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 INGENIERIA EN SISTEMAS DE INFORMACIÓN

“MODELO DE MADUREZ DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRITICAS CASO DE ESTUDIO: ECUADOR”

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: CARLOS PATRICIO LOPEZ LOJA

DIRECTOR: ING. JOSE ANTONIO CARRRILLO ZENTENO.

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

“MODELO DE MADUREZ DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRITICAS CASO DE ESTUDIO: ECUADOR”

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: CARLOS PATRICIO LOPEZ LOJA

DIRECTOR: ING. JOSE ANTONIO CARRRILLO ZENTENO.

CAÑAR - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

AGRADECIMENTO

En primer lugar, quiero expresar mi agradecimiento al Ser Supremo por concederme la sabiduría y el discernimiento necesarios para lograr un nuevo logro en mi vida. También quiero dar las gracias a mis padres, abuelos y familiares, quienes han sido una fuente constante de orientación, experiencia y amor en mi camino.

Mi profundo agradecimiento se extiende a los educadores que han desempeñado el papel de guías y mentores en mi vida. Su contribución a mi desarrollo académico y personal es inestimable.

El desarrollo de este artículo científico no fue precisamente sencilla, pero lo que puedo afirmar con certeza es que a lo largo de este proceso, pude encontrar satisfacción en cada momento. Cada investigación, proceso y proyecto que formaron parte de esta experiencia fue disfrutado al máximo, y esto no se debió únicamente a mi propia disposición, sino también al constante apoyo de mis amigos. La vida misma me enseñó que las acciones que emprendo serán reciprocadas, y esto se reflejó en cada paso que di..

DEDICATORIA

Este articulo se la dedico a mi querido Dios que me gia desde el cielo para triunfar como un buen hombre que soy atravez de su fuerza de voluntad que me ha hecho seguir adelante en los desafios que se me presentaban, enseñandome a encarar las adversidades sin perder nunca la dignidad ni caerme en el intento.

Quiero dedicar este pequeño trabajo a mi familia en especial a mis padres Ambrosio, Griselda como tambien a mis abuelos Fulgencia, Manuel y a mis tios Mercy, Jose quienes por haberme forjado como la persona que soy en la actualidad, muchos de mis logros se los debos a ustedes entre los que se incluye este. Me formaron con reglas y con algunas libertades, pero al final de cuentas a sido motivaciones para alcanzar mis metas.

Declaratoria de Autoría y Responsabilidad

Carlos Patricio López Loja portador(a) de la cédula de ciudadanía N° **030301685-1.** Declaro ser el autor de la obra: **"MODELO DE MADUREZ DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRÍTICAS CASO DE ESTUDIO: ECUADOR",** 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.

Cuenca, **30 de junio de 2023**

Carlos Patricio López Loja

C.I. **0303016851**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Est. Carlos Patricio López Loja, bajo mi supervisión.

Ing. José Antonio Carrillo Zenteno

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATOLICA DE CUENCA.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Modelo de madurez de ciberseguridad para infraestructuras críticas caso de estudio: Ecuador

Cybersecurity Maturity Model for Critical Infrastructures Case Study: Ecuador

Carlos Patricio López [1]

Estudiante, Universidad Católica de Cuenca, Ecuador

patricio.lopez@est.ucacue.edu.ec

José Antonio Carrillo[2]

Docente, Universidad Católica de Cuenca, Ecuador

jacarrilloz@ucacue.edu.ec

Cristhian Flores Urgilés[3]

chfloresu@ucacue.edu.ec

Diana Ormaza Vintimilla [4]

daormazav@yahoo.com

ORCID 0000-0002-4159-0882

[1] Título de pregrado, título de posgrados (si lo tiene)
[2] Título de pregrado, título de posgrados (si lo tiene)

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

RESUMEN

En la era digital, la infraestructura crítica, sistemas financieros e incluso la seguridad nacional se encuentran en riesgo de ataques cibernéticos, por lo que los países deben adoptar un enfoque integral que ayude a protegerse de la creciente amenaza de estos. Por ello, presente estudio propone un modelo de madurez de ciberseguridad enfocado en infraestructuras críticas para el estado ecuatoriano denominado ECU-C2M2, basado en el modelo Cybersecurity Capability Maturity Model (C2M2). Los objetivos planteados para realizar la presente investigación fueron: a) Realizar un estudio teórico sobre los diferentes modelos de madurez para las Infraestructuras Críticas, b) Realizar un levantamiento de Información en base a la información existente de las páginas gubernamentales, c) Proponer un modelo de madurez de ciberseguridad para Infraestructuras Críticas.

Para la creación del modelo, se realizó un análisis comparativo de los modelos de madurez de ciberseguridad existentes, así mismo se cotejó sus dominios y subdominios. El estudio presenta también un análisis de la ciberseguridad en el Ecuador, con la finalidad de que el modelo propuesto se encuentre alineado a las necesidades del país y permita la colaboración y la cooperación entre diferentes entidades, tanto gubernamentales como del sector privado.

Palabras Clave: ECU-C2M2, ciberseguridad, infraestructuras críticas.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

ABSTRACT

In the digital age, critical infrastructure, financial systems, and even national security are at risk from cyberattacks, so countries must adopt a comprehensive approach to protect themselves from the growing threat of these. Therefore, this study proposes a cybersecurity maturity model focused on critical infrastructures for the Ecuadorian state called ECU-C2M2, based on the Cybersecurity Capability Maturity Model (C2M2). The objectives set to carry out this research were: a) Carry out a theoretical study on the different maturity models for Critical Infrastructures, b) Carry out an information survey based on the existing information from government pages, c) Propose a cybersecurity maturity model for Critical Infrastructures.

For the creation of the model, a comparative analysis of existing cybersecurity maturity models was carried out, as well as checking their domains and subdomains. The study also presents an analysis of cybersecurity in Ecuador, with the aim that the proposed model is aligned with the country's needs and allows collaboration and cooperation between different entities, both governmental and private sector.

KEYWORDS: ***ECU-C2M2, cybersecurity, critical infrastructures.***

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

INTRODUCCIÓN

Actualmente, países y organizaciones a nivel mundial, han adoptado la tecnología modificando la forma en la que se administra un país y sus infraestructuras críticas. Automatizando procesos de los entes gubernamentales, lo que ha convertido a los gobiernos en blancos más atractivos para los ciber atacantes (Gamboa Suárez, 2020). Es así que, la hiperconectividad ha servido como una herramienta de crecimiento, para todo tipo de organización, sin embargo, ha facilitado el acceso a personas criminales con conocimientos en la informática (Lominchar Jiménez & Zunzarren Denis, 2022). Representando así una amenaza para las naciones a nivel internacional, en sectores públicos y privados. Es por ello, que las naciones deben definir una visión de seguridad cibernética, así como también, implementar un modelo de madurez de ciberseguridad que brinde mejora continua, ya que últimamente los ataques a infraestructuras críticas se han vuelto preocupantes, debido a que los atacantes buscan generar ganancias financieras o lo hacen por desmejorar la credibilidad de los gobiernos (Peña, 2022).

Debido a los ataques cibernéticos realizados directamente a los gobiernos, el Ecuador ha tratado de proteger sus activos cibernéticos mediante estrategias nacionales de Ciberseguridad, como políticas y objetivos estratégicos (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022). No obstante, se requiere de una estrategia aún más eficaz, puesto que los ataques más frecuentes realizados en los últimos años a las infraestructuras críticas, han sido directamente al sector eléctrico y las telecomunicaciones (Mullane, 2019). Es por ello, que se propone un Modelo de Madurez de Ciberseguridad para Infraestructuras Críticas analizando el nivel de madurez de Ciberseguridad con la que cuenta el país.

Marco Teórico

Modelo de capacidad de madurez

Global Cyber Security Capacity Centre (2021) define que el modelo de Capacidad de Madurez (CMM), está compuesto por cinco dimensiones, permitiendo a países y organizaciones de todo tamaño entender la ciberseguridad y el grado de implementación o madurez de los procesos

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

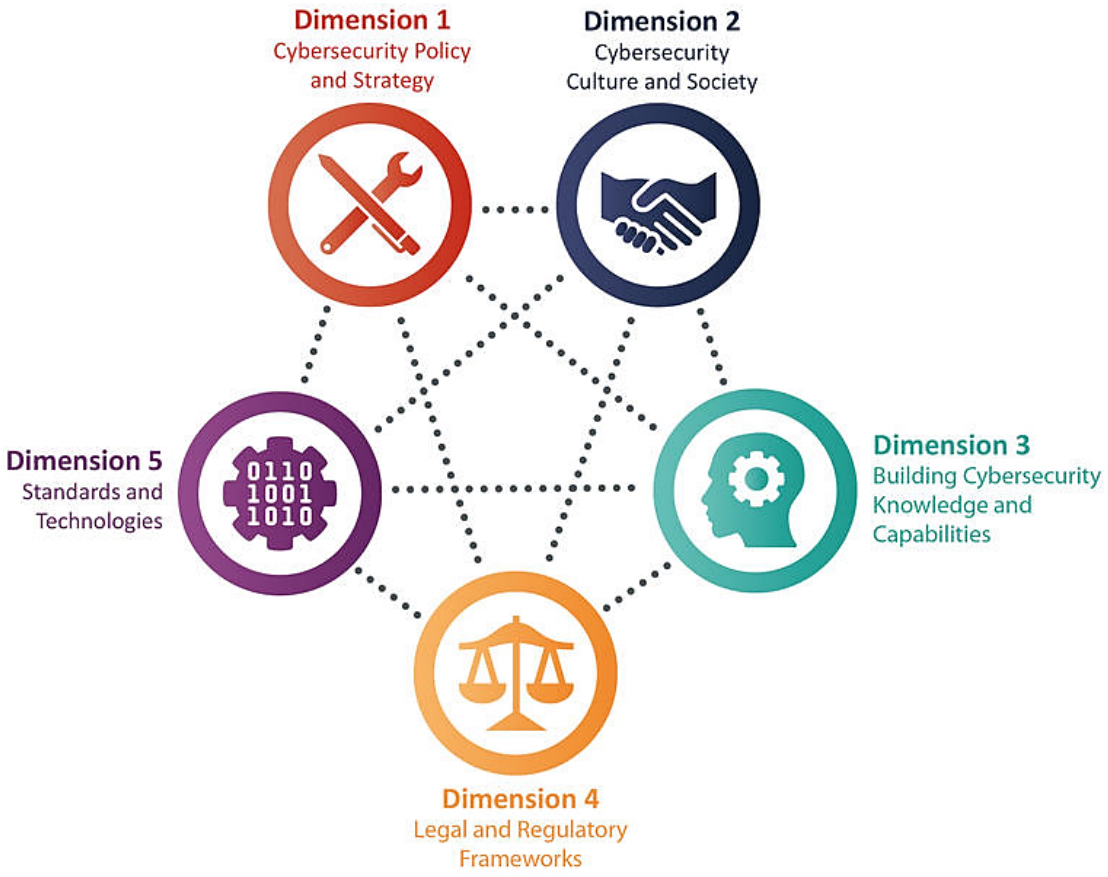


Ilustración 1. Dimensiones del modelo CMM. Fuente: (Global Cyber Security Capacity Centre, 2021)

La dimensión 1 denominada *Política y estrategia de ciberseguridad*, permite la capacidad de seguridad cibernética nacional a través de políticas efectivas y estrategias para mejorar la respuesta a incidentes (Global Cyber Security Capacity Centre, 2021, pág. 6)

De acuerdo con (Global Cyber Security Capacity Centre, 2021), la dimensión 2 *Ciberseguridad Cultura y Sociedad* "permite la comprensión de los riesgos relacionados con la cibernética en la sociedad, el nivel de confianza en los servicios de Internet, el gobierno electrónico y los servicios de comercio electrónico y la protección de la información personal en línea" (pág. 19)

La dimensión 3: Construyendo Ciberseguridad Conocimiento y capacidades permite determinar programas de ciberseguridad para concientizar a las partes interesadas. Por otro lado, la dimensión 4 Marcos Legal y Regulatorios, "examina los requisitos normativos de la seguridad cibernética y la legislación establecida en una nación para combatir el ciberdelito" (Global Cyber Security Capacity Centre, 2021, pág. 38)

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Por último, la dimensión 5 Estándares y Tecnologías, analiza el uso de la tecnología de ciberseguridad y los estándares y buenas prácticas utilizadas para proteger a los ciudadanos, a los entes gubernamentales y a las infraestructuras críticas nacionales (Global Cyber Security Capacity Centre, 2021).

De esta manera las dimensiones mencionadas anteriormente permiten analizar la estructura para evaluar y mejorar la madurez de una organización en la creación del modelo de madurez de ciberseguridad de infraestructuras críticas para el Ecuador.

Modelo de madurez de la capacidad de ciberseguridad (C2M2)

El modelo de madurez de la capacidad de ciberseguridad (C2M2), engloba una orientación con la finalidad de mejorar la alineación con los estándares cibernéticos. "Orientado a la protección de las infraestructuras críticas, cambiando enfoques de la estrategia, con prácticas de identificación, análisis y respuesta al riesgo con una categorización y priorización. El modelo permite que un país u organización, mejore las prácticas de ciberseguridad a través de acciones e inversiones para mejorar la ciberseguridad" (U.S Department of ENERFY, 2021).

Entre las versiones del modelo se encuentran las siguientes:

- ***ONG-C2M2***

  "Este modelo de madurez tiene como objetivo contemplar tanto amenazas como vulnerabilidades de la infraestructura crítica *Petróleo y Gas,* a través de la investigación, recolección, producción, procesamiento, almacenamiento y transporte de petróleo, líquidos y gas natural" (Garba, Siraj, & Othman, 2020, pág. 765)

- ***ES-C2M2***

  Abdullahi (2020) comenta que **"**el objetivo de este modelo es mejorar la capacidad de la ciberseguridad en el sector eléctrico, a través de una evaluación continua que tiene cuatro funciones tales como:

  1. Generación
  2. Transmisión
  3. Distribución
  4. Mercados" (pág. 765).

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

NIST Cybersecurity Framework (CSF)

El marco NIST CSF, contiene estándares industriales para guiar a empresas y organizaciones a través de actividades y prácticas de ciberseguridad. Además, se compone de tres secciones principales:

- *Marco básico:* Son actividades de ciberseguridad, resultados y referencias comunes a los sectores de infraestructuras críticas.
- *Niveles de implementación del marco:* Permite que la organización pueda ser clasificada en un nivel predefinido basado en sus prácticas actuales de gestión de riesgo, su entorno de amenazas, los requerimientos legales y regulatorios, sus objetivos y misión empresarial, así como las restricciones propias de la empresa.
- *Perfil del marco:* Se utiliza para describir el nivel actual de seguridad cibernética y para establecer actividades que ayuden a identificar brechas en la seguridad que deben ser gestionadas para cumplir con la gestión de riesgos (Almagro, y otros, 2019)

Participa en actividades de organizaciones nacionales, industriales, entre otras que tiene como fin abordar los riesgos cibernéticos tomando en cuenta principalmente la infraestructura crítica de un país (U.S. DEPARTMENT OF COMMERCE, 2023). Cuenta además con 5 dominios como el "***identificar***, en el que se puede desarrollar un entendimiento organizacional en cuanto a los riesgos de ciberseguridad; ***proteger,*** este dominio hace mención a las medidas de ciberseguridad para garantizar la entrega de servicios de las infraestructuras críticas; ***detectar***, en el que se establece las actividades que permiten identificar la ocurrencia de un evento de ciberseguridad; ***responder***, incluyendo actividades para tomar medidas ante un evento de ciberseguridad y ***recuperar***, dominio que implica la identificación de actividades para conservar los planes de resiliencia y para restaurar algún servicio que haya sido deteriorado ante un incidente cibernético" (Almagro, y otros, 2019, págs. 5-6)

En base al estudio de los diferentes modelos de madurez de ciberseguridad para naciones, se ha considerado la importancia de realizar un análisis FODA, que permita identificar de mejor manera los factores internos como externos de cada modelo.

Es así que el análisis FODA para el modelo de madurez de ciberseguridad para naciones (CMM), permite identificar los factores externos que pueden causar daño en la nación y también los que pueden causar un resultado exitoso, así como sus debilidades que le imposibilitarían lograr un nivel óptimo.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Table 1. Matriz FODA del modelo CMM. Fuente: Autoría Propia

Cybersecurity Capacity Maturity Model for Nations | CMM	
Fortalezas	***Oportunidades***
- Enfoque en la gestión de riesgos de ciberseguridad, en toda la organización proporciona un modelo de madurez para evaluar la efectividad de los controles de ciberseguridad y la gestión de riesgos - Ofrece una guía para la mejora continua y la evolución de los controles de seguridad	- Mejora la efectividad de los controles de ciberseguridad en la organización - Establece un marco de mejora continua para la gestión de riesgos de ciberseguridad - Obtiene una evaluación objetiva de la madurez de la organización en cuanto a la ciberseguridad
Debilidades	***Amenazas***
- Implementación puede ser compleja y requerir de recursos significativos - Puede ser difícil para las organizaciones con recursos limitados el alcanzar los niveles de madurez más altos - No se centra específicamente en la protección de datos personales	- Una implementación inadecuada podría llevar a una falsa sensación se seguridad - La falta de recursos o la complejidad podrían disuadir a las organizaciones de utilizar el marco

En la siguiente tabla el análisis FODA del modelo C2M2, se determina que se enfoca directamente en las infraestructuras críticas y este permite mejorar la capacidad de gestión de riesgos cibernéticos.

Table 2. Matriz FODA modelo C2M2. Fuente: Autoría Propia.

Cybersecurity Capability Maturity Model | C2M2	
Fortalezas	***Oportunidades***
- Enfoque en la gestión de riesgos de ciberseguridad específicos de la industria y los sectores críticos de infraestructura	- Mejora la capacidad de gestión de riesgos de ciberseguridad específicos de la industria y los sectores críticos de infraestructura

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

- Ofrece un modelo de madurez y una guía de implementación para ayudar a las organizaciones a mejorar su capacidad de gestión de riesgos	- Establece un marco de mejora continua para la gestión de riesgos de ciberseguridad
Debilidades	***Amenazas***
- Puede no se aplicable a organizaciones fuera de los sectores críticos de infraestructura - Puede ser difícil para las organizaciones con recursos limitados alcanzar los niveles de madurez más altos	- Una implementación inadecuada podría llevar a una falsa sensación se seguridad - La falta de recursos o la complejidad podrían disuadir a las organizaciones de utilizar el marco

De la misma manera, el FODA del marco NIST CSF, permite concluir que se puede adaptar a organizaciones de cualquier tamaño para el análisis de la ciberseguridad, es decir desde un estado hasta una empresa pequeña.

Table 3. Matriz FODA del marco NIST CSF. Fuente: Autoría Propia.

Nist Cybersecurity Framework | NIST CSF	
Fortalezas	***Oportunidades***
- Enfoque holístico de la gestión de riesgos de ciberseguridad que incluye la identificación, protección, detección, respuesta y recuperación - Adaptable a organizaciones de cualquier tamaño y sector - Basado en prácticas y estándares reconocidos en la industria	- Mejora la capacidad de gestión de riesgos de ciberseguridad en toda la organización - Promover la colaboración entre equipos de tecnología, operaciones y negocio - Facilitar la adopción de un enfoque integrado de ciberseguridad a través de estándares aceptados
Debilidades	***Amenazas***
- Al ser un marco legal puede que algunas organizaciones requieran mayores especificaciones para su contexto	- Una implementación inadecuada podría llevar a una falsa sensación se seguridad

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

- Es posible que las organizaciones con menor nivel de madurez en gestión de riesgos de ciberseguridad tengan dificultades para su implementación	- La falta de recursos o la complejidad podrían disuadir a las organizaciones de utilizar el marco - Puede haber resistencia al cambio y a la integración entre los equipos.

Infraestructura crítica

Las infraestructuras críticas son esenciales para el funcionamiento del país y cuya interrupción o degradación podría tener un impacto significativo en la seguridad, la economía, la salud pública o el bienestar de la población. El Ecuador cuenta con las siguientes infraestructuras críticas:

1. ***Energía eléctrica***: La red de generación, transmisión y distribución de energía eléctrica es una infraestructura crítica fundamental para el funcionamiento del país.
2. ***Telecomunicaciones***: Las redes de telecomunicaciones, incluyendo la telefonía móvil, la telefonía fija, el internet y la televisión, son críticas para la comunicación y la transmisión de información en el país.
3. ***Transporte***: Las carreteras, puentes, aeropuertos, puertos y ferrocarriles son infraestructuras críticas para el transporte de personas y bienes en todo el país.
4. ***Agua potable y saneamiento***: La infraestructura para el suministro de agua potable y saneamiento es esencial para la salud pública y el bienestar de la población.
5. ***Salud***: Los hospitales, clínicas y centros de salud son infraestructuras críticas para la atención médica y la respuesta a emergencias sanitarias.
6. ***Servicios financieros***: La infraestructura para los servicios financieros, como los bancos y los sistemas de pago electrónico, son críticos para la economía del país.
7. ***Instalaciones gubernamentales***: Las instalaciones gubernamentales, como los edificios gubernamentales y los sistemas de información, son críticos para el funcionamiento del gobierno y la provisión de servicios públicos (Morillo & Duque, 2020)

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Seguridad informática

De acuerdo con Postigo (2020), la seguridad informática hace referencia a la protección de operaciones que no estén autorizadas, a través de técnicas, herramientas y medidas para proteger sistemas informáticos, así como información de daños, robo, manipulación o interrupción de los servicios que se ofrecen en el entorno digital. Para lo que es importante que cualquier organización, independientemente del tamaño, cuente con un plan de seguridad informática para controlar el entorno de TI (pág. 3).

Situación actual de la ciberseguridad en Ecuador

El Ecuador, cuenta con estrategias nacionales de ciberseguridad enfocándose en encontrar responsables de esta área con el objetivo de gestionar riesgos y mitigarlos. Contando con tecnologías de Automatización Robótica de Procesos (RPA), para optimizar costos operativos, modificando procesos y mejorando los servicios (Chávez, 2020).

De acuerdo con el Ministerio de Telecomunicaciones y de la Sociedad de la Información (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022), el Ecuador cuenta con un Plan Estratégico de Defensa Institucional, que tiene como propósito evaluar periódicamente escenarios que incluyen vulnerabilidades, amenazas y riesgos. Cuentan además con principios como:

- **Liderazgo y responsabilidad compartida**
- **Salvaguardar los derechos digitales**
- **Gestión de riesgos de ciberseguridad y resiliencia cibernética**
- **Visión inclusiva y colaborativa**

Posee además 6 pilares de gobernanza y coordinación nacional, cada uno con objetivos, siendo el más importante el pilar número 4 que tiene por objetivo “Incrementar y fortalecer las capacidades de Ciberdefensa del Estado ecuatoriano para alcanzar la actitud estratégica defensiva definida en la Política de la Defensa Nacional, para la protección de la infraestructura crítica digital (ICD) y servicios esenciales en el ciberespacio” (pág. 15).

Análisis de la estrategia nacional de ciberseguridad del Ecuador

La Estrategia Nacional de Ciberseguridad del Ecuador desarrollada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (2022), se presenta como una herramienta de apoyo en la época de la tecnología. Contando con una aplicación de 3 años desde el 2022 hasta

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

el año 2025, posee objetivos estratégicos y 6 pilares de ciberseguridad. Sin embargo, Chang (2020), considera que primeramente se debe definir el número exacto de infraestructuras críticas para realizar una adecuada estrategia de ciberseguridad. Por lo que en la revisión teórica realizada no se ha encontrado con exactitud el número de las infraestructuras críticas pertenecientes a Ecuador.

Analizado el documento antes mencionado, se ha tomado en cuenta el pilar 2 que hace referencia a la gestión de riesgos de ciberseguridad, a la protección de las infraestructuras críticas digitales y a la gestión de incidentes cibernéticos. Este pilar tiene el objetivo el adoptar un marco integral para la identificación, orientación y supervisión de las operadoras de las ICD.

Infraestructuras críticas Ecuador

De acuerdo con el Ministerio de Defensa del Ecuador, el número de infraestructuras críticas del país se encuentran en un catálogo provisional como:

- Energía Eléctrica
- Agua Potable
- Redes de Telecomunicaciones y tecnologías de la información
- Transporte aéreo, marítimo y terrestre
- Sistemas de salud y hospitales
- Instalaciones de producción y distribución de combustibles y gas
- Militar (Ministerio de Defensa Nacional, 2020)

Trabajos previos

El trabajo que se considera más favorable y que aporta de mejor manera como una guía en la presente investigación, es el artículo realizado por Dean (2019), quien crea un modelo propio para Qatar denominado ***Q-C2M2***, basado en los modelos de madurez de ciberseguridad existentes y sus dominios, además de los documentos referentes a la ciberseguridad que tiene el país. Proponiendo dominios como “comprender, asegurar, exponer, recuperar y sostener”, desarrollando de esta manera un marco de seguridad cibernética (pág. 2).

Leyva (2021) en su artículo, realiza un estudio de las políticas públicas de seguridad cibernética en el Ecuador a través de una investigación sistemática-documental, haciendo un estudio desde el año 2012, estudiando también los mecanismos que tiene el país para proteger a sus activos digitales. Sin embargo, menciona la inexistencia de “políticas públicas basadas en un modelo de

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

gobernanza en seguridad cibernética, que integre y materialice de manera efectiva los esfuerzos aislados, que a lo largo del tiempo no han supuesto una solución global al objetivo de la ciberseguridad y ciberdefensa del Ecuador" (pág. 1248).

Páez en su trabajo investigativo en el año (2022) que tiene por título "Análisis comparativo de modelos de selección y protección de infraestructuras críticas, como aporte a la Política Nacional de ciberseguridad del Ecuador", en el que analiza el marco NIST, ENISA, INCIBE, con el fin de identificar la gestión de riesgos. Utilizan el método ad-hoc, además del método analítico comparativo. Comparan el marco NIST con ENISA, analizando sus niveles de madurez, los sectores críticos del Ecuador, así como las autoridades de TI y agencias de ciberseguridad para ver qué modelo se acopla de mejor manera al Ecuador.

Así mismo Cedeño (2022), al analizar la situación actual de la ciberseguridad en el Ecuador utilizando una metodología con un enfoque cualitativo de tipo documental. Presentando los ataques cibernéticos que el Ecuador ha atravesado, desde el año 2009 hasta el 2019. Analiza también los artículos del Código Orgánico Integral Penal del país. Concluyendo que una empresa independientemente de su tamaño debe trabajar con modelos de madurez de ciberseguridad, así como desarrollar planes y acciones para mitigar vulnerabilidades de los equipos tecnológicos, implementando Firewalls y demás controles.

METODOLOGÍA

Enfoque de la investigación

Para la elaboración del presente trabajo se han tomado en cuenta variables cualitativas, mismas que permiten la recolección de información referente a la infraestructura crítica del Ecuador. Analizando el estado actual de la ciberseguridad en las infraestructuras críticas, a través de una revisión de artículos relacionados directamente al tema de investigación.

Nivel de la investigación

El presente artículo es de tipo descriptivo, ya que se analizará el estado actual de la ciberseguridad en el Ecuador, centrándose también en analizar la relación entre las prácticas actuales de ciberseguridad y su madurez.

Técnicas e instrumentos de la investigación

La recolección de la información se realizará con la técnica de observación, a través de la revisión de documentos, se analizará políticas, procedimientos y otros artículos con el fin de

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

obtener una comprensión detallada de las medidas de ciberseguridad implementadas en las infraestructuras críticas del Ecuador.

Tratamiento de la información

La información obtenida de los resultados se representará en matrices comparativas.

RESULTADOS

Analizados los diferentes modelos de madurez de ciberseguridad en las naciones, se puede realizar una comparativa de las fases de cada modelo, con la finalidad de analizar de mejor manera los elementos temáticos para la construcción del modelo de madurez de ciberseguridad de infraestructuras críticas para el Ecuador:

Tabla 1. Fases de los modelos de madurez de ciberseguridad para naciones. Fuente: Autoría Propia.

INDICADOR	CMM	C2M2	NIST CSF
Identificación de las infraestructuras críticas	X	X	X
Evaluación de la capacidad actual	X	X	X
Desarrollo del modelo	X	X	X
Validación del modelo	X	X	X
Implementación del modelo	X	X	X
Monitoreo y evaluación continua	X	X	X
Identificación y evaluación de riesgos		X	X
Desarrollo de controles y políticas	X	X	X
Implementación de controles y políticas	X	X	X
Monitoreo y mejora continua	X	X	X
Comunicación y colaboración		X	X

Como se puede observar en la tabla, los modelos comparten las primeras seis fases, que se enfocan en la identificación de las infraestructuras críticas, la evaluación de la capacidad actual,

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

el desarrollo y validación del modelo, la implementación del modelo y la monitorización y evaluación continua.

El marco NIST así como el modelo C2M2 incluyen dos fases adicionales, el marco NIST CSF se puede adaptar a varios sectores siendo un marco muy general, mientras que el Modelo de Madurez de Capacidad Cibernética ofrece una evaluación detallada de la madurez de ciberseguridad de las infraestructuras críticas, para su mejora continua.

Por ello, para el desarrollo del modelo, se utilizarán como base las fases del modelo C2M2, ya que este se enfoca directamente en las infraestructuras críticas.

Las siguientes infraestructuras críticas se han determinado en base al catálogo provisional del Ministerio de Defensa del Ecuador.

De esta manera en primera instancia se realiza la identificación de infraestructuras críticas del Ecuador en las que se encuentran:

- Energía Eléctrica
- Agua Potable
- Redes de Telecomunicaciones y tecnologías de la información
- Transporte aéreo, marítimo y terrestre
- Sistemas de salud y hospitales
- Instalaciones de producción y distribución de combustibles y gas
- Militar

Definidas las infraestructuras críticas, se ha realizado una evaluación de la madurez de estas identificando sus vulnerabilidades y amenazas, descritas en la siguiente tabla:

Tabla 2. Vulnerabilidades y amenazas de las Infraestructuras Críticas del Ecuador. Fuente: Autoría Propia.

Infraestructura Crítica	Vulnerabilidades	Amenazas
Energía	Falta de actualizaciones de seguridad y parches	Ataques de malware y ransomware
	Configuraciones inseguras de sistemas y redes	Ataques DDoS
Telecomunicaciones	Falta de cifrado en las comunicaciones	Intercepción y manipulación de datos

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

	Sistemas obsoletos y sin soporte	Ataques de fuerza bruta y robo de credenciales
	Infraestructura de red vulnerable	Sabotaje y degradación del servicio
Agua	Sistemas de control industrial (ICS) vulnerables	Contaminación de datos y manipulación de sistemas
	Falta de monitoreo y detección de amenazas	Ataques de malware y ransomware dirigidos a ICS
Salud	Dispositivos médicos conectados con vulnerabilidades	Ataques a dispositivos médicos para manipular su funcionamiento
	Sistemas de TI obsoletos y sin soporte	Robo de información personal y datos de salud
	Falta de políticas y procedimientos de seguridad	Ataques de phishing y suplantación de identidad (spoofing)
Transporte (aéreo, terrestre, marítimo)	Redes de comunicaciones inseguras entre vehículos y sistemas de control	Intercepción y manipulación de datos de comunicación entre vehículos y sistemas de control
	Falta de protección contra acceso no autorizado	Intrusión y sabotaje de sistemas críticos de transporte
Militar	Sistemas de control y comando vulnerables, sistemas obsoletos, falta de medidas de autenticación y autorización, falta de control de accesos	Ataques de denegación de servicio (DoS), ataques de manipulación de datos, intrusión y robo de información
Gas	Sistemas de control de procesos vulnerables	Ataques de denegación de servicio (DoS)
	Falta de control de accesos	Ataques de manipulación de datos

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Las amenazas y vulnerabilidades presentadas en la tabla anterior, se exhiben como una visión general que pueden afectar a las infraestructuras críticas en Ecuador. Cabe mencionar que, de acuerdo a una revisión de la literatura, estas son muy comunes y se han presentado en diversos países. Además han sido tomadas en cuenta de acuerdo a la información proporcionada por la Agencia de Regulación y Control de las Telecomunicaciones (2022) y a la norma ISO 27005.

Por consiguiente, es necesario la construcción del modelo adaptando el modelo C2M2 y sus dimensiones:

Tal y como se señaló anteriormente, se han analizado los modelos de madurez de ciberseguridad para naciones más utilizados entre los que se encuentran el modelo CMM, el C2M2 y el marco NIST CSF.

La siguiente tabla presenta los dominios de los modelos de madurez de ciberseguridad para países CMM, C2M2, el marco NIST CSF y la estrategia Nacional de Ciberseguridad del Ecuador

Tabla 3. Comparativa de los dominios de los modelos de madurez de ciberseguridad. Fuente: Autoría Propia.

NIST CSF (DOMINIOS)	NIST CSF (SUBDOMINIOS)	CMM (DOMINIOS)	C2M2 (DOMINIOS)	ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR
IDENTIFICAR	Gobernanza	Ciberseguridad Política y estrategia	Gestión del programa de ciberseguridad	Gobernanza y coordinación nacional
			Set, Cambio y gestión de Configuración	
	Gestión de activos		Gestión de riesgos	
	Evaluación de Riesgos			
PROTEGER	Estrategia de gestión de riesgos		Gestión de amenazas y vulnerabilidades	
	Control de acceso		Gestión de identidad y acceso	
			Gestión de riesgos de terceros	

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

IDENTIFICAR	Análisis	Ciberseguridad Cultura y Sociedad	Conciencia situacional	Habilidades y capacidades de ciberseguridad
PROTEGER	Mitigación			
	Monitoreo Continuo de Seguridad			
IDENTIFICAR	Ambiente de negocios	Construyendo ciberseguridad Conocimiento y capacidades	Gestión de la fuerza laboral	
	Concienciación y Formación		Respuesta a eventos e incidentes y continuidad de operaciones	
DETECTAR	Anomalías y eventos			Resiliencia cibernética (Infraestructuras Críticas Digitales)
	Procesos de detección			
RESPONDER	Planificación de la respuesta			Ciberdefensa
RECUPERAR	Planificación de recuperación			
		Legal y Marcos Regulatorios		Prevención y combate a la ciberdelincuencia
PROTEGER	Procesos y Procedimientos de Protección de la Información	Normas y Tecnologías	Arquitectura de ciberseguridad	
	Seguridad de datos			
	Tecnología de protección			
RESPONDER	Mejoras			
	Comunicaciones			
RECUPERAR	Mejoras			
	Comunicaciones			

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

La tabla anterior permite observar los dominios de los modelos de madurez de ciberseguridad y la estrategia nacional de ciberseguridad del Ecuador, en donde el análisis temático revela que la *gestión de riesgos* no se encuentra como dominio principal del modelo CMM, no obstante, este dominio se encuentra en el marco NIST CSF y en el modelo C2M2. La estrategia nacional de ciberseguridad a través de sus ejes, permite fortalecer la postura de seguridad cibernética de Ecuador, proporcionando una hoja de ruta clara que el gobierno debe seguir para proteger la infraestructura crítica y sus activos de información ante amenazas cibernéticas.

Las cinco dimensiones del modelo CMM, cubren el área de capacidad requerida por un país con el fin de mejorar la postura de seguridad cibernética, sin embargo, no se enfocan directamente en el área de la protección de las infraestructuras críticas. Por otro lado, como se puede observar en la Tabla 3 el marco NIST tiene cinco funcionales principales: identificar, detectar, proteger, responder y recuperar.

El modelo C2M2 conjuntamente con sus dimensiones permiten determinar que es un marco flexible que se adapta a las necesidades de cualquier organización.

Al comparar los dominios de los marcos existentes, se establece que la estrategia nacional de Ciberseguridad del Ecuador no es un modelo de madurez de ciberseguridad, sino un documento que tiene como objetivo principal el mejorar significativamente la postura de ciberseguridad del país.

Modelo de madurez de la capacidad de ciberseguridad de Ecuador (ECU-C2M2)

La presente investigación realizó una comparación de los dominios presentes en los modelos de madurez de ciberseguridad más prominentes a nivel mundial, así como el análisis de la Estrategia Nacional de Ciberseguridad de Ecuador. Uno de los principales objetivos del estudio es proponer un modelo de madurez denominado ECU-C2M2 que incluya un marco legislativo.

A través de este modelo de madurez, se podrán identificar las áreas en las que Ecuador necesita mejorar su nivel de ciberseguridad, lo cual permitirá establecer prioridades y dirigir los

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

esfuerzos hacia aquellas áreas que requieren atención inmediata. Además, al examinar los modelos implementados en otros países, se ha determinado que contar con un modelo de madurez de ciberseguridad sólido y efectivo enviará un mensaje claro a nivel nacional e internacional sobre el compromiso de Ecuador en la protección de sus activos digitales, infraestructuras críticas y la privacidad de sus ciudadanos. Esto contribuirá a fortalecer la confianza de inversores, socios comerciales y la población en general.

En esta sección se propone un conjunto predefinido de dominios para el modelo ECU-C2M2, el cual, al trabajar a nivel temático, ayudará a simplificar y agilizar la implementación de la Estrategia Nacional de Ciberseguridad de Ecuador. La capacidad de prueba se refiere a la posibilidad de que los usuarios prueben la innovación sin compromiso. Dado que el ECU-C2M2 no es una empresa comercial, se sugiere que entidades gubernamentales y organizaciones no gubernamentales de Ecuador puedan evaluar y probar el modelo sin asumir obligaciones. Sin embargo, si se incorpora el ECU-C2M2 como un requisito o política legislativa, se recomienda establecer un período de prueba y capacitación.

Dominios y subdominios

Basado en el modelo C2M2, se propone cinco funciones como dominios principales del modelo propuesto para Ecuador, estos son aplicables en el contexto de las infraestructuras críticas. Los dominios que se proponen a continuación pueden ser un medio para simplificar el gobierno.

Tabla 4. Dominios y Subdominios del modelo ECU-C2M2. Fuente: Autoría Propia.

DOMINIOS	SUBDOMINIOS
Gestión de riesgos de ciberseguridad de infraestructuras críticas	Gestión de riesgos de ciberseguridad de infraestructuras críticas
	Análisis de impacto
	Mitigación
Protección física de infraestructuras críticas	Control de acceso físico
	Vigilancia y monitoreo de instalaciones
	Protección contra amenazas físicas
	Gestión de identidad y acceso
Normativas y estándares de ciberseguridad	Adherencia a estándares y regulaciones
	Auditoría y cumplimiento de políticas de ciberseguridad

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

	Gestión de incidentes y reporte a autoridades competentes
Educación y concientización en infraestructuras críticas	Programas de capacitación y concientización
	Promoción de buenas prácticas de seguridad
	Sensibilización sobre amenazas y riesgos cibernéticos
Resiliencia y continuidad operativa en IC	Planificación de continuidad de negocio
	Recuperación ante desastres
	Pruebas y ejercicios de continuidad operativa

1. ***Gestión de riesgos de ciberseguridad de infraestructuras críticas***

   El dominio *Gestión de riesgos de ciberseguridad de infraestructuras críticas* incluye tres subdominios: Gestión de riesgos de ciberseguridad de infraestructuras críticas, análisis de impacto, mitigación. Estos han sido apoyados en el modelo **C2M2** existente y sus versiones ***ONG-C2M2; ES-C2M2.*** Este dominio es fundamental para entender y mitigar los riesgos garantizando la protección de las infraestructuras críticas vitales del Ecuador y minimizar el impacto de los posibles incidentes cibernéticos. Fundamentalmente, el dominio permite mejorar el enfoque de la estrategia Nacional de Ciberseguridad del Ecuador agregando la gestión de los sectores que ofrecen servicios digitales, incluyendo la gestión de protección de datos sensibles, sistemas e instalaciones.

2. ***Protección física de infraestructuras críticas***

   El dominio Protección física de Infraestructuras Críticas se centra en la implementación de controles y sistemas de seguridad que permitan prevenir y mitigar amenazas físicas, como intrusiones, sabotajes, daños intencionales o desastres naturales, que puedan comprometer el funcionamiento de las infraestructuras críticas. Su principal subdominio: control de acceso físico aborda la implementación de medidas para controlar y supervisar el acceso físico a las instalaciones de las infraestructuras críticas. Así mismo los otros dos subdominios permiten llevar a cabo de mejor manera la detección y respuesta de forma inmediata a posibles amenazas cibernéticas o físicas.

3. ***Normativas y estándares de ciberseguridad***

   Este dominio se centra en establecer y cumplir con las regulaciones, políticas y estándares específicos relacionados con la ciberseguridad. Siendo esencial para garantizar que las organizaciones y entidades en Ecuador adopten un enfoque sistemático y consistente para proteger sus activos digitales y la información sensible.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Los subdominios propuestos permitirán alinearse al marco legal del Ecuador para la protección de datos personas, seguridad de las infraestructuras críticas, el delito informático y la privacidad de la información. Este dominio incorpora un marco legal que contiene un conjunto de actividades afines al cumplimiento legal y regulatorio.

4. ***Educación y concientización en infraestructuras críticas***

   El dominio Educación y concientización en infraestructuras críticas promueve a conciencia y el conocimiento sobre la ciberseguridad entre el personal y los usuarios involucrados en la operación y mantenimiento de las infraestructuras críticas. Este dominio es esencial para fortalecer la cultura de seguridad cibernética y garantizar que todos los actores relevantes estén informados y capacitados para mitigar los riesgos cibernéticos.

5. ***Resiliencia y continuidad operativa en infraestructuras criticas***

   El dominio 5 denominado resiliencia y continuidad operativa en Infraestructuras Críticas se enfoca en la capacidad de las infraestructuras críticas para resistir, adaptarse y recuperarse de manera efectiva ante posibles incidentes cibernéticos o desastres que puedan interrumpir su funcionamiento normal. El objetivo principal es garantizar la disponibilidad continua de estas infraestructuras vitales y minimizar los impactos en caso de interrupciones. Los subdominios aseguran el funcionamiento continuo incluso en situaciones de crisis, a través de mecanismos y procesos para la recuperación rápida y eficiente de las infraestructuras críticas del Ecuador.

Con el objetivo de garantizar la implementación y seguimiento efectivo del modelo propuesto, cada área que pretenda utilizar el modelo debe definirse de acuerdo a los siguientes niveles de madurez:

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

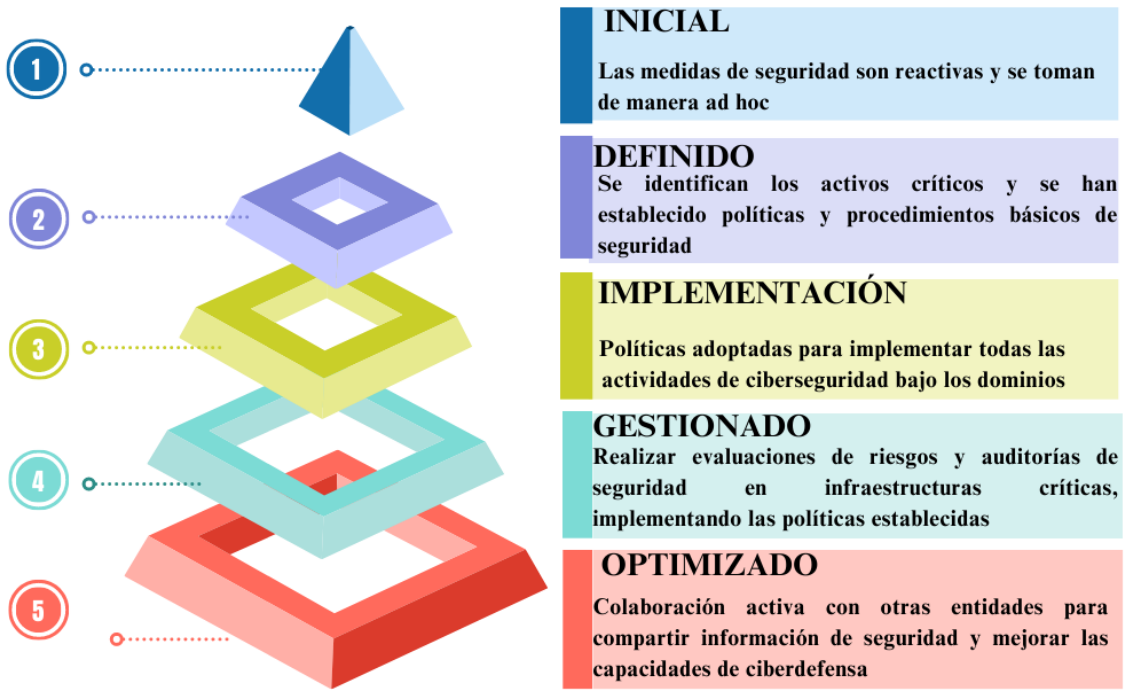


Ilustración 2. Niveles de madurez de ciberseguridad del modelo ECU-C2M2. Fuente: Autoría Propia.

Los niveles de madurez planteados son una propuesta, en la etapa de inicio, una organización al carecer de un enfoque estructurado formal de ciberseguridad para infraestructuras críticas solamente empleará prácticas y procesos de ciberseguridad ad-hoc, es decir que se hace referencia que implica medidas de seguridad de forma reactiva, en respuesta a incidentes o amenazas ya ocurridas.

El nivel 2 se establecen controles de ciberseguridad más sólidos y se documentan en políticas y procesos formales; en la etapa de implementación, se lleva a cabo la identificación documentación de activos críticos conjunto con una evaluación periódica de riesgos; la etapa 4, la organización debe realizar evaluaciones periódicas y pruebas de ciberseguridad monitoreando actividades y eventos de seguridad en infraestructuras críticas. La última etapa de optimización, permite que la organizaciones busque constantemente nuevas formas de mejorar su postura de seguridad.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Adopción del modelo de madurez

La adopción del modelo ECU-C2M2 podría ser una adición a las políticas o estándares existentes bajo la Estrategia Nacional de Ciberseguridad del Ecuador. Además de que se enfoca en fomentar la colaboración entre las entidades responsables de las infraestructuras críticas en Ecuador, así como con organismos nacionales e internacionales relacionados con la ciberseguridad; compartir experiencias, buenas prácticas y lecciones aprendidas para fortalecer el enfoque de ciberseguridad en el país.

La implementación del modelo propuesta podría lograrse sin necesidad de una nueva legislación. Apoyando en la mejora continua del estado ecuatoriano, a través de una una evaluación sistemática de la ciberseguridad en las infraestructuras críticas, lo que brinda una visión clara de la postura de seguridad actual. Esto permite identificar áreas de mejora y establecer acciones concretas para fortalecer la seguridad de manera continua.

Además, el modelo de madurez ECU-C2M2 promueve una gestión basada en riesgos, lo que significa que las inversiones y esfuerzos de ciberseguridad se enfocan en las áreas de mayor riesgo. Esto ayuda a optimizar los recursos y garantizar una protección efectiva de las infraestructuras críticas.

DISCUSIÓN

El desarrollo e implementación de un modelo de madurez de ciberseguridad específico para las infraestructuras críticas en Ecuador es de vital importancia para fortalecer la protección de los activos y sistemas que son fundamentales para el funcionamiento del país. Por ello, el modelo propuesto denominado ECU-C2M2 está enfocado directamente a la protección de las infraestructuras críticas del estado ecuatoriano, a la redundancia dandonle uso a esta nuevo modelo propuesto para asi proteger datos criticos del sistema para dar mayor seguridad que le beneficiaría a identificar brechas para proteger contra las amenzas ciberneticas y áreas para la mejora específica, y establecer un plan de acción basado en prioridades para mitigar los riesgos existentes.

El modelo brindaría una estructura y un enfoque claros para implementar y mantener las medidas de seguridad necesarias en las infraestructuras críticas. Esto ayudaría a garantizar una implementación coherente y efectiva de las prácticas de ciberseguridad, asegurando una mayor protección frente a las amenazas y ataques cibernéticos en constante evolución.

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

Sin embargo, existen desafíos asociados a la implementación de este modelo en el contexto ecuatoriano. Uno de ellos es la necesidad de adaptar el modelo a las particularidades del país, considerando aspectos como las características de las infraestructuras críticas locales, la legislación y regulación vigente, y los recursos disponibles. Es fundamental que el modelo pase por un período de prueba y capacitación a las partes interesadas, es decir en organizaciones privadas, públicas, organismos responsables de la seguridad de las infraestructuras críticas. Esto con la finalidad de que exista una implementación exitosa.

Así mismo para la implementación del modelo y sus controles es fundamental considerar con recursos adecuados, tanto financieros como humanos, implicando inversiones en tecnología, capacitación al personal y establecimiento de capacidades internas para la gestión de la ciberseguridad en las infraestructuras críticas. De esta manera, y tomando en cuenta estos aspectos el desarrollo del modelo y su implementación a futuro podrían fortalecer la ciberseguridad y proteger a los activos vitales del país.

CONCLUSIONES

En base al estudio sistemático realizado, se puede concluir que los modelos de madurez de ciberseguridad más utilizados a nivel mundial son el modelo CMM, el modelo C2M2 y el marco NIST CSF, destacando que el modelo C2M2 se enfoca directamente en las infraestructuras críticas.

Así mismo, de acuerdo a la investigación teórica de la ciberseguridad en el Ecuador, se ultima que la ciberseguridad en infraestructuras críticas en el país es una preocupación creciente, debido a que el país tiene varios sectores de infraestructura importantes, que incluyen energía, agua, transporte y telecomunicaciones. Estos sectores dependen cada vez más de las tecnologías digitales, lo que los hace vulnerables a los ciberataques.

Por ello, se propuso el modelo de madurez ECU-C2M2, determinando que este permite una evaluación sistemática de la postura de seguridad de las infraestructuras críticas en Ecuador, brindando una visión clara de las brechas y áreas de mejora, permitiendo establecer prioridades y desarrollar un plan de acción adecuado.

Se define también que la implementación exitosa del modelo requiere una estrecha colaboración entre las entidades gubernamentales, las organizaciones privadas y los organismos responsables de la seguridad de las infraestructuras críticas. La colaboración permite el intercambio de información, mejores prácticas y el desarrollo de capacidades conjuntas.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Referencias

Agencia de Regulación y Control de las Telecomunicaciones. (14 de 02 de 2022). *www.ecucert.gob.ec.* Obtenido de www.ecucert.gob.ec: https://www.ecucert.gob.ec/wp-content/uploads/2022/02/Alerta-varios-CVEs.pdf

Almagro, L., Urrutia, F. D., Treppel, A. A., Contreras, B., Paz, S., Santellán, F., . . . Subero, D. (01 de 01 de 2019). *www.oas.org.* Obtenido de www.oas.org: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Brown, R. D. (2019). Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework. *International Review of Law*, 1-36.

Chang, J. E. (2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. *Revista Científica Aristas*, 18-27.

Chávez, R. (01 de 01 de 2020). *www.itahora.com.* Obtenido de www.itahora.com: https://www.itahora.com/wp-content/uploads/2020/06/ESTADO-ACTUAL-DE-CIBERSIGURIDAD-ECUADOR-2020-1.pdf

Gamboa Suárez, J. L. (2020). IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD EN EL MUNDO ACTUAL. *Universidad Piloto de Colombia, Gamboa, Seguridad Informática y Ciberseguridad*, 1-12.

Garba, A. A., Siraj, M. M., & Othman, S. H. (2020). An Explanatory Review on Cybersecurity Capability Maturity Models. *ASTES*, 762-769.

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#:~:text=The%20CMM%202021%20Edition%20and,a%20rigorous%20analysis%20of%20data

Jahir, P. Q. (22 de 08 de 2022). *repositorio.espe.edu.ec.* Obtenido de repositorio.espe.edu.ec: https://repositorio.espe.edu.ec/bitstream/21000/23641/1/T-ESPE-044247.pdf

Lominchar Jiménez, J., & Zunzarren Denis, H. (2022). La transversalidad estratégica de la ciberinteligencia. *Revista Venezolana de Gerencia*, 258-273.

Méndez, A. E. (2021). Análisis de políticas públicas de seguridad cibernética. Estudio del caso . *Polo del Conocimiento*, 1229-1250.

Ministerio de Defensa Nacional. (02 de 10 de 2020). *www.defensa.gob.ec.* Obtenido de www.defensa.gob.ec: https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/02/plan-sectorial-final-2020-web.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (22 de 08 de 2022). *www.gobiernoelectronico.gob.ec.* Obtenido de www.gobiernoelectronico.gob.ec:

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf

Morillo, F. R., & Duque, P. R. (2020). LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS EN EL ÁMBITO DE LAS FUERZAS ARMADAS. *Revista de Ciencias de Seguridad y Defensa*, 1-22.

Mullane, M. A. (2019). Ciberataques dirigidos a infraestructuras críticas. *UNE*, 1-6.

Palacios, A. P. (2020). *Seguridad Informática (Edición 2020).* Madrid: Paraninfo.

Peña, J. E. (01 de 01 de 2022). *repository.unad.edu.co.* Obtenido de repository.unad.edu.co: https://repository.unad.edu.co/bitstream/handle/10596/53985/Jealmariop.pdf?sequence=1&isAllowed=y

U.S Department of ENERFY. (01 de 01 de 2021). *www.energy.gov.* Obtenido de www.energy.gov: https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf

U.S. DEPARTMENT OF COMMERCE. (19 de 01 de 2023). *www.nist.gov.* Obtenido de www.nist.gov: https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

Villacís, R. P. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador . *REVISTA TECNOLÓGICA ciencia y eduacación Edwards Deming*, 5162.

Universidad Católica de Cuenca

ANEXOS

Trabajo de Titulación

Tema:

Modelo de madurez de ciberseguridad para Infraestructuras críticas caso de estudio: Ecuador

Unidad Académica

Informática, Ciencias de la Computación e Innovación Tecnológica

Carrera

Ingeniería de Sistemas de la Información

Alumno

Carlos Patricio Lopez Loja

Tutor:

Ing. José Antonio Carrillo Zenteno

Octubre – Marzo 2023

A. TÍTULO
Modelo de madurez de ciberseguridad para infraestructuras críticas caso de estudio: Ecuador

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Sistemas de Información	
		Ingeniería de Software	
		Algoritmos computacionales	
		Inteligencia de negocios	
		Gobierno de Ti	
		Auditoria y seguridad informática	X
		Simulación	

C. PLANTEAMIENTO DEL PROBLEMA

Actualmente países y organizaciones a nivel mundial, han adoptado la tecnología modificando la forma en la que se administra un país y sus infraestructuras críticas. Automatizando procesos de los entes gubernamentales, lo que ha convertido a los gobiernos en blancos más atractivos para los ciber atacantes. La hiperconectividad ha servido como una herramienta de crecimiento, para todo tipo de organización, sin embargo, ha facilitado el acceso a personas criminales con conocimientos en la informática.

Representando así una amenaza para las naciones a nivel internacional, en sectores públicos y privados. Es por ello que las naciones deben definir una visión de seguridad cibernética, así como también implementar un modelo de madurez de ciberseguridad que brinde mejora continua, ya que últimamente los ataques a infraestructuras críticas se han

vuelto preocupantes debido a que los atacantes o buscan generar ganancias financieras o lo hacen por desmejorar la credibilidad de gobiernos.

D. OBJETIVO GENERAL
Proponer un modelo de madurez de la ciberseguridad para infraestructuras críticas para el Ecuador

E. OBJETIVOS ESPECÍFICOS
1. Realizar un estudio teórico sobre los diferentes modelos de madurez para las infraestructuras críticas
2. Realizar un levantamiento de información en base a la existente en páginas gubernamentales.
3. Proponer un modelo de madurez de ciberseguridad para infraestructuras críticas.

F. JUSTIFICACIÓN

Debido a los ataques cibernéticos realizados directamente a los gobiernos, el Ecuador ha tratado de proteger sus activos cibernéticos mediante estrategias nacionales de ciberseguridad, como talleres con la participación de los sectores gubernamentales. No obstante, se requiere de una estrategia aún más eficaz, puesto que los ataques más frecuentes realizados en los últimos años a las infraestructuras críticas, han sido directamente al sector eléctrico y las telecomunicaciones.

Es por ello que se propone un modelo de madurez de ciberseguridad para infraestructuras críticas analizando el nivel de madurez de ciberseguridad con la que cuenta el país.

G. ALCANCE

El alcance de la presente investigación va a permitir definir el modelo de madurez de ciberseguridad enfocado en las infraestructuras críticas, el levantamiento de información solamente se regirá a información encontrada en páginas gubernamentales, estudios previos o se contactará telefónicamente con las instituciones para obtener la información necesaria.

H. CONCEPTOS RELACIONADOS

Modelo de madurez de la capacidad de ciberseguridad (C2M2)

El modelo de madurez de capacidad de ciberseguridad, se orienta en la ejecución y gestión de las buenas prácticas de la ciberseguridad relacionados con las tecnologías de la información y en donde estos manejan.

De acuerdo con (U.S Department of Energy, 2022), el modelo se puede utilizar en diferentes áreas como:

- Fortificar capacidades de ciberseguridad de empresas.
- Permitir que las organizaciones evalúen y comparen de manera efectiva.

- Participar conocimientos, mejores prácticas y referencias relevantes entre organizaciones. Además de priorizar acciones e inversiones para mejorar capacidades de ciberseguridad.

Infraestructura Crítica

"Una infraestructura crítica es un elemento, sistema o parte de una organización, que es vital para el mantenimiento de funciones sociales vitales, la salud o la integridad física, la seguridad y el bienestar social y económico de la población" Lopez et. al (2021)

Madurez

(Marcovecchio, 2019) comenta que la madurez es una medida de la capacidad de una organización para la mejora continua en una disciplina en particular. Los niveles de madurez y capacidad se pueden utilizar como punto de partida para la creación de un programa de certificación, que sería de gran importancia para las autoridades.

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, Gutierrez et al. (2022)

Ciberseguridad

"Es un conjunto de actividades y herramientas que se ejecutan con la finalidad de proteger la información digital"(Gamón, 2017)

Amenaza Informática

Es un suceso que daña a los procedimientos o recursos informáticos, entre los tipos de amenazas, se encuentran:

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje (T, 2018)

Ataques

Abad W et al. (2019) manifiesta que:

Últimamente han incrementado los ataques a las redes, ya que el espacio radioeléctrico no se puede proteger, sin embargo, se puede diseñar la red de forma que la distribución de equipos y potencia de transmisión sea la mínima imprescindible. Así mismo se dan los ataques a servidores web debido a las vulnerabilidad que presentan.

I. TRABAJOS RELACIONADOS

Para el presente proyecto se toma como referencia los siguientes trabajos y se puntualizara los temas que nos servirán.

Cedeño (2021) presenta en su artículo la situación de la ciberseguridad en el Ecuador en el año 2020, a través del método cualitativo y documental. Como resultados elabora una estrategia nacional de ciberseguridad y analiza además como las empresas y universidades se enfocan en la mitigación de riesgos tecnológicos.

Este artículo permitirá recopilar información del Código Integral Penal del Ecuador además determinar el punto de vista del autor sobre la ciberseguridad con la finalidad de tener un enfoque más profundo de la estrategia en el Ecuador.

Borbúa en el año (2017) en su artículo denominado "Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa", analiza temáticas de la seguridad y defensa en el ciberespacio utilizando la metodología analítico-conceptual, además propone un modelo local de gobernanza en ciberdefensa. Para la presente investigaciones servirá como guía para proponer un modelo de madurez de ciberseguridad.

Una tesis denominada "Ciberseguridad en Infraestructuras Críticas" realizado por Aguirre (2017), determina las infraestructuras críticas y la falta de controles de ciberseguridad para estas en el Ecuador. Considera los ciberataques a infraestructuras en países como Estonia, Irán, Ucrania y otros. Este estudio sirve para analizar los sectores más críticos de ciberseguridad, conjuntamente con los entes gubernamentales y empresas públicas y privadas.

Un estudio de la Organización de los Estados Americanos presenta un reporte de seguridad cibernética e infraestructuras críticas de las Américas, en el cual analiza los ataques cibernéticos más comunes a infraestructuras críticas como los malware, spam, phishing, entre otros. Manifestando la situación actual de América Latina y el Caribe y las diferentes estrategias que pueden ser utilizadas en los gobiernos para proteger a los activos informáticos y a la sociedad en general. Este estudio permitirá comprender las políticas de ciberseguridad, el presupuesto de Ecuador destinado a mejorar la ciberseguridad y la preparación para los incidentes cibernéticos para la construcción del modelo de madurez.

Por otro lado Rea (2020), estudia los diferentes modelos de madurez de ciberseguridad (CMM-C2M2, SSE-CMM), sus dominios y sus capacidades, además de los riesgos en ciberseguridad y su mitigación a través de controles. Al mismo tiempo realiza una investigación en el Instituto Ecuatoriano de Seguridad Social (IESS), considerando los activos de la organización, calificándolos a través de la metodología Magerit.

Este documento permite comprender la influencia de los modelos de madurez de ciberseguridad en una nación y la forma de contrarrestar medidas de protección a los activos de una infraestructura crítica como el servicio de respuesta a emergencias.

Cuenca: Av. de las Américas y Tarqui. *Telf: 2830751, 2824365, 2826563* **Azogues:** Campus Universitario "Luis Cordero El Grande", (Frente al Terminal Terrestre). *Telf: 593 (7) 2241 - 613, 2243-444, 2245-205, 2241-587* **Cañar:** Calle Antonio Ávila Clavijo. *Telf: 072235268, 072235870* **San Pablo de la Troncal:** Cdla. Universitaria km.72 Quinceava Este y Primera Sur *Telf: 2424110* **Macas:** Av. Cap. José Villanueva s/n *Telf: 2700393, 2700392*

J. METODOLOGÍA

El metodo que se utilizará en la investigación será descriptivo, es decir se estudiará a detalle los modelos de madurez para las infraestructuras críticas de Ecuador, con la finalidad de determinar la eficiencia de ciberseguridad.

La informacion se obtendra de las páginas web de las instituciones gubernamentales, misma que seran analizada además de las estrategias utilizadas para proteger las infraestructuras físicas y organizativas.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES I			MES II				MES III				MES IV				MES V	MEDIOS DE VERIFICACIÓN
		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		
1	**Realizar un estudio teórico sobre los conceptos relacionados a los modelos de madurez de ciberseguridad**																	
1.1	Bases teóricas y trabajos relacionados	x	x															Lista de documentos almacenados en la herramienta Mendeley
1.2	Realizar un estado del arte de artículos relacionados al tema propuesto			X	x													
2	**Analizar estrategias de ciberseguridad utilizadas en el Ecuador**																	
2.2	Realizar un diagnóstico del estado de las infraestructuras críticas del Estado Ecuatoriano en base a informes y páginas institucionales				x	x	x											. Información de páginas gubernamentales y artículos.
3	**Proponer un modelo de madurez de ciberseguridad para Infraestructuras Críticas**																	
3.1	Proponer un modelo de madurez para las infraestructuras críticas de Ecuador									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. José Antonio Carrillo Zenteno
ESTUDIANTE 1	Carlos Patricio López Loja

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	CAÑAR
Fecha:	15 de Noviembre del 2022
Firmas:	
Nombre: Ing. José Antonio Carrillo Zenteno. CC: 0103304531 **Director del Proyecto**	Nombre: Carlos Patricio López Loja C.C.: 0303016851 **Estudiante / Egresado**

P. REFERENCIAS

Referencias

Enrique, G. A., & Necochea Mendoza, P. (28 de 10 de 2022). *repositorioacademico.upc.edu.pe.* Obtenido de repositorioacademico.upc.edu.pe: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/660408/Gutierrez_AJ.pdf?sequence=3&isAllowed=y

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *R e vista Latinoamericana de Estudios de Seguridad*, 80-93. Obtenido de repositorio.flacsoandes.edu.ec: https://repositorio.flacsoandes.edu.ec/bitstream/10469/12243/1/RFLACSO-06-Pons.pdf

Lopez, F. A., Ruete, D., & Gatica, G. (01 de 07 de 2021). *www.researchgate.net.* Obtenido de www.researchgate.net: https://www.researchgate.net/profile/Felipe-A-Lopez-2/publication/355574499_Infraestructura_Critica_y_Ciberseguridad_en_Chile_orientaciones_para_su_consenso/links/61770874a767a03c14b4d334/Infraestructura-Critica-y-Ciberseguridad-en-Chile-orientaciones-par

Parrales, W. M., Rodríguez, T. C., Cevallos, M. E., Santana, H. L., Pilozo, Á. R., Arias, F. J., . . . Castro, V. F. (01 de 12 de 2019). *www.3ciencias.com.* Obtenido de www.3ciencias.com: https://www.3ciencias.com/wp-content/uploads/2019/12/LA-CIBERSEGURIDAD-PR%C3%81CTICA-APLICADA-A-LAS-REDES-SERVIDORES-Y-NAVEGADORES-WEB-.pdf

T, C. H. (27 de 08 de 2018). *core.ac.uk.* Obtenido de core.ac.uk: https://core.ac.uk/download/pdf/230095193.pdf

U.S Department of Energy. (01 de 06 de 2022). *www.energy.gov.* Obtenido de www.energy.gov: https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

Cañar, 03 de octubre 2023

Asunto: Embargo Temporal del Trabajo de Titulación

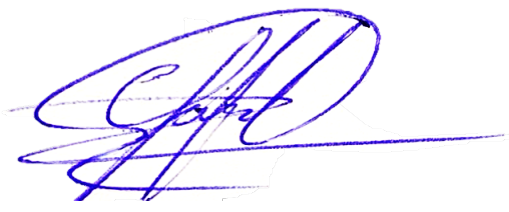
Señor,
Ing. Leopoldo Pauta Ayabaca
DECANO DE LA UNIDAD ACADÉMICA DE ADMINISTRACIÓN DE INFROMATICA, CIENCIAS DE LACOMPUTACION, E ENOVACCION TECNOLÓGICA
Cuenca.

De mi consideración:

Señor Decano, CARLOS PATRICIO LOPEZ LOJA , como autora del Trabajo de Titulación "MODELO DE MADUREZ DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRITICAS CASO DE ESTUDIO: ECUADOR" y JOSE ANTONIO CARRILO ZENTENO , 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,



Carlos Patricio Lopez Loja
CI: 0303016851
Autor

C.C.: Biblioteca.