Estrategia de Ciberseguridad y Ciberdefensa en Honduras: Desafíos en el Ciberespacio

Mayor (FAH) Walther Antonio Meléndez Castellanos

Artículo para optar al título profesional:

Magíster en Estrategia y Geopolítica

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2023

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (FAH) Walther Antonio Meléndez Castellanos
Identificación	**:**	E0146660
Programa académico	**:**	Maestría en Estrategia y Geopolítica
Tutor metodológico	**:**	CR. Andrés Eduardo Fernández Osorio
Tutor temático	**:**	TC (R) Jesús Eduardo Moreno Peláez
Fecha de entrega	**:**	10 de septiembre de 2023
Extensión	**:**	7.080 palabras

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Estrategia de Ciberseguridad y Ciberdefensa en Honduras: Desafíos en el Ciberespacio

Cybersecurity and Cyber Defense Strategy in Honduras: Challenges in Cyberspace

Walther Antonio Meléndez Castellanos[1]

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El artículo se enfoca en la importancia de desarrollar e implementar una estrategia de ciberseguridad y ciberdefensa efectiva en Honduras. Para lo cual se empleará un enfoque holístico con una visión neorrealista para poder proporcionar una comprensión integral de la Estrategia de La estrategia de seguridad y defensa cibernética en Honduras y los desafíos que enfrenta en el ciberespacio; en la actualidad el país enfrenta desafíos significativos en el ciber espacio como la falta de recursos, conciencia, educación y una infraestructura de seguridad informática suficiente. Estas estrategias deben abordar estas limitaciones y promover la colaboración entre el sector público y privado, así como políticas y regulaciones gubernamentales sólidas. Además, es importante abordar los desafíos culturales y educativos para fomentar la conciencia y la educación sobre las amenazas en el ciberespacio en la sociedad hondureña. La implementación de una estrategia efectiva de ciberseguridad y ciberdefensa en Honduras es crucial para garantizar la protección de los sistemas informáticos del país.

Palabras clave: amenazas cibernéticas, ciberdefensa, ciberseguridad, ciberespacio, seguridad informática, sistemas informáticos.

Abstract: The article focuses on the importance of developing and implementing an effective cybersecurity and cyber defense strategy in Honduras. To achieve this, a holistic approach with a neorealistic vision will be employed to provide a comprehensive understanding of the Cybersecurity and Cyber Defense Strategy in Honduras and the challenges it faces in cyberspace. Currently, the country faces significant challenges in cyberspace, such as lack of resources, awareness, education, and sufficient cybersecurity infrastructure.

These strategies must address these limitations and promote collaboration between the public and private sectors, as well as strong government policies and regulations. Additionally, it is important

[1] Mayor de la Fuerza Aérea Hondureña. Candidato a magíster en estrategia y geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Ingeniero Mecatrónico, Universidad de Defensa de Honduras, Honduras. https://orcid.org/0009-0006-6917-9821 - Contacto: melendezw@esdeg.edu.co.

to address cultural and educational challenges to foster awareness and education about cyber threats in Honduran society. The implementation of an effective cybersecurity and cyber defense strategy in Honduras is crucial to ensure the protection of the country's computer systems.

Keywords: cyber threats, cyber defense, cybersecurity, cyberspace, information security, computer systems.

Desafíos en el ciberespacio para Honduras

La ciberseguridad y ciberdefensa se han convertido en temas de alta relevancia en la era digital en la que vivimos. Los avances tecnológicos, la creciente interconexión de sistemas y datos han generado nuevas oportunidades a si como desafíos y amenazas cibernéticas cada vez más sofisticadas y persistentes. Honduras, al igual que todos los países que se encuentra interconectados en el mundo debido a la globalización, se enfrenta a estos desafíos por lo cual se requiere implementar una estrategia de ciberseguridad y ciberdefensa para proteger sus activos digitales y salvaguardar la seguridad y privacidad de su información.

La Asamblea General de las Naciones Unidas el 27 de diciembre de 2018 adoptó la "Resolución sobre Desarrollo de la Confianza en el Uso de la Tecnología de la Información y las Comunicaciones en el Contexto de la Seguridad Internacional" (UNGA Resolution A/RES/73/27). La cual se enfoca en el uso responsable de las tecnologías de la información y las comunicaciones (TIC) en el contexto de la seguridad internacional. La resolución destaca la importancia de fortalecer la cooperación entre los estados y la protección de la infraestructura crítica de las TIC. (ONU, 2018)

Por otra parte, el papel de la Organización de los Estados Americanos (OEA) se destaca entre los esfuerzos conjuntos de cooperación regional la cual publicó la Estrategia Interamericana Integral de Seguridad Cibernética (2004) y la declaración de Fortalecimiento de la Seguridad Cibernética en las Américas (2012). (OEA, 2004)

Según el informe de del banco interamericano de desarrollo para el 2020 con el apoyo de la OEA (BID, 2020), "12 países habían aprobado estrategias nacionales de ciberseguridad, incluidos Colombia (2011 y 2016), Panamá (2013), Trinidad y Tobago

(2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), México (2017), Guatemala (2018), República Dominicana (2018), Argentina (2019) y Brasil (2020)" (p.13).

Honduras carece de una política de Estado en materia de ciberseguridad y ciberdefensa, por ende, no cuenta con una estrategia nacional en esta área. Tampoco cuenta con el CIRT (Computer Incident Response Team): Equipo de Respuesta e Incidentes Informáticos, que es una unidad especializada encargada de detectar, analizar y responder a incidentes de seguridad cibernética en una organización o país. De acuerdo con el informe de ciberseguridad del Banco Interamericano de Desarrollo de 2016, (BID, 2016)

El ciberespacio presenta una serie de desafíos para Honduras, como ser la protección de la Información, salvaguarda de activos digitales, cibercrimen, cultura de seguridad digital, capacidades de ciberdefensa, cooperación público-privada, educación y concienciación, marco legal y normativo, resiliencia cibernética, estos desafíos son complejos y multifacéticos, y requieren una respuesta integral y coordinada por parte del gobierno, el sector privado y la sociedad.

En este sentido, González-Ruiz (2020) señala que "la ciberseguridad y ciberdefensa son elementos clave en la protección de la información y la salvaguarda de los activos digitales en un mundo cada vez más interconectado" (p. 23). La creciente interconexión digital ha generado una mayor exposición a amenazas cibernéticas, como ataques cibernéticos, robo de datos, fraude en línea, entre otros.

Estas amenazas representan un riesgo para la integridad y confidencialidad de la información sensible de los ciudadanos, empresas e instituciones gubernamentales en Honduras.

Además, Martínez (2018) destaca que "la protección de la infraestructura crítica es un desafío fundamental en la ciberseguridad y ciberdefensa, ya que un ataque exitoso a la infraestructura crítica puede tener un impacto devastador en la economía y la seguridad del país" (p. 45). La infraestructura crítica, como la energía, el transporte, las comunicaciones y el agua, depende en gran medida de sistemas y redes digitales, lo que la hace vulnerable a posibles ataques cibernéticos. En este contexto, es imperativo que Honduras desarrolle una estrategia de ciberseguridad y ciberdefensa que garantice la protección de su infraestructura crítica y minimice los riesgos asociados.

El avance de la tecnología ha dado lugar a nuevas formas de delitos cibernéticos, como el robo de identidad, el fraude en línea, el phishing que IBM lo define como "correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos diseñados para manipular personas para que descarguen malware" (IBM, 2023). Y el malware que según McAfee "es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable" (McAfee, 2023). Entre otros. Estos delitos pueden tener un impacto significativo en la economía, la seguridad y la confianza de la población en el uso de la tecnología en Honduras. Al respecto Torres (2018) señala "el cibercrimen es una amenaza creciente en el país, con consecuencias económicas y sociales graves, como la pérdida de datos, el daño a la reputación de las empresas y el robo de información sensible" (p. 56).

Metodología

Esta investigación se fundamenta y se basa en una metodología con un enfoque holístico con una visión neorrealista para el desarrollo del presente artículo sobre la Estrategia de Ciberseguridad y Ciberdefensa en Honduras y los desafíos en el ciberespacio ya que un enfoque holístico implica considerar todos sus componentes relevantes y analizar cómo interactúan entre sí. Esto implica tener en cuenta no solo aspectos técnicos y tecnológicos, sino también factores políticos, económicos, sociales y culturales que pueden afectar la seguridad cibernética de Honduras.

Y la perspectiva neorrealista, la cual según Kenneth Waltz establece que la seguridad es el objetivo principal de cada nación, pero se ve constantemente amenazada debido a la anarquía en el sistema internacional. (Hernández, 2008), al utilizar esta perspectiva en el estudio de la ciberseguridad, se puede analizar cómo las acciones y motivaciones de otros estados pueden influir en la seguridad cibernética de Honduras. Por ejemplo, el lector puede considerar cómo las disputas regionales o las tensiones geopolíticas pueden manifestarse en Internet y tener un impacto en la seguridad cibernética del país.

Y tomando en cuenta que en la actualidad el constante desarrollo del ciberespacio definido por el Ministerio de Defensa Español como:

> Dominio global y dinámico dentro del entorno de la información, compuesto por una infraestructura de redes, de tecnologías de la información y telecomunicaciones interdependientes, que incluye el internet, los sistemas de información y controladores, y procesadores integrados, junto con sus usuarios y operadores. (Lira, 2017, pp 38-51),

ha impactado en la tecnología cibernética en la forma en que las fuerzas armadas y las fuerzas del orden se enfrentan a un entorno cambiante para hacer frente a las amenazas actuales como ser la ciberguerra.

El termino ciberguerra no es nuevo, fue acuñado por el centro de estudios de defensa estadounidense Rand Corportion a principios de los noventa del siglo pasado para referirse a un tipo de conflictos no conocido hasta entonces en el que las tecnologías de la comunicación serian la principal arma. (Quintana, 2017, p. 15)

Para realizar esta investigación se consultaron más de 87 fuentes de medios de acceso público electrónico, académico y comerciales refiriéndose a los diferentes análisis tomados por las diferentes entidades, quienes recopilan datos de los ataques cibernéticos a los diferentes países de las cuales solo fueron útiles 33 documentos.

Desafíos que enfrenta Honduras en materia de ciberseguridad y ciberdefensa.

La cibernética es una disciplina que se enfoca en el estudio de los sistemas de control y comunicación en seres vivos y máquinas. En el contexto de la seguridad cibernética, la cibernética se refiere al estudio de los sistemas de información y comunicación en línea, y cómo se pueden proteger contra amenazas y ataques cibernéticos. (FEM, 2023)

La ciberseguridad y la ciberdefensa son áreas importantes de la cibernética, ya que se enfocan en proteger los sistemas informáticos y la información digital contra amenazas externas.

Es importante destacar que la cibernética no se limita solo a los sistemas informáticos, sino que abarca una amplia gama de sistemas, desde los biológicos hasta los tecnológicos. En el contexto de la seguridad cibernética, la cual proporciona un marco teórico y conceptual para comprender los sistemas de información y comunicación en línea y desarrollar estrategias para protegerlos contra amenazas y ataques cibernéticos.

A medida que los usuarios se vuelven más dependientes de los sistemas de información, la seguridad del ciberespacio está evolucionando para incluir nuevos conceptos que son relevantes para una nación u organización. Esta relevancia está ligada al avance tecnológico representado por la actual cuarta revolución industrial, específicamente la industria 4.010 Marcada por la convergencia de tecnologías digitales, físicas y biológicas, (BBC, 2016) Esta seguridad dentro del ciberespacio define la ciberdefensa, por

lo que es necesario determinar la ciberseguridad, que, según la definición del organismo internacional ITU, es la seguridad del ciberespacio.

La colección de herramientas, políticas, conceptos de seguridad, salvaguardas de acción, capacitación, prácticas correctas, tecnologías seguras y procedimientos que pueden usarse para salvaguardar a los usuarios y las actividades organizacionales en el entorno cibernético se conoce como ciberseguridad. (ITU, 2008, p.3)

Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber entorno (UIT, 2010, p. 20).

En la actualidad, las amenazas a la seguridad cibernética no solo provienen directamente de otros estados, facción del propio estado, sino también de organizaciones internacionales o transnacionales de crimen organizado, piratería y terrorismo, que en muchos casos se basan en estados que no ejercen el control adecuado sobre su territorio y población y las utilizan para su propio beneficio.

Los ataques a nivel mundial tienen como objetivo principal identificar perfiles de blancos de organizaciones y agencias militares, destacando los de inteligencia. (ABAD, 2020), por lo que se define como una amenaza principal a nivel mundial para los ataques cibernéticos, la delincuencia cibernética y el terrorismo. A nivel internacional, los Estados y las organizaciones han creado estructuras de ciberdefensa para proteger la seguridad y la infraestructura de TIC, pero más del 50% de los ataques causan daños y su recuperación puede tardar meses o incluso años. (CISCO, 2018, p. 17)

La estrategia nacional de seguridad de los estados organiza la defensa de la seguridad, se diseñan y fortalecen diversas estrategias de defensa en respuesta a las amenazas y los riesgos, lo que da como resultado diversas facetas de la defensa, como la defensa territorial, la defensa aérea, la defensa marítima, la defensa de fronteras, la defensa económica y, entre ellas, la defensa en el ciberespacio, que también necesita una defensa de la información para garantizar la seguridad cibernética.

La ciberseguridad es una parte crucial de la seguridad nacional porque si el ciberespacio no se controla adecuadamente, una nación puede verse amenazada en cuanto a su libertad de acción y seguridad, no solo su ciberseguridad sino toda la seguridad nacional.

Teniendo en cuenta que las amenazas cibernéticas se dan o se desarrollan en el ciberespacio el cual se definió anteriormente, pero también existen otras definiciones dadas por diferentes instituciones o países que engloban más actores, la Real Academia Española de la Lengua lo define como el ámbito virtual creado por medios informáticos. (Real Academia Española, 2022b), el Reino Unido en su estrategia del 2011 lo define como un dominio interactivo conformado por redes digitales que son usadas para almacenar, modificar y comunicar información. Esto incluye el internet, pero también cualquier otro sistema de información que soporta nuestros negocios, infraestructura y servicios.(Centro Superior de Estudios de la Defensa Nacional (España), 2012), las Fuerzas armadas y marina de México lo definen como el Ámbito intangible, de naturaleza global, soportado por las tecnologías de la información y comunicaciones (TIC´s), que es utilizado para la interacción entre individuos y entidades públicas y privadas (Centro Superior de Estudios de la Defensa Nacional (España), 2012).

Haciendo referencia a estas definiciones nos podemos atrever a dar una definición propia del ciberespacio diciendo que es un espacio intangible y virtual que se crea mediante la interconexión de sistemas informáticos y redes electrónicas en todo el mundo que coexiste en el mundo físico que facilita la forma de comunicarnos, acceder a la información y conectarnos con otras personas.

En base a estas definiciones podemos caracterizar al ciberespacio en cinco puntos:

1. El ciberespacio es universal, ya que no tiene límites físicos ni temporales.
2. Además, existe una fuerte interacción con las tecnologías de información y comunicaciones, que son su forma de acceder a ella.
3. El espacio electromagnético, los sistemas de información, los sistemas de comunicación y las redes dependen de su infraestructura, que no siempre es la misma.
4. La persona traslada su esencia al dominio virtual, y una foto, comentarios e información son una prolongación de su propio ser.
5. El manejo de información ocurre en todos los niveles: personal, privado, industrial y gubernamental.

En el ciberespacio se dan varias actividades de la vida cotidiana como comunicación en redes sociales, comercio electrónico, banca y finanzas, educación, gobierno electrónico entre otras actividades, de ahí el interés de ciber delincuentes que la RAE lo define como persona que delinque a treves del internet (Real Academia Española, 2022)

En los medios de comunicación no solo escritos, sino también radio, televisión y, naturalmente, los medios electrónicos de Internet se han vuelto comunes las noticias de

ciberataques a ciudadanos, organizaciones, empresas y hasta instalaciones críticas de países como plantas de energía química, centrales nucleares o fábricas de diversas índoles. Por lo que en el presente artículo se exponen algunas noticias publicadas en la prensa hondureña e internacional más relevantes.

Suplantación de entidades bancarias: Los ciberdelincuentes han incrementado sus ataques a nivel mundial y desde hace unos meses están acechando a los hondureños utilizando fachadas bancarias para suplantar entidades bancarias y obtener información confidencial de los usuarios(Romero, 2022)

En septiembre de 2021, el sitio web de la Secretaría de Finanzas de Honduras fue hackeado por un grupo de ciberdelincuentes, quienes publicaron información confidencial en línea (DLP, 2023)

En 2020, el Ministerio de Salud de Honduras sufrió un ataque cibernético que afectó su sistema informático y puso en riesgo la información de los pacientes (Revista Seguridad 360, 2023)

Resulta evidente la importancia de contar con una estrategia de ciberseguridad y ciberdefensa en Honduras que aborde de manera integral las amenazas y desafíos presentes en el ciberespacio. Una estrategia bien diseñada y ejecutada puede contribuir a proteger la información sensible, salvaguardar los activos digitales, fortalecer la seguridad de la infraestructura crítica, combatir el cibercrimen y promover una cultura de seguridad digital en la población.

Como lo señala Mejía (2020) "una estrategia de ciberseguridad y ciberdefensa bien implementada es fundamental para proteger la soberanía y la seguridad nacional de un país en el ciberespacio" (p. 34). Honduras, al igual que otros países como México, Colombia,

Costa rica etc., enfrenta amenazas en el ciberespacio que pueden poner en riesgo su soberanía, seguridad y estabilidad. Una estrategia de ciberseguridad y ciberdefensa robusta y efectiva puede ayudar a prevenir y mitigar estas amenazas, garantizando la protección de los intereses nacionales en el ciberespacio.

Además, una estrategia de ciberseguridad y ciberdefensa bien diseñada puede contribuir al desarrollo económico y social de Honduras. La confianza en el uso de la tecnología y la protección de la información son elementos fundamentales para el crecimiento de la economía digital y la atracción de inversiones en el país. Como lo destaca (Fernández, 2019), "la ciberseguridad y ciberdefensa son factores clave para fomentar la confianza de los inversionistas y promover un entorno propicio para el desarrollo de la tecnología en Honduras" (p 42).

Una estrategia de ciberseguridad y ciberdefensa sólida puede brindar la confianza necesaria a las empresas y ciudadanos para utilizar la tecnología de manera segura, lo que a su vez puede impulsar la innovación, la competitividad y el crecimiento económico del país.

Asimismo, una estrategia de ciberseguridad y ciberdefensa adecuada puede contribuir a la protección de los derechos y la privacidad de los ciudadanos hondureños en el ciberespacio. La creciente digitalización de la información personal y el uso de plataformas en línea para diversos fines, como el comercio electrónico, la banca en línea y el acceso a servicios gubernamentales, ha aumentado la necesidad de proteger los datos personales y la privacidad de los individuos.

Por lo cual es fundamental que Honduras cuente con una estrategia de ciberseguridad y ciberdefensa que incluya medidas eficaces para prevenir, detectar y responder a los delitos cibernéticos.

Además, otro desafío importante que enfrenta Honduras en el ciberespacio es la promoción de una cultura de seguridad digital en la población. La falta de conciencia y conocimiento sobre las buenas prácticas de seguridad en línea puede hacer que los individuos sean más vulnerables a los ataques cibernéticos y pongan en riesgo su información personal y financiera. Como señala Gómez (2017), "la educación y concientización sobre la importancia de la seguridad digital son fundamentales para proteger a los ciudadanos y empresas en el ciberespacio" (p. 78). Por lo tanto, es necesario que la estrategia de ciberseguridad y ciberdefensa de Honduras incluya programas de educación y sensibilización que promuevan una cultura de seguridad digital en la población, fomentando el uso responsable y seguro de la tecnología.

Describir las capacidades necesarias para enfrentar las amenazas cibernéticas actuales y futuras.

Para enfrentar las amenazas cibernéticas actuales y futuras, se requiere capacidades técnicas y estratégicas, así como una cultura cibernética, por lo cual se tratará de describir algunas capacidades necesarias para enfrentar las amenazas cibernéticas.

Conocimientos técnicos

La era digital ha creado un mundo interconectado donde las redes electrónicas fluyen constante con información y datos. No obstante, la presencia de esta conexión ha puesto a las personas, empresas y gobiernos en riesgo de diversas amenazas cibernéticas cada vez más sofisticadas. La ciberseguridad se ha convertido en una parte importante para la protección

de la información y la integridad digital. En este contexto, la comprensión técnica de la ciberseguridad se vuelve crucial. Es esencial contar con profesionales capacitados en ciberseguridad que tengan conocimientos técnicos en campos como redes, sistemas operativos, bases de datos y criptografía, y que estén informados sobre las amenazas y tendencias más recientes.

Los ciberataques evolucionan a la par que las tecnologías cambiantes. Los delincuentes utilizan nuevas herramientas y elaboran nuevas estrategias para el acceso no autorizado al sistema. (AWS, 2023)

La ciberseguridad está en constante cambio debido a las nuevas amenazas y tecnologías. Esto demuestra lo crucial que es que los profesionales estén al tanto de las últimas tendencias y amenazas cibernéticas. Porque los ciberdelincuentes son ingeniosos y adaptables, los defensores de la ciberseguridad deben avanzar.

La falta de especialistas en ciberseguridad es un problema que afecta un hacer el Mundo. Según un informar del Foro Económico Mundial, para 2022 habrá una escasez de 3,4 millones de expertos en ciberseguridad en hacer el Mundo. (FEM, 2023) Esto demuestra la importancia de fomentar la formación en ciberseguridad. Las empresas, los gobiernos y las universidades deben trabajar juntas para brindar programas de capacitación y certificación en ciberseguridad que prepara un profesional para hacer frente unas las amenazas digitales.

Reforzar la Defensa Digital

La proliferación de amenazas cibernéticas sofisticadas requiere una estrategia integral de defensa, en la que las herramientas de seguridad son un componente esencial. La importancia de contar con herramientas de seguridad adecuadas, como cortafuegos, sistemas

de detección de intrusos y antivirus, y cómo su configuración y actualización adecuadas son esenciales para proteger contra las amenazas cibernéticas que están creciendo.

Firewalls

Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente (CISCO, 2023) esta herramienta de seguridad evita que una red privada se vea afectada por amenazas exteriores. El sistema funciona filtrando el tráfico de la red utilizando un conjunto de reglas predeterminadas. Un buen firewall puede detectar intentos de acceso no autorizado y protector los sistemas internos de ataques externos. Además, tiene la capacidad de monitorear y registrador el tráfico de la red para identificador patronos de actividad sospechosa.

Sistemas de Detección de Intrusiones

Los sistemas de detección de intrusos (IDS) son herramientas que monitorean el tráfico de red o la actividad de un sistema para vigilar y analizar la actividad de los usuarios y del sistema, revisar las configuraciones del sistema y de las vulnerabilidades, evaluar la integridad de los archivos críticos del sistema, reconocimiento de los modelos de la actividad que reflejan ataques conocidos. (Mauricio et al., 2006)

La principal ventaja de los sistemas de detección de intrusos es su capacidad para detectar amenazas que puede haber sido evitadas por el firewall en un principio. En tiempo real, puede detectar intrusos y enviar alertas para que los administradores tomen medidas.

Antivirus

Los programas antivirus son cruciales para el combate de los malware (software o código informático diseñado para infectar, dañar o acceder a sistemas informáticos.) (Belcic, 2023), que puede incluir virus, gusanos, troyanos y otros programas maliciosos. Estos programas buscan firmas y comentarios relacionados con amenazas en archivos y sistemas. El antivirus elimina o pone en cuarentena una amenaza.

Configuración y Actualización

El uso de estas herramientas de seguridad es crucial, pero su configuración y actualización también son cruciales. La seguridad informática es un campo en constante evolución, por lo que es necesario actualizar y mejorar regularmente las medidas de seguridad a fin de estar protegidos adecuadamente contra nuevas amenazas. (Coppola, 2023)

Una configuración inadecuada puede permitir que las amenazas pasen desapercibidas o causar bloqueos innecesarios. Sin embargo, la falta de actualización aumenta el riesgo de no identificador nuevas amenazas.

Políticas y Procedimientos de Seguridad en Ciberseguridad

En un mundo cada vez más interconectado, la ciberseguridad se ha convertido en una preocupación importante tanto para las personas como para las organizaciones, contar con políticas y procedimientos de seguridad robustos es crucial para enfrentar las amenazas del ciberespacio.

Políticas de Seguridad

La política de seguridad consiste en desarrollar el marco de actuación apropiado para salvaguardar la información de la organización. (ISO 27001, 2018), la cual describe cómo proteger la información y los activos de una organización. Estas políticas establecen las expectativas para los empleados y usuarios finales y definen las mejores prácticas en seguridad de la información. Una política de seguridad sólida debe incluir aspectos como el acceso un sistemas y datos, la gestión de contraseñas, la retención de registros y la respuesta a incidentes.

Procedimientos de Seguridad

La política de seguridad requiere no solamente conocer las amenazas a las que están expuestas la información y los recursos de una organización, sino también establecer el origen de estas, que pueden ser internas o externas a la organización. (Vega, 2008) en aspecto práctico las políticas de seguridad son los procedimientos de seguridad.

Las políticas establecen las reglas generales, pero los procedimientos explican cómo se deben aplicar esas reglas en circunstancias particulares. Por ejemplo, una política de seguridad puede establecer que el acceso a un cierto dato confidencial debe estar restringido, mientras que un procedimiento puede describir cómo se asignan y revocan esos permisos de acceso.

Responsabilidades de Usuarios y Administradores

Las políticas y procedimientos de seguridad especialmente qué deben hacer los usuarios y administradores de sistemas. Es responsabilidad de los usuarios cumplir con las políticas y procedimientos, como proteger sus credenciales de acceso, informar sobre

actividades sospechosas y seguir las políticas de uso aceptable. Los administradores de sistemas están encargados de aplicar y hacer cumplir las políticas y procedimientos, como la configuración segura de sistemas y la supervisión constante de la seguridad.

Actualización y Revisión Continua

Las amenazas cibernéticas están en constante cambio. Las políticas y procedimientos de seguridad deben actualizar con frecuencia para mantenerse al día con las amenazas emergentes porque los atacantes constantemente desarrollan nuevas tácticas y técnicas. La política que funcionó hace unos años puede no ser adecuada en la actualidad.

Es crucial revisar continuamente las políticas y procedimientos. Esto implica la implementación de modificaciones basadas en los conocimientos adquiridos de eventos de seguridad anteriores y en el desarrollo de las amenazas.

La capacidad de detección y respuesta en seguridad cibernética es esencial para reducir las amenazas digitales.

En la era de la información, las amenazas cibernéticas son una realidad presente y en constante cambio. La ciberseguridad es esencial para asegurar la integridad, la confidencialidad y la disponibilidad de datos y sistemas.

La capacidad de detección y respuesta es esencial para identificar y mitigar de manera efectiva las amenazas cibernéticas.

La Evolución de las Amenazas Cibernéticas

La constante evolución de las amenazas cibernéticas hace que las organizaciones tengan la necesidad de contar con una estrategia integral que les permita comprender, comunicar, gestionar y reducir los riesgos en el ecosistema tecnológico. (OEA, 2022)

Las amenazas cibernéticas han cambiado mucho en los últimos años. Los ciberdelincuentes emplean tácticas cada vez más complejas para infiltrarse en sistemas y extraer datos confidenciales. Las amenazas cibernéticas van desde el malware y el phishing hasta los ataques de denegación de servicio (DDoS) y el ransomware el cual es un software extorsivo, su finalidad es impedirte usar el dispositivo hasta que se haya pagado un rescate (Kaspersky, 2023)

Detección Temprana

Una estrategia de ciberseguridad efectiva depende de la capacidad de detección temprana. El uso de sistemas de monitoreo y alerta temprana busca actividad sospechosa en el tráfico y los sistemas de la red. Estos sistemas pueden detectar patrones de comportamiento anormales que puede ser una señal de un ataque o una violación de seguridad en los sistemas informáticos, el monitoreo de seguridad en tiempo real es crucial para identificador amenazas antes de que causen un daño significativo.

Respuesta Rápida: Mitigando el Impacto

Después de la detección, la capacidad de respuesta rápida es crucial. Es esencial tomar medidas rápidas y efectivas para reducir el impacto de una amenaza y evitar su exposición

futura. La contención de amenazas, la eliminación de malware y la restauración de sistemas atacados son ejemplos de esto.

Para que las organizaciones estén preparadas para enfrentar ciberataques, es esencial Tener equipos de respuesta un incidente. Estos equipos establecen roles y responsabilidades claros, procedimientos de comunicación y acciones particulares que deben tomate en caso de un incidental de seguridad.

Capacitación y Concienciación

Sin un personal capacitado y concientizado de la importancia de la ciberseguridad; la capacidad de detección y respuesta es ineficaz. La capacitación de los empleados es esencial para que puedan identificar y reportar actividades sospechosas y seguir los procedimientos de respuesta de incidentes.

La concientización sobre ciberseguridad es esencial para la prevención y la respuesta. Los empleados deben estar familiarizados con las amenazas comunes, los riesgos y las mejores prácticas de seguridad.

Cultura de Seguridad Cibernética

En la actualidad, vivimos en un mundo cada vez más digitalmente conectado. La vida, el trabajo y la comunicación han cambiado gracias a las tecnologías de la información y la comunicación (TIC).

Amenazas Cibernéticas

En el mundo digital, las amenazas cibernéticas son una realidad constante. Las personas y las empresas están expuestas a una variedad de amenazas cibernéticas, incluidos ataques de phishing y ransomware, vulnerabilidades de software y robo de datos. Estos ataques pueden causar daños significativos, incluyendo la pérdida de datos confidenciales e interrupciones significativas en las operaciones.

La Importancia de una Cultura de Seguridad Cibernética

La conciencia y la responsabilidad de todos los usuarios de sistemas informáticos son la base de una cultura de seguridad cibernética. Ayuda a las personas a reconocer las amenazas cibernéticas, adoptar buenas prácticas de seguridad y tener una mentalidad vigilante. Esta cultura es importante a nivel organizacional y nacional para garantizar la seguridad de infraestructuras críticas y la protección de los ciudadanos.

Promoción de Buenas Prácticas de Seguridad

Una parte fundamental de la cultura de seguridad cibernética es la promoción de buenas prácticas de seguridad. Esto requiere la implementación de políticas y procedimientos claros para garantizar las mejores prácticas de seguridad. La gestión adecuada de contraseñas, la segmentación de redes y la implementación de reglas de seguridad.

Todos los aspectos de una organización o sociedad deben tener seguridad. Esto incluye Tener en cuenta la seguridad cuando se desarrolla software, se implementan medidas de seguridad física y se realizan evaluaciones regulares de posturas de seguridad.

El Papel Transformador de la Inteligencia Artificial en la Ciberseguridad

A medida que los ciberataques crecen en volumen y complejidad, la inteligencia artificial (IA) ayuda a los analistas de operaciones de seguridad con pocos recursos a anticiparse a las amenazas. (UNESCO, 2023)

El Entorno Cibernético Actual

El mundo digital en el que vivimos está lleno de muchas conexiones. Las organizaciones dependen cada vez más de la tecnología para sus operaciones porque la información fluye a través de redes globales. sin embargo, las vulnerabilidades también surgen de esta interconexión. Los ciberdelincuentes utilizan las brechas de seguridad para robar información confidencial, interrumpir servicios y dañar la privacidad de las personas.

La Inteligencia Artificial como Defensora en la Ciberseguridad

La inteligencia artificial (IA) se ha convertido en una herramienta útil para combate las amenazas cibernéticas. Ella es vital para la detección temprana de ataques porque puede analizar grandes cantidades de datos en tiempo real y encontrar patronos anómalos. Los sistemas de IA pueden monitorear continuamente la actividad en la red y alertar sobre acciones sospechosos, lo que permite a las organizaciones tomar medidas antes de que un ataco se materialice por completo, colaboran categorizando los ataques según el nivel de amenaza; los encargados de ciberseguridad, por su parte, asignan la prioridad con que se debe atender cada uno, iniciando por los más peligrosos para el estado de la información de la empresa. (Conzultek, 2023)

los sistemas de detección de intrusiones (IDS) basados en IA pueden detectar y bloquear automáticamente el tráfico de red malicioso, sin intervención humana. (CORRONS, 2023)

La Automatización y la Respuesta Rápida

Los sistemas de IA pueden actuar de inmediato para detener el ataque y reducir el daño. Esto incluye la capacidad de ajustar las configuraciones de seguridad en tiempo real, aislar sistemas comprometidos y bloquear direcciones IP maliciosas.

La automatización reducir la carga de trabajo de los equipos de seguridad cibernética y acelera la respuesta a los ataques.

Desafíos y Consideraciones Éticas

A pesar de los evidentes beneficios, el uso de la IA en la ciberseguridad presenta cuestiones éticas. Por un lado, una excesiva dependencia de la automatización podría resultar en una supervisión humana inadecuada y en una toma de decisiones precipitadas. Además, existe la posibilidad de que los oponentes utilicen técnicas de inteligencia artificial para crear ataques más complejos y difíciles de detectar.

Además, la privacidad y la ética son importantes preocupaciones cuando se recopilan y analizan datos para detectar amenazas. Es fundamental asegurarse de que el uso de la IA en la ciberseguridad cumpla con las leyes de privacidad y protección de datos y no comprometa la privacidad de las personas sin su consentimiento. Según la Unesco la inteligencia artificial da resultados sesgados. La tecnología de los motores de búsqueda no

es neutral, ya que procesa macrodatos y prioriza los resultados con la mayor cantidad de clics dependiendo tanto de las preferencias del usuario como de la ubicación. (UNESCO, 2023)

Determinar la estrategia a desarrollar para la implementación de una política en materia de ciberseguridad y ciberdefensa para Honduras.

Honduras debe tomar medidas proactivas para proteger su soberanía y sus intereses en el ciberespacio, ya que la ciberseguridad y la ciberdefensa son cruciales en la era digital actual. La implementación de una estrategia integral ayudará a fortalecer la seguridad en línea del país y a crear un entorno digital seguro y estable para todos los hondureños.

Creación de una Ley de Ciberseguridad en Honduras

En la era digital actual, los gobiernos, las empresas y los ciudadanos están cada vez más preocupados por la ciberseguridad. Debido a la creciente interconexión de sistemas y la creación de vastos depósitos de información en línea, la seguridad cibernética es crucial. Para abordar este problema en Honduras, es necesario establecer una ley de ciberseguridad que establezca estándares y requisitos mínimos para la protección de la información y los sistemas digitales.

Debido a la preocupación global por la ciberseguridad, muchos países como por ejemplo Colombia, México, Costa Rica entre otros, ya han implementado leyes y regulaciones específicas en este ámbito. Estas leyes abordan temas fundamentales de ciberseguridad, como la protección de datos personales, la prevención de ataques cibernéticos y la gestión de incidentes.

Al implementar una ley de seguridad cibernética en Honduras, el país se ajustará a las prácticas más avanzadas a nivel mundial y podría aprender de las experiencias de otros países.

La aplicación de una ley de ciberseguridad permitirá establecer un marco legal sólido para la protección de datos y sistemas digitales en Honduras. Las responsabilidades de las partes involucradas, como empresas, gobiernos y ciudadanos, podrían estar claramente definidas en esta ley. También podría sancionar a aquellos que infrinjan las normas de seguridad cibernética, con el fin de prevenir a futuros ciberdelincuentes.

Creación de un Equipo de Respuesta a Incidentes

En el mundo digital real, la amenaza de ciberataques es constante y omnipresente. Los usuarios individuales, las empresas y las organizaciones gubernamentales están en riesgo de sufrir ataques cibernéticos. Para enfrentar esta amenaza cada vez mayor, es necesario establecer un equipo de respuesta contra incidentes cibernéticos (CSIRT) que tenga la capacidad de detectar y responder ante estos ataques de manera rápida y efectiva.

Un CSIRT es un grupo de especialistas en seguridad cibernética que monitorean, detectan y responden a incidentes cibernéticos. La principal responsabilidad de un CSIRT es reducir las consecuencias de estos incidentes y garantizar que las operaciones continúen. (Mendoza, 2015)

La formación de un CSIRT en Honduras representaría un avance significativo en la protección de los sistemas digitales y los datos confidenciales. Este equipo de estancia está formado por profesionales con conocimientos tecnológicos en seguridad cibernética que pueden detectar amenazas y tomar medidas inmediatas para reducirlas. Tener un CSIRT

dedicado permite una respuesta más rápida y coordinada a los incidentes, lo que es esencial para limitar el daño causado por los ciberataques.

Un CSIRT puede desempeñar un papel importante en la prevención y la preparación, además de su función de respuesta.

Fortalecimiento de la Educación y Conciencia en Ciberseguridad: Prevenir para Proteger

En un mundo cada vez más digitalizado, es fundamental adquirir conocimientos y habilidades sobre la seguridad cibernética. Debido a la creciente dependencia de la tecnología y la interconexión digital, la población en general debe estar preparada para enfrentar el aumento de los ciberataques. Para evitar que las personas sean víctimas de ciberataques, es necesario fomentar la educación y la conciencia en ciberseguridad.

La educación en ciberseguridad es proporcionar a las personas los conocimientos y habilidades necesarios para protegerse en línea. Esto incluye el reparo de riesgos cibernéticos, el reconocimiento de amenazas y la comprensión de cómo reducir los riesgos. (OEA, 2020)

La educación en ciberseguridad debe comenzar desde una edad temprana y extenderse a lo largo de la vida porque las amenazas cibernéticas evolucionan constante.

Aumentar la conciencia sobre la seguridad cibernética es fundamental. Se refiere a los riesgos cibernéticos en la vida diaria. Es importante que las personas sepan que están en constante riesgo de ser víctimas de ataques cibernéticos, como phishing, malware y robo de identidad. Gracias a esta conciencia, puede tomar precauciones y mantener prácticas seguras en línea.

Establecimiento de Medidas de Seguridad para la Infraestructura Crítica

La infraestructura fundamental de una nación es la base de su funcionamiento, que incluye dominios como la energía, las finanzas y la salud. Los fundamentos para el bienestar y la prosperidad de la sociedad y la economía en su conjunto se derivan de estos pilares. Por tal razón, los ciberdelincuentes buscan esta infraestructura. Por lo cual, es fundamental mantener medidas de seguridad adecuadas y estables para proteger estos activos delicados.

El sector financiero es uno de los principales objetivos de los ciberataques porque maneja una gran cantidad de datos sensibles y transacciones financieras. (OEA, 2019) Para protegerlo, se deben usar cortafuegos, sistemas de detección de intrusos y monitoreo constante.

La infraestructura energética es un objetivo relevante adicional. Un ataque exitoso podría detener la gestión de energía de una zona o incluso convertirla en una nación.(Ayerbe, 2020) Para evitar esto, se deben implementar protocolos de seguridad en las redes eléctricas y sistemas de control industrial.

Debido a que en el sistema de salud se manejan datos de atención médica cruciales y datos médicos confidenciales, el sector de la salud también es vulnerable. Las medidas de seguridad esenciales incluyen la encriptación de datos y el control de acceso de los usuarios.

Fomento de la Colaboración Público-Privada en Ciberseguridad: Una Estrategia Esencial

Los ciberataques pueden dañar gravemente la economía, la infraestructura y la privacidad de las personas. Para enfrentar esta creciente amenaza, es esencial promover la colaboración entre el sector público y privado en el ámbito de la ciberseguridad.

La colaboración público-privada implica que gobiernos y empresas mejoren las prácticas de seguridad, compartan datos sobre amenazas cibernéticas y coordinen las respuestas a incidentes.(Arteaga, 2022) Hay muchas razones por las que esto es importante.

Primero, los ciberataques pueden tener un impacto en organizaciones de cualquier tamaño y sector porque no tienen límites. Los gobiernos tienen la capacidad de utilizar recursos e inteligencia que pueden ayudar a las empresas a identificar y reducir amenazas. Sin embargo, las empresas tienen la capacidad de ayudar a los gobiernos a responder a los ataques en tiempo real.

En segundo lugar, la protección cibernética es cambiante y costosa. Las empresas deben invertir en tecnología y personal especializado para protegerse, mientras que los gobiernos deben estar al tanto de las amenazas y tendencias más recientes.

Aunque las pequeñas y medianas empresas pueden no poder enfrentar esta amenaza por sí solas, la cooperación puede ayudar a compartir estos costos y recursos.

En tercer lugar, la cooperación entre los sectores público y privado puede ayudar a establecer normas y regulaciones de ciberseguridad más efectivas. Los gobiernos pueden trabajar con la industria para desarrollar políticas y leyes que protejan a las personas y las empresas al mismo tiempo que fomentan la competencia y la innovación.

Conclusiones

En conclusión, la implementación de una estrategia de ciberseguridad y ciberdefensa en Honduras es crucial para asegurar un entorno cibernético seguro y resistente. Una estrategia integral que involucre a todas las partes interesadas y se adapte a la situación legislativa, cultural, económica y estructural de Honduras debe implementarse para abordar los desafíos de la ciberseguridad en el país, como la falta de una política nacional de seguridad cibernética, la falta de formación y capacitación de profesionales en ciberseguridad y ciberdefensa, y la falta de coordinación y colaboración entre diferentes sectores y actores.

La capacitación de profesionales en ciberseguridad y ciberdefensa también es crucial para garantizar que el ciberespacio de Honduras sea seguro y resistente. Un ejemplo de cómo se pueden formar profesionales altamente capacitados en ciberseguridad y ciberdefensa es la Maestría en Ciberseguridad y Ciberdefensa que se imparte la Escuela Superior de Guerra Gral. Rafael Reyes Prieto en Colombia.

Además, para garantizar un ciberespacio seguro y resistente en Honduras, es esencial que varios actores, incluidos el gobierno, las empresas, las universidades y la sociedad civil, trabajen juntos. Además, es esencial investigar y difundir documentos técnicos, herramientas e informes para orientar a los responsables de la formulación de políticas, los CSIRT, los operadores de infraestructura, las organizaciones privadas y otros actores relevantes en Honduras.

Para proteger la soberanía del espacio ciberespacial hondureño, es necesario desarrollar medidas de contrapoder ciberespacial.

Para garantizar un entorno digital seguro y estable en Honduras, Para abordar los desafíos de la ciberseguridad en Honduras, es necesario establecer una política nacional de seguridad cibernética, formar y capacitar a profesionales en ciberseguridad y ciberdefensa, coordinar y colaborar entre diferentes sectores y actores, investigar y divulgar documentos técnicos, herramientas e informes, y desarrollar medidas de contrapoder ciberespacial. A través de estas acciones, Honduras puede garantizar un entorno digital seguro y robusto para su progreso y expansión en la era digital.

Es fundamental enfatizar que la implementación de una estrategia de ciberseguridad y ciberdefensa en Honduras es esencial para proteger al país de amenazas cibernéticas y garantizar los derechos humanos y la libertad de expresión en línea. La adopción de medidas que protejan contra los actos de odio y discriminación en línea es un paso importante en esta dirección.

Para garantizar un entorno cibernético seguro y resistente, es esencial que Honduras implemente una estrategia de ciberseguridad y ciberdefensa. En Honduras, se pueden implementar medidas para garantizar un ciberespacio seguro y resistente, como la capacitación y capacitación de profesionales en ciberseguridad y ciberdefensa, la coordinación y colaboración entre diversos actores y sectores, la investigación y divulgación de documentos técnicos, herramientas e informes, y el desarrollo de medidas para contrapoder ciberespacial.

Honduras puede proteger los derechos humanos y las libertades en línea, atraer inversiones e impulsar su industria tecnológica con estas medidas.

Referencias

Aguilar Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de Estudios En Seguridad Internacional*, *6*(2), 17–43. https://doi.org/10.18847/1.12.2

BID. (2016). *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? | Publications*. https://publications.iadb.org/publications/spanish/viewer/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

BID. (2020). *Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe*. 13.

Centro Superior de Estudios de la Defensa Nacional (España). (2012). *El ciberespacio : nuevo escenario de confrontación*. Ministerio de Defensa, Subdirección General de Publicaciones y Patrimonio Cultural.

Cibernética - Qué es, teoría, definición y concepto. (n.d.). Retrieved August 28, 2023, from https://definicion.de/cibernetica/

Ciberseguridad: Por qué debemos cerrar la brecha de cualificaciones | Foro Económico Mundial. (n.d.). Retrieved September 5, 2023, from https://es.weforum.org/agenda/2023/02/ciberseguridad-como-cerrar-la-brecha-de-cualificaciones-puede-mejorar-la-resistencia-y-apoyar-a-una-mano-de-obra-en-transicion/

Fernández, J. (2019). *La importancia de la ciberseguridad en el desarrollo de la tecnología en Honduras. Revista de Investigación Académica.* 39–49.

Gómez, J. (2017). La importancia de la seguridad digital en Honduras. . *Revista de Seguridad Cibernética*, 76–80.

González-Ruiz, J. (2020). *Ciberseguridad y protección de datos personales en el ámbito militar. Anales de la Academia Nacional de Derecho y Ciencias Sociales de Buenos Aires*. 43-53.

Hernández, S. (2008). *LA TEORIA DEL REALISMO ESTRUCTURALISTA Y LAS INTERACCIONES ENTRE LOS ESTADOS EN EL ESCENARIO INTERNACIONAL: Vol. XIV* (Issue 2).

Inteligencia artificial: ejemplos de dilemas éticos | UNESCO. (n.d.). Retrieved September 6, 2023, from https://www.unesco.org/es/artificial-intelligence/recommendation-ethics/cases

Inteligencia artificial (IA) para ciberseguridad | IBM. (n.d.). Retrieved September 6, 2023, from https://www.ibm.com/es-es/security/artificial-intelligence

Inteligencia artificial y ciberseguridad: cómo la tecnología puede pasar de ser tu mejor aliada a tu mayor enemigo. (n.d.). Retrieved September 6, 2023, from https://www.20minutos.es/tecnologia/ciberseguridad/la-ia-en-la-ciberseguridad-lo-bueno-y-lo-malo-5102134/

ISO 27001 ¿En que se basa la política de seguridad de la información? (n.d.). Retrieved September 5, 2023, from https://www.pmg-ssi.com/2018/12/iso-27001-en-que-se-basa-la-politica-de-seguridad-de-la-informacion/

Lira, C. (2017). Armada de Mexico operaciones ciberespacio. *Revista Del Centro de Estudios Superiores Navales. , 38*, 51.

Martínez, J. (2018). *Los desafíos de la ciberseguridad en América Latina. Observatorio Iberoamericano de Seguridad*. .

Mauricio, C., Carbajal, O., Rivera, C. I., Patricia, Z. I., & Romero, P. (n.d.). *XVII 1 34 polibits 31 Sistemas de Detección de Intrusos (IDS), Seguridad en Internet*. http://www.guardiacivil.org/

Mejía, M. (2020). *Estrategias de ciberseguridad y ciberdefensa para la protección de la soberanía nacional en Honduras. Revista de Política Internacional*. 32–44.

OEA. (2004). *Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética."*

OEA. (2022). Información_ampliada_Cyberwomen2022. *OEA*.

ONU. (2018). *Resolución sobre Desarrollo de la Confianza en el Uso de la Tecnología de la Información y las Comunicaciones en el Contexto de la Seguridad Internacional*.

(PDF) Estrategias Nacionales de Ciberseguridad en América Latina. (n.d.). Retrieved September 9, 2023, from https://www.researchgate.net/publication/325397629_Estrategias_Nacionales_de_Ciberseguridad_en_America_Latina

¿Qué es el malware y cómo funciona? | Definición | Avast. (n.d.). Retrieved September 5, 2023, from https://www.avast.com/es-es/c-malware

¿Qué es la ciberseguridad? - Explicación de la ciberseguridad - AWS. (n.d.). Retrieved September 4, 2023, from https://aws.amazon.com/es/what-is/cybersecurity/

¿Qué es un firewall? - Cisco. (n.d.). Retrieved September 5, 2023, from https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Quintana, Y. (2017). *Ciberguerra*.

Real Academia Española. (2022a). *ciberdelincuente. En Diccionario de la lengua española*. .

Real Academia Española. (2022b). *Ciberespacio. En Diccionario de la lengua española*.

Seguridad informática: qué es, tipos y características. (n.d.). Retrieved September 5, 2023, from https://blog.hubspot.es/website/que-es-seguridad-informatica

Torres, L. (2018). *Amenazas cibernéticas en Honduras: retos y desafíos. Revista de Tecnologías de Información y Comunicación*. 55–62.

UIT. (2010). *Ciberseguridad Definiciones y terminología relativas a la creación de confianza y seguridad.* . 20. https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, *20*, 31. https://doi.org/10.17141/URVIO.20.2017.2571

Vega Velasco, W. (2008). POLITICAS Y SEGURIDAD DE LA INFORMACION. *Fides et Ratio - Revista de Difusión Cultural y Científica de La Universidad La Salle En Bolivia*, *2*(2), 63–69. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008&lng=es&nrm=iso&tlng=es