7926861

Obando, C., Garcés, L., Quiroz, J., Benjumea, M., & Valencia, A. (2022). *Evaluación de riesgos en ciberseguridad: una revisión bibliométrica.* https://www.proquest.com/openview/30ab36bec36b2b520b869c1fbbe32eb6/1?pq-origsite=gscholar&cbl=1006393

Ojeda, F., Moreno, V., & Torres, M. (2020). *Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador.* https://mail.cienciamatriarevista.org.ve/index.php/cm/article/view/366

Oltra, J., & Ibáñez, R. (2019). *Ciberseguridad.* https://riunet.upv.es/handle/10251/159532

Pérez, H. (2021). *Seguro de riesgos cibernéticos: enfoque y perspectivas en la nueva normalidad.* https://revistas.bibdigital.uccor.edu.ar/index.php/RFD/article/view/5016

Perez, M., & Correa, L. (2019). *Implantación del sistema de gestión de seguridad de la información para las bases de datos oracle del sistema muisca de la subdirección de gestión de tecnología de la información y telecomunicaciones en la dirección de impuestos y aduanas nacionales DIAN.* https://repository.unad.edu.co/handle/10596/5515

Pérez, Y. (2021). *Importancia de la Ciberseguridad. [En línea]. Articulo. Universidad Piloto de Colombia. Bogotá D.C.* http://polux.unipiloto.edu.co:8080/00003620.pdf

Ramos, A., Romario, E., & Quispe, A. (2023). *Exploración del comercio global: una revisión integral del comercio internacional y el comercio exterior.* Quipukamayoc, 31(66), 85-100.https://dx.doi.org/10.15381/quipu.v31i66.25573

Ravichagua, C., Medina, P., & Zavaleta, M. (2023). *Método para la optimización de inversión en ciberseguridad aplicado a una institución educativa de educación básica basado en un modelo determinístico.* https://repositorioacademico.upc.edu.pe/handle/10757/673059

Rincón, G., & Albarracín, F. (2019). *Análisis y evaluación de la seguridad informática para la página web publicada en hosting gratuito de la Institución Técnica de Firavitoba, para la detección y remediación de vulnerabilidades y riesgos en la información.* https://repository.unad.edu.co/handle/10596/17281?locale-attribute=es

Rodríguez , O. (2022). *Percepción de la ciberseguridad.* http://portal.amelica.org/ameli/journal/225/2254099006/html/

Rodríguez, E. (2019). *Metodología de la Investigación.* https://books.google.es/books?hl=es&lr=&id=r4yrEW9Jhe0C&oi=fnd&pg=PA1&dq=Libros+de+metodologia&ots=8Cf5-LA6j7&sig=5z_BFFf6WF3HFsDywswrMmsKwEs#v=onepage&q=Libros%20de%20metodologia&f=false

Romo, E. (2021). *Integración de la gestión de seguridad cibernética a la gestión de riesgo empresarial.* https://repository.eafit.edu.co/items/fd730d6d-4177-4f96-957c-450a068b0e13

Rutz, G. (2021). *Ciberdefesa como campo intelectual.* https://periodicos.unb.br/index.php/repam/article/view/36509

Samaniego, J. E. (2024). *Seguridad cibernética: amenazas emergentes y estrategias de defensa.* https://sociencytec.com/index.php/sct/article/view/20

Sampieri, R. (2018). *Metodología de la investigación.* https://d1wqtxts1xzle7.cloudfront.net/38911499/Sampieri-libre.pdf?1443413652=&response-content-disposition=inline%3B+filename%3DSampieri.pdf&Expires=1688385262&Signature=dX

6URYJUYPkOWB3kQcvxVac21qydlLBE6ja85vjNFzYxBD8Hax~vkXZ7QtOS8v5smyCHf SrqcsLbRgRrpzBAV

Torre, S. (2023). *Fundamentos del Comercio Electrónico.* https://ridaa.unq.edu.ar/handle/20.500.11807/4223

Urcuqui, C. (2020). *Ciberseguridad un enfoque desde la ciencia de datos.1 ed. Cali. Editorial Universidad.* ISBN: 978-958-8936-55-0

Varela, C. (2023). *Riesgo cibernético y ciberseguros.* https://revista.fasecolda.com/index.php/revfasecolda/article/view/911

Villacres, L. (2021). *Análisis de vulnerabilidad en la infraestructura tecnológica de la organización UNISCA .* https://dspace.ups.edu.ec/bitstream/123456789/25255/1/UPS-CT010629.pdf

Zabalo, E. (2019). *La ciberseguridad como norma.* https://addi.ehu.es/handle/10810/32240