UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

"DIAGNÓSTICO Y LÍNEA BASE DE LOS ACTIVOS DE LA INFORMACIÓN E INFRAESTRUCTURA CRÍTICA PARA LA GESTIÓN DE CIBER SEGURIDAD DEL ESTADO ECUATORIANO, UTILIZANDO CSF NIST"

TRABAJO DE TITULACIÓN PREVIO

A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: EVELIN GIOMARA CRIOLLO NEIRA.

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS.

CAÑAR – ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

“DIAGNÓSTICO Y LÍNEA BASE DE LOS ACTIVOS DE LA INFORMACIÓN E INFRAESTRUCTURA CRÍTICA PARA LA GESTIÓN DE CIBER SEGURIDAD DEL ESTADO ECUATORIANO, UTILIZANDO CSF NIST”

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: EVELIN GIOMARA CRIOLLO NEIRA

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS.

CAÑAR - ECUADOR

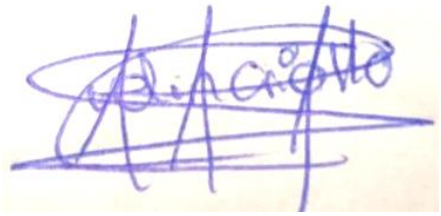
2023

DIOS, PATRIA, CULTURA Y DESARROLLO

Declaratoria de Autoría y Responsabilidad

Yo Evelin Giomara Criollo Neira portador (a) de la cédula de ciudadanía N$^{O.}$ 0302420815. Declaro ser el autor de la obra: "**DIAGNÓSTICO Y LÍNEA BASE DE LOS ACTIVOS DE LA INFORMACIÓN E INFRAESTRUCTURA CRÍTICA PARA LA GESTIÓN DE CIBER SEGURIDAD DEL ESTADO ECUATORIANO, UTILIZANDO CSF NIST**" sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 03 de octubre de 2023



F:.....

Evelin Giomara Criollo Neira

C.I. 0302420815

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por la Est. Evelin Giomara Criollo Neira, bajo mi supervisión.

Ing. Cristhian Humberto Flores Urgilés

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA

DEDICATORIA

Dedico mi trabajo de titulación a mi padre que estaré agradecida eternamente por todo su apoyo.

A mis hijas quienes fueron mi inspiración y motor de mi vida a seguir adelante creciendo como profesional.

A mi esposo William, por ser parte importante en el logro de mis metas profesionales, el cual me brindo su apoyo, cariño y me acompaño en estos años motivándome a ser una mejor persona.

AGRADECIMIENTO

En primer lugar, agradezco a Dios, por darme salud para permitirme llegar a este momento de mi formación como profesional. A mi padre, quién fue el pilar más importante poniéndose no solo en el papel de padre sino también de madre, a pesar de la distancia física, por demostrarme su constante apoyo en las buenas y en las malas. A mis abuelos Carlos y Balvina, a mis Suegros José y Mercedes. A mi tía y amiga Ana quienes me apoyaron de manera incondicional y me dieron todo su cariño.

De igual manera agradezco a Carlos y Jessica, quienes fueron mis compañeros de estudio, gracias por su amistad sin ustedes no.

Mis agradecimientos a la universidad católica y a los docentes de la carrera de ingeniería en Sistemas. En especial, al Ing. Cristhian Flores Urgilés, Mgs, director de mi trabajo de titulación, por sus consejos, por sus palabras sabias y por compartir sus conocimientos. Gracias por su orientación y sobre todo por su paciencia.

RESUMEN

El presente estudio brinda un panorama integral del estado actual de la ciberseguridad en el país, identificando claramente sus fortalezas, debilidades y áreas de mejora. Provee una línea base valiosa para futuras evaluaciones y para informar el desarrollo de estrategias en este ámbito. Para lo que se llevó a cabo los siguientes objetivos: a) Realizar un diagnóstico y establecer una línea base de los activos de información e infraestructura crítica de ciberseguridad del Estado ecuatoriano, b) Realizar el levantamiento de información de los activos de información e infraestructura crítica de ciberseguridad del Ecuador, c) Realizar una evaluación exhaustiva de la situación actual de los activos de información y las infraestructuras críticas identificadas.

Utilizando el marco NIST CSF bajo sus fases (identificar, proteger, detectar, responder y recuperar), utilizando además un enfoque cualitativo a través de una revisión de literatura para establecer el contexto y la situación actual, así se ha clasificado la infraestructura crítica de Ecuador en 7 sectores: agua, electricidad, salud, militar, telecomunicaciones, petróleo y gas. Evaluando también la madurez de ciberseguridad de Ecuador aplicando el modelo CMM, ubicándolo mayormente en las etapas iniciales de "formativo" y "puesto en marcha".

***Palabras Clave**:* infraestructuras críticas, línea base, activos de información, ciberseguridad.

ABSTRACT

This study provides a comprehensive overview of the current state of cybersecurity in the country, clearly identifying its strengths, weaknesses, and areas for improvement. It offers a valuable baseline for future evaluations and for informing the development of strategies in this area. To this end, the following objectives were achieved: a) Conduct a diagnosis and establish a baseline of Ecuador's state cybersecurity information assets and critical infrastructure, b) Collect information on Ecuador's critical cybersecurity information assets and infrastructure, c) Conduct a thorough assessment of the current situation of identified information assets and critical infrastructures. A qualitative approach has been used through a literature review to establish the context and current situation. Ecuador's critical infrastructure has been classified into 7 sectors: water, electricity, health, military, telecommunications, oil, and gas. The study also evaluates Ecuador's cybersecurity maturity using the CMM model, mainly placing it in the initial stages of "formative" and "implemented.

Keywords: critical infrastructures, baseline, information assets, cybersecurity-

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Diagnóstico y línea base de los activos de la información e infraestructura crítica para la gestión de Ciber seguridad del estado ecuatoriano, utilizando CSF NIST

Diagnosis and baseline of information assets and critical infrastructure for cybersecurity management of the Ecuadorian state, using CSF NIST

Evelin Giomara Criollo Neira [1]

Estudiante, Universidad Católica de Cuenca, Ecuador

evelin.criollo@est.ucacue.edu.ec

Cristhian Humberto Flores Urgilés [2]

chflores@ucacue.edu.ec

Cristina Mariuxi Flores Urgilés [3]

cmfloresu@ucacue.edu.ec

Julio Jhovany Santacruz Espinoza [4]

jsantacruze@ucacue.edu.ec

Mario Bernabé Ron Egas [5]

mbron@espe.edu.ec

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

INTRODUCCIÓN

La creciente dependencia de la tecnología de la información y las comunicaciones ha hecho que la ciberseguridad se convierta en un componente crítico para los estados, organizaciones y ciudadanos en el mundo. Esta importancia es particularmente relevante cuando se trata de la seguridad de la información y la infraestructura crítica de un país (Coello Ochoa, 2021).

El estado ecuatoriano, al igual que muchos otros, ha experimentado una creciente digitalización de sus servicios y operaciones, lo que ha llevado a una necesidad imperante de garantizar la seguridad y protección de sus activos de información y su infraestructura crítica (Servigón, 2021). Sin embargo, el establecimiento de un programa de ciberseguridad efectivo requiere primero un entendimiento claro de la situación actual: los riesgos, las vulnerabilidades, las fortalezas y las debilidades que caracterizan el panorama actual de la ciberseguridad en Ecuador. Dentro de este contexto, este estudio realiza una investigación con la finalidad proporcionar una visión clara y objetiva del estado actual de la ciberseguridad en Ecuador, y establecer un marco de referencia a partir del cual se puedan tomar decisiones informadas para mejorar la protección de los activos de información y la infraestructura críticas.

Las preguntas que abordan en esta investigación son: ¿Cuál es el estado actual del Ecuador ante la ciberseguridad? ¿Qué infraestructuras críticas digitales y activos de información posee el país? ¿Cuáles son las mejores prácticas para asegurar los activos de información del Ecuador? ¿Cómo puede el estado ecuatoriano mejorar su postura de ciberseguridad?

MARCO TEÓRICO

Ciberseguridad

La ciberseguridad hace referencia a la protección de sistemas, redes, información y dispositivos informáticos ante ataques, intrusiones y mal uso de estos. Tiene como objetivo principal el avalar la seguridad de la información, manejada en entornos digitales protegiendo los recursos informáticos (García, 2019) (Sarker, y otros, 2020).

Ciberataque

De acuerdo con Crawford (2019), un ciberataque es un ataque malintencionado realizado por un individuo o un grupo de personas a través de medios electrónicos con el objetivo de dañar, robar o manipular información y sistemas informáticos. Los ciberataques pueden ser realizados con diversas finalidades, como el robo de información confidencial, la extorsión, el espionaje, el sabotaje, la interrupción de servicios o la manipulación de datos.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Los ciberataques pueden ser llevados a cabo por individuos, grupos o gobiernos. Los ciberataques pueden tener un impacto significativo en las víctimas, desde el robo de datos hasta la interrupción de los servicios críticos (J & M, 2020)

Infraestructura Crítica

El Centro de Ciberseguridad Industrial (2020), determina que las infraestructura crítica se refieren a los sistemas, redes, activos y servicios físicos y de información cuyo funcionamiento ininterrumpido es esencial para garantizar la seguridad, la economía, la salud o el bienestar social de una nación.

Ciberseguridad en el estado ecuatoriano

Ecuador ha estado trabajando en mejorar su ciberseguridad en los últimos años. En 2021, el gobierno aprobó una ley sobre seguridad digital, ciberseguridad, ciberdefensa y ciber inteligencia. La ley creó un nuevo Subsistema de Ciberseguridad, que es responsable de proteger la infraestructura digital crítica y los servicios esenciales del país. El Subsistema está integrado por la Policía Nacional, el Ministerio de Gobierno y el Ministerio de Telecomunicaciones (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

De acuerdo con el Ministerio de Telecomunicaciones y de la Sociedad de la Información (2022), el gobierno también ha estado trabajando para mejorar la educación en seguridad cibernética en el país. En 2022, el gobierno lanzó una Estrategia Nacional de Ciberseguridad, que incluye un plan para capacitar a más personas en habilidades de ciberseguridad El gobierno también está trabajando para promover la cooperación entre los sectores público y privado en temas de ciberseguridad (Acosta, 2022).

Activos de la información del estado ecuatoriano

El Estado ecuatoriano cuenta con una amplia gama de activos de información, entre ellos:

- Datos gubernamentales: Esto incluye datos sobre ciudadanos, empresas y operaciones gubernamentales. Se utiliza para una variedad de propósitos, como brindar servicios sociales, hacer cumplir las leyes y administrar la economía.
- Datos de infraestructura crítica: esto incluye datos sobre infraestructura crítica, como redes eléctricas, sistemas de agua y redes de transporte. Se utiliza para monitorear y controlar estos sistemas y para responder a las interrupciones.
- Propiedad intelectual: esto incluye patentes, marcas registradas y derechos de autor. Se utiliza para proteger la economía ecuatoriana y fomentar la innovación.
- Datos personales: Esto incluye datos sobre individuos, como sus nombres, direcciones y números de Seguro Social. Se utiliza para una variedad de propósitos, como la prestación de servicios gubernamentales, la comercialización de productos y la realización de investigaciones (García & Moreta, 2019) (Secaira, Ocampo, Mera, & Kovalenko, 2020).

Infraestructura crítica del Ecuador

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

El Ecuador no cuenta con un documento que permita determinar con exactitud el número de infraestructuras críticas con las que cuenta el país. Sin embargo varios documentos como el realizado por Santos (2022), mencionan que las IC están conformadas por:

- Telecomunicaciones
- Sector Eléctrico
- Transporte
- Salud
- Sector Militar
- Agua
- Petróleo y Gas

Marco Legal y regulatorio

El gobierno de Ecuador ha tomado medidas para mejorar la ciberseguridad, que incluyen:

COIP: El Código Orgánico Integral Penal del Ecuador (COIP) contiene una serie de disposiciones que se relacionan con la protección de la infraestructura crítica y los activos de información. Estas disposiciones se encuentran en el Título IV, Capítulo II, Sección 3 del COIP, que trata de los delitos contra la seguridad pública (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2021).

Ley de Protección de Datos Personales: Esta ley protege la privacidad de los datos personales en el Ecuador (ASAMBLEA NACIONAL, 2021)

Ley de Protección de la Propiedad Intelectual: Esta ley protege los derechos de propiedad intelectual en el Ecuador. (COMISION DE LEGISLACION Y CODIFICACION, 2014)

Estrategia nacional de ciberseguridad: documento que describe la estrategia del gobierno para proteger la infraestructura crítica y los activos de información del país de las amenazas cibernéticas, compuesta por seis pilares tales como:

> Pilar 1. Gobernanza y coordinación nacional: La ENC establece un marco para la coordinación nacional de los esfuerzos de ciberseguridad. Esto incluye la creación de un Consejo Nacional de Ciberseguridad, que será responsable de supervisar la implementación de la ENC.
>
> Pilar 2. Resiliencia cibernética: Tiene como objetivo mejorar la resiliencia cibernética de la infraestructura crítica y los activos de información de Ecuador. Esto incluye medidas como mejorar la conciencia de seguridad, implementar controles de seguridad y realizar evaluaciones de riesgo periódicas
>
> Pilar 3. Prevención y combate a la ciberdelincuencia: Tiene como objetivo fortalecer la capacidad del gobierno para combatir el ciberdelito. Esto incluye medidas como mejorar la cooperación en materia de aplicación de la ley, desarrollar nuevas leyes contra el ciberdelito y aumentar la conciencia pública sobre el ciberdelito.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Pilar 4. Ciberdefensa: tiene como objetivo fortalecer la capacidad del gobierno para defenderse contra los ataques cibernéticos y recopilar inteligencia cibernética. Esto incluye medidas como el desarrollo de un plan nacional de ciberdefensa, el establecimiento de un centro nacional de ciberinteligencia y la mejora de la cooperación con socios internacionales.

Pilar 5. Habilidades y capacidad de ciberseguridad: La ENC tiene como fin mejorar las habilidades y capacidades en ciberseguridad de los ecuatorianos. Esto incluye medidas como el desarrollo de un programa nacional de capacitación en seguridad cibernética, la provisión de incentivos financieros para los profesionales de la seguridad cibernética y el fomento del desarrollo de la investigación y el desarrollo de la seguridad cibernética.

Pilar 6. Cooperación Internacional: Se enfoca en fortalecer la cooperación de Ecuador con socios internacionales en temas de ciberseguridad. Esto incluye medidas como participar en iniciativas internacionales de ciberseguridad, compartir información con socios internacionales y trabajar para desarrollar estándares internacionales de ciberseguridad (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).

Política Nacional de Ciberseguridad de Ecuador: El Ministerio de Telecomunicaciones y de la Sociedad de la Información (2021). La política define la ciberseguridad como la capacidad del Estado para proteger a las personas, sus activos de información y servicios esenciales contra los riesgos y peligros que se identifiquen en el ciberespacio (pág. 9). Describiendo una serie de medidas que se tomarán para implementar estos ejes estratégicos, incluida la creación de un Consejo Nacional de Ciberseguridad, el desarrollo de una estrategia nacional de ciberseguridad y la provisión de capacitación y recursos para ayudar a los ecuatorianos a mejorar sus habilidades en ciberseguridad.

Estudios previos

Dado el notable aumento de la importancia de la ciberseguridad en diversas naciones, incluyendo Ecuador, múltiples investigadores han contribuido a la literatura con estudios que enriquecen el entendimiento de la ciberseguridad en contextos de países en desarrollo.

Es el caso de Ron et al. (2019), quienes se encargan de explorar el estado actual de la ciberseguridad en Ecuador y propone un modelo para mejorar la postura de ciberseguridad del país. El documento se basa en un análisis comparativo de las métricas e indicadores de ciberseguridad de países con altos niveles de ciberseguridad. El documento concluye que Ecuador tiene una oportunidad significativa para mejorar su postura de seguridad cibernética y recomienda una serie de pasos que el gobierno puede tomar para hacerlo.

El documento se divide en cuatro secciones. La primera sección ofrece una visión general del estado actual de la ciberseguridad en Ecuador. La segunda sección proporciona un análisis comparativo de las métricas e indicadores de ciberseguridad de países con altos niveles de ciberseguridad. La tercera sección propone un modelo para mejorar la postura de ciberseguridad de Ecuador. La cuarta sección analiza las implicaciones de los hallazgos del documento para el gobierno de Ecuador y sus ciudadanos.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Así mismo, un documento realizado por Calcaterra (2022), brinda una visión general del estado actual de la ciberseguridad en Uruguay y analiza la situación del país. esfuerzos para adherirse al Convenio de Budapest sobre Ciberdelincuencia. El informe encuentra que Uruguay ha logrado un progreso significativo en la mejora de su postura de seguridad cibernética en los últimos años. El país ha promulgado una serie de leyes y reglamentos para abordar la seguridad cibernética y ha establecido una serie de instituciones para coordinar e implementar políticas de seguridad cibernética. Sin embargo, el informe también encuentra que Uruguay enfrenta una serie de desafíos para mejorar su postura de seguridad cibernética.

Semante & Recalde (2023), analizan los diferentes roles que el estado puede desempeñar en la defensa del ciberespacio. Argumentando que el estado tiene la responsabilidad de proteger a sus ciudadanos de las ciber amenazas, y que puede hacerlo desarrollando una estrategia nacional integral de ciberseguridad, invirtiendo en investigación y desarrollo de ciberseguridad y trabajando con el sector privado para desarrollar e implementar soluciones de ciberseguridad efectivas. El artículo concluye discutiendo los desafíos y oportunidades asociados con el papel del Estado en la defensa del ciberespacio. Argumenta que el estado enfrenta una serie de desafíos, incluida la necesidad de equilibrar la seguridad con la privacidad, la necesidad de seguir el ritmo de la naturaleza en rápida evolución del ciberespacio y la necesidad de trabajar con otros países para abordar las amenazas globales a la ciberseguridad.

METODOLOGÍA

El presente estudio emplea el marco NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) como guía metodológica para llevar a cabo el diagnóstico y establecer la línea base de ciberseguridad del Ecuador**.**

El NIST CSF proporciona una estructura organizada en torno a cinco funciones centrales: Identificar, Proteger, Detectar, Responder y Recuperar. Cada una de estas funciones involucra una serie de categorías y subcategorías que contemplan los diferentes aspectos de un programa de ciberseguridad.

En este estudio, el proceso metodológico sigue los siguientes pasos alineados a las funciones del NIST CSF:

- Identificar: Levantamiento de los activos de información críticos y la infraestructura crítica del país, que requieren protección frente a amenazas cibernéticas.
- Proteger: Análisis de las políticas, estrategias y controles actuales orientados a proteger los activos identificados previamente.
- Detectar: Revisión de las capacidades de detección de incidentes y monitoreo de amenazas cibernéticas.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

- Responder: Evaluación de los procesos y protocolos existentes para responder y contener incidentes de seguridad.
- Recuperar: Identificación de las capacidades de recuperación y restauración frente a incidentes de ciberseguridad.

Adicionalmente, el estudio emplea un enfoque cualitativo a través de una revisión de literatura para establecer el contexto y la situación actual de la ciberseguridad en el país. Los resultados del diagnóstico se analizan en base al modelo de madurez CMM.

RESULTADOS

El presente apartado expone los hallazgos del diagnóstico realizado para establecer la línea base de ciberseguridad en Ecuador, siguiendo la metodología planteada en base al marco NIST CSF. Este marco guía el proceso a través de sus funciones centrales: Identificar, Proteger, Detectar, Responder y Recuperar.

Inicialmente, se presenta información contextual sobre la situación de la ciberseguridad en el país y la importancia de realizar este estudio. Posteriormente, en la fase Identificar se lleva a cabo un levantamiento de los principales activos de información y la infraestructura crítica que requiere protección frente a amenazas.

Información contextual

La ciberseguridad es de suma importancia para el Ecuador, dado que el país está experimentando una creciente digitalización en su sociedad. Por lo tanto, resulta esencial establecer una línea base de ciberseguridad específica para el Ecuador, con el fin de brindar a las organizaciones una orientación sobre cómo salvaguardar sus sistemas, redes y datos de las amenazas cibernéticas.

En el año 2022, el gobierno ecuatoriano promulgó su primera Estrategia Nacional de Ciberseguridad, la cual se enfoca en proteger las infraestructuras críticas, la información personal y los servicios gubernamentales de la nación. Conformada por seis ejes:

1. *Gobernanza y coordinación nacional*
2. *Resiliencia cibernética*
3. *Prevención y lucha contra la cibercriminalidad*
4. *Ciberdefensa nacional*
5. *Habilidades y capacidades de ciberseguridad*
6. *Cooperación internacional*

De acuerdo con la Unión Internacional de Telecomunicaciones (UIT, 2022), en cuanto al ranking mundial sobe el desarrollo del Gobierno Electrónico, Ecuador se encuentra en la posición 84 de 193 países con el índice EGDI. Mientras que en el año 2020 ocupada el puesto 74, lo que significa que el país ya sea por la pandemia COVID-19 o por falta de inversión ha disminuido la infraestructura digital del gobierno y servicios públicos en línea.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

El siguiente gráfico demuestra el índice de servicios en línea, en donde se identifica que en el año 2020, existian mayor número de servicios mientras que en el 2022 estos han disminuido, también se puede observar que existe una diferencia de valores en el índice de infraestructura de telecomunicaciones, y el índice de capitla humano.

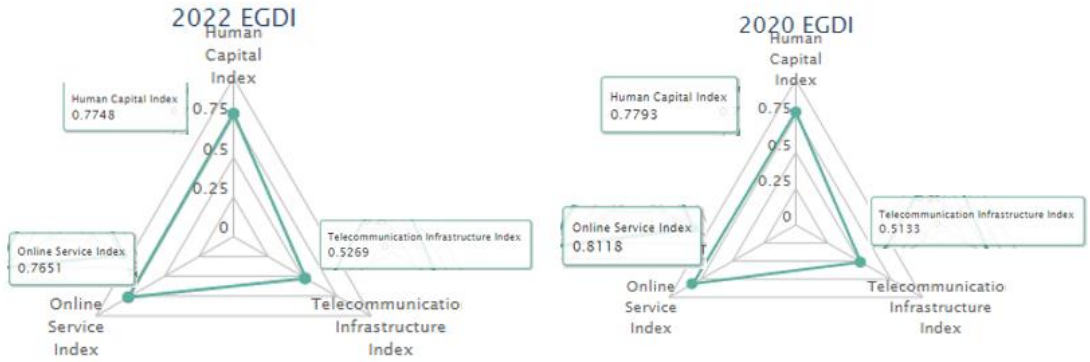


Ilustración 1. Comparativa del índice de EGDI del año 2022 y el año 2020. Fuente: (UN E-Government Knowledgebase, 2022)

1. *Identificar*:

Identificación de activos de información e infraestructura crítica

La identificación de activos de información e infraestructura crítica del Ecuador es un proceso fundamental para garantizar la seguridad y la resiliencia de la nación. Este proceso implica identificar todos los activos de información y de infraestructura que son críticos para el funcionamiento del país, en donde de acuerdo a la estrategia nacional de ciberseguridad del Ecuador, la infraestructura crítica incluye los siguientes sectores:

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

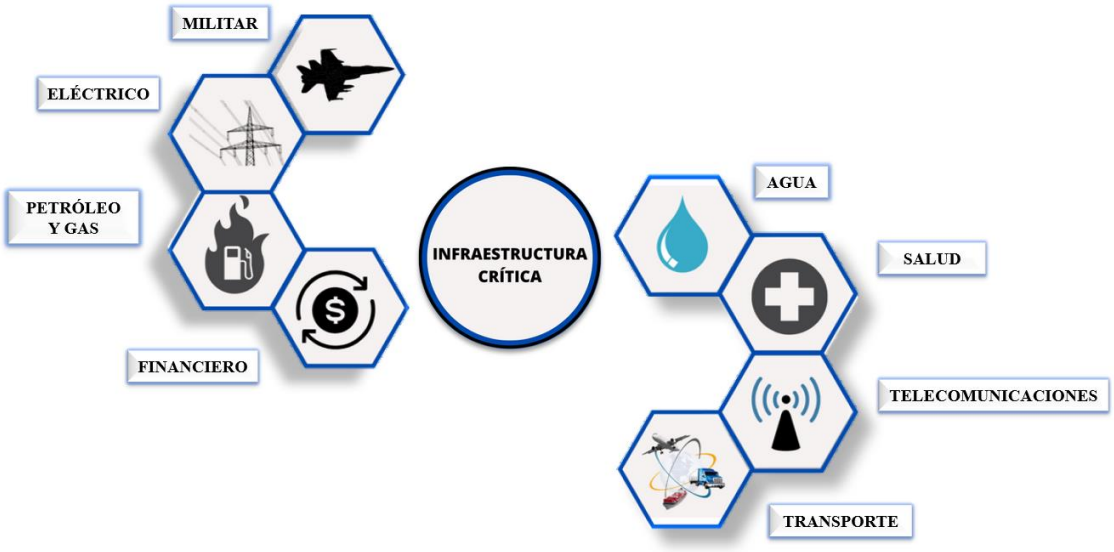


Ilustración 2. IC del Ecuador. Fuente: Autoría Propia.

Analizada la estrategia nacional de ciberseguridad se clasifica a las infraestructuras en:

- *Infraestructuras críticas:* Agua, Servicio eléctrico, salud, militar, telecomunicaciones, petróleo y gas.
- *Infraestructura estratégica:* Instalaciones, redes, sistemas y equipos físicos y de tecnología de la información.

2. ***Proteger.*** **-** Analiza las políticas, estrategias y controles actuales para la protección de activos en el Ecuador.

Políticas y estrategias de ciberseguridad

El Ecuador ha desarrollado una serie de políticas y estrategias de ciberseguridad en los últimos años. Estas políticas y estrategias están diseñadas para proteger los sistemas informáticos, las redes y los datos del país de las amenazas cibernéticas.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Centro de Operaciones de Seguridad (GSoC): es un centro de operaciones de seguridad cibernética que fue creado por el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) en 2016. El GSoC tiene como objetivo coordinar las actividades de ciberseguridad del gobierno ecuatoriano y proporcionar asistencia a las entidades públicas en la prevención y respuesta a incidentes de ciberseguridad.

Estrategia Nacional de Ciberseguridad del Ecuador: es un documento que establece el marco de políticas y acciones para la protección de la seguridad cibernética del país. Fue publicada en 2022 y tiene un alcance de 5 años.

Política nacional de Ciberseguridad: Desarrollado por el Ministerio de Telecomunicaciones y de la Sociedad de la Información, es un documento que establece el marco legal, técnico y organizacional para la protección de la infraestructura crítica y los datos del país de las amenazas cibernéticas. Además promueve la cooperación entre el gobierno, empresas y la sociedad para la protección deg la ciberseguridad del país. Esta política, menciona 6 pilares tales como:

Tabla 1. Pilares y responsabilidades de la política Nacional de Ciberseguridad del Ecuador. Fuente: (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, pág. 40)

PILAR		***INSTITUCIÓN RESPONSABLE***
I.	Gobernanza de la ciberseguridad	Ministerio de Telecomunicaciones (MINTEL)
II.	Sistemas de información y gestión de incidentes	Ministerio de Telecomunicaciones (MINTEL)
III.	Protección de la infraestructura crítica digital y servicios esenciales	Ministerio de Defensa Nacional (MDN)
IV.	Soberanía y defensa	
V.	Seguridad pública y ciudadana	Ministerio de Gobierno (MDG)
VI.	Diplomacia en el ciberespacio y cooperación internacional	Ministerio de relaciones Exteriores (MREMH)
VII.	Cultura y educación de la ciberseguridad	Ministerio de Telecomunicaciones (MINTEL)

Además establece un análisis de riesgos y amenazas cibernéticas para las infraestructuras críticas, para lo que se requiere tomar en cuenta los pilares mencionados anteriormente.

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

3. ***Detectar.*** – Explora las capacidades de detección y monitoreo de incidentes

Marco de gobernanza y coordinación

El marco de gobernanza y coordinación de ciberseguridad en el Ecuador está en constante evolución para garantizar que sea efectivo para proteger los sistemas informáticos, las redes y los datos del país de las amenazas cibernéticas.

Entidades responsables

- ***Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL)****:* Es un ministerio del gobierno ecuatoriano que se encarga de desarrollar, regular y promover las telecomunicaciones y la sociedad de la información en el país.
- ***Fuerzas Armadas del Ecuador (FAE):*** Son responsables de la defensa nacional y de la ciberdefensa. Las FAE trabajan en coordinación con el MINTEL para proteger los sistemas de información críticos de Ecuador de los ataques cibernéticos.
- ***Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL****):* Es una entidad gubernamental ecuatoriana que tiene como objetivo regular y controlar las actividades de las empresas de telecomunicaciones en el país. Tiene las siguientes la función de regular y controlar las actividades de las empresas de telecomunicaciones en el país, además de proteger los derechos de los usuarios y promover la competencia en el mercado de las telecomunicaciones.

CSIRT del Ecuador

- *EcuCERT:* Es un tipo de CSIRT a nivel nacional, que forma parte de ARCOTEL, está conformado por un equipo de profesionales especializados en seguridad informática disponible las 24 horas del día, 7 días a la semana para responder incidentes de seguridad informática que afectan a los operadores de telecomunicaciones en el Ecuador.
- *COCIBER:* CSIRT a nivel militar, que se encarga de proteger la infraestructura crítica del país de las amenazas cibernéticas. COCIBER

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

fue creada en 2017 y forma parte de las Fuerzas Armadas del Ecuador. Tiene una serie de responsabilidades tales como:

- Seguimiento y detección de ciber amenazas.
- Respuesta a incidentes cibernéticos.
- Capacitación y sensibilización en ciberseguridad.
- Cooperar con socios internacionales para combatir las amenazas cibernéticas.

4. ***Responder.*** **–** Evalúa los procesos para responder y contener incidentes de seguridad.

Capacidades de ciberseguridad

Cultura de ciberseguridad y concienciación

Educación. El Ministerio de Educación del Ecuador ha tomado medidas para mejorar la ciberseguridad, por ejemplo, creando un programa de educación sobre ciberseguridad y lanzando una campaña nacional de concienciación. Sin embargo, todavía se necesitan más esfuerzos para educar a los estudiantes sobre los riesgos cibernéticos y para ayudarlos a desarrollar hábitos seguros.

Se ha creado además proyectos institucionales como *Child Fund-Ecuador, Ministerio de Educación – Ecuador*, que brindan contenido para niños, niñas, adolescentes y adultos sobre el Internet y la ciberseguridad. Contenidos que se pueden encontrar en el siguiente enlace:

https://internetsegura.gob.ec/?page_id=971

No obstante, es necesario mencionar que las escuelas tanto públicas como fiscales no cuentan con una malla curricular que contenga la asignatura de Computación desde el año 2015, lo cual afecta a los niños; por otro lado, la educación pública tiene falta de infraestructura en lo que se incluye las computadoras, lo que limita a loe estudiantes a tener una mayor flexibilidad de pensamiento, ya que la computadora estimula la búsqueda de soluciones de un determinado problema.

Desarrollo de la capacidad. En el ámbito de la seguridad de la información, las organizaciones ecuatorianas disponen de un número limitado de equipos especializados en este campo. Según el Índice Mundial de Ciberseguridad (ICG), Ecuador ocupó la posición 119 a nivel global y 19 a nivel regional en el año 2020, mientras que en el presente año Ecuador se encuentra en el sexto puesto de 19 países de América Latina

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

(Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2023). Este índice identifica que las áreas con potencial de crecimiento dentro del país se encuentran en los aspectos organizativos y cooperativos (ITU, 2022).

Marco regulatorio y legal

El Código Orgánico Integral Penal (COIP), establece una serie de delitos informáticos, proporciona penas para estos delitos y establece una serie de medidas de seguridad que las empresas y los ciudadanos deben adoptar para proteger sus sistemas informáticos de los ciberataques. El COIP es un instrumento importante para la ciberseguridad en el Ecuador. Sin embargo, es importante que el código se actualice para abordar los desafíos cibernéticos más recientes.

Desde el año 2019 los delitos informáticos en el Ecuador fueron 10279, mientras que en el 2020 han disminuido a 5048, de acuerdo con la fiscalía general del Estado, los delitos más frecuentes son la intercepción ilegal de los datos, suplantación de identidad, falsificación, acceso no autorizado, contacto con finalidad sexual, apropiación fraudulenta, ataque a la integridad de los sistemas informáticos.

Ley orgánica de protección de datos personales: Esta ley fue promulgada el 26 de mayo de 2021 y entró en vigencia el 1 de julio de 2021, tiene como objetivo proteger los datos personales de las personas naturales, garantizar sus derechos y libertades fundamentales y regular el tratamiento de datos personales realizado por personas naturales o jurídicas, públicas o privadas, domiciliadas o instaladas en el territorio ecuatoriano.

Ley orgánica de seguridad digital. Tiene como objetivo establecer un sistema de seguridad digital que permita proteger la soberanía, seguridad integral, las infraestructuras críticas públicas y privadas, la integridad política, la seguridad económica y la seguridad nacional del Ecuador, así como salvaguardar los sistemas de información digital de los organismos estratégicos, operacionales y tácticos ante ataques, riesgos o amenazas en el ciberespacio.

5. ***Recuperar.*** – Esta fase permite evaluar los procesos de recuperación y restauración. Mediante la aplicación de un modelo de madurez de ciberseguridad para países se analiza el Ecuador en materia de ciberseguridad con el objetivo de

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

activar planes de recuperación con el fin de fortalecer la infraestructura y protocolos de seguridad.

Aplicación del modelo de madurez de ciberseguridad CMM

Tomando en cuenta al Modelo de Madurez de Capacidad de Ciberseguridad para Naciones CMM; se analiza al país de acuerdo a una escala de madurez que consta de 5 aspectos a tomar en cuenta (Puesta en marcha, formativo, establecido, estratégico, dinámico) esto para el año 2020.

Tabla 2. Análisis del estado actual del Ecuador en base a indicadores del modelo CMM. Fuente: (OEA; BID, 2020)

Subdimensión	**Puesta en marcha**	**Formativo**	**Establecido**	**Estratégico**	**Dinámico**
Estrategia Nacional de Seguridad			X		
Respuesta a incidentes			X		
Protección de infraestructuras críticas		X			
Gestión de Crisis	X				
Consideración de ciberdefensa		X			
Redundancia de comunicaciones	X				
Mentalidad de ciberseguridad		X			
Confianza en Internet		X			
Comprensión del usuario sobre la protección de la información personal en línea	X				
Medios y Redes Sociales	X				
Sensibilización		X			
Marco para la educación		X			
Marco para la Formación Profesional	X				
Marcos Legales				X	
Sistema de justicia penal		X			
Cumplimiento de las normas			X		
Resiliencia de la infraestructura de Internet			X		
Calidad del software	X				
Controles técnicos de seguridad		X			
Controles criptográficos		X			
Mercado de ciberseguridad	X				
Divulgación responsable	X				

En base a la tabla, se puede observar que Ecuador se encuentra principalmente en las etapas iniciales de "formativo" y "puesto en marcha" en la mayoría de subdimensiones analizadas. Por ejemplo, el país está en la fase de puesta en marcha en áreas como protección de infraestructura crítica, calidad del software, controles técnicos de seguridad

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

y mercado de ciberseguridad. Asimismo, está en la etapa formativa en cuanto a respuesta a incidentes, consideración de la ciberdefensa, mentalidad de ciberseguridad, confianza en internet, concientización y desarrollo de capacidades. Solamente alcanza la fase de "establecido" en estrategia nacional de ciberseguridad y cumplimiento de normas.

El análisis evidencia que, si bien existen ciertos avances, el país aún tiene un camino importante por recorrer para alcanzar una postura sólida en materia de ciberseguridad. Se requiere trabajar para transitar de las etapas iniciales y alcanzar los estadios superiores de madurez.

DISCUSIÓN

A partir de la información presentada en distintos escenarios, se infiere que Ecuador ha emprendido acciones iniciales alentadoras en la formulación de políticas, estrategias y organismos relacionados con la ciberseguridad. No obstante, aún es preciso un desarrollo significativo para llegar a un estado de preparación avanzado. Una deficiencia notoria radica en la formación y sensibilización. Es imprescindible intensificar esfuerzos educativos orientados tanto al sector estudiantil como a la población en su totalidad para inculcar una mentalidad de ciberseguridad, a través de campañas informativas y contenidos académicos en competencias digitales. En cuanto al fortalecimiento de competencias en ciberseguridad, Ecuador muestra ciertas restricciones, subrayando la necesidad de una inversión robusta para capacitar expertos capaces de resguardar los sistemas esenciales del país. La colaboración entre sectores público y privado aún se encuentra en una etapa temprana; es vital incentivar la sinergia entre entidades gubernamentales, el ámbito académico y el sector empresarial para promover soluciones holísticas en ciberseguridad. Es esencial mantener una revisión constante del marco jurídico sobre crímenes cibernéticos para abordar amenazas emergentes y complejas. Una legislación precisa es fundamental para proceder adecuadamente contra tales infracciones. La investigación orientada a las amenazas y debilidades específicas del contexto ecuatoriano se vuelve crucial, ya que guiaría estrategias y permitiría una asignación eficiente de recursos. Para sintetizar, Ecuador, a pesar de sus avances, aún tiene desafíos significativos en ciberseguridad. Es esencial monitorear la ejecución de los

e-ISSN: 2588-1000
Pro Sciences
Revista de Producción, Ciencias e Investigación

proyectos vigentes, analizando su impacto, y sumar estrategias adicionales para superar las deficiencias detectadas.

CONCLUSIONES

El presente artículo establece una línea base integral de la situación actual de la ciberseguridad en el país, que habilita el monitoreo de progreso y orienta la toma informada de decisiones para mejorar la preparación de Ecuador ante amenazas cibernéticas. En donde se establece que el país ha dado pasos iniciales positivos para mejorar su ciberseguridad, como la creación de la Estrategia Nacional de Ciberseguridad y política pública. Sin embargo, el país aún se encuentra en una etapa temprana de preparación.

Por ello, se ultima que Ecuador enfrenta el reto de implementar efectivamente las iniciativas existentes y complementarlas con nuevas acciones estratégicas para cerrar las brechas en ciberseguridad.

Es clave dar seguimiento y evaluar continuamente la efectividad de las medidas adoptadas, para promover mejoras constantes en la preparación ante las amenazas cibernéticas.

Basado en lo anterior, el estado ecuatoriano puede mejorar su postura de ciberseguridad formando a los funcionarios públicos y a los ciudadanos en materia de ciberseguridad con la finalidad de que puedan identificar y evitar los ataques cibernéticos. Considerando la creación de un marco regulatorio para la ciberseguridad que obligue a las empresas a adoptar medidas de seguridad adecuadas, además de cooperar con otros países para compartir información sobre las amenazas cibernéticas y coordinar las respuestas a los incidentes de ciberseguridad.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Referencias

Santos Vidal , M. D. (01 de 01 de 2022). *repositorio.uasb.edu.ec.* Obtenido de repositorio.uasb.edu.ec: https://repositorio.uasb.edu.ec/bitstream/10644/9076/1/T3975-MRI-Santos-Marco.pdf

Semanate Esquivel , A., & Recalde, L. L. (2023). EL ESTADO Y LA DEFENSA DEL CIBERESPACIO. *Revista Academia de Guerra del Ejército Ecuatoriano*, 99-109.

Acosta, L. P. (09 de 09 de 2022). *repositorio.iaen.edu.ec.* Obtenido de repositorio.iaen.edu.ec: https://repositorio.iaen.edu.ec/bitstream/handle/24000/6103/Tesis-Lauro%20Pozo.pdf?sequence=1&isAllowed=y

ASAMBLEA NACIONAL. (26 de 05 de 2021). *www.finanzaspopulares.gob.ec.* Obtenido de www.finanzaspopulares.gob.ec: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Centro de Ciberseguridad Industrial. (01 de 01 de 2020). *www.cci-es.org.* Obtenido de www.cci-es.org: https://www.cci-es.org/activities/documento-la-proteccion-de-infraestructuras-criticas-y-la-ciberseguridad-industrial/

CÓDIGO ORGÁNICO INTEGRAL PENAL. (17 de 02 de 2021). *www.defensa.gob.ec.* Obtenido de www.defensa.gob.ec: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Coello Ochoa, I. N. (01 de 07 de 2021). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/20738/1/UPS-GT003334.pdf

COMISION DE LEGISLACION Y CODIFICACION. (10 de 02 de 2014). *www.gobiernoelectronico.gob.ec.* Obtenido de www.gobiernoelectronico.gob.ec: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/10/Ley-de-Propiedad-Intelectual.pdf

Crawford, J. C. (2019). CIBERATAQUE AL TRANSPORTE MARÍTIMO. ¿UNA AMENZA REAL O CIENCIA FICCIÓN? *Revista de Marina*, 15-23.

Dufour, V. C. (01 de 01 de 2022). *www.colibri.udelar.edu.uy.* Obtenido de www.colibri.udelar.edu.uy: https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/37183/1/TCPPas_CalcaterraVictoria.pdf

García, A. A. (2019). *Ciberseguridad: ¿Por qué es importante para todos?* México: siglo ventinuno.

García, F. Y., & Moreta, L. M. (2019). Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras. *Revista Ibérica de Sistemas de Tecnologias de Información*, 1-17.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

ITU. (23 de 03 de 2022). *www.itu.int.* Obtenido de www.itu.int: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf

J, J., & M, C. (2020). Ciberataques. *Tecnología y equidad social*, 67-74.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (19 de 05 de 2021). *telecomunicaciones.gob.ec.* Obtenido de telecomunicaciones.gob.ec: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-Anexo-Politica-de-Ciberseguridad..pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (01 de 01 de 2021). *www.telecomunicaciones.gob.ec.* Obtenido de www.telecomunicaciones.gob.ec: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (22 de 08 de 2022). *asobanca.org.ec.* Obtenido de asobanca.org.ec: https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2 de 05 de 2023). *www.telecomunicaciones.gob.ec*. Obtenido de www.telecomunicaciones.gob.ec: https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/#:~:text=%2D%20Seg%C3%BAn%20el%20%C3%8Dndice%20Global%20de,19%20pa%C3%ADses%20de%20Am%C3%A9rica%20Latina.

OEA; BID. (01 de 01 de 2020). *CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE.*

Ron, M. B., Rivera, O., Fuertes, W., Díaz, J., & Toulkeridis, T. (2019). Cybersecurity Baseline, An Exploration, Which Permits to Delineate National Cybersecurity Strategy in Ecuador: Helping Teachers Develop Research Informed Practice. *Springer*, 848-857.

Sarker, q. H., Kayes, A. S., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, 1-29.

Secaira, J. M., Ocampo, R. D., Mera, E. Z., & Kovalenko, I. E. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). *revista científico - educacional de la provincia Granma.*, 546-559.

Servigón, C. E. (2021). Desafíos del comercio electrónico para las PYMES ecuatorianas. *Espíritu Emprendedor TES*, 19-39.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

UIT. (28 de 09 de 2022). *publicadministration.un.org*. Obtenido de publicadministration.un.org: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/52-Ecuador/dataYear/2022

UN E-Government Knowledgebase. (28 de 09 de 2022). *publicadministration.un.org*. Obtenido de publicadministration.un.org: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/52-Ecuador

ANEXOS

1.25 Anexo 1: Protocolo de Tesis

A. TÍTULO
Diagnóstico y establecer una línea base de los activos de la información e infraestructura de la ciberseguridad del Estado Ecuatoriano, utilizando CSF NIST.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Energía eléctrica y tecnologías de información para la innovación y el desarrollo sostenible	**Ciencia de los ordenadores, Analítica de datos y Algoritmos computacionales**	Analítica de Datos	
		Ingeniería de Software	
		Algoritmos computacionales	
		Inteligencias de negocios	
		Gobierno de TI	
		Auditoria y Seguridad informática	X
		Simulación	

C. PLANTEAMIENTO DEL PROBLEMA
Actualmente los países y las entidades públicas y privadas han sufrido varias amenazas cibernéticas las cuales han afectado directamente un activo sumamente importante como es la información. Siendo así el caso de Ecuador, en el que un ataque cibernético, afectó datos de miles de ecuatorianos, es por ello que el presente estudio tiene como fin evaluar los diferentes marcos de trabajo internacionalmente reconocidos buscando uno que mejor se adapte de mejor manera al estado ecuatoriano para medir la ciberseguridad del país.

En base a que no se ha aplicado un marco de trabajo en el Ecuador, las entidades públicas proponen estrategias no son altamente factibles para proteger la información, por lo cual es necesario proponer analizar los activos críticos y proponer un marco que ayude a mejorar mecanismos, estrategias, controles y que ayude a mejorar la ciberseguridad el país.

D. OBJETIVO GENERAL
Realizar un diagnóstico y establecer una línea base de los activos de información e infraestructura crítica de ciberseguridad del Estado ecuatoriano, utilizando CSF NIST

E. OBJETIVOS ESPECÍFICOS
1. Realizar una investigación teórica sobre los activos de información y la infraestructura crítica.
2. Determinar un protocolo para levantamiento de los activos de información e infraestructura crítica de ciberseguridad del Ecuador.
3. Realizar el levantamiento de información de los activos de información e infraestructura crítica de ciberseguridad del Ecuador.

F. JUSTIFICACIÓN

Actualmente, Ecuador ha sido víctima de ataques informáticos que ponen en peligro los datos más importantes, ya que muchas entidades, tanto públicas como privadas, carecen de una seguridad confiable.

Esta investigación tiene como objetivo analizar los marcos de trabajo internacionales reconocidos para evaluar su adecuación al estado ecuatoriano, buscando el que mejor se adapte para medir la ciberseguridad del país.

G. ALCANCE

El alcance de esta actual investigación, consiste en que el parámetro permita construir un diagnóstico del estado de la ciberseguridad en el estado ecuatoriano, basado en información que se obtendrá en páginas web gubernamentales.

H. CONCEPTOS RELACIONADOS

Ciberseguridad

La ciberseguridad hace referencia a la protección de sistemas, redes, información y dispositivos informáticos ante ataques, intrusiones y mal uso de estos. Tiene como objetivo principal el avalar la seguridad de la información, manejada en entornos digitales protegiendo los recursos informáticos (García, 2019)

Marco de trabajo

Un marco de trabajo, posee mecanismos tanto físicos como lógicos, que puedan ser reutilizados para diseñar y desarrollar nuevos sistemas o proyectos.

NIST Cybersecurity Framework

El marco NIST CSF, ofrece orientación a las organizaciones independientemente de su tamaño, con el fin de que estas puedan comprender, administrar, reducir y comunicar de mejor manera los riesgos cibernéticos. Siendo además un "recurso fundamental y esencial utilizado por todos los sectores en todo el mundo" (U.S. DEPARTMENT OF COMMERCE, 2023)

CMM

Este modelo ayuda a los países a comprender qué funciona, qué no funciona y por qué, en todas las áreas de la capacidad de seguridad cibernética. Esto es importante para que los gobiernos y las empresas puedan adoptar políticas y realizar inversiones que tengan el potencial de mejorar significativamente la seguridad y la protección en el ciberespacio (Global Cyber Security Capacity Centre, 2021).

ISO 27001

La norma ISO 27001, está orientada de manera específica a los SGSI. Define de qué manera se deben implementar operar, mantener y mejorar continuamente controles de seguridad de la información (NQA-ISO-27001, 2019).

COBIT

Modelo de madurez

Es un mapa que guía a una determinada organización independientemente de su tamaño, medir el estado actual de esta en un ámbito delimitado, permitiendo así el autoanálisis y la definición de la madurez a alcanzar. Brindando oportunidades de mejora y de optimización de procesos interrelacionados (Enrique & Necochea Mendoza, 2022)

Ciberataque

De acuerdo con Crawford (2019), un ciberataque es un ataque malintencionado realizado por un individuo o un grupo de personas a través de medios electrónicos con el objetivo de

dañar, robar o manipular información y sistemas informáticos. Los ciberataques pueden ser realizados con diversas finalidades, como el robo de información confidencial, la extorsión, el espionaje, el sabotaje, la interrupción de servicios o la manipulación de datos.

I. TRABAJOS RELACIONADOS

Roxana (Cedeño Villacís, 2022) manifiesta que la tecnología ha evolucionado y las herramientas informáticas son utilizadas por los ecuatorianos en la vida diaria, en entidades públicas y privadas, esto da una atención a los ciberdelincuentes, los cuales buscan la forma de cometer delitos ingresando a los sistemas. Analiza la ciberseguridad en el Ecuador, determinando diferentes tipos de ataques informáticos como el caso de Julián Assange. Establece tambien, un marco legal ante estos ciber ataques.

Pastrano en el año (2019), en su trabajo de titulación, realiza una investigación de la situación del Ecuador referente a la ciberseguridad, a través de una metodología práctica denominada japonesa Tankyu, aplicando sus fases. Utilizando además el método PCM para determinar la problemática del Ecuador ante la ciberseguridad. Concluye que se requiere realizar una articulación de varias instituciones públicas y privadas del país, construyendo un documento de línea base que permitiría establecer la estrategia política nacional del área. El autor establece que el país carece de directrices que puedan fortalecer la gestión de riesgo en una determinada área.
Et Al (Ron , Rivera, & Fuertes) menciona realiza un estudio de campo se basa en la selección de un diagrama de afinidad que define los principales actores de la elaboración de la política, de acuerdo al impacto de la organización, pertinencia, capacidad, etc., con los cuales se elaboró un plan estratégico evaluando criterios que se convierten en objetivos de investigación. Se presenta una descripción la situación del estado ecuatoriano, mediante un proceso metodológico que ha permitido seleccionar el criterio más utilizado a nivel mundial.

J. METODOLOGÍA

El presente trabajo manejará una investigación descriptiva en la cual se analizará los niveles de madurez y la ciberseguridad en el estado de Ecuador, indagando el marco de trabajo que mejor se adapte, para obtener un diagnóstico de la situación, a través de las páginas web gubernamentales.

K. CRONOGRAMA DE ACTIVIDADES																	
N°	ACTIVIDAD	MES I				MES II				MES III				MES IV				MES V	
		S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3		MEDIOS DE VERIFICACIÓN	
1	Realizar una investigación teórica sobre los activos de información e infraestructura crítica																		
1.1	Bases teóricas y trabajos relacionados. Estado del arte.	x	x	x	x	x												Lista de documentos almacenados en la herramienta Mendeley	
2	Determinar un protocolo para el levantamiento de los activos de información e infraestructura critica de ciberseguridad del Ecuador.																		
2.2	Determinar un protocolo para el levantamiento de los activos de información						x	x	x	x	x							. Información de páginas gubernamentales y artículos.	
3	Realizar un protocolo para el levantamiento de los activos de información e infraestructura crítica de la ciberseguridad del ecuador																		
3.1	Realizar un protocolo para el levantamiento de los activos de información e infraestructura crítica de la ciberseguridad del ecuador											x	x	x	x	x			

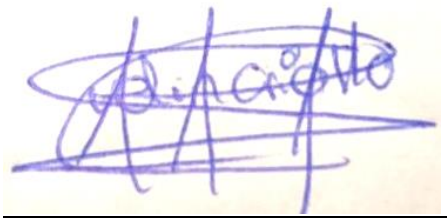
L. DECLARACIÓN FINAL
Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES	
DIRECTOR:	ING. Cristhian Humberto Flores Urgilés
ESTUDIANTE 1	Evelin Giomara Criollo Neira

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	
Fecha:	

Firmas:

Nombre: ING. CRISTHIAN FLORES
CC:
Director del Proyecto



Nombre: Evelin Giomara Criollo Neira
C.C.: 0998009192
Estudiante / Egresado

P. REFERENCIAS

Referencias

(s.f.).

Cedeño Villacís, R. p. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la. *Revista Tecnológica eiencia y educación Eduars Deming*, 50-62.

Crawford, J. C. (2019). CIBERATAQUE AL TRANSPORTE MARÍTIMO. ¿UNA AMENZA REAL O CIENCIA FICCIÓN? *Revista de Marina*, 15-23.

García, A. A. (2019). *Ciberseguridad: ¿Por qué es importante para todos?* México: siglo ventinuno.

Global Cyber Security Capacity Centre. (01 de 01 de 2021). *gcscc.ox.ac.uk.* Obtenido de gcscc.ox.ac.uk: https://gcscc.ox.ac.uk/cmm-2021-edition

NQA-ISO-27001. (11 de 10 de 2019). *www.nqa.com.* Obtenido de www.nqa.com: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Pastrano, L. O. (01 de 01 de 2019). *repositorio.espe.edu.ec.* Obtenido de repositorio.espe.edu.ec: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/21189/T-ESPE-038971.pdf?sequence=1&isAllowed=y

Rivera Pastrano, L. O. (14 de 06 de 2019). *repositorio.espe.edu.ec.* Obtenido de repositorio.espe.edu.ec: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/21189/T-ESPE-038971.pdf?sequence=1&isAllowed=y

Ron , M., Rivera, O., & Fuertes, W. (s.f.). Cybersecurity Baseline: An Exploration, wich permits to delineate National Cibersecurity Strategy in Ecuador.

U.S. DEPARTMENT OF COMMERCE. (19 de 01 de 2023). *www.nist.gov.* Obtenido de www.nist.gov: https://www.nist.gov/cyberframework

Cañar, 03 de octubre 2023

Asunto: Embargo Temporal del Trabajo de Titulación

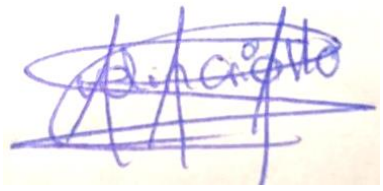
Señor,
Ing. Leopoldo Pauta Ayabaca
DECANO DE LA UNIDAD ACADÉMICA DE ADMINISTRACIÓN DE INFROMATICA, CIENCIAS DE LACOMPUTACION, E ENOVACCION TECNOLÓGICA
Cuenca.

De mi consideración:

Señor Decano, EVELIN GIOMARA CRIOLLO NEIRA, como autora del Trabajo de Titulación "DIAGNÓSTICO Y LÍNEA BASE DE LOS ACTIVOS DE INFORMACIÓN E INFRAESTRUCTURA CRÍTICA PARA LA GESTIÓN DE CIBER SEGURIDAD DEL ESTADO ECUATORIANO, UTILIZANDO CSF NIST" y CRISTHIAN HUMBERTO FLORES URGILÉS, MSC como director de la misma, solicitamos a usted y por su digno intermedio a Biblioteca y al responsable del repositorio institucional, el EMBARGO TEMPORAL del mismo, por un lapso de 6 meses, con la finalidad de evaluar su contenido con fines de: evaluación de artículo científico para publicación en revista indexada. Entiendo que luego de vencido este período automáticamente la obra será puesta a disposición del público bajo las normas de gestión de la Universidad.

Por la atención que sepa dar al presente, nos suscribimos de usted muy agradecidos.

Atentamente,



_____
Evelin Giomara Criollo Neira
CI: 0302420815
Autor

C.C.: Biblioteca.