Tipo de artículo: Artículo original

Elementos de ciberseguridad en los países en desarrollo y su impacto en la seguridad nacional: una encuesta sobre el derecho informático en Ecuador

Elements of cybersecurity in developing countries and their impact on national security: a survey on computer law in Ecuador

Sergio Israel Peña Guano [1*], https://orcid.org/0000-0003-4021-1892
Evelyn Romina Castillo Cruz [2], https://orcid.org/0009-0008-8016-8546
Patricia Marisol Peña Guano [3], https://orcid.org/0009-009-9883-3070

[1] Universidad de Guayaquil. Ecuador. Correo electrónico: sergio.penagua@ug.edu.ec
[2] Seripacar S.A. Ecuador. Correo electrónico: evelynrcastilloc36@gmail.com
[3] Fiscalía General del estado "La Merced". Ecuador. Correo electrónico: pegumarisol@gmail.com

*** Autor para correspondencia: sergio.penagua@ug.edu.ec**

Resumen

En los países en desarrollo, la ciberseguridad es un tema cada vez más relevante debido al aumento del uso de la tecnología y la conectividad a Internet. Sin embargo, estos países suelen enfrentar desafíos en términos de infraestructura, recursos y capacitación para abordar eficazmente este tema. El objetivo de esta investigación es analizar los elementos de ciberseguridad en los países en desarrollo y su impacto en la seguridad nacional. En este sentido, se realiza una encuesta a especialistas ecuatorianos en ciberseguridad forense y derecho informático, sobre el marco jurídico de ciberseguridad en Ecuador. Los resultados indican que las formas particulares de exposición a ciberataques pueden contribuir a respaldar diversos tipos de legislación sobre ciberseguridad y contribuir a su legitimidad pública. Además, los hallazgos cualitativos sugieren que incorporar el conocimiento y la comprensión de la ciberseguridad dentro de los consejos de administración empresarial, es un fuerte impulsor del cambio de comportamiento.

Palabras clave: ciberseguridad; ciberataques; derecho informático; países en desarrollo; seguridad nacional

Abstract

In developing countries, cybersecurity is an increasingly relevant issue due to the increased use of technology and Internet connectivity. However, these countries often face challenges in terms of infrastructure, resources and training to effectively address this issue. The objective of this research is to analyze the elements of cybersecurity in developing countries and their impact on national security. In this sense, a survey is carried out among Ecuadorian specialists in forensic cybersecurity and computer law, about the legal framework of cybersecurity in Ecuador. The results indicate that particular forms of exposure to cyberattacks can help support various types of cybersecurity legislation and contribute to their public legitimacy. Furthermore, qualitative findings suggest that incorporating knowledge and understanding of cybersecurity within corporate boards of directors is a strong driver of behavioral change.

Keywords: *cybersecurity; cyber attacks; computer law; developing countries; National security*

Recibido: 08/10/2023
Aceptado: 22/11/2023

En línea: 01/12/2023

Introducción

El desarrollo de Tecnologías de la Información y las Comunicaciones (TIC) y la transferencia de información al ciberespacio, aumenta la calidad de los procesos y actividades de información, y garantiza una mayor competitividad y eficiencia (Chang & Coppel, 2020). Sin embargo, esto también tiene consecuencias negativas, como la pérdida de información electrónica importante o incluso la ciberdelincuencia. A medida que aumenta el número de incidentes cibernéticos, surge una amenaza no solo para sujetos separados sino también para la seguridad nacional, ya que los ciberataques pueden utilizarse como medio de presión política y económica (N. F. Khan et al., 2023). En este sentido, la garantía de la ciberseguridad es un tipo de actividad muy importante y específica que requiere una regulación legal coherente y detallada, ya que constituye una piedra angular de la sociedad de la información (Pandey et al., 2022).

La importancia de una ley de ciberseguridad es incuestionable, porque establece reglas generales primarias que tienen un poder legal específico. La existencia de normas de esta naturaleza es muy importante en un país y su influencia es muy grande. La ley de ciberseguridad puede definirse como un marco legal que promueve la confidencialidad, integridad y disponibilidad de información, sistemas y redes públicas y privadas, mediante el uso de regulaciones e incentivos prospectivos, con el objetivo de proteger los derechos y la privacidad individuales, los intereses económicos y la seguridad nacional (Srinivas et al., 2019).

En Ecuador, la ciberseguridad está regulada por varias leyes y reglamentos, incluyendo la Ley Orgánica de Telecomunicaciones; la Ley Orgánica de Comunicación; y la Ley Orgánica de Protección de Datos Personales; sin embargo no existe una ley específica de ciberseguridad (Campos, 2019). Desafortunadamente, las leyes ecuatorianas no tienen una visión unificada y coherente para la regulación y promoción de la ciberseguridad (Saltos Salgado et al., 2021). Dado que el derecho informático es relativamente nuevo en Ecuador, al definir el alcance y los objetivos de este nuevo campo jurídico, los formuladores de políticas pueden examinar cómo los legisladores podrían mejorar las leyes existentes (Zambrano & Ordoñez, 2016).

En los países en desarrollo, la ciberseguridad es un tema cada vez más relevante debido al aumento del uso de la tecnología y la conectividad a Internet. Sin embargo, estos países suelen enfrentar desafíos en términos de infraestructura, recursos y capacitación para abordar eficazmente este tema (Baker, 2014). El objetivo de esta investigación es analizar los elementos de ciberseguridad en los países en desarrollo y su impacto en la seguridad nacional; en este sentido, se realiza una encuesta a especialistas ecuatorianos en ciberseguridad forense y derecho informático, sobre el marco jurídico de ciberseguridad en Ecuador.

Materiales y métodos

Según el enfoque, se presenta una investigación mixta con inclinación hacia la modalidad cualitativa porque en la recolección y análisis de datos se incorporan métodos cualitativos como el análisis de documentos y métodos cuantitativos como la encuesta. Por su alcance es de tipo descriptiva, pues prevé la caracterización de los elementos de ciberseguridad en los países en desarrollo y su impacto en la seguridad nacional.

Se utilizan métodos teóricos como el análisis-síntesis, inducción-deducción, y enfoque en sistema para la conformación del estado del arte. Los autores examinaron la literatura científica relacionada con los elementos de ciberseguridad en los países en desarrollo y su impacto en la seguridad nacional. Al utilizar referencias a la literatura científica, los autores utilizaron el método de deducción, lo que permitió sacar conclusiones suficientemente fiables. Se utilizó además, el método de análisis empírico de documentos legales para identificar la regulación legal de la ciberseguridad vigente en Ecuador. Se analizaron los actos jurídicos y leyes estratégicos de Ecuador, con lo cual se pudo identificar y describir con precisión la relación relevante entre las normas legales existentes. Se aplica una encuesta dirigida a 20 especialistas en ciberseguridad forense y abogados con perfil en derecho informático.

Resultados y discusión

Los riesgos habitualmente asociados a cualquier ciberataque tienen en cuenta tres variables de seguridad: amenazas de quién ataca; vulnerabilidades; e impactos o daños provocados por la agresión. Los principales problemas de la ciberseguridad son el conocimiento de los distintos ciberataques y el desarrollo de mecanismos de protección complementarios (Lee & Kim, 2020). Para efectos de esta investigación, se define como daño cibernético a cualquier menoscabo a la integridad o disponibilidad de datos, un programa, un sistema o información que provoque o implique la destrucción, corrupción o eliminación de archivos electrónicos; la destrucción física de un disco duro; o cualquier disminución en la integridad o usabilidad de los datos en un sistema informático.

Un incidente de seguridad es un acto que amenaza la confidencialidad, integridad o disponibilidad de los activos y sistemas de información. La obtención de acceso ilegal, la destrucción y la alteración de información para dañar posiblemente sean solo algunos ejemplos de posibles violaciones de seguridad en un sistema informático o dispositivo móvil. Las amenazas describen todos los riesgos y peligros potenciales de las infracciones de seguridad mencionadas anteriormente, y los ataques describen cualquier intento de cometer una infracción. En la tabla 1 se describen los factores de riesgos y las familias de malware representan algunas de las amenazas más comunes y peligrosas en el panorama de la ciberseguridad en 2023, descritos por la literatura científica.

Tabla 1. Factores de riesgos de ciberseguridad más comunes en 2023.

Ataques	Descripción	Referencia
Phishing	Consiste en el envío de correos electrónicos fraudulentos que buscan obtener información confidencial, como contraseñas o datos bancarios, de forma engañosa.	(N. A. Khan et al., 2023; Mijwil et al., 2023)
Malware	Se refiere a software malicioso diseñado para dañar o infiltrarse en sistemas informáticos sin el consentimiento del usuario.	(Aslan et al., 2023)
Spyware	Diseñado para recopilar información sobre las actividades de un usuario sin su conocimiento, como contraseñas, historial de navegación, etc.	(Church & Chandrasekar, 2023)
Ataques de denegación de servicio (DDoS)	Consisten en inundar un sistema con tráfico de red falso para sobrecargarlo y hacerlo inaccesible para los usuarios legítimos.	(Javaheri, Gorgin, et al., 2023)
Adware	Muestra anuncios no deseados en el dispositivo del usuario, a menudo con el propósito de generar ingresos para los creadores del malware.	(Adnyana et al., 2023; Babu et al., 2023)
Troyanos	Se disfrazan como software legítimo para engañar a los usuarios y luego dañar o robar información de sus dispositivos.	(Celi Sandoya, 2023; Javaheri, Fahmideh, et al., 2023)
Gusanos	Se propagan a través de redes y sistemas informáticos, a menudo sin necesidad de la interacción del usuario, con el objetivo de dañar o robar información.	(Aslan et al., 2023)
Virus	Se adjuntan a archivos legítimos y se replican cuando estos archivos se ejecutan, con el objetivo de dañar o robar información.	(Qi, 2023)
Botnets	Redes de dispositivos infectados que son controlados de forma remota por los ciberdelincuentes para llevar a cabo actividades maliciosas, como ataques DDoS.	(Kalidindi & Arrama, 2023; Rbah et al., 2023)
Rootkits	Se ocultan en el sistema operativo del dispositivo infectado y proporcionan acceso no autorizado al ciberdelincuente, permitiéndoles controlar el dispositivo de forma encubierta.	(Rath, Das, et al., 2023; Rath, Intriago, et al., 2023)
Robo de datos	Se refiere al acceso no autorizado a información confidencial, como datos personales o financieros, con el fin de utilizarlos de manera fraudulenta.	(Chen et al., 2023; Karanam, 2023; Mijwil et al., 2023)
Vulnerabilidades en software y hardware	Son debilidades en los sistemas informáticos que pueden ser explotadas por ciberdelincuentes para infiltrarse o dañar los sistemas.	(Aslan et al., 2023; Shepita et al., 2023)
Ataques de ransomware	Consisten en bloquear el acceso a los datos de un sistema y exigir un rescate para restaurar el acceso.	(McIntosh et al., 2023)

El objetivo de los ciberataques es perjudicar económicamente a las empresas. En algunos otros casos, los ciberataques pueden tener fines militares o políticos. Algunos de estos daños son: virus informáticos, roturas de datos, servicio de distribución de datos (DDS) y otros vectores de ataque. Para ello, diversas organizaciones utilizan diversas soluciones

para prevenir los daños causados por los ciberataques. Algunos software utilizados para detectar ataques y brechas de ciberseguridad se muestran en la tabla 2.

Tabla 2. Software utilizados para detectar ataques y brechas de ciberseguridad.

Software	Descripción	Referencia
FireEye	Es una empresa de ciberseguridad que ofrece soluciones de detección de amenazas avanzadas. Su plataforma utiliza inteligencia artificial y análisis de comportamiento para identificar y responder a ataques cibernéticos.	(Ahmed, 2022; Aljabri et al., 2023)
Symantec Endpoint Protection	Es un software de seguridad que proporciona protección contra malware, *ransomware* y amenazas avanzadas. Utiliza tecnologías de detección de comportamiento y análisis de reputación para identificar y bloquear ataques.	(Arfeen et al., 2021; Wickline, 2021)
McAfee	Es una empresa de seguridad cibernética que ofrece soluciones de detección de amenazas, incluyendo antivirus, firewall y protección contra intrusiones. Su plataforma utiliza inteligencia artificial y aprendizaje automático para identificar y responder a ataques.	(Craig Jr & McKenna Jr, 2012; Solutions & Cummings, 2017; Surisetty & Kumar, 2010)
Palo Alto Networks	Ofrece soluciones de seguridad cibernética que incluyen firewalls de próxima generación, detección de amenazas y análisis de tráfico de red para identificar y mitigar ataques.	(Perminov et al., 2020; Yılmaz)
Cisco Security	Ofrece una amplia gama de soluciones de seguridad cibernética, incluyendo firewalls, sistemas de prevención de intrusiones y detección de amenazas avanzadas para proteger las redes empresariales.	(Mason & Newcomb, 2001; Tsochev et al., 2020)
IBM QRadar	Es una plataforma de seguridad cibernética que utiliza análisis de datos en tiempo real para detectar y responder a amenazas. Utiliza inteligencia artificial y aprendizaje automático para identificar patrones y comportamientos maliciosos.	(Chakrabarty et al., 2021; Hossain et al., 2021)
Splunk	Es una plataforma de análisis de datos que se utiliza para la detección de amenazas y la respuesta a incidentes de seguridad. Utiliza análisis de registros y datos en tiempo real para identificar comportamientos sospechosos.	(Hristov et al., 2021; Saraf & Malathi, 2020)
Check Point Software Technologies	Ofrece soluciones de seguridad cibernética que incluyen firewalls, prevención de intrusiones y detección de amenazas avanzadas para proteger las redes empresariales.	(Adu-Gyamfi et al., 2020)
Trend Micro	Ofrece soluciones de seguridad cibernética que incluyen protección contra malware, *ransomware* y amenazas avanzadas. Utiliza tecnologías de detección de comportamiento y análisis de reputación para identificar y bloquear ataques.	(Huq, 2015)

Impacto en la seguridad nacional

En la actualidad, la mayoría de las actividades e interacciones económicas, comerciales, culturales, sociales y gubernamentales de los países, en todos los niveles, incluidos los individuos, las organizaciones no gubernamentales y los gobiernos e instituciones gubernamentales, se llevan a cabo en el ciberespacio. Recientemente, muchas empresas

privadas y organizaciones gubernamentales de todo el mundo se enfrentan al problema de los ciberataques y al peligro de las tecnologías de comunicación inalámbrica.

En el mundo cibernético, la amenaza más importante se centra en la infraestructura crítica (CI). La IC abarca las estructuras y funciones que son vitales para el funcionamiento ininterrumpido de la sociedad. Comprende instalaciones y estructuras físicas, así como funciones y servicios electrónicos. Los sistemas de infraestructura crítica comprenden una mezcla heterogénea de elementos dinámicos, interactivos y no lineales. En los últimos años, los ataques contra infraestructuras críticas, infraestructuras de información e Internet se han vuelto cada vez más frecuentes, complejos y dirigidos a objetivos porque los perpetradores se han vuelto más profesionales. Los atacantes pueden infligir daños o perturbar la infraestructura física al infiltrarse en los sistemas digitales que controlan los procesos físicos; dañar equipos especializados e interrumpir servicios vitales sin un ataque físico. Esas amenazas continúan evolucionando en complejidad y sofisticación (Tvaronavičienė et al., 2020).

Algunas de las limitaciones de ciberseguridad de los países en desarrollo incluyen la falta de infraestructura de red segura y confiable, que hace que los sistemas y datos estén más expuestos a ataques cibernéticos; la falta de conciencia sobre la importancia de la ciberseguridad y la capacitación en este ámbito genera una mayor vulnerabilidad; y la ausencia de leyes y regulaciones claras en materia de ciberseguridad dificulta la protección de datos y la persecución de delitos cibernéticos (Farías et al., 2023).

En el caso específico de Ecuador, ha sido víctima de ciberataques que atentan contra la seguridad nacional. Por ejemplo, en 2019, el Banco del Instituto Ecuatoriano de Seguridad Social (IESS) sufrió un ataque cibernético que afectó a sus sistemas informáticos, lo que provocó interrupciones en los servicios en línea y generó preocupaciones sobre la seguridad de los datos de los usuarios (Leyva-Méndez, 2021). En 2020, el Servicio de Rentas Internas (SRI) reportó un intento de ataque cibernético a su plataforma en línea, lo que llevó a la implementación de medidas de seguridad adicionales para proteger la información financiera y personal de los contribuyentes. En 2021, se detectaron múltiples casos de *phishing* y suplantación de identidad en correos electrónicos dirigidos a empresas y organizaciones en Ecuador, lo que puso de manifiesto la importancia de la concienciación sobre la ciberseguridad y la necesidad de medidas preventivas. Estos ejemplos muestran la relevancia de fortalecer las defensas cibernéticas de los países en desarrollo y resaltar la importancia de la educación y concienciación sobre las amenazas digitales.

Derecho informático en Ecuador

A medida que las violaciones de datos, los ataques de denegación de servicio y otros incidentes de ciberseguridad tienen consecuencias económicas y de seguridad nacional extraordinarias en los países en desarrollo; los especialistas jurídicos buscan cada vez más soluciones en el sistema legal. En esta investigación, se aplicó una encuesta a 20 especialistas en

ciberseguridad forense y abogados con perfil en derecho informático, con el objetivo de conocer la perspectiva actual del derecho informático en Ecuador. Los principales resultados se resumen a continuación:

Pregunta 1 ¿Cuáles son las principales categorías de la ciberseguridad qué usted ha procesado en Ecuador?

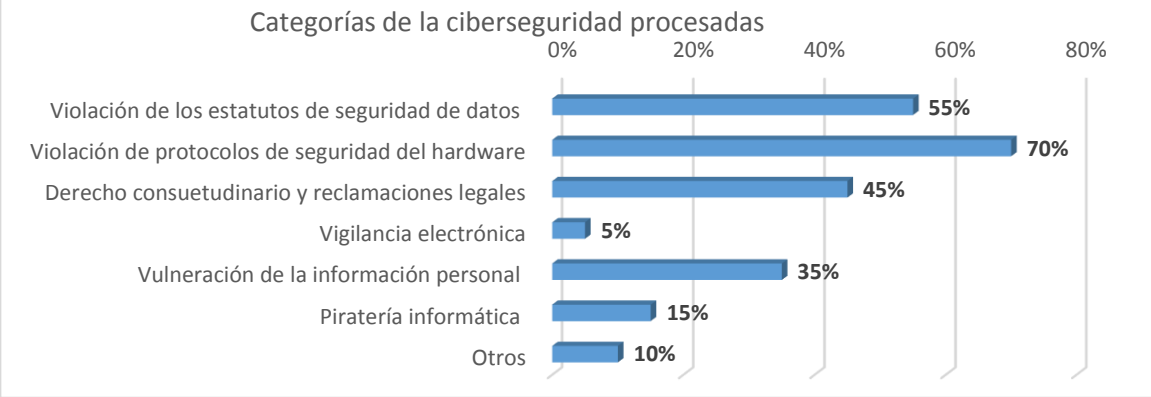

Figura 1. Categorías de la ciberseguridad procesadas por los encuestados.

Relacionado con la pregunta 1, las principales categorías abordadas por los encuestados en espacios jurídicos son: violación de los estatutos de seguridad de datos (55% de los encuestados); violación de protocolos de seguridad del hardware (70% de los encuestados); litigios sobre seguridad de datos a través del derecho consuetudinario y reclamaciones legales (45 % de los encuestados); piratería informática (15 % de los encuestados); vigilancia electrónica (5% de los encuestados); y vulneración de la información personal en redes sociales (35 % de los encuestados). En las discusiones generales se pudo conocer que la mayoría de los tribunales ecuatorianos solo permitirán que se lleven a cabo demandas sobre seguridad de datos a través del derecho consuetudinario y reclamaciones legales, si los demandantes han sufrido un daño real, como el robo de identidad. Siendo de consenso general que se debe permitir que las demandas procedan, basándose en la perspectiva de daños futuros; dado que, desde una visión más amplia, la mera ansiedad de la posibilidad de robo de identidad es un daño suficiente para otorgarle legitimación al demandante.

La falta de certeza sobre la legitimación reduce la probabilidad de que la perspectiva de un litigio sobre seguridad de datos haga que las empresas inviertan significativamente en salvaguardias de ciberseguridad. Los litigios sobre seguridad de datos pueden tener más visión de futuro que los estatutos de seguridad de datos y notificación de violaciones, en el sentido de que brindan a las empresas incentivos aún mayores para prevenir futuras violaciones. Además, las demandas colectivas suelen atraer mucha publicidad y normalmente requieren que se notifique a todos los consumidores afectados, por lo que los litigios pueden dañar la marca de una empresa. Sin embargo, al igual que los estatutos de seguridad de datos, los litigios sobre seguridad de datos se centran únicamente en proteger la confidencialidad y la privacidad individual, y hacen poco para abordar preocupaciones más amplias de ciberseguridad.

Pregunta 2 ¿Cuáles son las actividades de piratería informática más recurrentes en Ecuador?

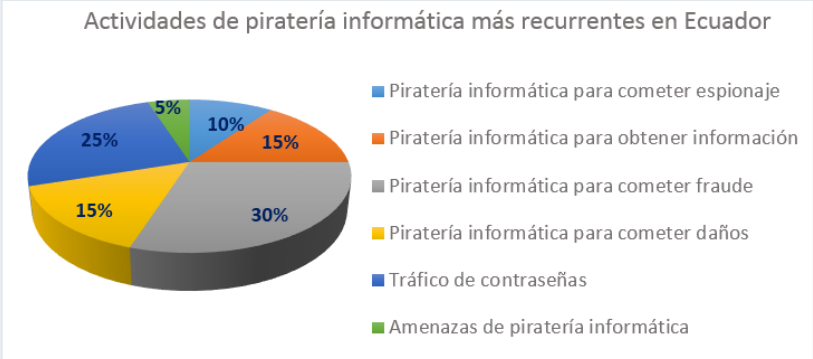

Figura 2. Actividades de piratería informática más recurrentes en Ecuador.

De manera general, los encuestados manifestaron que la actividad de piratería informática más recurrente en Ecuador es la piratería informática para cometer fraude **(n=6)** y el tráfico de contraseñas **(n=5)**.

Pregunta 3 ¿Cuáles son los criterios que se tienen en cuenta al juzgar delitos de ciberseguridad en Ecuador?

Todos los profesionales del derecho informático encuestados manifestaron que los criterios que toman en cuenta de forma permanente al juzgar delitos de ciberseguridad son: 1: la legislación y normativas vigentes; 2: las pruebas forenses digitales (son analizadas las pruebas digitales, como registros de actividad, metadatos, direcciones IP y otros datos técnicos, para determinar la autoría y la intención del delito); 3: los daños y perjuicios ocasionados (se evalúan los daños causados por el delito, como la pérdida de datos, la interrupción de servicios o el robo de información confidencial, para determinar la gravedad del delito); 4: la intención y la motivación del delito (se examina la intención detrás del delito, como si fue realizado con fines de lucro, sabotaje, espionaje o vandalismo cibernético); 5: la responsabilidad y la culpabilidad (se determina si el acusado era consciente de sus acciones y si actuó intencionalmente para cometer el delito); y 6: los antecedentes y las reincidencias (se considera si el acusado tiene antecedentes previos relacionados con delitos informáticos o ciberseguridad).

Pregunta 4 ¿Considera que el marco legal de ciberseguridad existente en Ecuador pasa por alto elementos de ciberseguridad?

Referente a la pregunta 4, el 100% de los encuestados manifestaron que el marco legal de ciberseguridad existente en Ecuador sí pasa por alto elementos de ciberseguridad; ya que se centra en gran medida en proteger la confidencialidad de la información con el fin de proteger la privacidad individual. Sin embargo, las leyes podrían mejorarse para centrarse en otros aspectos, incluidos la integridad y disponibilidad de la información; la protección de sistemas y redes; y la

promoción de intereses económicos y de seguridad nacional. Además, la ley de ciberseguridad podría beneficiarse de un enfoque más prospectivo, con el objetivo de prevenir incidentes futuros, en lugar del enfoque actual de penalizar a las instituciones por no protegerse contra ataques anteriores.

Pregunta 5. ¿Cuáles son los principales desafíos para identificar y comprobar delitos de ciberseguridad?

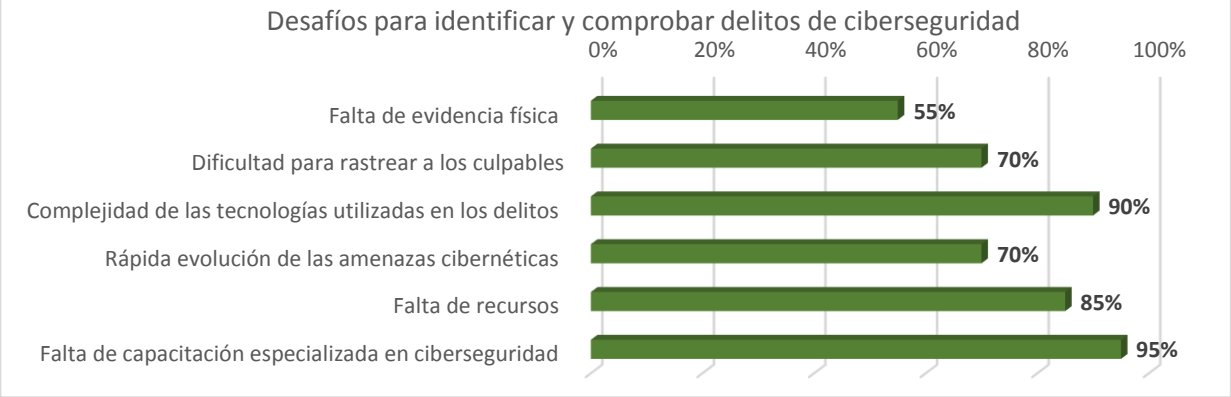

Figura 3. Desafíos para identificar y comprobar delitos de ciberseguridad.

Relacionado con la pregunta 5, los encuestados refieren que hasta la fecha, los principales desafíos que han enfrentado para identificar y comprobar delitos de ciberseguridad incluyen la falta de evidencia física, la dificultad para rastrear a los perpetradores, la complejidad de las tecnologías utilizadas en los delitos cibernéticos, la necesidad de colaboración internacional para investigar casos transfronterizos, y la rápida evolución de las amenazas cibernéticas que dificultan la detección y prevención de delitos. Además, la falta de recursos y capacitación especializada en ciberseguridad propia de los países en desarrollo, también representa un desafío significativo a la hora de juzgar y combatir estos delitos.

Pregunta 6. ¿Desde su experiencia, cuáles son los elementos de ciberseguridad que afectan la seguridad nacional de los países en desarrollo?

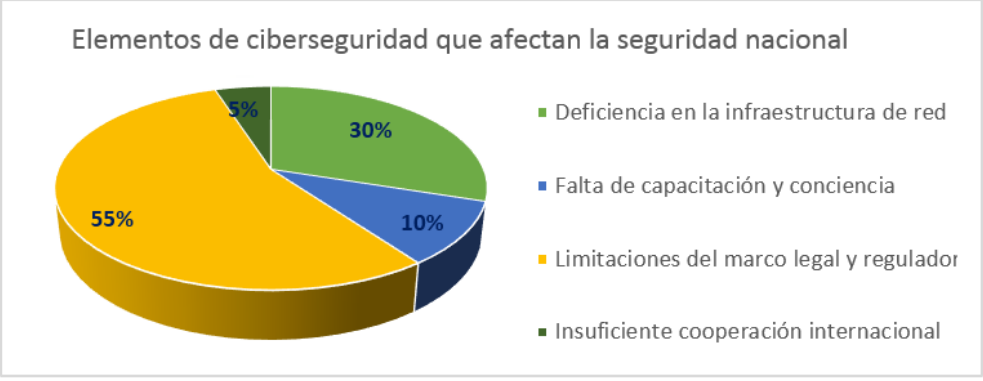

Figura 4. Elementos de ciberseguridad que afectan la seguridad nacional

Relacionado con la pregunta 6, los encuestados manifiestan los principales elementos de ciberseguridad que afectan la seguridad nacional de los países en desarrollo son la falta de infraestructura de red segura y confiable que provoca que los sistemas y datos estén más expuestos a ataques cibernéticos **(n=6)**; la falta de conciencia sobre la importancia de la ciberseguridad y la capacitación en este ámbito genera una mayor vulnerabilidad frente a los ataques **(n=2)**; las limitaciones y ausencia de leyes y regulaciones claras para garantizar la protección de datos y la persecución de delitos cibernéticos **(n=11)**; y la insuficiente colaboración con otros países y organizaciones internacionales que limita el tratamiento de amenazas transnacionales y la protección de la seguridad nacional **(n=1)**.

Análisis de los resultados

Para los académicos interesados en el dominio cibernético, la evaluación de la información derivada de medios disponibles públicamente es una opción tan atractiva como problemática. La captura y el tratamiento de cantidades masivas de datos publicados relacionados con conflictos cibernéticos promete un recurso único para quienes buscan evaluar el contexto de los compromisos de seguridad cibernética. Sin embargo, estos enfoques a menudo generan amplias críticas relacionadas con la generalización y la metodología (Mishra et al., 2022). Dentro de los elementos recomendados para lograr un ciberespacio abierto, seguro y protegido en los países en desarrollo, se destaca:

- La necesidad primaria de lograr la ciberresiliencia;
- Reducir totalmente el cibercrimen;
- Desarrollar políticas y capacidades de ciberdefensa colectivas e individuales; y
- Desarrollar los recursos industriales y tecnológicos necesarios para la ciberseguridad;
- Establecer una política internacional coherente en el ciberespacio para los países en desarrollo.

Para implementar una adecuada ciberseguridad en Ecuador se debe crear una entidad cuyo principal objetivo se enfoque en la protección cibernética a nivel nacional, identificando y clasificando cuáles son las infraestructuras críticas del país y que sectores pueden ser los más afectados en caso de un ataque cibernético. El país presenta indicadores muy bajos en comparación con países de la región. El MINTEL ya inicio la creación de una importante herramienta jurídica que consiste en implementar la estrategia de ciberseguridad; la cual debería estar enfocada en la protección de los recursos que están en peligro dentro del contexto del uso del ciberespacio en Ecuador, con una postura realista y actualizada y con la participación de los sectores público y privado, acompañados de profesionales expertos del área. En este contexto, existen varias metodologías y modelos de madurez que se pueden utilizar para medir la ciberseguridad de una organización. Algunos de los más comunes se muestran en la tabla 2:

Tabla 2. Metodologías y modelos de madurez de ciberseguridad.

Modelo	Descripción	Referencia
Modelo de madurez de la seguridad cibernética	Este modelo evalúa la madurez de la seguridad cibernética de una organización en cinco niveles, desde ad hoc hasta optimizado. Se centra en áreas clave como la gestión de riesgos, la protección de la red, la detección de amenazas, la respuesta a incidentes y la recuperación.	(Rabii et al., 2020; White, 2011)
Marco de seguridad cibernética del NIST	El Instituto Nacional de Estándares y Tecnología (NIST) ha desarrollado un marco de seguridad cibernética que proporciona pautas y mejores prácticas para evaluar y mejorar la postura de seguridad cibernética de una organización. Se centra en identificar, proteger, detectar, responder y recuperarse de las amenazas cibernéticas.	(Almuhammadi & Alsaleh, 2017)
ISO 27001	Esta norma internacional establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI) y proporciona un marco para evaluar y mejorar la seguridad cibernética de una organización. Se centra en la identificación de activos críticos, la evaluación de riesgos, la implementación de controles de seguridad y la monitorización continua.	(Culot et al., 2021)
COBIT	Es un marco de referencia para la gestión de la seguridad de la información para ayudar a las organizaciones a evaluar sus riesgos de seguridad e implementar controles de seguridad adecuados. Gestiona seguridad de la información que cubre la confidencialidad, integridad y disponibilidad de los recursos.	(Sulistyowati et al., 2020; Yasin et al., 2020)

Estas metodologías y modelos de madurez pueden ayudar a las organizaciones ecuatorianas a evaluar su postura de seguridad cibernética, identificar áreas de mejora y desarrollar un plan para fortalecer sus defensas cibernéticas. Es importante que las organizaciones en Ecuador consideren la implementación de estas metodologías y modelos para protegerse contra las crecientes amenazas cibernéticas.

Conclusiones

El impacto de la ciberseguridad en la seguridad nacional de los países en desarrollo puede ser significativo. Los ataques cibernéticos pueden afectar infraestructuras críticas, sistemas financieros, servicios de salud, entre otros, lo que podría tener consecuencias graves para la estabilidad y el desarrollo del país. Además, la vulnerabilidad frente a ciberataques puede socavar la confianza en el gobierno y las instituciones, así como en la economía y el comercio digital. Por lo tanto, es fundamental que los países en desarrollo fortalezcan sus capacidades en materia de ciberseguridad, inviertan en infraestructura segura, promuevan la conciencia y capacitación en este ámbito, establezcan marcos legales y regulatorios sólidos, y fomenten la cooperación internacional para proteger su seguridad nacional en el ciberespacio.

Las amenazas cibernéticas son un componente crítico y creciente de la seguridad nacional. A medida que esta amenaza continúa creciendo en todo el mundo, tanto en su percepción pública como en su verdadero alcance, también crecerá la necesidad de implementar regulaciones estrictas de ciberseguridad. Nuestros hallazgos indican que formas particulares

de exposición a ciberataques pueden contribuir a respaldar diversos tipos de legislación sobre ciberseguridad y contribuir a su legitimidad pública. Esto es especialmente importante ya que la introducción de estas regulaciones constituye un sacrificio de las libertades civiles, un sacrificio que los ciudadanos tienden a apoyar sólo bajo condiciones particulares.

Conflictos de intereses

Los autores no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Sergio Israel Peña Guano, Evelyn Romina Castillo Cruz, Patricia Marisol Peña Guano
2. Curación de datos: Sergio Israel Peña Guano, Evelyn Romina Castillo Cruz
3. Análisis formal: Sergio Israel Peña Guano, Patricia Marisol Peña Guano
4. Investigación: Sergio Israel Peña Guano, Evelyn Romina Castillo Cruz, Patricia Marisol Peña Guano
5. Metodología: Sergio Israel Peña Guano, Evelyn Romina Castillo Cruz, Patricia Marisol Peña Guano
6. Administración del proyecto: Sergio Israel Peña Guano
7. Software: Evelyn Romina Castillo Cruz, Patricia Marisol Peña Guano
8. Supervisión: Sergio Israel Peña Guano
9. Validación: Sergio Israel Peña Guano, Evelyn Romina Castillo Cruz, Patricia Marisol Peña Guano
10. Visualización: Sergio Israel Peña Guano, Evelyn Romina Castillo Cruz, Patricia Marisol Peña Guano
11. Redacción – borrador original: Sergio Israel Peña Guano, Evelyn Romina Castillo Cruz, Patricia Marisol Peña Guano
12. Redacción – revisión y edición: Sergio Israel Peña Guano, Evelyn Romina Castillo Cruz, Patricia Marisol Peña Guano

Financiamiento

La investigación no requirió fuente de financiamiento externa.

Referencias

Adnyana, I. G., Thalib, E. F., Harum, M. A., Nagas, M. A. C., & Jawa, M. W. (2023). A Discussion of Malware Attacks Targeting Smart Homes and Connected Devices: Investigating Cybersecurity Risks in Everyday Living. *Journal of Digital Law and Policy*, *3*(1), 13-25. https://ejournal.sidyanusa.org/index.php/jdlp/article/view/507

Adu-Gyamfi, E., Al Muarrawi, G., & Ofori, K. (2020). RCAP Solutions Breach Management-Case Study. https://commons.clarku.edu/sps_masters_papers/64/

Ahmed, Y. (2022). *Data-driven framework and experimental validation for security monitoring of networked systems* Birmingham City University]. https://www.open-access.bcu.ac.uk/id/eprint/13432

Aljabri, S., Almalki, A., & Altalhi, A. (2023). Cyber Security Risks for Global Businesses and Solutions Expected. *International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068*, *2*(2), 21-25. https://ijmirm.com/index.php/ijmirm/article/view/16

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, *7*(3), 51-62. https://www.csitcp.com/paper/7/73csit05.pdf

Arfeen, A., Ahmed, S., Khan, M. A., & Jafri, S. F. A. (2021). Endpoint detection & response: A malware identification solution. 2021 International Conference on Cyber Warfare and Security (ICCWS),

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333. https://www.mdpi.com/2079-9292/12/6/1333

Babu, C. S., Suruthi, G., & Indhumathi, C. (2023). Malware Forensics: An Application of Scientific Knowledge to Cyber Attacks. In *Malware Analysis and Intrusion Detection in Cyber-Physical Systems* (pp. 285-312). IGI Global. https://www.igi-global.com/chapter/malware-forensics/331309

Baker, E. W. (2014). A model for the impact of cybersecurity infrastructure on economic development in emerging economies: evaluating the contrasting cases of India and Pakistan. *Information Technology for Development*, *20*(2), 122-139. https://www.tandfonline.com/doi/abs/10.1080/02681102.2013.832131

Campos, N. J. O. (2019). Normativa legal sobre delitos informáticos en Ecuador. *Revista Científica Hallazgos21*, *4*(1), 100-111. https://dialnet.unirioja.es/servlet/articulo?codigo=7148227

Celi Sandoya, A. M. (2023). *Soluciones de ciberseguridad contra los ataques a redes IoT en América Latina, una Revisión Sistemática de la Literatura* https://dspace.ups.edu.ec/handle/123456789/25904

Craig Jr, P. A., & McKenna Jr, T. P. (2012). McAfee®. https://nsi.org/ReferenceLibrary/1064.pdf

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, *33*(7), 76-105. https://www.emerald.com/insight/content/doi/10.1108/TQM-09-2020-0202

Chakrabarty, B., Patil, S. R., Shingornikar, S., Kothekar, A., Mujumdar, P., Raut, S., & Ukirde, D. (2021). *Securing Data on Threat Detection by Using IBM Spectrum Scale and IBM QRadar: An Enhanced Cyber Resiliency Solution*. IBM Redbooks.

https://www.google.com/books?hl=es&lr=&id=c69CEAAAQBAJ&oi=fnd&pg=PA26&dq=Software+used+to+detect+cybersecurity+attacks+and+breaches+%2B+IBM+QRadar&ots=ARTIP77kw9&sig=9QJpKgVg25_5eq2JVYzLRADEaoM

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security*, *97*, 101959. https://www.sciencedirect.com/science/article/pii/S0167404820302352

Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, *187*(1), 199-224. https://link.springer.com/article/10.1007/s10551-022-05107-z

Church, K. W., & Chandrasekar, R. (2023). Emerging trends: Risks 3.0 and proliferation of spyware to 50,000 cell phones. *Natural Language Engineering*, *29*(3), 824-841. https://www.cambridge.org/core/journals/natural-language-engineering/article/emerging-trends-risks-30-and-proliferation-of-spyware-to-50000-cell-phones/E493E2949551DB0D1CCB3C873E30C143

Farías, J. J. C., Romero, V. J. S., Lumbano, C. A. S., & Millingalle, J. V. C. (2023). Implementación de sistemas de facturación electrónica en el marco del derecho informático: Desafíos y oportunidades para el desarrollo de sitios web en Ecuador. *Revista Científica FIPCAEC (Fomento de la investigación y publicación científico-técnica multidisciplinaria). ISSN: 2588-090X. Polo de Capacitación, Investigación y Publicación (POCAIP)*, *8*(3), 259-281. https://www.fipcaec.com/index.php/fipcaec/article/view/866

Hossain, S. M., Couturier, R., Rusk, J., & Kent, K. B. (2021). Automatic event categorizer for SIEM. Proceedings of the 31st Annual International Conference on Computer Science and Software Engineering,

Hristov, M., Nenova, M., Iliev, G., & Avresky, D. (2021). Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT. 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA),

Huq, N. (2015). Follow the data: Dissecting data breaches and debunking myths. *TrendMicro Research Paper*. https://nsi.org/ReferenceLibrary/1238.pdf

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, 122697. https://www.sciencedirect.com/science/article/pii/S0957417423031998

Javaheri, D., Gorgin, S., Lee, J.-A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. *Information Sciences*. https://www.sciencedirect.com/science/article/pii/S0020025523000683

Kalidindi, A., & Arrama, M. B. (2023). Botnet attack detection in IoT using hybrid optimisation enabled deep stacked autoencoder network. *International Journal of Bio-Inspired Computation*, *22*(2), 77-88. https://www.inderscienceonline.com/doi/abs/10.1504/IJBIC.2023.134981

Karanam, V. (2023). Is there a Trojan!: Literature survey and critical evaluation of the latest ML based modern intrusion detection systems in IoT environments. *arXiv preprint arXiv:2310.10778*. https://arxiv.org/abs/2310.10778

Khan, N. A., Brohi, S. N., & Zaman, N. (2023). Ten deadly cyber security threats amid COVID-19 pandemic. *Authorea Preprints*. https://www.authorea.com/doi/full/10.36227/techrxiv.12278792.v1

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2023). Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Security Journal*, *36*(2), 373-405. https://link.springer.com/article/10.1057/s41284-022-00343-4

Lee, C. S., & Kim, J. H. (2020). Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts. *Computers & Security*, *97*, 101995. https://www.sciencedirect.com/science/article/pii/S0167404820302686

Leyva-Méndez, A. E. (2021). Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano. *Polo del conocimiento*, *6*(3), 1229-1250. https://polodelconocimiento.com/ojs/index.php/es/article/view/2431

Mason, A. G., & Newcomb, M. J. (2001). *Cisco secure Internet security solutions*. Cisco press. https://www.google.com/books?hl=es&lr=&id=8D90NjKvmBAC&oi=fnd&pg=PR2&dq=Software+used+to+detect+cybersecurity+attacks+and+breaches+%2B+Cisco+Security&ots=EWM_sgLnN7&sig=B_53zE3QIwJcOjOx2hc8ayJm4mg

McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Computers & Security*, *134*, 103424. https://www.sciencedirect.com/science/article/pii/S0167404823003346

Mijwil, M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian journal of cybersecurity*, *2023*, 57-63. https://www.researchgate.net/profile/Maad-Mijwil/publication/369022012_Exploring_the_Top_Five_Evolving_Threats_in_Cybersecurity_An_In-Depth_Overview/links/6405730a0d98a97717e085f1/Exploring-the-Top-Five-Evolving-Threats-in-Cybersecurity-An-In-Depth-Overview.pdf

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820. https://www.sciencedirect.com/science/article/pii/S0167404822002140

Pandey, A. B., Tripathi, A., & Vashist, P. C. (2022). A survey of cyber security trends, emerging technologies and threats. *Cyber Security in Intelligent Computing and Communications*, 19-33. https://link.springer.com/chapter/10.1007/978-981-16-8012-0_2

Perminov, P., Kosachenko, T., Konev, A., & Shelupanov, A. (2020). Automation of information security audit in the Information System on the example of a standard "CIS Palo Alto 8 Firewall Benchmark". *International Journal*, *9*(2), 2085-2088. https://www.academia.edu/download/63271882/ijatcse18292202020200511-103697-on4apc.pdf

Qi, J. (2023). Loss and premium calculation of network nodes under the spread of SIS virus. *Journal of Intelligent & Fuzzy Systems*(Preprint), 1-15. https://content.iospress.com/articles/journal-of-intelligent-and-fuzzy-systems/ifs222308

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information & Computer Security*, *28*(4), 627-644. https://www.emerald.com/insight/content/doi/10.1108/ICS-03-2019-0039/full/html

Rath, S., Das, T., & Sengupta, S. (2023). Improvise, Adapt, Overcome: Dynamic Resiliency Against Unknown Attack Vectors in Microgrid Cybersecurity Games. *arXiv preprint arXiv:2306.15106*. https://arxiv.org/abs/2306.15106

Rath, S., Intriago, A., Sengupta, S., & Konstantinou, C. (2023). Lost at Sea: Assessment and Evaluation of Rootkit Attacks on Shipboard Microgrids. *arXiv preprint arXiv:2305.18667*. https://arxiv.org/abs/2305.18667

Rbah, Y., Mahfoudi, M., Balboul, Y., Chetioui, K., Fattah, M., Mazer, S., Elbekkali, M., & Bernoussi, B. (2023). A machine learning based intrusions detection for IoT botnet attacks. AIP Conference Proceedings,

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. *Conrado*, *17*(78), 343-351. http://scielo.sld.cu/scielo.php?pid=s1990-86442021000100343&script=sci_arttext

Saraf, K. R., & Malathi, P. (2020). Cyber physical system security by Splunk. *I-Manager's Journal on Communication Engineering & Systems*, *9*(2). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=227

75102&AN=154451292&h=ruM1Pv3Lmbxv86qyAE1U%2FsZEWeb%2BMMZMpzyI5B87ZPkD0FB80sCPQUkFve2ZtyKbmVPc6zgW2vH15xvlNy1HaQ%3D%3D&crl=c

Shepita, P., Tupychak, L., & Shepita, J. (2023). Analysis of Cyber Security Threats of the Printing Enterprise. *Journal of Cyber Security and Mobility*, 415–434-415–434. https://journals.riverpublishers.com/index.php/JCSANDM/article/download/18825/18109

Solutions, P., & Cummings, C. (2017). The Effectiveness of McAfee Host Intrusion Prevention. https://ininet.org/the-effectiveness-of-mcafee-host-intrusion-prevention.html

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178-188. https://www.sciencedirect.com/science/article/pii/S0167739X18316753

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *JOIV: International Journal on Informatics Visualization*, *4*(4), 225-230. http://joiv.org/index.php/joiv/article/view/482

Surisetty, S., & Kumar, S. (2010). Is McAfee securitycenter/firewall software providing complete security for your computer? 2010 Fourth International Conference on Digital Society,

Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., & Pavlova, G. (2020). Cyber security: Threats and Challenges. 2020 International Conference Automatics and Informatics (ICAI),

Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into regional development*, *2*(4), 802-813. https://hal.science/hal-03298796/

White, G. B. (2011). The community cyber security maturity model. 2011 IEEE international conference on technologies for homeland security (HST),

Wickline, T. (2021). *The Capabilities of Antivirus Software to Detect and Prevent Emerging Cyberthreats* Utica College]. https://search.proquest.com/openview/f04aec327c82562b1e7ce152964e442a/1?pq-origsite=gscholar&cbl=18750&diss=y

Yasin, M., Arman, A. A., Edward, I. J. M., & Shalannanda, W. (2020). Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001: 2013 (Case Study Ditreskrimsus Polda XYZ). 2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA,

Yılmaz, O. Penetration Tools To Prevent Organizational Data Security Breaches. *European Proceedings of Social and Behavioural Sciences*. https://www.europeanproceedings.com/article/10.15405/epsbs.2019.12.03.27

Zambrano, K. I. D., & Ordoñez, L. M. M. (2016). Delito Informático. Procedimiento Penal en Ecuador. *Dominio de las Ciencias*, *2*(2), 204-215. https://dialnet.unirioja.es/servlet/articulo?codigo=5761561