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

"PROPUESTA DE UN MODELO DE MADUREZ DE CIBERSEGURIDAD PARA ECUADOR"

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

AUTOR: GERSON LEONARDO VERDUGO CRESPO

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES.

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

“PROPUESTA DE UN MODELO DE MADUREZ DE CIBERSEGURIDAD PARA ECUADOR”

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

AUTOR: GERSON LEONARDO VERDUGO CRESPO

DIRECTOR: ING.CRISTHIAN HUMBERTO FLORES URGILES.

CAÑAR - ECUADOR

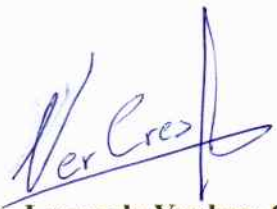
2023

DIOS, PATRIA, CULTURA Y DESARROLLO

Declaratoria de Autoría y Responsabilidad

Gerson Leonardo Verdugo Crespo portador(a) de la cedula de ciudadanía N° **030274067-5.** Declaro ser el autor de la obra: **"PROPUESTA DE UN MODELO DE MADUREZ DE CIBERSEGURIDAD PARA 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.

Cañar, **19 de octubre de 2023**



Gerson Leonardo Verdugo Crespo

C.I. 0302740675

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Est. Gerson Leonardo Verdugo Crespo

Ing. Cristhian Humberto Flores Urgiles, Mgs.
DIRECTOR DEL TRABAJO INVESTIGATIVO
UNIVERSIDAD CATOLICA DE CUENCA
CI: 0301638375
TUTOR

DEDICATORIA

A mis queridos padres, Rosa Crespo Guaraca y Leonardo Verdugo Flores, les dedico este trabajo con todo mi amor y gratitud. Su apoyo inquebrantable, sabiduría y sacrificio han sido la luz que iluminó mi camino hacia este logro. Gracias por inspirarme a ser la mejor versión de mí mismo(a) y por brindarme amor incondicional en cada etapa de mi vida.

A mi familia y amigos, que siempre estuvieron a mi lado, celebrando mis triunfos y alentándome en los momentos de desafío, les agradezco de todo corazón. Su amor y apoyo han sido fundamentales para que hoy pueda escribir estas líneas de agradecimiento.

Este trabajo es un testimonio de la importancia de rodearse de personas que creen en tus sueños y te empujan a alcanzarlos. A todos ustedes, mi más profundo agradecimiento.

AGRADECIMENTO

Quiero expresar mi más sincero agradecimiento a las personas que hicieron posible la realización de este trabajo:

A mis padres, quienes han sido mi fuente inagotable de amor, apoyo y orientación a lo largo de mi vida. Su ejemplo de tenacidad y sacrificio ha sido mi inspiración constante.

A mis queridos abuelitos, cuyas palabras de aliento y sabios consejos siempre han iluminado mi camino. Su amor incondicional es un tesoro inigualable.

A mis demás familiares, cuyo respaldo inquebrantable me ha dado fuerzas en los momentos de desafío y ha multiplicado la alegría en los momentos de triunfo.

A mis profesores, quienes han compartido su conocimiento y han sido guías en mi formación académica. En particular, deseo agradecer al ingeniero Cristhian Flores, cuya dedicación y apoyo han sido fundamentales en este proceso. Su paciencia y sabiduría han marcado una diferencia significativa en mi camino hacia el éxito.

Gracias a todos ustedes por formar parte de este viaje y por ser pilares en mi vida. Sus contribuciones han sido invaluables y han dejado una huella imborrable en mi corazón.

RESUMEN

Este artículo tiene como fin proponer un modelo de madurez de ciberseguridad adaptado a las necesidades y características del Ecuador, el cual permitirá evaluar y mejorar la capacidad de ciberseguridad en organizaciones, organismos gubernamentales e infraestructuras críticas del país. El Modelo lleva por nombre, Cybersecurity Maturity Model of Ecuador (CMME), y los principales objetivos son; Desarrollar un modelo de madurez de la ciberseguridad, con una propuesta para el Estado Ecuatoriano, determinando sus dominios, niéveles de madurez, funciones y categorías en base a estándares y marcos de referencia reconocidos, que al aplicarlo permita establecer y evaluar la ciberseguridad en el país, se realizara un levantamiento de información documental sobre los modelos y marcos de referencia que permitirá establecer las faces que se deberán seguir para la elaboración del mismo. Además de elaborar un marco de referencia para futuros proyectos sobre modelos de madurez de ciberseguridad para naciones. Para realizar la propuesta del siguiente modelo se estudió la norma ISO 27001 y tres marcos fundamentales de ciberseguridad como son: CMM (Cybersecurity Capacity Maturity Model for Nations), C2M2 (Cybersecurity Capacity Maturity Model for Organizations), y NIST CSF (National Institute of Standards and Technology) (Cybersecurity Framework), a los cueles se realizaron dos tipos de análisis comparativo para la obtención de las fases presentadas más adelante, y evaluación de las capacidades de ciberseguridad en el Ecuador. Siguiendo las fases planteadas en este artículo, se logró desarrollar tres de las seis plantadas, las cuales son: Análisis del Contexto Ecuatoriano, Definición de Objetivos y el Desarrollo del Modelo, las tres faltantes no fueron desarrolladas ya que al ser una propuesta no se puede probar, implantar, evaluar y por ende mejorar. En conclusión, se logró desarrollar un modelo de madurez de ciberseguridad, con sus dominios y subdominios, establecer los niveles de madurez,

funciones y categoría las culés servirán de referencia al momento de evaluar la capacidad de ciberseguridad del Ecuador, además de servir de guía para la elaboración de otros marcos de ciberseguridad para naciones.

PALABRAS CLAVE

Ciberseguridad, Modelo de Madurez, Ecuador, Tecnología, CMM, C2M2, NIST CSF.

ABSTRACT

The purpose of this article is to propose a cybersecurity maturity model adapted to the needs and characteristics of Ecuador, which will allow the evaluation and improvement of cybersecurity capacity in organizations, government agencies and critical infrastructures in the country. The Model is called Cybersecurity Maturity Model of Ecuador (CMME), and the main objectives are; Develop a cybersecurity maturity model, with a proposal for the Ecuadorian State, determining its domains, maturity levels, functions and categories based on recognized standards and reference frameworks, which when applied allows establishing and evaluating cybersecurity in the country , a survey of documentary information will be carried out on the models and reference frameworks that will allow establishing the steps that must be followed for its preparation. In addition to developing a reference framework for future projects on cybersecurity maturity models for nations. To propose the following model, the ISO 27001 standard and three fundamental cybersecurity frameworks were studied, such as: CMM (Cybersecurity Capacity Maturity Model for Nations), C2M2 (Cybersecurity Capacity Maturity Model for Organizations), and NIST CSF (National Institute of Standards). and Technology) (Cybersecurity Framework), to which two types of comparative analysis were carried out to obtain the phases presented below, and evaluation of cybersecurity capabilities in Ecuador. Following the phases proposed in this article, it was possible to develop three of the six planned, which are: Analysis of the Ecuadorian Context, Definition of

Objectives and Development of the Model, the three missing ones were not developed since being a proposal it cannot be test, implement, evaluate and therefore improve. In conclusion, it was possible to develop a cybersecurity maturity model, with its domains and subdomains, establish the maturity levels, functions and category that will serve as a reference when evaluating Ecuador's cybersecurity capacity, in addition to serving as a guide for the development of other cybersecurity frameworks for nations.

KEYWORDS

Cybersecurity, Maturity Model, Ecuador, Technology, CMM, C2M2, NIST CSF.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Propuesta de un modelo de madurez de ciberseguridad para Ecuador

Proposal for a cybersecurity maturity model for Ecuador

Gerson Leonardo Verdugo Crespo[1]

Estudiante, Universidad Católica de Cuenca, Ecuador

gerson.verdugo@est.ucacue.edu.ec

Cristhian Humberto Flores Urgilés [2]

Docente, Universidad Católica de Cuenca, Ecuador

chflores@ucacue.edu.ec

Cristina Mariuxi Flores Urgilés [3]

Docente, Universidad Católica de Cuenca, Ecuador

cmfloresu@ucacue.edu.ec

Julio Jhovany Santacruz Espinoza [4]

Docente, Universidad Católica de Cuenca. Ecuador

jsantacruze@ucacue.edu.ec

Mario Bernabe Ron Egas [5]

Docente, ESPE, Ecuador

mbron@espe.edu.ec

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

RESUMEN

Este artículo tiene como fin proponer un modelo de madurez de ciberseguridad adaptado a las necesidades y características del Ecuador, el cual permitirá evaluar y mejorar la capacidad de ciberseguridad en organizaciones, organismos gubernamentales e infraestructuras críticas del país. El Modelo lleva por nombre, Cybersecurity Maturity Model of Ecuador (CMME), y los principales objetivos son; Desarrollar un modelo de madurez de la ciberseguridad, con una propuesta para el Estado Ecuatoriano, determinando sus dominios, niéveles de madurez, funciones y categorías en base a estándares y marcos de referencia reconocidos, que al aplicarlo permita establecer y evaluar la ciberseguridad en el país, se realizara un levantamiento de información documental sobre los modelos y marcos de referencia que permitirá establecer las faces que se deberán seguir para la elaboración del mismo. Además de elaborar un marco de referencia para futuros proyectos sobre modelos de madurez de ciberseguridad para naciones.

Para realizar la propuesta del siguiente modelo se estudió la norma ISO 27001 y tres marcos fundamentales de ciberseguridad como son: CMM (Cybersecurity Capacity Maturity Model for Nations), C2M2 (Cybersecurity Capacity Maturity Model for Organizations), y NIST CSF (National Institute of Standards and Technology) (Cybersecurity Framework), a los cueles se realizaron dos tipos de análisis comparativo para la obtención de las fases presentadas más adelante, y evaluación de las capacidades de ciberseguridad en el Ecuador.

Siguiendo las fases planteadas en este artículo, se logró desarrollar tres de las seis plantadas, las cuales son: Análisis del Contexto Ecuatoriano, Definición de Objetivos y

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

el Desarrollo del Modelo, las tres faltantes no fueron desarrolladas ya que al ser una propuesta no se puede probar, implantar, evaluar y por ende mejorar.

En conclusión, se logró desarrollar un modelo de madurez de ciberseguridad, con sus dominios y subdominios, establecer los niveles de madurez, funciones y categoría las culés servirán de referencia al momento de evaluar la capacidad de ciberseguridad del Ecuador, además de servir de guía para la elaboración de otros marcos de ciberseguridad para naciones.

ABSTRACT

The purpose of this article is to propose a cybersecurity maturity model adapted to the needs and characteristics of Ecuador, which will allow the evaluation and improvement of cybersecurity capacity in organizations, government agencies and critical infrastructures in the country. The Model is called Cybersecurity Maturity Model of Ecuador (CMME), and the main objectives are; Develop a cybersecurity maturity model, with a proposal for the Ecuadorian State, determining its domains, maturity levels, functions and categories based on recognized standards and reference frameworks, which when applied allows establishing and evaluating cybersecurity in the country , a survey of documentary information will be carried out on the models and reference frameworks that will allow establishing the steps that must be followed for its preparation. In addition to developing a reference framework for future projects on cybersecurity maturity models for nations.

To propose the following model, the ISO 27001 standard and three fundamental cybersecurity frameworks were studied, such as: CMM (Cybersecurity Capacity Maturity

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Model for Nations), C2M2 (Cybersecurity Capacity Maturity Model for Organizations), and NIST CSF (National Institute of Standards). and Technology) (Cybersecurity Framework), to which two types of comparative analysis were carried out to obtain the phases presented below, and evaluation of cybersecurity capabilities in Ecuador.

Following the phases proposed in this article, it was possible to develop three of the six planned, which are: Analysis of the Ecuadorian Context, Definition of Objectives and Development of the Model, the three missing ones were not developed since being a proposal it cannot be test, implement, evaluate and therefore improve.

In conclusion, it was possible to develop a cybersecurity maturity model, with its domains and subdomains, establish the maturity levels, functions and category that will serve as a reference when evaluating Ecuador's cybersecurity capacity, in addition to serving as a guide for the development of other cybersecurity frameworks for nations.

PALABRAS CLAVE

Ciberseguridad, Modelo de Madurez, Ecuador, Tecnología, CMM, C2M2, NIST CSF.

KEYWORDS

Cybersecurity, Maturity Model, Ecuador, Technology, CMM, C2M2, NIST CSF.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

INTRODUCCIÓN

La ciberseguridad en la actualidad se ha convertido en un desafío crítico y urgente para la protección de los sistemas, datos, activos, e infraestructuras críticas de un país.

Ecuador, como una nación en constante desarrollo tecnológico, no es ajeno a esta realidad y enfrenta una creciente necesidad de abordar las amenazas cibernéticas de manera efectiva y proactiva.

Un modelo de madurez de ciberseguridad se presenta como una herramienta fundamental para evaluar, mejorar y optimizar los esfuerzos de protección contra amenazas cibernéticas. Este modelo establece un marco de referencia que permite al Ecuador, medir su capacidad para prevenir, detectar, responder y recuperarse de incidentes de cibernéticos.

En este trabajo se propone el desarrollo de un modelo de madurez de ciberseguridad adaptado específicamente a las necesidades y características de Ecuador. Este modelo se diseñará considerando el panorama actual de amenazas cibernéticas que afectan al país, así como las particularidades de su infraestructura crítica y la capacidad de sus instituciones para hacer frente a estos desafíos.

Para la construcción de este modelo de madurez, se tomarán en cuenta las mejores prácticas, marcos y normas de ciberseguridad las cuales se verán plasmadas en las siguientes secciones, donde se detallará el proceso de construcción del modelo, los factores y dimensiones que se evaluarán. La implementación de un modelo de este tipo

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

en el país ayudaría a mejorar la capacidad de defensa contra los ciberataques y mejorar la seguridad en línea en el país.

MARCO TEÓRICO

La ciberseguridad en general es de vital importancia a nivel de naciones y organizaciones, ya que mediante la buna gestión de la misma nos ayuda con la protección y la privacidad de datos, las naciones almacenan y procesan una gran cantidad de datos sensibles, tanto a nivel gubernamental como empresarial. También es esencial para prevenir y combatir los ciberdelitos, como el fraude cibernético, el robo de información financiera y la piratería informática (1).

Así mismo la ciberseguridad es crucial para proteger la infraestructura crítica de un país, como los sistemas de energía, transporte, salud y comunicaciones, de ataques cibernéticos, una nación con una buena postura de ciberseguridad inspira confianza en sus ciudadanos, empresas e inversores extranjeros (1).

Para la evaluación del estado de ciberseguridad de un país es necesario la aplicación de un modelo de madurez ya que estos proporcionan un marco de referencia para medir y mejorar las capacidades de ciberseguridad de una nación. Al utilizar un modelo, los países pueden evaluar y comparar su nivel de madurez en términos de protección contra amenazas cibernéticas, capacidad de respuesta a incidentes de seguridad y capacidad para prevenir y mitigar riesgos de seguridad en el ámbito digital (2).

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

Estos modelos pueden tomar en cuenta diferentes aspectos de la ciberseguridad, como políticas, normativas, educación y capacitación, infraestructuras críticas, gestión de riesgos y colaboración internacional (3).

Estado de la ciberseguridad en Ecuador

Hace unos años Ecuador no contaba con una estrategia de seguridad ciberseguridad, pero avanzo significativamente con mejoras en sus capacidades cibernéticas y en el enfrentamiento de amenazas, apoyado por el establecimiento de un grupo de trabajo para el desarrollo de la estrategia nacional de ciberseguridad. Esto se debe en gran parte al establecimiento de EcuCERT (Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones), equipo de respuesta ante incidentes cibernéticos del país que depende de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). Desde el año 2018, el Banco Interamericano de Desarrollo (BID) ha estado brindando orientación técnica al país con el propósito de ayudar en la identificación, evaluación y elaboración de planes para los niveles de preparación en ciberseguridad a nivel nacional (4). El reporte de Patricio Real viceministro de tecnologías de información y comunicación del gobierno en (2017-2021), informo que se registraron más de 40 millones de ataques cibernéticos en menos de dos días (5).

En la actualidad Vianna Maino Ministra de Telecomunicaciones de la Sociedad de la información dio a conocer que el Ecuador cuenta con una estrategia Nacional de Ciberseguridad un documento con lineamientos para la seguridad nacional en el ciber espacio y todas las instituciones que conforman el Comité Nacional de Ciberseguridad,

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

organismo creado en el actual Gobierno y que aglutina los Ministerios de Telecomunicaciones y de la Sociedad de la Información, Los sectores de Defensa Nacional, Gobierno, Interior, Relaciones Exteriores y Movilidad Humana, así como el Centro de Inteligencia Estratégica y la Secretaría General de la Administración Pública de la Presidencia (6).

Activos de Información en Ecuador e Infraestructuras Criticas

Los activos de información de un país son aquellos datos, documentos y registros que son propiedad de la nación que deben ser gestionados adecuadamente para garantizar su disponibilidad, integridad, accesibilidad y confidencialidad (7). Tales como software, hardware, bases de datos, videos, imágenes, infraestructuras físicas, recursos humanos (8).

Las infraestructuras críticas son activos vitales para la seguridad pública, el bienestar económico y la seguridad nacional de los países (9). Dependen de los sistemas y servicios de infraestructura críticos, así como de las personas y los sistemas cibernéticos que los operan, monitorean y suministran (10).

En Ecuador en los últimos años se han realizado estudios sobre las infraestructuras críticas del país y la necesidad de protegerlas. En 2011, se estableció un Plan Nacional de Infraestructuras Criticas, y en 2021 la política de Ciberseguridad para proteger las infraestructuras criticas las misma que se muestran en la Ilustración 1 (11).

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

Ilustración 1 Infraestructuras críticas en el Ecuador, Autor: Autoría propia.

Modelos de madurez de ciberseguridad

Un modelo de madurez de ciberseguridad se basa en la idea de que la seguridad cibernética es un proceso continuo y evolutivo, y no un estado estático. Modelos como CMM ayuda a las naciones a comprender qué funciona, qué no funciona y por qué, en todas las áreas de ciberseguridad. Esto es importante para que los gobiernos y las empresas pueden adoptar políticas y hacer inversiones que tienen el potencial de mejorar significativamente la seguridad y seguridad en el ciberespacio, respetando también los derechos humanos, como la privacidad y la libertad de expresión (12).

CMM

El Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM) es una herramienta para evaluar el nivel de madurez de ciberseguridad de un país (13). CMM asigna una puntuación según su nivel de desarrollo en distintas áreas de

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

ciberseguridad, lo que permite identificar áreas de mejora y establecer objetivos específicos para mejorar la postura de ciberseguridad en el país.

Este modelo cuenta con dimensiones que abarcan una amplia extensión que debe ser considerada al momento de mejorar la capacidad de ciberseguridad, dentro de cada dimensión, hay varios factores, aspectos, estados de desarrollo e indicadores de capacidad en ciberseguridad (14). Dimensiones que serán expuestas en la Tabla 1.

Tabla 1 Dimensiones del modelo de madurez CMM, Autor: Autoría propia.

1	Política y estrategia de seguridad cibernética.	3	Formación, capacitación y habilidades de seguridad cibernética.	5	Estándares, organizaciones, y tecnologías.
2	Cultura cibernética y sociedad.	4	Marcos legales y regulatorios.		

NIST

El modelo NIST Framework Core es un marco de trabajo de ciberseguridad desarrollado por el instituto nacional de Estándares y Tecnología de los Estados Unidos (NIST) que tiene como objetivo ayudar a las organizaciones a gestionar y reducir sus riegos de ciberseguridad. Si bien este marco fue diseñado principalmente para empresas, puede ser aplicado por gobiernos y naciones para fortalecer la seguridad en línea y sus infraestructuras críticas (15).

NIST forma parte de la unión de los mejores estándares internacionales en materia de ciberseguridad en un marco conocido como Cyber Strategy Framework (CSF), cuenta con 4 niveles de implementación las cuales se puede observar en la Tabla 2, estas describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización exhiben las características definidas en el Marco (16).

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

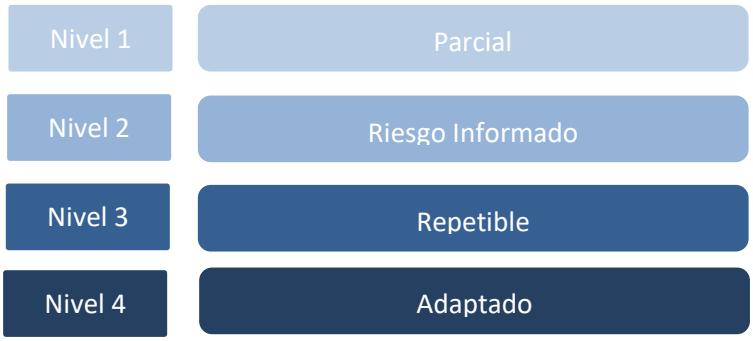


Ilustración 2 Niveles del Marco de Ciberseguridad NIST CSF, Autor: Autoría propia.

Este marco está compuesto de igual manera por cinco funciones las cuales son el nivel más alto abstracción incluido en el Marco. Actúan como la columna vertebral del Framework Core en el que se organizan todos los demás elementos. Estas funciones se presentan a continuación en la Ilustración 3.

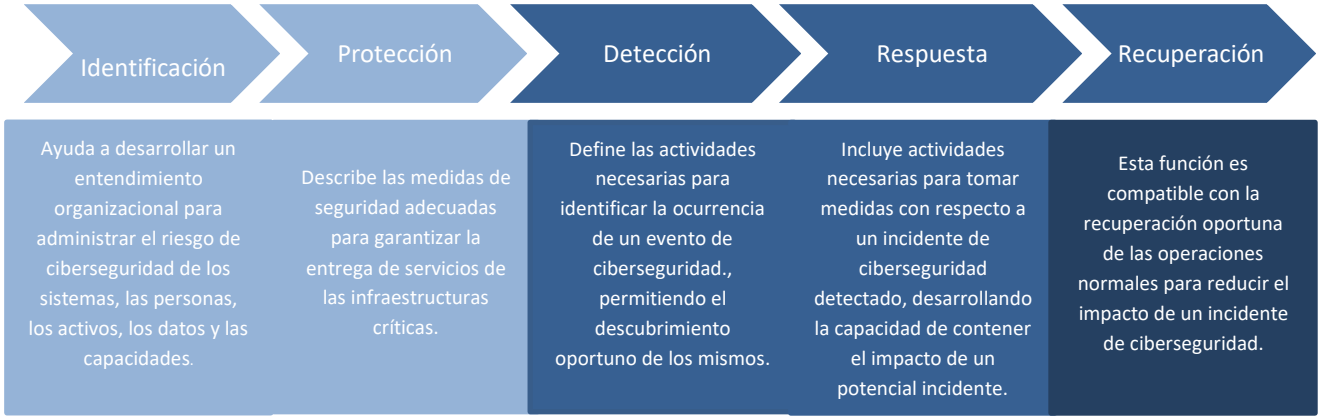


Ilustración 3 Funciones Incluidas de NIST CSF, Autor: Autoría propia.

CM2M2

El modelo C2M2 es un marco de madurez de capacidades en ciberseguridad, diseñado para medir y mejorar la capacidad de las organizaciones, sin embargo, ha sido adaptado para su uso por naciones y empresas de todos los sectores. El modelo C2M2 puede ser útil para que las naciones evalúen su madurez en ciberseguridad y desarrollen estrategias para mejorarla (17). Este modelo se enfoca en la evaluación y medición de las

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

capacidades de los países en ciberseguridad y es utilizado por muchos países como una guía para la mejora de sus estrategias de ciberseguridad. Por lo tanto, si un país quiere evaluar su nivel de madurez en ciberseguridad, el modelo C2M2 puede ser una herramienta útil para este propósito (18).

Este modelo está organizado en 10 dominios. Cada dominio es una agrupación lógica de prácticas de ciberseguridad. Las practicas dentro de un dominio se agrupan por objetivos. Dentro de cada objetivo, las practicas están ordenadas por niveles de indicadores de madurez (MIL). En la siguiente figura se muestra un resumen de la organización y estructura de este modelo (18).

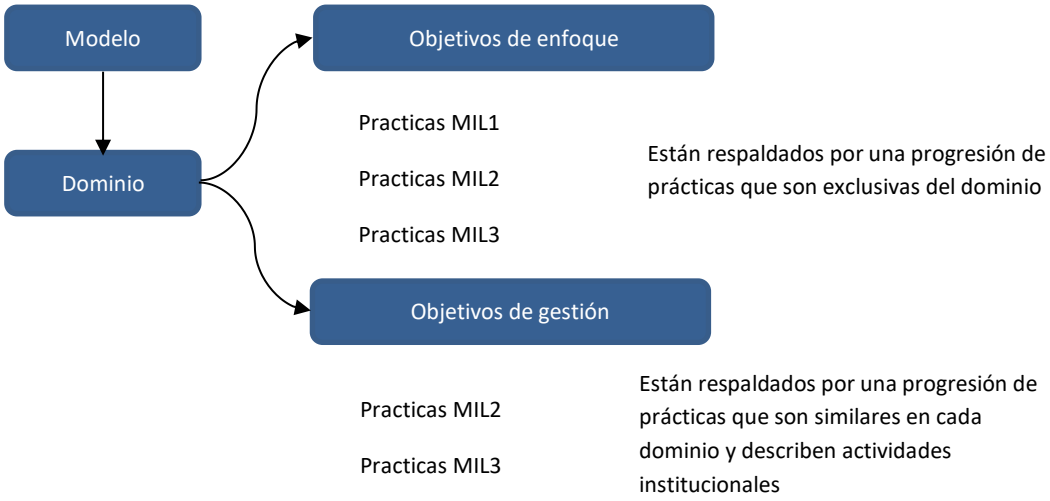


Ilustración 4 Estructura del modelo de madurez C2M2, Autor: Autoría propia.

ISO/IEC 27001

Esta es una norma internacional para la gestión de la seguridad de la información. Proporciona un enfoque estructurado y sistemático para establecer, implementar, operar,

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

monitorear, revisar, mantener y mejorar la gestión de la seguridad de la información en una organización (19).

METODOLOGÍA

Enfoque de la investigación

El presente trabajo considera la necesidad de analizar los diferentes tipos de modelos de ciberseguridad, para la obtención de un nuevo modelo orientado a la ciberseguridad en el país. Se utilizará un enfoque mixto ya que se maneja variables cualitativas y cuantitativas.

Nivel de Investigación

El presente estudio es de tipo descriptivo ya que se realiza una recolección de datos de los diferentes tipos de modelos de madurez de ciberseguridad de países.

Métodos de Investigación

El proyecto presenta el método inductivo ya que estudiara y analizara de manera directa modelos de ciberseguridad, el estudio de la relación que existe entre ellos, generar nuevas hipótesis y reglamentos que serán aplicados para el caso de estudio. Combinado con la metodología de Becker, que se basa en un análisis detallado de las capacidades de ciberseguridad existentes y cómo estas deben evolucionar para alcanzar un nivel deseado de madurez. (3)

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

RESULTADOS

Análisis comparativo de modelos y normas con el fin de la obtención de fases para la creación un modelo de madurez de ciberseguridad para el Ecuador.

Desde una perspectiva de ciberseguridad, se han sometido a análisis profundo tres modelos reconocidos como: C2M2, CMM, NIST e ISO 27001. Se ha realizado una comparación exhaustiva entre estos paradigmas, centrándose en la identificación y extracción de los atributos relevantes para el escenario en estudio.

Los parámetros de evaluación propuestos en el siguiente cuadro comparativo son los siguientes: Enfoque, Estructura, Aplicabilidad, Propósito, Flexibilidad, los cuales se obtuvieron del estudio de dos investigaciones enfocadas en la comparativa de modelos de madurez como son; la investigación de Rea Guzmán Ángel et al, en su artículo "Comparative study of cybersecurity capability maturity models" y de Diah Sulistyowati et al, en su artículo "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology" (20) (21).

En el siguiente cuadro se observa una comparativa entre los diferentes modelos de madurez y los parámetros de evaluación propuestos.

Tabla 2 Análisis comparativo de los modelos de ciberseguridad, Autor: Autoría propia.

Metodología	CMM	NIST CSF	C2M2	ISO 27001
Enfoque	Mejora de la madurez de procesos organizacionales, incluida la ciberseguridad.	Evaluación y mejora de la madurez de la ciberseguridad en infraestructura crítica.	Gestión de la ciberseguridad y la resiliencia a nivel nacional.	Establecimiento, implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Estructura	Basado en dimensiones y factores	Basado en funciones, categorías y subcategorías	Basado en niveles de madurez	Basado en requisitos de un sistema de gestión
Aplicabilidad	Principalmente aplicable a procesos organizacionales en diversos dominios.	Específico para la ciberseguridad en infraestructura crítica.	Aplicable a nivel nacional y a diferentes sectores y agencias gubernamentales.	Aplicable a nivel nacional y a organizaciones gubernamentales.
Propósito	Mejorar la madurez de los procesos organizacionales, incluyendo la ciberseguridad.	Evaluar y mejorar la madurez de la ciberseguridad en infraestructura crítica.	Proporcionar un marco para la gestión de la ciberseguridad a nivel nacional.	Establecer un enfoque coherente y estructurado para la gestión de la seguridad.
Flexibilidad	Requiere adaptación a contextos específicos	Es adaptable y aplicable a diversas organizaciones y contextos	Requiere adaptación a contextos específicos	Requiere adaptación a contextos específicos

El cuadro resalta las diferencias claves entre estos modelos en términos de sus enfoques principales la forma en que realizan las evaluaciones, su enfoque en el desarrollo de capacidades, su adaptabilidad y su grado de adopción.

Definición de fases que permitan la creación de un modelo de madurez de ciberseguridad

Después del estudio y comparación de cada modelo de ciberseguridad, se observa que servirán para la elaboración de cada una de las fases, ya que estos se enfocan y son mejores en distintos aspectos; por lo que basado en el estudio de los modelos previamente aquí presentados y en estudios anteriores como el de Aurelian Buzdugan, en su artículo “Cyber Security Maturity Model for Critical Infrastructures”, se propone las siguientes fases que se expondrán a continuación en la Tabla 3, nos indica de que modelo se basa cada fase (22).

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

Tabla 3 Detalle de los modelos en que se basó para la propuesta de las fases, Autor: Autoría propia

Fase	CMM	NIST CSF	C2M2	ISO 27001
Análisis del Contexto Ecuatoriano				x
Definición de Objetivos y Principios	X	X	X	
Desarrollo del Modelo	X	X	X	
Revisión y Prueba del Modelo		X	X	
Implementación		X	X	
Evaluación y Mejora Continua	X	X	X	

Cada fase está compuesta por diferentes componentes, mismos que han sido tomados de las metodologías estudiadas y los modelos ya mencionados, en la siguiente tabla se puede observar la correspondencia entre los componentes de cada fase y de las metodologías de referencias.

Ahora se detallará específicamente las partes de cada una de las fases que se obtuvieron de cada modelo.

Tabla 4 Descripción de las capacidades de las modelos en las cuales se basó para la propuesta de las fases, Autor: Autoría propia

Fase	CMM	NIST CSF	C2M2	ISO 27001
Análisis del Contexto Ecuatoriano				Análisis del contexto de una entidad
Definición de Objetivos y Principios	Dimensión de "Política y Estrategia"	Función de "Identificar"	Proceso de mejora de capacidades	Política de seguridad de la información
Desarrollo del Modelo	Estructura de factores y atributos	Funciones y categorías, niveles de implementación	Niveles de madurez, proceso de mejora de capacidades	Requisitos de los sistemas de gestión de seguridad de la información
Revisión y Prueba del Modelo		Ciclo de vida del framework	Evaluación de madurez	Revisión de la dirección
Implementación		Guías de implementación	Proceso de mejora de capacidades	Implementación y operación del sistema de gestión de seguridad de la información

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Evaluación y Mejora Continua	Enfoque hacia la mejora continua	Función de "Aprender y Mejorar"	Evaluación de madurez, proceso de mejora de capacidades	Mejora continua, revisión y ajuste

Descripción de cada una de las fases

1. **Análisis del Contexto Ecuatoriano:** Se realiza el análisis del contexto de la ciberseguridad en el Ecuador. Que incluye el entendimiento de las amenazas cibernéticas actuales y potenciales, las capacidades existentes en ciberseguridad, las políticas y regulaciones relevantes, y otros factores relevantes.
2. **Definición de Objetivos y Principios Rectores:** En base a los resultados obtenidos del análisis de contexto, se definen los objetivos y principios que guiarán el desarrollo del modelo de madurez. Los objetivos estarán relacionados con resiliencia de las infraestructuras críticas, ciberseguridad, fortalecimiento de la cooperación internacional
3. **Desarrollo del Modelo:** En esta fase, se utilizará y combinará la información de los modelos de referencia (CMM, NIST CSF y C2M2) a las necesidades y el contexto del Ecuador. Se utilizará la estructura de dominios y subdominios del CMM, los niveles de madurez del C2M2 y las funciones y categorías del NIST CSF para crear una estructura híbrida.
4. **Revisión y Prueba del Modelo:** En esta fase se realiza la revisión y pruebas del modelo generado; que implica recoger un feedback de las partes interesadas y realizar pruebas de funcionamiento del modelo.

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

5. **Implementación:** en esta fase de se introducirá el modelo en la comunidad de ciberseguridad de Ecuador y trabajará con diferentes partes interesadas para que lo adopten. Esta fase también incluirá la formación y la educación para ayudar a las personas a entender y utilizar el modelo.
6. **Evaluación y Mejora Continua:** Una vez implementado el modelo, se debe monitorear y evaluar su eficacia, y hacer ajustes según sea necesario. Este es un paso clave para asegurar que el modelo se mantenga relevante y útil a medida que cambian las condiciones de ciberseguridad.

Desarrollo de las fases

Análisis del Contexto Ecuatoriano

En el contexto actual, la ciberseguridad en el Ecuador ha cobrado mayor relevancia debido al aumento de las amenazas cibernéticas y los incidentes de ciberdelincuencia (23). Actualmente el Gobierno ecuatoriano ha creado el Comité Nacional de Ciberseguridad, que aglutina los Ministerios de Telecomunicaciones y de la Sociedad de la Información.

Actualmente los ataques cibernéticos que más afectan al estado ecuatoriano son, por ejemplo, el robo de información digital aprovechar las fallas encontradas de software (múltiples programadores) y hardware (múltiples proveedores), donde las víctimas no conocen que su información ha sido comprometida por un ataque de los hackers que aprovechan las debilidades mencionadas para engañar a los usuarios.

Cárdenas (2020) detalla que, en el Ecuador, las estadísticas relacionadas a violaciones a la ciberseguridad en su mayoría han sido dirigidas al sector financiero, ya que se busca

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

la afectación de los sistemas de banca virtual, sistemas de tarjetas de créditos y cajeros electrónicos, así como también los ataques direccionados a la prensa, específicamente en sus plataformas digitales (24).

El contexto actual de la ciberseguridad en el Ecuador se caracteriza por la implementación de la Estrategia Nacional de Ciberseguridad, el fortalecimiento de la infraestructura digital y la promoción de la concienciación y educación en esta materia.

Definición de Objetivos y Principios Rectores

Basado en una estrategia de ciberseguridad creada en el actual gobierno se plantearon los siguientes objetivos estratégicos los cuales serán la guía del modelo de madurez de ciberseguridad para el ecuador.

1. Gobernanza y coordinación nacional: establecer un enfoque coordinado de la ciberseguridad nacional (25).
2. Resiliencia cibernética: mejorar la resiliencia cibernética a nivel nacional y organizacional para prepararse, responder y recuperarse de los incidentes cibernéticos (25).
3. Prevención y lucha contra la cibercriminalidad: Fortalecimiento de las capacidades para prevenir, investigar y perseguir los delitos cibernéticos (25).
4. Ciberdefensa nacional: reforzar las capacidades de ciberdefensa para proteger las Infraestructuras de Información Crítica (IIC) nacionales y los servicios esenciales del Estado y desarrollar capacidades en ciber inteligencia que permitan obtener

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

información útil y oportuna de las amenazas presentes en ciberespacio para la toma de decisiones (25).

5. Habilidades y capacidades de ciberseguridad: mejorar y ampliar las habilidades y capacidades cibernéticas de la nación en todos los niveles
6. Cooperación internacional: maximizar los beneficios de la cooperación internacional (25).

Desarrollo del Modelo

De acuerdo a las necesidades y contexto actual del Ecuador, se ha planteado un modelo de madurez de ciberseguridad CMME que por sus cifras en ingles se denomina (*Cybersecurity Maturity Model of Ecuador*)

Dominios y Subdominios

Este modelo de madurez está formado por 5 dominios, que cuentan con sus respectivos subdominios, estos dominios se presentan a continuación:

***Dominio 1: Gestión Política y Estratégica de Ciberseguridad*:** Esta dimensión se enfoca en la capacidad del país para desarrollar políticas y estrategias de ciberseguridad, para la detección, el mejoramiento y respuesta ante incidentes, ataques y protección de la infraestructura critica.

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

- **Subdominio 1.1: Política y Estrategia:** En este apartado se define y se comunica las políticas de ciberseguridad del país, se integra la estrategia nacional de ciberseguridad.
- **Subdominio 1.2: Gobierno y Gestión Ejecutiva:** Aquí resalta el compromiso que se debe tener al momento de gestionar la ciberseguridad, se debe establecer roles y responsabilidades sobre la materia.
- **Subdominio 1.3: Evaluación de Riesgos y Priorización:** En este apartado, se debe identificar y evaluar los riesgos cibernéticos que enfrenta actualmente el país, priorizando las medidas de seguridad basadas en los riegos encontrados.
- **Subdominio 1.4: Protección de las infraestructuras criticas:** Se determina la capacidad del gobierno al momento de identificar las infraestructuras criticas y los riesgos que puede llegar a tener, participar en la planificación de respuestas y medidas de protección de estas.

Dominio 2: Gestión de Riesgos: Este dominio se ocupa de la identificación, evaluación y gestión de los riesgos de ciberseguridad. Comprende la implementación de procesos para identificar y evaluar los riesgos, así como la planificación y aplicación de medidas para tratar y mitigar dichos riesgos.

- **Subdominio 2.1: Identificación y Evaluación de Riesgos:** Implementación de procesos para identificar, evaluar y priorizar los riesgos de ciberseguridad en el país, considerando amenazas, vulnerabilidades y el impacto potencial en los sistemas, redes y activos de información.

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

- **Subdominio 2.2: Planificación y Tratamiento de Riesgos:** Desarrollo de planes y estrategias para mitigar y tratar los riesgos identificados, incluyendo la asignación de recursos, la implementación de controles de seguridad y la definición de responsabilidades y roles en la gestión de riesgos.
- **Subdominio 2.3: Monitoreo y Control de Riesgos:** Establecimiento de mecanismos de monitoreo y control continuo de los riesgos de ciberseguridad, incluyendo la supervisión de los controles implementados, la evaluación del cumplimiento y la realización de auditorías periódicas.

Dominio 3: Protección de la Información y Privacidad: Este dominio se centra en la protección de la información y la privacidad de los datos. Incluye la clasificación y manejo adecuado de la información, la protección de datos personales, así como la implementación de medidas de seguridad de la información en sistemas y redes. El objetivo es asegurar la confidencialidad, integridad y disponibilidad de la información.

- **Subdominio 3.1: Clasificación y Manejo de la Información**: Establecimiento de políticas y procedimientos para la clasificación adecuada de la información en función de su nivel de confidencialidad, integridad y disponibilidad, así como la implementación de controles de acceso y gestión de la información.
- **Subdominio 3.2: Protección de Datos Personales:** Implementación de medidas y controles para garantizar la protección de los datos personales de los ciudadanos, incluyendo la adopción de buenas prácticas en la gestión de datos, el cumplimiento de la normativa de privacidad y la protección contra la divulgación no autorizada.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

- **Subdominio 3.3: Seguridad de la Información en Sistemas y Redes**: Implementación de controles de seguridad de la información en los sistemas y redes, como el cifrado, la autenticación, la gestión de contraseñas, el control de acceso, la monitorización de eventos y la protección contra malware y ataques de red.

Dominio 4: Detección y Respuesta a Incidentes: Este dominio se refiere a la preparación y gestión de incidentes de ciberseguridad. Incluye el establecimiento de planes de respuesta a incidentes, la detección y notificación oportuna de incidentes, así como la implementación de procesos de investigación y recuperación de los mismos. El objetivo es garantizar una respuesta rápida y efectiva ante incidentes de seguridad.

- **Subdominio 4.1: Monitorización y Detección:** Establecimiento de sistemas y mecanismos para la detección temprana de incidentes de ciberseguridad, así como la notificación oportuna a las autoridades competentes y a las entidades afectadas para facilitar la respuesta y la colaboración en la gestión de incidentes.
- **Subdominio 4.2: Respuesta a Incidentes:** Elaboración e implementación de planes de respuesta a incidentes de ciberseguridad que establezcan los procedimientos, roles y responsabilidades para detectar, contener, investigar y recuperarse de los incidentes de seguridad de manera efectiva.
- **Subdominio 4.3: Investigación y Recuperación de Incidentes:** Desarrollo de capacidades para investigar y analizar los incidentes de ciberseguridad, así como para llevar a cabo la recuperación de los sistemas y datos afectos. Esto implica la

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

implementación de procesos forenses, la recopilación de evidencia, el análisis de la causa raíz y la restauración de los sistemas y servicios afectados.

Dominio 5: Colaboración y Cooperación en Ciberseguridad: Este dominio se centra en la importancia de colaborar y cooperar con otras organizaciones y entidades en el ámbito de la ciberseguridad. Reconoce que las amenazas cibernéticas pueden afectar a múltiples partes interesadas y que la colaboración efectiva puede mejorar la detección, la respuesta y la mitigación de amenazas.

- **Subdominio 5.1: Coordinación Interinstitucional:** En este subdominio, se enfatiza la necesidad de coordinar y colaborar con otras instituciones, tanto gubernamentales como del sector privado. Se busca establecer canales efectivos de comunicación y compartir información relevante sobre amenazas y vulnerabilidades.
- **Subdominio 5.2: Colaboración Internacional:** La colaboración internacional es esencial en un mundo interconectado. En este subdominio, se fomenta la colaboración con entidades de otros países y regiones.
- **Subdominio 5.3: Compartir Amenazas e Inteligencia:** Este subdominio se centra en el intercambio activo de información sobre amenazas y de inteligencia cibernética. Se busca compartir datos relevantes sobre ataques, tácticas, técnicas y procedimientos utilizados por los adversarios.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

NIVELES DE MADUREZ

Los niveles de madurez se estructuran en una escala gradual que refleja el progreso desde un enfoque inicial e inmaduro hasta un estado de madurez avanzado y optimizado. Los mismos que para su desarrollo fueron basados en el modelo C2M2 y se presentan en la Ilustración 5:

Ilustración 5 Niveles de madurez del modelo propuesto CMME, Autor: Autoría propia

Nivel 0: Inicial

- La organización tiene capacidades mínimas o nulas en ciberseguridad.
- No hay un enfoque formal en la gestión de riesgos cibernéticos.
- La respuesta a incidentes es reactiva y no estructurada.

Nivel 1: Básico

- Se están estableciendo políticas y procedimientos básicos de ciberseguridad.
- La gestión de riesgos está en una etapa inicial de implementación.
- Se realizan esfuerzos iniciales para sensibilizar al personal sobre ciberseguridad.

Nivel 2: Implementado

- Las políticas de ciberseguridad son más detalladas y se comunican al personal.
- La gestión de riesgos incluye una evaluación más sistemática de amenazas y vulnerabilidades.
- Existen mecanismos para detectar y responder a incidentes, aunque pueden ser reactivos.

Nivel 3: Gestionado

- Se implementan prácticas de ciberseguridad más avanzadas y documentadas.
- La gestión de riesgos es continua y se basa en evaluaciones regulares.
- La respuesta a incidentes se gestiona de manera coordinada y planificada.

Nivel 4: Mejorado

- Las prácticas de ciberseguridad son maduras y se ajustan según sea necesario.
- La gestión de riesgos incluye una comprensión profunda de las amenazas y se adapta a los cambios.
- La respuesta a incidentes es proactiva y se basa en simulacros y ejercicios.

Nivel 5: Optimizado

- La ciberseguridad está completamente integrada en todas las operaciones y procesos.
- La gestión de riesgos es una parte integral de la toma de decisiones estratégicas.
- La respuesta a incidentes es altamente eficiente y se basa en la mejora continua.

Ilustración 6 Niveles de madurez del modelo propuesto CMME y sus características, Autor: Autoría propia

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Funciones y Categorías

El modelo de madurez está formado por 4 funciones las cuales esta subdivididas en categorías, para la formación de los mismos se utilizó como referencia el modelo de madurez de ciberseguridad para Ecuador utilizando la estructura del modelo NIST CSF, las funciones con sus respectivas categorías se detallan a continuación:

Función 1: Identificar: Es comprender y gestionar los riesgos de ciberseguridad asociados con los activos de la organización.

Categoría 1: Gestión de Activos

- Identificación y clasificación de activos de información críticos.
- Mantenimiento de un inventario actualizado de activos.

Categoría 2: Gestión de Riesgos

- Evaluación y análisis continuo de riesgos cibernéticos.
- Priorización de medidas de mitigación basadas en el riesgo.

Categoría 3: Gestión de Cambios

- Proceso formal para evaluar y aprobar cambios en sistemas y aplicaciones

Función 2: Responder: Es responder de manera eficiente y efectiva ante incidentes para minimizar los impactos.

Categoría 1: Planes de Respuesta a Incidentes

- Definición y documentación de procesos de respuesta a incidentes.

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

- Asignación de roles y responsabilidades en el manejo de incidentes.

Categoría 2: Comunicaciones de Incidentes

- Comunicación efectiva con partes interesadas internas y externas.

Categoría 3: Recuperación de Datos y Sistemas

- Planificación para la recuperación de datos y sistemas después de un incidente.

Función 3: Detectar: Es establecer mecanismos para la identificación de posibles amenazas y eventos de ciberseguridad.

Categoría 1: Detección Anómala

- Implementación de sistemas de detección de intrusiones y comportamientos anómalos.
- Alertas tempranas ante actividades sospechosas.

Categoría 2: Eventos y Análisis

- Monitorización constante de eventos de seguridad.
- Análisis de logs y eventos para identificar patrones de ataque.

Categoría 3: Respuesta a Incidentes

- Planificación y procedimientos claros para la respuesta a incidentes.

Equipo designado para manejar y mitigar

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

Función 4: Recuperar: Es restaurar las operaciones normales y la funcionalidad después de un incidente de ciberseguridad.

Categoría 1: Planificación de Continuidad

- Desarrollo de planes para mantener la continuidad operativa durante interrupciones.
- Identificación de procesos y recursos críticos para la recuperación.

Categoría 2: Recuperación de Negocio

- Implementación de estrategias para la recuperación del negocio después de incidentes.
- Pruebas regulares de los planes de recuperación de negocio.

Categoría 3: Recuperación Técnica

- Restauración de sistemas y servicios técnicos después de interrupciones.

DISCUSIÓN

Esta investigación se centró en el desarrollo de un modelo de madurez de ciberseguridad adaptado al contexto ecuatoriano, representa un paso importante hacia la mejora de la ciberseguridad en Ecuador. La adaptación y personalización de modelos de madurez de ciberseguridad reconocidos internacionalmente brinda al país un marco sólido y estructurado para fortalecer su capacidad de ciberseguridad, brindando así un marco de referencia y formando un pilar importante para futuras investigaciones.

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

La falta de información sobre este tema en concreto refleja la carencia de modelos, marcos de referencia y estrategias al momento de salvaguardar la información e infraestructuras críticas del país, por lo que se anima a continuar estudiando y desarrollando estrategias y marco de ciberseguridad para evitar que se sigan suscitando ataque a información gubernamental.

Al estar basado en los principales y más importantes marcos de ciberseguridad cibernética, este modelo garantiza su relevancia y aplicabilidad en el contexto ecuatoriano. Además, al alinear el modelo con regulaciones y necesidades específicas del país, se promueve la conformidad y la resiliencia cibernética.

Sin embargo, es importante reconocer que la implementación exitosa de este modelo requerirá recursos, capacitación y un compromiso continuo por parte de todas las partes interesadas. Además, la evaluación y mejora continua del modelo son esenciales para mantener su efectividad a medida que evolucionan las amenazas cibernéticas y las tecnologías.

CONCLUSIONES

En conclusión, la propuesta del presente modelo de madurez de ciberseguridad para el Ecuador representa un paso fundamental hacia la protección, la mejora y fortalecimiento de la seguridad cibernética en el país. Este modelo proporciona un marco integral que aborda los diversos aspectos de la ciberseguridad, mediante la ejecución exitosa de las fases iniciales, se ha sentado una base sólida que puede guiar la implementación y fortalecimiento de las capacidades en Ecuador.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

La implementación de este modelo de madurez permitirá a Ecuador evaluar su nivel actual de seguridad cibernética, identificar brechas y áreas de mejora, y establecer un camino claro hacia la resiliencia y la protección efectiva contra las amenazas digitales en constante evolución.

La fase de Investigación y Análisis de Referencias sentó los cimientos al examinar a fondo los modelos de madurez de ciberseguridad existentes, permitiendo la extracción de elementos clave que son aplicables al entorno ecuatoriano. El Análisis del Contexto Ecuatoriano brindó una comprensión profunda de las características y necesidades únicas del país, garantizando que el modelo propuesto sea relevante y adecuado a la realidad local. La Definición de Objetivos y Principios estableció una guía clara para la creación del modelo, asegurando que esté alineado con las metas específicas y la visión estratégica de ciberseguridad de Ecuador. El Desarrollo del Modelo permitió la conceptualización de dominios, subdominios y niveles de madurez, proporcionando un marco estructurado para la evaluación y el avance de la ciberseguridad en el país.

Al seguir este modelo, Ecuador podrá establecer políticas y regulaciones sólidas, promover la colaboración a nivel nacional e internacional, capacitar a profesionales y concienciar a la población sobre las buenas prácticas de seguridad digital. Además, se fomentará la implementación de controles y medidas de protección adecuadas en los sistemas y redes, así como la capacidad de respuesta y recuperación eficaz frente a incidentes cibernéticos.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

1 Referencias

1. Organización de los Estados Americanos. OAS. [Online].; 2020 [cited 2023 Julio 28. Available from: https://www.oas.org/es/sms/cicte/docs/ESP-Revision-de-capacidades-de-Ciberseguridad.pdf.

2. Guamán AR. UNIVERSIDAD POLITÉCNICA DE MADRID. [Online].; 2020 [cited 2023 Septiembre 20. Available from: https://oa.upm.es/65871/1/ANGEL_MARCELO_REA_GUAMAN.pdf.

3. Anna Sarri PKATFCYD. enisa. [Online].; 2020 [cited 2023 Julio 28. Available from: https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-es.pdf.

4. Banco Interamericano de Desarrollo. CIBERSEGURIDAD, RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE. Banco Interamericano de Desarrollo. 2020 Mrazo; I(1).

5. Lauro AP. CIBERSEGURIDAD Y MEDIDAS DE PROTECCIÓN DE LA INFORMACIÓN ADOPTADAS POR EL ESTADO ECUATORIANO. Instituto de Altos Estudios Nacionales. 2022 Febrero; I(522).

6. Ministerio de Telecomunicaciones y Sociedad de la Información. ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR. Ministerio de Telecomunicaciones y Sociedad de la Información. 2022 Agosto.

7. IRS. IRS. [Online].; 2023 [cited 2023 Jilio 26. Available from: https://www.irs.gov/es/businesses/small-businesses-self-employed/digital-assets.

8. Andrea APY. GUÍA DE GESTIÓN Y CLASIFICACIÓN DE ACTIVOS. Agencia Nacional Digital. 2020 Octubre; I(1).

9. Bilge Karabacak SOYNB. Enfoques regulatorios para la ciberseguridad. The International Journal of Technology Law and Practice. 2016 Febrero.

10. Nathaniel Evans WH. Infraestructura Crítica Regional. Springer. 2019 Enero.

11. Fernando Recalde Morillo PRD. LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS EN EL ÁMBITO DE LAS FUERZAS ARMADAS. Ciencias de Seguridad y Defensa. 2020 Diciembre; V(1).

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

12. Oxford. Cybersecurity Capacity Maturity. Global Cyber Security Capacity Centre. 2021; I(1): p. 1-63.

13. Valenzuela DÁ. Linkedin. [Online].; 2020 [cited 2023 Agosto 04. Available from: https://es.linkedin.com/pulse/reporte-sobre-ciberseguridad-en-am%C3%A9rica-latina-y-el-daniel.

14. Global Cyber Security Capacity Centre. University of Oxford. [Online].; 2021 [cited 2023 Agosto 04. Available from: https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf.

15. Comisión federal de comercio. FTC. [Online].; 2019 [cited 2023 Agosto 17. Available from: https://www.ftc.gov/es/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf.

16. AWS,OEA. OAS. [Online].; 2019 [cited 2023 Agosto 17. Available from: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf.

17. Banco Interamericano de Desarrollo; Organización de los Estados Americanos. BID. [Online].; 2016 [cited 2023 Agosto 17. Available from: https://publications.iadb.org/publications/spanish/viewer/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf.

18. Universidad Carnegie Mellon. Modelo de madurez de la capacidad de ciberseguridad (C2M2). C2M2. 2021 Jilio; II(2).

19. García Jiménez Miguel RMHF. Aplicabilidad del manual de Tallin en l legislación ecuatoriana como respuesta a transgresiones de ciberseguridad. Uisrael. 2020 2023; I(425).

20. Angel Marcelo Rea-Guaman TSFJACM&IDSG. Springer. [Online].; 2017 [cited 2023 Octubre 02. Available from: https://link.springer.com/chapter/10.1007/978-3-319-67383-7_8.

21. Diah Sulistyowati FHYS. JOIV. [Online].; 2020 [cited 2023 Octubre 02. Available from: https://joiv.org/index.php/joiv/article/view/482/298.

22. Capatana AB&G. Springer. [Online].; 2022 [cited 2023 Octubre 03. Available from: https://link.springer.com/chapter/10.1007/978-981-16-8866-9_19.

e-ISSN: 2588-1000

Pro Sciences
Revista de Producción, Ciencias e Investigación

23. García Jiménez Miguel RMHF. Aplicabilidad del manual de Tallin en l legislación ecuatoriana como respuesta a transgresiones de ciberseguridad. Uisrael. 2020 2023; I(425).

24. Méndez AEL. Propuesta de estrategias de seguridad cibernética. Aproximaciones teórico prácticas hacia el aprestamiento en países latinoamericanos. Dominio de las ciencias. 2021 Febrero; XII(1).

25. Maino V. ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR. Ministerio de Telecomunicaciones y Sociedad de la Información. 2022;: p. 1-58.

ANEXOS

Trabajo de Titulación

Tema:

Propuesta de un modelo de madurez de ciberseguridad para el Ecuador

Unidad Académica

Informática, Ciencias de la Computación e Innovación Tecnológica

Carrera

Ingeniería de Sistemas de la Información

Alumno

Gerson Leonardo Verdugo Crespo

Tutor:

Ing. Cristhian Humberto Flores Urgiles

Octubre – Marzo 2023

Anexo: Formato del Anteproyecto.

A. TÍTULO
PROPUESTA DE UN MODELO DE MADUREZ DE CIBERSEGURIDAD PARA ECUADOR.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Inteligencia de Negocios	
		Sistemas de Información	
		Gobierno y administración de tecnologías de información	
		Auditoría Informática	x
		Seguridad Informática	X
		Redes y comunicación	
		Arquitectura de Hardware	
		Arquitectura de desarrollo de software	
		Ingeniería de Software	
		Gestión y gobierno de proyectos de tecnología informática	
		Ingeniería de requerimientos	
		Algoritmos y programación	
		Ciencias exactas y naturales (Matemáticas, Física, Química, Biología, etc.)	
		Modelaje y simulación	

C. PLANTEAMIENTO DEL PROBLEMA

En los últimos años Ecuador ha sido uno de los países latinoamericanos que más han sido golpeados por los delitos cibernéticos. Según el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, agencia de la Organización de las Naciones Unidas, Ecuador se encuentra en el puesto 119 de 182 países en vulnerabilidad por ataques cibernéticos.

Pese a esto no se ha creado un marco o modelo de madurez para el país, que nos ayude a evaluar y diagnosticar el estado de la ciberseguridad en Ecuador. Además, existen modelos de madurez para países desarrollados, pero, por lo contrario, no se han consolidado modelos para países en vías de desarrollo.

D. OBJETIVO GENERAL

Desarrollar un Modelo de Madurez de la ciberseguridad, con una propuesta para el Estado Ecuatoriano, determinando sus categorías, con base en estándares y marcos de referencia reconocidos, que al aplicarlo permita establecer y evaluar la Ciberseguridad en el país.

E. OBJETIVOS ESPECÍFICOS
1. Realizar un levantamiento de información documental sobre los modelos para evaluar la ciberseguridad en un país.
2. Proponer un modelo para medir el estado de ciberseguridad en países en vías de desarrollo
3. Elaborar Un marco de referencia para trabajos futuros sobre un modelo de madurez de ciberseguridad para Ecuador.

F. JUSTIFICACIÓN
Conociendo la necesidad en nuestro país Ecuador, de disponer de un modelo de madurez de ciberseguridad por la falta del mismo y no poder evaluar el estado de seguridad en el país. Se ha visto imperativo la elaboración de un modelo mediante un proceso de investigación científica confiable, para que los estados tengan una referencia validada al evaluar el nivel aplicado actualmente a las medidas de protección de la información crítica y establecer objetivos para conseguir un nivel más avanzado mediante una Estrategia Nacional de Ciberseguridad.

Mediante este proceso se busca mejora la medición de riesgo de ciberseguridad, así como los tiempos de detección, contención de incidentes y restablecimiento del servicio para responder de manera más oportuna a la complejidad y cantidad de los ataques existentes.

Además de tener un marco de referencia para poder elaborar tanto políticas de seguridad, fomentar a la sociedad una cultura responsable, crear tanto leyes como marcos regulatorios y controlar los riesgos a través de normas, organizaciones y tecnologías.

G. ALCANCE

El alcance de la presente investigación va a permitir generar una propuesta para un modelo de madures de ciberseguridad, que servirá como guía de referencia para medir el nivel de ciberseguridad en Ecuador.

H. CONCEPTOS RELACIONADOS

Los principales modelos de madurez que destacan a nivel global y que por tanto serán objeto de revisión teórica en esta investigación son los siguientes:

1. "C2M2" Cybersecurity Capability Maturity Model. Es un modelo que está enfocado a ciberseguridad y que debido a su importancia se crearon dos variantes, una para el sector energético y otra para el sector de gas y combustibles de los Estados Unidos de Norteamérica.

2. "SSE-CMM" Systems Security Engineering Capability Maturity Model. Origen de la Norma ISO/IEC 21827:2002 Es una de las normas más utilizadas internacionalmente en relación con la definición e implantación de los procesos de seguridad, ya que define en detalle los procesos que deben tenerse en cuenta en cualquier organización que desea implantar un "Proceso Global de Seguridad". Este modelo es el más mencionado en los trabajos de investigación y es un modelo aplicado a seguridad de la información, pero se ha acoplado en los diferentes trabajos para abordar ciberseguridad.
3. "COBIT" Control Objectives for Information and related Technology. Es un modelo conocido y aplicado en TI, desarrollado por ISACA, donde se manejan 5 niveles de madurez. Se desarrolló para medir el nivel de madurez en el dominio de gobierno de TI, pero se ha usado de referencia en los trabajos investigados que incluyen al gobierno de TI como uno de los factores claves de la ciberseguridad, complementando COBIT con otros modelos.
4. •"ISM3" Information Security Management Maturity Model. Lo relevante de este modelo es que se manejan métricas de Seguridad de la Información, que ayudan a 288 Proceedings of the 12th Iberian Conference on Information Systems and Technologies mantener a la organización en un nivel de riesgo aceptable, se ajusta tanto a pequeñas como a grandes organizaciones, es muy utilizado y adaptable para necesidades específicas como ciberseguridad.
5. "CCSMM" Community Cyber Security Maturity Model. Este modelo fue desarrollado por la Universidad de San Antonio Texas, es un modelo holístico que

determina la postura de ciberseguridad en organizaciones, comunidades y naciones. (Calvo Manzano & San Feliu, 2017)

6. “NICE” Capability Maturity Model (CMM). Es un modelo de ciberseguridad, enfocado en la gestión de la planificación del trabajo de todos los participantes en la gestión de la ciberseguridad, y en los objetivos de la organización.

7. "Telecomunicaciones [UIT] la define como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías La Unión Internacional de Telecomunicaciones [UIT] la define como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías." (Flores Cantos, Pozo Curo, Flores Conislla, & Adauto Medina, 2021)

8. “La ciberseguridad es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente de la información contenida en computadoras o que circula a través de las redes de computadoras. Existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que signifique un riesgo si la información confidencial llega a manos de otras personas". (Hinojosa Calzada, 2021)

I. TRABAJOS RELACIONADOS

Para el siguiente proyecto se tomará en cuenta los siguientes trabajos.

1. (Dube, 2021) en su artículo "La aplicación del modelo de madurez de la capacidad de seguridad cibernética para identificar el impacto de los factores de eficiencia interna en la efectividad externa de la seguridad cibernética", se construye factores de eficiencia y eficacia de la ciberseguridad mediante el uso de metodologías de teoría fundamentada y desarrollamos modelos para identificar el impacto de los factores de eficiencia interna en la efectividad externa de la ciberseguridad utilizando técnicas SEM.
2. (Cazares, 2021) en su artículo "Un estudio integral sobre las capacidades de respuesta ante incidentes de ciberseguridad en Ecuador", explica sobre el incremento de amenazas y ataques a la seguridad en el Ecuador, motiva la implementación de equipos de respuesta a incidentes de seguridad (CSIRT) en las diferentes organizaciones ecuatorianas en diferentes dominios. El propósito de este estudio es desarrollar un análisis de cada uno de los pasos propuestos por el NIST en el contexto ecuatoriano, para identificar el estado actual de las capacidades de respuesta a incidentes de seguridad en el Ecuador y analizar posibles acciones para mejorar estas capacidades.
3. 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. Presentando la estrategia nacional de ciberseguridad, 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 de determinar el punto de vista del autor sobre la ciberseguridad con la finalidad de tener un enfoque más profundo de la estrategia de ciberseguridad utilizada en el Ecuador.

4. (Naseir, 2020) en su artículo "Marco Nacional de Creación de Capacidades en Ciberseguridad para Países en una Fase de Transición", Este documento propone un Marco Nacional de Creación de Capacidad de Seguridad Cibernética (NCCBF) que se basa en una variedad de estándares, pautas, y prácticas para permitir que los países en una fase de transición transformen su postura actual de seguridad cibernética mediante la aplicación de actividades que reflejen los resultados deseados. El NCCBF brinda estabilidad contra amenazas no cuantificables y mejora la seguridad mediante la incorporación de medidas de seguridad de desempeño avanzadas y rezagadas a nivel nacional.
5. (Dube, Towards development of a cyber security capability maturity model, 2020) en su artículo "Hacia el desarrollo de un modelo de madurez de capacidades de seguridad cibernética", Este documento presenta la formulación y validación de un nuevo modelo de madurez de capacidad de seguridad cibernética (CSCMM) mediante la comparación de las fortalezas y limitaciones de nueve modelos de madurez contemporáneos y la realización de un análisis empírico de las aportaciones de 200 profesionales relevantes del sector de la industria. Se espera que CSCMM mejore la postura de seguridad cibernética de las organizaciones para combatir las amenazas de nueva generación.

6. (Jaquire & Solms, 2017) en su artículo denominado “Desarrollo de un modelo de madurez de contrainteligencia cibernética para países en desarrollo”, plantea lo siguiente que es necesario identificar cómo se utilizan dentro de los países desarrollados y su aplicación y utilización general como parte de la estrategia para proteger y asegurar el ciberespacio y especialmente la infraestructura de información crítica nacional, tanto por parte del gobierno como del sector privado. Esto, además de las medidas defensivas tradicionales de seguridad cibernética como parte de la estrategia cibernética dentro de los países en desarrollo.
7. (Wolfson Building, 2021) en publicación denominado “Cybersecurity Capacity Maturity Model for Nations (CMM)” El modelo de madurez de la capacidad de ciberseguridad para las naciones (CMM) ayuda a las naciones a comprender qué funciona, qué no funciona y por qué, en todas las áreas de ciberseguridad capacidad. Esto es importante para que los gobiernos y las empresas pueden adoptar políticas y hacer inversiones que tienen el potencial de mejorar significativamente la seguridad y seguridad en el ciberespacio, respetando también los derechos humanos, como la privacidad y la libertad de expresión.

J. METODOLOGÍA

La presente investigación tiene un enfoque mixto es decir cualitativo y cuantitativo, puesto que se analizarán datos cualitativos relacionado a la calidad de la bibliografía y cuantitativo pues se analizarán datos estadísticos producto de la revisión sistemática de la literatura.

Además de un método deductivo para referirse a una forma específica de pensamiento o razonamiento, que extrae conclusiones lógicas y válidas a partir de un conjunto dado de premisas o proposiciones. Dicho de otra forma, un modo de pensamiento que va de lo más general (como leyes y principios) a lo más específico.

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 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. Cristhian Humberto Flores Urgiles
ESTUDIANTE 1	Leonardo Verdugo Crespo

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	CAÑAR
Fecha:	28 noviembre 2022

Firmas:

Nombre: Ing. Cristhian Humberto Flores Urgiles. CC: 0301638375 **Director del Proyecto**	Nombre: Gerson Leonardo Verdugo Crespo C.C.: 0302740675 **Estudiante / Egresado**

P. REFERENCIAS

Bibliografía

Campoverde-Molina, M., & Valverde, L. (2019). Accessibility analysis of the web portals of the educational institutions in Cuenca, Ecuador. *Revista Cátedra, 2*(2), 55-75.

Cascón-Katchadourian, J., Ruiz-Rodríguez, A.-Á., & Alberich-Pascual, J. (2018). USOS Y APLICACIONES DE GEORREFERENCIACIÓN Y GEOLOCALIZACIÓN EN GESTIÓN DOCUMENTAL CARTOGRÁFICA Y FOTOGRÁFICA ANTIGUAS. *1*, 11.

Catarí, X. B. (Julio-Diciembre de 2012). DESARROLLO DE UN SISTEMA DE INFORMACIÓN. *Terra Nueva Etapa*, 29.

Cazares, R. O.-G.a. (2021). A Comprehensive Study About Cybersecurity Incident Response Capabilities in Ecuador. *Springer*, 281–292 .

Dube, D. M. (2020). Towards development of a cyber security capability maturity model. *Scopus*, 373–380.

Dube, D. M. (2020). Towards development of a cyber security capability maturity model. *Scopus*, 104–127.

Dube, D. M. (2021). The application of cyber security capability maturity model to identify the impact of internal efficiency factors on the external effectiveness of cyber security. *Scopus*, 367-392.

Garzón, D. P. (2017). Implementación de aplicaciones móviles. *Biblioteca de la Universidad Central, Colombia.*, 11.

Jaquire, V., & Solms, S. v. (2017). Developing a cyber counterintelligence maturity model for developing countries. *IEEE*, 1-9.

Lopez, V. (s.f.). Introducción a Android . *E.ME.Editorial*, 121.

Naseir, M. D. (2020). National cybersecurity capacity building framework for countries in a transitional phase. *Scopus*, 1-9.

Simbaña-Gallardo, V., & Luján-Mora, S. (2018). Instructions about the manuscript structureof Revista Cátedra. *Revista Cátedra, 1*(1), 36-52.

Universidad Católica de Cuenca. (2020). *Directrices para autores/as*. Obtenido de https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/about/submissions

Wolfson Building, P. R. (2021). Cybersecurity Capacity Maturity Model for Nations (CMM) . *Global Cyber Security Capacity Centre*, 1-63.

Cañar, 19 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 DELACOMPUTACION, E ENOVACCION TECNOLÓGICA
Cuenca.

De mi consideración:

Señor Decano, GERSON LEONARDO VERDUGO CRESPO, como autora del Trabajo de Titulación "**PROPUESTA DE UN MODELO DE MADUREZ DE CIBERSEGURIDAD PARA ECUADOR**" y CRISTHIAN HUMBERTO FLORES URGILES, 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,

Gerson Leonardo Verdugo Crespo
CI: 0303016851
Autor

C.C.: Biblioteca.