Análisis comparativo de modelos de selección y protección de infraestructuras críticas, como aporte a la Política Nacional de ciberseguridad del Ecuador

Páez Quishpe, Juan Jahir

Departamento de Ciencias de la Computación

Carrera de Ingenieria de Sistemas e Informática

Trabajo de Titulación previo a la obtención del título de Ingeniero en Sistemas e Informática

Ing. Ron Egas, Mario Bernabé

22 de Agosto del 2020

URKUND

Document Information

Analyzed document	Tesis-Análisis Comparativo De Modelos De Selección Y Protección De Infraestructur as Críticas, Como Aporte A La Política Nacional De Ciberseguridad Del Ecuador.docx (D78063555)
Submitted	8/22/2020 3:02:00 PM
Submitted by	RON EGAS MARIO BERNABE
Submitter email	mbron@espe.edu.ec
Similarity	3%
Analysis address	mbron.espe@analysis.urkund.com

Revisado y aplicado

MARIO BERNABE RON EGAS

Firmado digitalmente por MARIO BERNABE RON EGAS
Fecha: 2020.08.22 08:20:58 -05'00'

Sources included in the report

SA	**Universidad de las Fuerzas Armadas ESPE / Operaciones Ciberdefensa v1.4.docx** Document Operaciones Ciberdefensa v1.4.docx (D58456656) Submitted by: alexpaultapia@gmail.com Receiver: aamacias1.espe@analysis.urkund.com	3
SA	**Universidad de las Fuerzas Armadas ESPE / TESIS PROAÑO GUERRERO 04 AGOSTO 020 corrección.docx** Document TESIS PROAÑO GUERRERO 04 AGOSTO 020 corrección.docx (D77521555) Submitted by: eegalarza@espe.edu.ec Receiver: eegalarza.espe@analysis.urkund.com	1
W	URL: https://www.museumwaalsdorp.nl/wp-content/uploads/2020/03/guia-de-buenas-practicas ... Fetched: 5/17/2020 1:22:57 PM	8
SA	**Universidad de las Fuerzas Armadas ESPE / Rev_Estrategia Nacional de Ciberseguridad.docx** Document Rev_Estrategia Nacional de Ciberseguridad.docx (D77228014) Submitted by: secardenas@espe.edu.ec Receiver: secardenas.espe@analysis.urkund.com	2
SA	**Tesis Ciberseguridad VF.docx** Document Tesis Ciberseguridad VF.docx (D46789721)	2
SA	**TESIS_CIBERSEGURIDAD_PEREZ_Academia de Guerra.docx** Document TESIS_CIBERSEGURIDAD_PEREZ_Academia de Guerra.docx (D63054340)	1
SA	**Universidad de las Fuerzas Armadas ESPE / PAPER FINAL Crnl Juan Carlos Jácome G..docx** Document PAPER FINAL Crnl Juan Carlos Jácome G..docx (D60844158) Submitted by: llrecalde@espe.edu.ec Receiver: llrecalde.espe@analysis.urkund.com	1
W	URL: https://www.meridianprocess.org/siteassets/web_106011_tno_brochure-good-practice-g ... Fetched: 10/29/2019 1:25:49 AM	1
SA	**Paper de grado UEES.doc** Document Paper de grado UEES.doc (D69763731)	1

URL: https://dlc.rae.es/Robinson

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

CARRERA DE INGENIERIA DE SISTEMAS E INFORMATICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**Análisis comparativo de modelos de selección y protección de infraestructuras críticas, como aporte a la Política Nacional de ciberseguridad del Ecuador**" fue realizado por el señor **Páez Quishpe, Juan Jahir** el que ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 22 de agosto de 2020.

Firma:

MARIO BERNABE RON EGAS

Firmado digitalmente por MARIO BERNABE RON EGAS
Fecha: 2020.10.29 12:47:58 -05'00'

.....

Ing. Ron Egas, Mario Bernabé

C. C. 1704229747

4

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

CARRERA DE INGENIERIA DE SISTEMAS E INFORMATICA

RESPONSABILIDAD DE AUTORÍA

Yo, **Páez Quishpe, Juan Jahir**, con cédula de ciudadanía n° 1717984049, declaro que el contenido, ideas y criterios del trabajo de titulación: "**Análisis comparativo de modelos de selección y protección de infraestructuras críticas, como aporte a la Política Nacional de ciberseguridad del Ecuador**" es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 22 de agosto de 2020

Firma

Páez Quishpe, Juan Jahir

C.C. 1717984049

5

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

CARRERA DE INGENIERIA DE SISTEMAS E INFORMATICA

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Páez Quishpe, Juan Jahir,** con cédula de ciudadanía n° 1717984049, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Análisis comparativo de modelos de selección y protección de infraestructuras críticas, como aporte a la Política Nacional de ciberseguridad del Ecuador"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 22 de agosto de 2020

Firma

Páez Quishpe, Juan Jahir

C.C. 1717984049

DEDICATORIA

Quiero dedicar este trabajo a todas las personas que estuvieron día y noche a mi lado brindándome su apoyo y consejo, para todos ustedes:

En primer lugar, a Dios por permitirme terminar esta etapa de mi vida, por darme la sabiduría y el entendimiento para poder culminar uno de los anhelos más grandes de mi vida.

A mis padres César y Alba, quienes son los principales forjadores de este logro, ustedes que son el pilar de mi formación, ustedes que me supieron levantar en los momentos de debilidad y flaqueza, ustedes que me apoyaron en los momentos más difíciles de mi todo este proceso, para ustedes todo mi cariño y gratitud por ayudarme a ser la persona que soy, este logro es más suyo que mío.

A mi hermana Liz, quien fue la persona que con su cariño y su comprensión estuvo conmigo durante día y noche dándome ánimo y su fortaleza para lograr culminar cada uno de las etapas de esta carrera universitaria.

AGRADECIMIENTO

Agradecer en primer lugar a Dios por darme la vida y la sabiduría para lograr este gran objetivo.

A mi familia, a mis padres, mi hermana, mis primos y mis tíos quienes de una forma u otra compartieron sus experiencias y me brindaron su apoyo incondicional, gracias a todos ustedes.

A mis amigos, Lenin, Diego, Esteban, quienes con su apoyo durante toda mi carrera universitaria contribuyeron a que logre culminar con este trabajo, gracias amigos por todos estos años de apoyo y su amistad.

A mi grupo de amigos de la universidad, Lenin, Jhon, Danny, Alexander, Michael, Christian, Diego, Ricardo quienes, supieron brindarme su amistad y compartieron conmigo tantos años, hicieron que la experiencia llamada universidad fuera inolvidable, por ustedes también logro este logro.

A mi tutor de tesis Ing. Mario Ron, gracias por sus consejos y su comprensión, su orientación y su conocimiento fue indispensable para lograr este objetivo.

A mi querida universidad que me abrió sus puertas para poder formarme profesionalmente, a mis maestros y su conocimiento impartido y que fue fundamental para desarrollar este trabajo.

INDICE DE CONTENIDO

Índice de tablas

Índice de figuras

Resumen

El Ecuador ha sufrido de varios ataques a nivel de seguridad de la información. Entre los casos más recientes, están los ataques a las plataformas web con dominios .gov.ec y .ec. La seguridad de la información y comunicación, se convierte en una parte importante de la vida de las personas, del estado y de sus actividades. Como parte de la protección y de la seguridad de la información, el estado ecuatoriano mediante decretos ordena la creación de un ente que regule todas las infraestructuras consideradas como críticas para el normal desarrollo de actividades, financieras, civiles, militares, etc. La identificación de infraestructuras críticas, se vuelve una parte importante y esencial para el desarrollo e implementación de una política nacional de ciberseguridad. La presente investigación, pretende describir una serie de guidelines que coadyuven en la identificación de infraestructuras críticas estratégicas para un estado. Se considera un análisis de diferentes metodologías para la identificación de infraestructuras tales como ENISA y NIST.

PALABRAS CLAVE:

- **SEGURIDAD DE LA INFORMACIÓN**
- **INFRAESTRUCTURAS CRÍTICAS**
- **FRAMEWORKS**

Abstract

Ecuador has suffered from several attacks at the information security level. Among the most recent cases are attacks on web platforms with .gov.ec and .ec domains. Information and communication security become an essential part of people's lives, the state, and their activities. As part of the protection and security of information, the Ecuadorian state, through decrees, orders the creation of an entity that regulates all the infrastructures considered critical for the normal development of activities, financial, civil, military, etcetera. Identifying critical infrastructures becomes an essential and essential part of the development and implementation of national cybersecurity policy. This research aims to describe a series of guidelines that help identify critical strategic infrastructures for a state. An analysis of different methodologies for the identification of infrastructures such as ENISA and NIST is considered.

KEYWORDS:

- **INFORMATION SECURITY**
- **CRITICAL INFRASTRUCTURES**
- **FRAMEWORKS**

Acrónimos

ITU/UIT	Unión Internacional de Telecomunicaciones
ENISA	European Network and Information Security Agency
IC	Infraestructuras Críticas
COCIBER	Comando de Ciberdefensa de las Fuerzas Armadas
MINTEL	Ministerio de Telecomunicaciones y la Sociedad de la Información y Conocimiento
NIST	Modelo de Instituto Nacional de Estándares y Tecnología
ISACA	Asociación de Sistemas de Información, Auditoría y Control
FISMA	Federal Information Security Management Act
INCIBE	Instituto Nacional de Ciberseguridad de España
NCS	National Cybersecurity Strategies / Estrategias Nacionales De Ciberseguridad
CII	Información de Infraestructuras Críticas

Capítulo I

Introducción

Antecedentes

Las redes de comunicación son un componente importante de la vida de millones de ciudadanos (Mattioli et al., 2014). El internet, los sistemas de información y otras tecnologías digitales son la columna vertebral de la sociedad y del mercado digital. Por tal motivo muchos países se han preocupado por la seguridad de sus sistemas de información, especialmente de algunos elementos de la infraestructura que son esenciales para las operaciones de un gobierno, así como para la economía de un país, estos elementos son conocidos como Infraestructuras Críticas (Anna et al., 2016).

Según la Unión Internacional de Telecomunicaciones (UIT/ITU) infraestructuras críticas se define como: “las computadoras, los sistemas informáticos y/o las redes, ya sean físicas o virtuales, y/o los programas informáticos, datos informáticos, datos de contenido y/o datos de tráfico tan vitales para un país que la incapacidad o destrucción o interferencia con tales sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad nacional o económica, la salud y seguridad públicas nacionales, o cualquier combinación de esos asuntos”.

Los países miembros de la Unión Europea que se preocupan por la protección de su información, afirman que muchos de los sectores críticos que operan en sus estados miembros (Europa), entre ellos energía, transporte, finanzas, son quienes necesitan directamente de la Información de la infraestructura crítica (Anna et al., 2016); por tanto, si uno de estos servicios llegaría a fallar afectaría de manera superlativa tanto a la economía como a la sociedad.

El interés por la seguridad de la información referente a infraestructuras críticas ha sido tan alto, que organizaciones como ENISA (European Network and Information Security Agency) han realizado importantes estudios e investigaciones conducentes a establecer y promover buenas prácticas en estrategias de seguridad de la información, planes nacionales de contingencia y métodos de selección de IC (Infraestructuras Críticas).

En el Ecuador existen varios organismos públicos que regulan la ciberseguridad industrial y que garantizarían su incorporación progresiva en las infraestructuras de las empresas, entre estos organismos se encuentra la Secretaría Nacional de Inteligencia, el Ministerio de Telecomunicaciones, la Agencia de Regulación y Control de Telecomunicaciones y en especial el Comando Conjunto de las Fuerzas Armadas (Guerrero Fernando, s/f).

Dentro del marco del gobierno, la Secretaría de Inteligencia incorpora en su plan estratégico institucional el objetivo de ampliar los mecanismos de ciberseguridad para los sistemas de comunicación estratégicos del país y la plenitud de la información y por Acuerdo Ministerial del 12 de Septiembre del 2014, se crea el Comando de Ciberdefensa de las Fuerzas Armadas (COCIBER), con la misión de “proteger y defender la Infraestructura Crítica e Información Estratégica del Estado”, a través de operaciones de protección del ciberespacio, acciones de sospecha, retractación, disfrute y respuesta ante eventuales amenazas o incidentes. Sin embargo, hasta el momento no hay un claro reconocimiento de infraestructuras críticas para el Estado y menos aún, un modelo de selección y amparo de las mismas (Vargas Borbúa et al., 2017).

Problemática

En la actualidad, los sistemas de información y comunicación son parte importante de la sociedad y sobretodo del estado, más aún cuando existen infraestructuras críticas que proveen servicios que son fundamentales para el normal desarrollo de las actividades de un estado o de las actividades de la sociedad. Las infraestructuras críticas utilizan sistemas informáticos susceptibles de ataques cibernéticos que afectarían a su normal funcionamiento por acciones del cibercrimen o ciberterrorismo.

Las estadísticas referentes a violaciones de seguridad han sido en su grandeza dentro del sistema financiero, para el 2014, se registró un aumento de 37% de robos a la banca virtual, 14% en tarjetas de crédito y 46% en cajeros electrónicos (Vargas Borbúa et al., 2017).

El Comando Conjunto de las Fuerzas Armadas ha sido designado para el resguardo de la información estratégica del Estado, a través de la creación del COCIBER, pero aún no se tiene un detalle claro de cuáles son las infraestructuras críticas del país, mientras que el Ministerio de Defensa ha elaborado un catálogo provisional de infraestructuras críticas de manera Ad-Hoc (Vargas Borbúa et al., 2017).

El problema radica en que este catálogo no ha sido realizado mediante un proceso sistemático de investigación científica que considere la realidad político-económica del Estado, por tal motivo no ha sido validado por los stakeholders relacionados al mismo. El Ministerio de Telecomunicaciones y la Sociedad de la Información y Conocimiento (MINTEL), en su afán por promover la Política Nacional de Ciberseguridad, contempla una investigación para establecer un Modelo Nacional de Selección de Infraestructuras Críticas, sin embargo, no se ha realizado aún un trabajo que detalle los parámetros y metodologías utilizadas a nivel mundial para el desarrollo de dichos modelos y que sirva

como base para el desarrollo del modelo que se plantearía en la investigación prevista por el MINTEL.

Justificación

La cantidad de ataques perpetrados a naciones por parte de piratas informáticos han ido en aumento durante los últimos años, en un estudio sobre la ciberdelincuencia en el Ecuador se detallan varios de ataques perpetrados en los últimos años entre los cuales se destacan: apropiación ilegal (skimming / pagos en línea / phishing), Publicación, uso o transferencia no autorizada de datos personales, Hacking / virus / spam, desaparición por medios electrónicos, diseminación de información falsa / Acoso sexual / Intimidación, Producción, distribución de pornografía infantil, violación de sistemas para acceder u obtener información protegida, con un total de 2974 crímenes desde el 2013 hasta el 2017 y el incremento del 13% en el 2017 con respecto al año anterior. Además, se explica que uno de los delitos más comunes es el Acceso no consentido a una computadora, sistema telemático o de telecomunicaciones, lo que implica el nivel de deficiencia en los controles de las instituciones, especialmente en las financieras (Ron et al., 2018).

Así mismo no se cuenta como país, con un plan de protección y mucho menos de respuesta ante eventuales amenazas o incidentes que involucren la información de las infraestructuras críticas del estado.

Siendo que la identificación de la infraestructura de información crítica, es el primer paso para proteger y asegurar la disponibilidad de la información crítica del estado (Mattioli et al., 2014), el COCIBER aún no detalla ni establece un modelo de identificación de infraestructuras críticas para el Ecuador, existe, sin embargo, un catálogo establecido por el Ministerio de Defensa que no ha sido desarrollado siguiendo un proceso sistemático que refleje la realidad del país.

La presente investigación proporcionará un estudio sobre los modelos de selección de infraestructuras críticas aplicados por la ENISA y otros organismos, analizando los casos de éxito y los parámetros que han sido establecidos para el desarrollo de los mismos y establecerá al final, recomendaciones para el desarrollo de un futuro modelo nacional de selección de infraestructuras críticas.

Objetivos

Objetivo general

Realizar un análisis comparativo de los modelos de selección y protección de infraestructuras críticas utilizadas mundialmente, que sirva de base para desarrollar el Modelo Nacional de Selección de Infraestructuras Críticas en el Ecuador, como aporte a la Política Nacional de Ciberseguridad.

Objetivos específicos

Identificar el procedimiento utilizado para la selección de las infraestructuras críticas en el Ecuador.

Identificar 2 modelos de selección de infraestructuras críticas a nivel mundial, sus principios y procedimientos de aplicación.

Desarrollar un análisis comparativo de 2 modelos de selección de infraestructuras críticas.

Establecer las conclusiones del análisis y las recomendaciones (Guidelines) para la elaboración posterior de un modelo nacional de selección de infraestructuras críticas en el Ecuador.

Alcance

La presente investigación comprende un estudio de 2 metodologías para el diseño de un modelo de selección de Infraestructuras Críticas utilizadas a nivel mundial, realizando un análisis comparativo mediante parámetros definidos en el transcurso de la investigación, los 2 modelos seleccionados para el análisis son: El Modelo de la ENISA (Unión Europea), y el Modelo de Instituto Nacional de Estándares y Tecnología (NIST) (Estados Unidos). Se analizan también, los problemas encontrados en el diseño del catálogo desarrollado por el Ministerio de Defensa del Ecuador, enfocando las necesidades y la realidad político-económica del estado, con el fin de proveer de recomendaciones (Guidelines) para el desarrollo del modelo nacional de selección de Infraestructuras Críticas del país. Esta investigación cuenta con el aval del Ministerio de Telecomunicaciones, quien ha trazado la meta del desarrollo del modelo.

Para el desarrollo de la presente investigación, se detallan a continuación varias preguntas de investigación asociadas a los objetivos específicos planteados.

Preguntas de investigación

Para definir y guiar el desarrollo de la presente tesis se plantearon las siguientes preguntas de investigación:

Tabla 1
Preguntas de investigación del proyecto de investigación

Objetivo Específico	Pregunta de Investigación
Identificar el procedimiento utilizado para la selección de las infraestructuras críticas en el Ecuador.	RQ1: Cuál es el problema con el procedimiento de selección de Infraestructuras Críticas

Objetivo Específico	Pregunta de Investigación
	RQ2: Cuál es la política de estado en torno a la Ciberdefensa de infraestructuras críticas
Identificar 2 modelos de selección de infraestructuras críticas a nivel mundial, sus principios y procedimientos de aplicación.	RQ3: Cuáles son los modelos de éxito de selección de infraestructuras críticas
	RQ4: Cuáles son los lineamientos de los 2 modelos seleccionados para el análisis.
Desarrollar un análisis comparativo de los 2 modelos de selección de infraestructuras críticas.	RQ5: Cuáles fueron los parámetros utilizados para la selección de Infraestructuras críticas
	RQ6: Cuáles son las metodologías aplicadas para la selección de Infraestructuras Críticas en el mundo
Establecer las conclusiones del análisis y las recomendaciones (Guidelines) para la elaboración posterior de un modelo nacional de selección de infraestructuras críticas en el Ecuador.	RQ7: Cuáles son las recomendaciones hacia el Ministerio de Defensa para el desarrollo del modelo de selección de infraestructuras criticas

Objetivo Específico	Pregunta de Investigación
	RQ8: Es posible el desarrollo de un modelo nacional de selección de Infraestructuras Críticas

Hipótesis

No todos los elementos de los modelos de selección de infraestructuras críticas son aplicables a la realidad del estado ecuatoriano y sus infraestructuras críticas.

Variables

Variable independiente.

- Modelos de Selección de Infraestructuras Críticas

Variable dependiente.

- Infraestructuras Críticas en el Ecuador

Capítulo II

Marco teórico

En este capítulo se presenta el marco teórico que se sustenta en la especificación de la red de categorías para las variables independiente y dependiente, establecidas en la Hipótesis, en el Capítulo I.

Señalamiento de variables

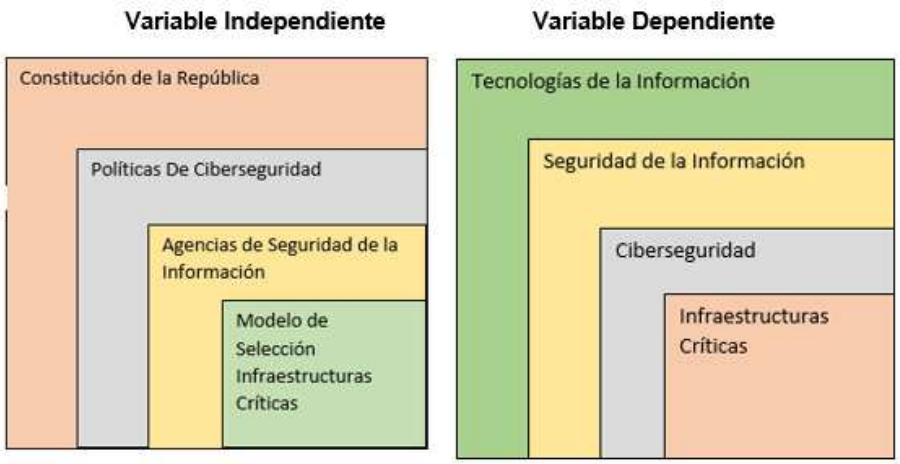
Variable independiente: Modelos de Selección de Infraestructuras Críticas
Variable dependiente: Infraestructuras Críticas en el Ecuador

Red de categorías

En el ámbito de fundamentar el marco teórico de la investigación planteada, se ha establecido una red de categorías principales que influyen en el objeto de estudio de la investigación. A continuación, se muestran los esquemas de la categorización de las variables Independiente y Dependiente.

Figura 1

Red de categorías para las variables de investigación



Seguridad de la información

Para empezar a definir lo que es la Seguridad de la Información, se debe tener presente que significa Seguridad. Según la Real Academia Española (RAE), la seguridad se define como “libre y exento de todo peligro, daño o riesgo” (RAE, s/f-a), pero puede ser visto como “una condición ideal”, porque no se puede tener certeza de que se pueda evitar todo daño, riesgo o peligro. De allí, que el propósito de la seguridad es el de intentar reducir todos los riesgos y mitigar las amenazas que puedan poner en riesgo o peligro al activo que se trate. (Mendoza, 2015).

Una vez definida la seguridad, se trata de enfocar ahora la seguridad de la información. La información enfocada como “el activo más importante de una organización”, puede presentarse de diferentes maneras, entre las cuales podemos encontrar:

- Digital: información que engloba el ambiente electrónico o medios digitales.
- Física: información que engloba el ambiente escrito o impreso en papel.
- No Representada: información que engloba las ideas de las personas.

Sin embargo, sin importar como se presente la información necesita medidas de protección que aseguren su autenticidad de acuerdo al valor de la mismas, y es allí donde la seguridad de la información juega un papel importante (Mendoza, 2015).

Por lo tanto, la seguridad de la Información puede ser definida como “un proceso por el cual se da cabida a un creciente número de elementos: aspectos tecnológicos, de gestión-organizacionales, de recursos humanos, de índole económica, de negocios, de

tipo legal, de cumplimiento, etc.; abarcando no sólo aspectos informáticos y de telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc."(Bertolín, 2008).

En un principio la seguridad de la información comenzó a ser empleada solo por entornos militares, diplomáticos y gubernamentales, luego paso a ser una necesidad empresarial, considerándose como un gasto necesario para permitirse ser competitivo en los negocios, mas hoy en día, es considerado una obligación para que empresas tanto públicas como privadas salvaguarden su información y no queden desprotegidas desde el punto legal, frente a leyes y reglamentos, por tal motivo Bertolín, define a la seguridad de la información como un *activo estratégico* que no puede estar separado del núcleo de toda organización. (Bertolín, 2008).

En referencia a esta tesis, se va a enfocar únicamente en la seguridad de la información digital.

Ciberseguridad

De acuerdo con la ITU, la ciberseguridad es definida como "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, garantía y tecnologías que pueden utilizarse para proteger el entorno cibernético y la organización y los activos de los usuarios. La organización y los activos del usuario incluyen dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información transmitida y / o almacenada en el entorno cibernético" (ITU, s/f).

Desde hace mucho tiempo atrás las amenazas latentes han envuelto a las empresas y a los gobiernos en la protección y aseguramiento de su información, dentro del ámbito de la seguridad de la información, la ciberseguridad se encarga de salvaguardar y proteger el entorno cibernético de una organización incluyendo su información. La Asociación de Sistemas de Información, Auditoría y Control (ISACA), define a la ciberseguridad como la "protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". Tomando en cuenta que podemos deducir que un "activo de información" son los datos, información o conocimiento que tiene un valor para una organización. Por lo tanto, podemos afirmar que la ciberseguridad está comprendida dentro del ámbito de la seguridad de la información y se encarga de la protección de la información presentada de manera digital, de igual forma de la tecnología utilizada para su tratamiento.

Cuando se habla de ciberseguridad, es inminente hablar sobre el ciberespacio y sus amenazas más latentes, el ciberespacio es un entorno no físico que lo componen equipos tecnológicos de información junto con la infraestructura de redes que los interconecta (Newmeyer, 2015). Una vez definido el ciberespacio se encuentran también las amenazas que tiene que sortear, estas amenazas existen y se renuevan día tras día de forma continua y entre las cuales tenemos la ciberguerra, el ciberterrorismo y el cibercrimen.

Ciberguerra

La guerra ha sido uno de los problemas más grandes de la humanidad desde su creación o su evolución, el ser humano es competitivo y belicoso y muchas veces resalta

por sus defectos más que por sus virtudes, por otro lado, sus causas son propias de las de un ser humano, competencia, afán de adquirir algo, orgullo, etc. (Brechner, 2016).

El termino ciberguerra es descrito por la Armada de los Estados Unidos como “un escalado conflicto cibernético entre estados”, es decir por este medio se ha utilizado el ciberespacio para realizar ataques cibernéticos a infraestructuras cibernéticas con fines delictivos y lucrativos (Bustamante, Fuertes, Toulkeridis, & Ron, 2018).

La ciberguerra, hoy en día, han convertido a los objetivos de las agencias militares de potencias mundiales en encontrar vulnerabilidades tecnológicas en sistemas de información e infraestructura tecnológica del enemigo para penetrarlas y atacarlas con el objetivo de robar información sensible que pudiera afectar al normal funcionamiento de, en el caso de estados, la sociedad civil, económica y política, más, sin embargo, el objetivo del gobierno de un estado no necesariamente es la voluntad nacional de una nación.

Varios autores han catalogado a la ciberguerra como una *guerra moderna* que se diferencia en gran medida de la guerra tradicional, Jeffrey Car define a la ciberguerra como “arte y la ciencia de luchar sin luchar. de derrotar a un oponente sin derramar su sangre” (Taddeo, s/f), sin embargo, asegurar que no se derrama sangre es una aseveración que puede estar distante de la realidad, ya que un ataque cibernético sobre las infraestructuras criticas de una nación, como el sistema financiero, la red eléctrica, etc. Puede producir perdida de vida en la sociedad civil.

Por otro lado, la ciberguerra también puede considerarse como el intento de tomar el control referente a la información y comunicación, con el objetivo de tener una ventaja sobre un oponente, mediante la realización y preparación de operaciones militares para investigar sobre “quien es”, “donde esta”, “que puede hacer”, “cuando puede hacerlo”, “que amenazas contrarrestar primero”, etc., es decir, trata de equilibrar la información y

el conocimiento en favor de uno mismo, especialmente sin que sea necesario gastar capital o mano de obra (Robinson et al., 2015).

De aquí que se puede producir otro termino interesante que tiene una relación directa con la ciberguerra, que es denominado la *guerra de la información*.

Guerra de la información.

El termino de guerra de información ha sido utilizado a lo largo de los años, Thomas Rhona define a la guerra de la información como “Las competencias a nivel estratégico, operativo y táctico en todo el espectro de paz, crisis, escalada de crisis, conflicto, guerra, finalización de la guerra y reconstitución / restauración, realizadas entre competidores, adversarios o enemigos utilizando medios de información para lograr sus objetivos” (Robinson et al., 2015).

Por otro lado, Martin Libicki nos expone 7 formas de guerras de la información.

Tabla 2

Las 7 formas de guerra de la información según Libicki.

Formas	Descripción
Comando y Control	Ataques sobre centros de comandos o sobre los comandos mismos para interrumpir su efectividad
Basado en la inteligencia	Aumenta su propia conciencia situacional y al mismo tiempo reduce la capacidad del enemigo.
Electrónico	Emplea el uso de criptografía y la degradación de la base física para transferir información

Formas	Descripción
Psicológico	Uso de la información contra la mente humana. Propaganda para desmoralizar a las tropas o influir en las poblaciones civiles.
Hacker	Utilización de virus sobre sistemas informáticos, se emplean bombas lógicas, troyanos, etc.
Información económica	Posesión y control de la información para llegar al poder
Cyber	Terrorismo a nivel informativo, ataques semánticos, guerras simuladas.

Nota: Tomado de (Robinson et al., 2015)

Ciberterrorismo

Resulta difícil encontrar una definición universal para el término del terrorismo, según la RAE, se define al terrorismo como una "sucesión de actos de violencia ejecutados para infundir terror" o también como el acto criminal realizado por bandas organizadas cuyo objetivo es crear alarma en la sociedad, por lo general, con fines políticos. (RAE, s/f-b).

Con respecto al ciberterrorismo, Subijana asegura que para definirlo se lo debe analizar desde dos perspectivas, una medial y otra final.

La perspectiva medial se refiere al aprovechamiento de las tecnologías de la información y comunicación por parte de los grupos terroristas para lograr sus fines maliciosos. Por lo tanto, se afirma que, desde esta perspectiva, el ciberterrorismo se constituye en base a dos elementos: un grupo terrorista y el uso de medios que provengan de una infraestructura tecnológica para lograr una capacidad delictiva mayor. Con relación a este criterio el Consejo de Europa define al ciberterrorismo como la forma de realizar terrorismo por medio del uso de infraestructuras tecnológicas con el objetivo de

intimidar, coaccionar o causar daños a grupos sociales con fines políticos o fines religiosos. (Subijana, 2008).

Por otro lado, en referencia a la perspectiva final, Subijana afirma que se relaciona con la devastación de información sensible contenido dentro de sistemas tecnológicos o informáticos. Con el pasar de los años, la tecnología ha ido evolucionando de maneras exponenciales, esto ha producido la informatización de sectores básicos como servicios públicos y sobretodo infraestructuras críticas, donde se incluyen sistemas bancarios y bursátiles, sistemas de transporte, sistemas energéticos, etc. Por lo tanto, se puede afirmar que, son objetivos codiciosos para un ataque terrorista, donde un posible ataque de dichos servicios puede producir consecuencias catastróficas para la economía de una nación. Por cual, desde este punto de vista se ha definido al ciberterrorismo como un ataque ilegal sobre equipos informáticos, sus redes y la información contenida en ellos con el fin de intimidar a un estado o a su población para lograr objetivos sociales, políticos o religiosos. (Subijana, 2008).

De lo anterior y juntando las dos perspectivas se puede definir al ciberterrorismo como cualquier acto realizado por medio de la utilización de tecnologías de la información y comunicación con el objetivo de causar directa o indirectamente terror o generar daños que pueden ser considerados maliciosos hacia un grupo social o político mediante la destrucción de infraestructuras tecnológicas consideradas críticas o fundamentales para el normal desarrollo de una nación y sus habitantes.

Cibercrimen

A pesar de que en la actualidad el delito relacionado con las TIC sigue causando sorpresa entre varios sectores de la sociedad, lo cierto es que ha formado parte de la criminología desde el siglo pasado, esto se ha reflejado, puesto que muchas personas le

han restado importancia a este tipo de delitos, mientras que otras personas exageran el nivel de amenaza que pueda producir. De cualquier forma, el concepto de cibercrimen es muy amplio y abierto. (Ron et al., 2018).

El término cibercrimen (*cybercrime* en inglés) es atribuido a Jhon Perry Barlow, teórico de la Sociedad de la Información y de Internet. (Miró Linares, 2012).

El cibercrimen o ciberdelito hace referencia a la actividad criminal que es llevada a cabo por medio del uso de equipos informáticos o el internet. Además, el cibercrimen puede utilizar diferentes herramientas y/o métodos, como el phishing, spyware, ransomware, etc, cuyo destino es la sustracción de la información personal con el fin de realizar actividades criminales. El cibercrimen se ha convertido en uno de los delitos más beneficiosos para delincuentes, debido a que este tipo de crimen se ha erigido como una de las mayores amenazas debido a la influencia y el protagonismo que ha generado el uso de equipos informáticos como tablets, equipos portátiles, smartphones, etc en la sociedad actual. (Avast, s/f).

Por otro lado, Gordon & Ford en su trabajo recopilan otras definiciones sobre el termino, el cibercrimen tiene muchas facetas sobre las cuales incurre, sobre todo en los escenarios y los entornos sobre los cuales se desenvuelve, en el Tratado de Cibercrimen del Consejo de Europa definen al termino del cibercrimen como una actividad delictiva que pueden abarcar desde robo de información hasta contravenciones de contenido y derechos de autor, sin embargo, para Zeviar-Geese, la definición del termino es mucho más amplia pues también se deben incluir actividades como fraude, acceso no autorizado, acoso cibernético y pornografía infantil. (Gordon & Ford, 2006).

Infraestructuras críticas

Existe un determinado grupo de instalaciones, edificaciones y/o departamentos que son de vital importancia para el normal desarrollo de un estado o de la sociedad del mismo, a estas infraestructuras se las ha denominado como Infraestructuras Críticas.

Cuando hablamos sobre infraestructuras críticas tenemos que pensar en sistemas físicos y virtuales cuyos funcionamientos y servicios son esenciales para respaldar a los sistemas económicos, sociales y ambientales de un estado. El Departamento de Seguridad de los Estados Unidos da a conocer a las infraestructuras críticas como aquellas que son tan vitales para un país o nación que una destrucción parcial o total en sus activos, sistemas o redes, sean físicas o virtuales, puede desencadenar en un efecto debilitante sobre la seguridad física, económica y/o pública. (Pagnotta, 2017).

Dada la naturaleza de este concepto, se puede apreciar que este es un espectro de instalaciones muy grande, por lo que pueden abarcar las siguientes infraestructuras.

- Instalaciones Químicas
- Instalaciones Comerciales
- Comunicaciones
- Fabricación Crítica
- Represas
- Bases Industriales de Defensa
- Servicios de Emergencia
- Energía
- Servicios Financieros
- Alimentación y Agricultura
- Instalaciones Gubernamentales

- Salud Pública
- Tecnologías de la Información
- Reactores, materiales y residuos nucleares
- Sistemas de transporte
- Sistemas de agua y agua residual

Dicho esto, se puede apreciar que se trata de sistemas, redes, activos prioritarios para la disponibilidad perpetua y normal funcionamiento de una sociedad. No obstante, las infraestructuras críticas son semejantes en todos los países, sin embargo, dependiendo de cada nación y su relevancia a nivel mundial, puede cambiar su estructura en relación a sus necesidades y a su nivel de desarrollo.

¿Qué es crítico?

En la actualidad, la sociedad vive una vida moderna, la cual, se maneja mediante la interconexión de una abundancia de infraestructuras muchas de ellas consideradas críticas. Sectores como la alimentación, el agua, la salud y el transporte y su infraestructura siempre han sido considerados críticos, sin embargo, las tecnologías de la información han ocasionado que su funcionamiento se convierta en un componente esencial de la vida.

En muchas ocasiones, el ciberespacio y sus componentes, son considerados como un sector discreto para la sociedad, pero lo cierto es que están tan profundamente ligados a sectores como el energético y el de transporte que hace que la conjunción de los mismos se traduzca en un sector de vital importancia para un país. Pero no solo dichos sectores se benefician del ciberespacio, Clemente, afirma que el ciberespacio puede ser visualizado como una analogía a un sistema nervioso, en el que el ciberespacio atraviesa

todos los demás sectores y les permite comunicarse y funcionar entre sí. (Clemente, 2013).

En 2011 Chatam House, realizó un informe sobre lo que se debe considerar como información crítica dentro de una sociedad moderna, dentro del mismo se plantean varias interrogantes que se debe tomar en cuenta para la protección de la información, como, por ejemplo, ¿Cuál es la medida en la que la dependencia de la tecnología en las sociedades, hace que las mismas se vuelvan vulnerables?, o, ¿cómo asegurar la economía y las libertades en la sociedad al mismo tiempo que se formulan propuestas y respuestas para combatir las amenazas al ciberespacio?, etc. Muchas preguntas que con el desarrollo de esta investigación pueden llegar a esclarecerse, pero, por otro lado, lo que sí nos ha quedado claro, es que, según Chatam House, es necesario esclarecer y sobretodo especificar la necesidad primar e invertir en medidas de seguridad. (Clemente, 2013).

Políticas de ciberseguridad

La seguridad informática es una preocupación latente en la actualidad, empresas grandes o pequeñas se preocupan por la seguridad de su información y, de la misma manera, de los posibles ataques que pueda sufrir su infraestructura. El ciberespacio ha pasado a ser uno de los términos más importantes dentro de la seguridad pública de una nación.

Para empezar a hablar sobre la seguridad pública enfocada en las tecnologías de la información es necesario entender sobre la soberanía de un estado o nación. Ethan Katsh, afirma que los seres humanos habitan dentro de espacios interconectados que limitan un territorio sobre cada uno de los estados soberanos. Según Rabinad, la

soberanía se define como “el ejercicio del poder supremo del Estado dentro y fuera de su territorio, en los casos de extraterritorialidad”. (Rabinad, 2008).

Frente a esta realidad, es innegable que el estado tenga cierta preocupación sobre los riesgos a los que se enfrenta en el ciberespacio, por ende, la ciberseguridad se vuelve un tópico importante en el desarrollo de la seguridad pública. La ciberseguridad y el ciberespacio son un problema transversal, y su problemática artificial dista mucho de ser una realidad. La ciberseguridad, como tal, supone un nuevo paradigma de seguridad global debiendo enfocarse en la inclusión de la totalidad de escenarios que pueden ser afectados por la existencia del uso del ciberespacio.

Para Carrillo, el ciberespacio incluye también un “nuevo modelo socio-político”, esto quiere decir que, la globalización de la vida social ha permitido graficar de mejor manera este fenómeno que hasta hace muy poco tiempo no era considerado ni conflictivo ni peligroso, cuando la realidad del modelo socio político y territorial del Estado, solo brindaba la protección una protección básica. (Carrillo, 2015).

De acuerdo a lo expuesto, nos podemos hacer la siguiente interrogante, ¿Quién gobierna el ciberespacio? Para Rabinad, la complicad red de relaciones en el ciberespacio deja abierta la posibilidad de conflicto en materia penal, civil, comercial o administrativa, se habla de un “lugar” donde se conjugan todo tipo de relaciones y asociaciones, desde familiares o de amistad, hasta relaciones comerciales o inclusive relaciones entre ciudadano y estado. Por esto, es que cada una de las ramas del derecho se debe sujetar a las nuevas tecnologías y ofrecer una solución a los posibles conflictos que se puedan suscitar. (Rabinad, 2008).

En la actualidad, el impacto de la tecnología dentro de la sociedad moderna ha sido enorme, pero no del todo positivo, especialmente por las actividades que genera dentro de las vidas humanas tanto en jóvenes, como en adultos. El uso de las tecnologías

de la información y comunicación ha crecido exponencialmente y esto conlleva al deseo de servir al desarrollo del país en materia de riesgos y como estos pueden llegar a afectar los derechos de las personas, la seguridad pública, las infraestructuras críticas y en esencial la seguridad de un país, estos riesgos pueden ser manifestados de diferentes maneras, ataques realizados por medio de espionajes, sabotaje, fraudes, etc. (Franco Crespo, 2013).

La obligación de una nación se cimienta en la necesidad de poseer una política que oriente al país en ciberseguridad y la protección del ciberespacio y el hecho de implementar medidas que cooperen en la seguridad de los usuarios dentro del ciberespacio incluyendo también, estrategias en la educación que estén orientadas al cuidado y la prevención dentro del ambiente digital y tecnológico.

¿Por qué se requiere una política nacional de ciberseguridad?

Según el Gobierno de Chile, la necesidad de una política de ciberseguridad se fundamente en 4 puntos esenciales:

- **Para resguardar la seguridad de las personas en el ciberespacio**

  La libertad de la sociedad en el acceso a la información y la libertad de expresión, así como también el normal desempeño en las actividades personales, sociales y comunitarias contempladas dentro del ciberespacio, garantizando la protección de la vida y la propiedad intelectual.

- **Para proteger la seguridad del país**

  El funcionamiento del país depende esencialmente del resguardo de las redes y sistemas informáticos tanto en entes públicos como privados, asegurando la operatividad en los servicios básicos.

- **Para promover la colaboración y coordinación entre instituciones**

  La comunicación entre organizaciones del sector público como privado tanto a nivel nacional e internacional es esencial para fortalecer las respuestas a los riesgos que promueven las actividades del ciberespacio.

- **Para gestionar los riesgos del ciberespacio**

  Analizar y gestionar las vulnerabilidades, amenazas y riesgos que implican el uso del ciberespacio y desarrollar procesos de gestión de los mismos para la prevención y recuperación frente a incidentes, haciendo de esta manera que el ciberespacio se convierta en algo estable y resistente.

Por ende, podemos establecer que las redes y los sistemas de información de la Defensa Nacional del estado componen una infraestructura crítica, la cual establece riesgos para la seguridad exterior y la propia soberanía del país. Durante el desarrollo de la política se establecerán, se prepararán y se publicarán políticas detalladas en materia de Ciberdefensa que decretarán los caminos en los cuales se protegerán las redes y como la Defensa Nacional puede colaborar en la enseñanza de un ciberespacio libre, abierto y seguro para el estado. (Chile, 2017)

Agencias de seguridad de la información

Se ha establecido que la ciberseguridad es uno de los tópicos principales alrededor del mundo, por ende, se han establecido varios organismos que apoyan en el desarrollo de políticas, leyes, normas, buenas prácticas, etc., enfocadas en la seguridad de la información de las IC.

ENISA

La Agencia Europea de la Seguridad de las redes y de la información (ENISA – European Union Agency for Cybersecurity) fue creada en el año de 2004 mediante el Reglamento (CE) N° 406/2004 por orden del Parlamento Europeo y del Consenso, específicamente el 10 de marzo de 2004. (Parlamento Europeo, 2014).

Se encuentra localizada en Grecia, específicamente en Atenas con una sucursal en Heeraklion, localidad también del país griego.

La ENISA preocupada por los incidentes relacionados a la seguridad de la información contribuye de manera activa a la Política Europea de Ciberseguridad, apoyando a cada uno de los estados miembros de la Unión Europea a dar respuestas a diferentes incidentes referidos a sustracción o infiltración del ciberespacio sucedidos a gran escala. (ENISA, s/f)

La colaboración que ofrece la ENISA está inmersa en la unión en conjunto el sector privado para brindar asesoramiento que puede incluir:

- Desarrollo y evaluación de estrategias de ciberseguridad
- Desarrollo y cooperación mediante CSIRT's
- Investigación sobre Internet de las Cosas (IoT) e Infraestructuras críticas abordando problemas sobre protección de la información, servicios confiables y análisis de amenazas del ciberespacio.

Otro de los aspectos en los que organizaciones como la ENISA brindan su apoyo, es en el desarrollo y la implementación de la política y la ley de la Unión Europea involucrado en materia de seguridad de las redes y la información (NIS) incluyendo también el desarrollo de políticas de divulgación de vulnerabilidad. (ENISA, s/f).

- ENISA se enfoca principalmente en las siguientes actividades:

- Recomendaciones y buenas prácticas sobre ciberseguridad y asesoramiento en los mismos temas.
- Asesoramiento sobre actividades que impulsan la formulación de políticas.
- Laboratorios prácticos en los que se colabore directamente con equipos operativos de la UE
- Trabajar en conjunto con todos los estados miembros para coordinar respuestas a incidentes de ciberseguridad.
- Elaboración de esquemas de certificación de ciberseguridad.

NIST

El Instituto Nacional de Normas y Tecnología (NIST – National Institute of Standards and Technology) fue fundada en el año de 1901, es uno de los departamentos de ciencias físicas más añejos de los Estados Unidos de América, establecido para hacer frente a la competitividad industrial, que por esos años era sumamente inferior comparada con rivales estratégicos como Reino Unido, Alemania, etc.

Hoy en día, el NIST pertenece al Departamento de Comercio de los Estados Unidos y su misión es la de incentivar la innovación y la contienda industrial por medio de avances tecnológicos, normas, buenas prácticas que perfeccionen la calidad de vida de la sociedad en general. (Materese, 2015).

El NIST cumple un papel fundamental dentro de la llamada Ley Federal de Administración de la Seguridad de la Información Federal Information Security Management Act, (FISMA) promulgada por la ley federal de los Estados Unidos en la que se impone que las agencias federales (infraestructuras críticas) desarrollen e implementen programas de seguridad y protección de la información, de esta manera el

NIST desarrolla estándares y directrices de seguridad, como por ejemplo FIPS 199, FIPS 200 y la serie SP 800.

El gobierno se apoya en el NIST para proteger los sistemas de información de posibles ataques cibernéticos, fallas humanas, catástrofes naturales, que puedan llegar a afectar sus funciones, su misión o hasta inclusive su imagen o reputación, utilizando la base de datos NIST 800-53 para establecer controles de privacidad y seguridad en operaciones organizativas. (Sciallo, 2019).

INCIBE

Otro de los organismos que apoya en la gestión de seguridad de la información es el Instituto Nacional de Ciberseguridad de España (INCIBE).

INCIBE, anteriormente conocido como Instituto Nacional de Tecnologías de la Comunicación, es un organismo que depende exclusivamente del Ministerio de Economía y Empresa de España, que funge como la entidad que desarrolla estrategias de ciberseguridad y protección de la información del estado (*Qué es INCIBE*, 2016).

INCIBE funge como un instrumento del gobierno de España para reflejar la confianza digital hacia sus ciudadanos y cuyo objetivo es progresar en temas de ciberseguridad para la evolución del estado en materia de transformación social y de innovación.

El INCIBE cuenta con una serie de agencias que atienden los diferentes aspectos de la ciberseguridad, los que son:

- INCIBE Cert: es el primer equipo de respuestas ante emergencias relacionadas con la ciberseguridad, entre sus objetivos se encuentran la de prevenir, mitigar y responder cualquier ataque cibernético relacionados con empresas e infraestructuras críticas incluyendo a ciudadanos.

- OSI: conocida como la Oficina de Seguridad de Internauta, su objetivo es buscar las buenas prácticas de seguridad de la información enfocadas hacia los usuarios, y la responsabilidad de estos con sus actos, minimizando el número de ataques que pueda recibir.

Según Samaniego, el INCIBE se concentra en 4 pilares fundamentales para lograr cumplir su misión:

- Prestación de Servicios
- Fomentar la Investigación
- Promoción y detección de talento
- Refuerzo de la organización

Todo esto orientándose hacia empresas y organizaciones del sector estratégico crítico, como, por ejemplo, plantas energéticas, centros de telecomunicaciones, mercados financieros, etc. (Samaniego, 2018).

Gestión de riesgos

Todas las guías de buenas prácticas y modelos de selección de infraestructura críticas evocan diferentes componentes como claves para el éxito del cuidado de las mismas, una de las más importantes es la Gestión y/o Análisis de Riesgos

“Por riesgo se entiende, al estado objetivo latente que: Presagia o anuncia probables daños y pérdidas futuras” (Toulkeridis et al., 2015).

De esta manera, podemos afirmar que la gestión del riesgo apoya en la necesidad de presagiar la posibilidad de un evento que de alguna manera pueda llegar a considerarse como problemático o que llegue a tener una consecuencia negativa para la planificación o el resultado de un determinado producto.

La gestión de riesgos se encuentra presente en varios ámbitos y distintos giros de negocio, es así que existe gestión de riesgos laborales, bancarios, corporativos y, sobretodo, de seguridad de la información. Los responsables de la gestión de riesgos tienen sensatez en eje a la existencia de distintas amenazas que pueden provocar riesgo para lograr sus objetivos planteados. El objetivo de una gestión de riesgos es mantener en un nivel consensuado por la organización los peligros, de tal manera emplean esfuerzo y recursos para lograr este objetivo.

Las organizaciones se encuentran cambiando sus directrices y la gestión de riesgos no es la excepción, se debe realizar un trabajo metódico, estructurado, pero sobretodo seguir una metodología que conlleve un perfeccionamiento continuo de los procesos adoptados, con el objetivo de garantizar que la gestión conlleve a éxitos tanto en el presente como en el futuro (INCIBE, s/f).

Dentro de la Gestión de riesgos encontramos ciertos términos utilizados, la Figura 2, muestra la relación entre ellos:

- **Activo**: recurso de la organización que es imprescindible para desarrollar las tareas diarias de una organización, el objetivo final de la gestión de riesgos es la protección de los activos, su valoración es fundamental en una evaluación del riesgo.
- **Amenaza:** situación perjudicial que puede suceder y cuando ocurre puede acarrear consecuencias negativas sobre los activos de una organización causando perdida de funcionalidad o perdida en su valor.
- **Vulnerabilidad:** debilidad de un activo que puede facilitar el surgimiento de una amenaza.

- **Impacto:** es la consecuencia del surgimiento de una amenaza, se suele evaluar mediante el porcentaje de degradación que altera el valor del activo, si es 100%, el activo ha perdido todo su valor.
- **Probabilidad:** es la posibilidad del acontecimiento de un suceso, la probabilidad implica directamente en la amenaza. Se puede estimar

Figura 2

Términos de la gestión de riesgos

Nota: Tomado de (INCIBE, s/f)

Nivel de riesgo

El nivel de riesgo es una aproximación de lo que pudiera suceder, de acuerdo al impacto que ocurre cuando se materializa una amenaza, generalmente se llega a valorar de forma cuantitativa como el producto de la consecuencia (impacto) de una amenaza por la probabilidad de que ocurra.

Figura 3

Calculo del riesgo

Nota: Tomado de (INCIBE, s/f)

Varios de los daños producidos con la materialización de una amenaza afectan a los activos de diferentes maneras, como pueden ser:

- Daños personales
- Pérdidas financieras
- Interrupción del servicio
- Perdida de reputación
- Disminución del rendimiento

La gestión del riesgo debe definir un umbral de riesgo, que es definido como un límite máximo de riesgo al cual la organización está dispuesta a soportar.

Pero, que se debe hacer con los riesgos. La finalidad de una buena gestión de riesgos mitigar los riesgos, pero para esto, una organización debe realizar dos grandes tareas.

- Análisis de Riesgos
- Tratamiento de los riesgos

Análisis de riesgos.

La protección de las Infraestructuras críticas pretende la ejecución de una evaluación de riesgos cuyo objetivo final sea establecer acciones a realizar o que componentes y medidas deben ser adoptadas para minorar el riesgo que ha de afrontarse.

El riesgo ha existido desde siempre como una acción propia del ser humano, sin embargo, en la actualidad, en un ambiente completamente tecnológico, en el cual, los epicentros de las actividades son las son las herramientas de TI, la dependencia de las mismas las ha transformado en un factor de riesgo importante e incluso etiquetado como uno de los más importantes de este siglo. De la misma manera, es conocido que no existe tecnología perfecta, todas pueden tener deficiencias, vulnerabilidades y fallas, pero los procesos de negocios, tanto en ámbito privada como en el público, dependen de las TI, de tal manera es necesario hacer una gestión de los posibles riesgos, ya que, de no realizarlo podrían generar gastos que se vean afectados a la organización (Gómez et al., 2010).

Como primer punto de la seguridad de la información es considerado el análisis de riesgos, de tal manera, que para realizar una gestión de los riesgos se tiene que tomar la decisión de eliminarlos, ignorarlos, transferirlos o mitigarlos, pero antes de ejecutar cualquier proceso de mejora en la seguridad de las TI se necesita conocer la prioridad de las aplicaciones y/o tecnologías y los lineamientos que pueden ser aplicados (Valarezo et al., 2016).

Cuando se producen esta clase de eventos accidentales, el conocimiento del público se modifica de forma dramática, ya que puede colocar en gran dificultad el papel que desempeña una organización en la sociedad, de tal manera el prestigio que pudo haber ganado durante toda su vida institucional se puede ver comprometido y reducido, por eso, es necesario saber identificar el nivel de amenaza al que se está enfrentando y como hacerle frente.

Una singularidad del riesgo es su naturaleza subjetiva, es decir, que muchas veces puede ser considerado como inaceptable, así como también, otras será considerada como admisible. Por esta razón, cualquier organización debe comprender y

fijar un umbral de riesgo tolerable y aceptable, tomando en cuenta la actividad del negocio al que se está protegiendo, por lo cual, el análisis de riesgos tiene que basarse en procesos con principio de valoración, objetivos y homogéneos que posibiliten conseguir valores que han de compararse.

La ciberseguridad en los ambientes industriales que más dependen de la tecnología empiezan a tomar una relevancia mayor, puesto que, el impacto que sería capaz de tener gran un ciberataque sobre estos sistemas y las infraestructuras que lo soportan. Estos ataques a infraestructuras críticas son como el pan de cada día y por ello cada país o nación realiza un enorme esfuerzo por incrementar los niveles de ciberseguridad (INCIBE, s/f).

Existen varias modelos para un análisis de riesgos, en la Figura 4 se muestran sus principales componentes y las relaciones entre ellas

Figura 4

Marco Conceptual del modelo de análisis de riesgos

Nota: Tomado de (INCIBE, s/f)

Entre los componentes que se analizan son:

- Activos: recursos que normalmente son técnicos estos son asociados, por lo general, a la operación de la organización.
- Vulnerabilidades: es la estimación de que un activo presente una amenaza, se lo puedo medir en frecuencia de aparición o degradación causada.
- Amenazas: es un suceso que puede desencadenar en un incidente y que va a afectar a los activos.
- Impactos: es el resultado de que una o más amenazas se hayan concretado.

Tratamiento del riesgo

Las organizaciones deben conocer los riesgos de acuerdo a metodologías y guías de buenas prácticas. Para los distintos procedimientos de riesgos se pueden realizar diferentes tareas:

- Evitar o eliminar el riesgo

  Se lo puede hacer eliminando el activo o sustituyéndolo, de la misma manera se puede actuar con la actividad que está afectando.

- Reducir o mitigar el riesgo

  Tomar medidas para que el riesgo quede por debajo del umbral de riesgo, se puede aplicar tomando en cuenta la frecuencia del riesgo y la probabilidad del impacto, de esta manera se debe tomar las medidas necesarias para que no afecte tanto a las actividades y/o recursos.

- Transferir o compartir el riesgo

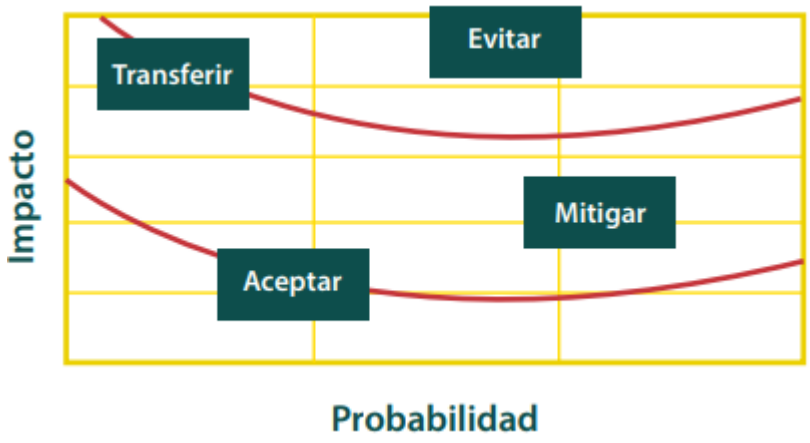
  Cuando la organización no tiene la capacidad para afrontar el riesgo y debe traspasarlo a un tercero para que sea tratado.

- Aceptar el riesgo

Se lo acepta cuando no supera el umbral de riesgo, verificando el impacto que pueda tener en los activos y actividades, o también, cuando, a pesar del impacto, la empresa no desea perder la oportunidad de negocio a la que está asociada.

Figura 5

Tratamiento del riesgo



Nota: Tomado de (INCIBE, s/f)

Capítulo III

Metodología

En este capítulo se procede a detallar el uso de una metodología de investigación ad-hoc de carácter exploratoria, apoyándose en el método deductivo, por el cual se pretende realizar una selección de las métricas en las que se basan las metodologías para la selección de infraestructuras críticas.

Para el desarrollo de esta metodología se ha realizado una investigación exhaustiva de documentos relacionados con la seguridad de la información y las entidades encargadas de emitir estos documentos. Los pasos detallados para la metodología propuesta son:

- Investigación: búsqueda y selección de documentación referente a metodologías y guías de buenas prácticas referentes a la seguridad de la información.
- Definición: definición de criterios para el análisis comparativo entre los documentos seleccionados.
- Validación: Aplicación del método comparativo para la producción de resultados.
- Análisis: Conclusión y recomendaciones sobre los resultados obtenidos.

Como resultado se espera obtener una guía de recomendaciones que sea un aporte para el desarrollo de un Modelo de Selección de Infraestructuras Críticas apoyados en el criterio de selección de modelos utilizados por diferentes organizaciones y países desarrollados y en desarrollo, analizando la situación actual del Ecuador y su postura ante las amenazas latentes concernientes a ciberseguridad.

De esta manera, se pretende demostrar la hipótesis planteada y a la vez contribuir a la identificación y selección de infraestructuras que sean de carácter crítico para un país

en vías de desarrollo, teniendo en cuenta la constitución política del estado y los derechos de los cuales sus ciudadanos son participes, de esta manera apoyando también al desarrollo de una política nacional de ciberseguridad mediante el desarrollo de estrategias nacionales de ciberseguridad (NCS – National Cybersecurity Strategies).

Los métodos que se utilizaran para el desarrollo de esta investigación son los siguientes:

- Método Deductivo

  Se utilizará este método porque se pretende realizar una serie de guías y recomendaciones evocando las metodologías y guías de buenas prácticas utilizadas en diferentes países relacionadas a la selección de infraestructuras críticas.

- Método Analítico

  Se utilizará este método para realizar los análisis pertinentes de los documentos relacionados con las NCS verificando su aplicabilidad o no para el Ecuador.

- Método Comparativo.

  Este método será utilizado para realizar una comparación entre las variables definidas en la investigación referentes a la selección de infraestructuras críticas, con ello se espera definir las variables a aplicarse en nuestro caso.

Búsqueda y selección de documentación

En esta fase, se pretende plantear metodologías de recolección de información con el objetivo de seleccionar diferentes modelos de selección de infraestructuras críticas

utilizados a nivel mundial que cumplan criterios de aceptación en todos sus campos. De esta manera se ha de realizar una revisión de literatura en las diferentes bases digitales considerando como principales entidades las agencias que regulan los métodos y modelos de protección de la información a nivel mundial como lo son NIST, CISA, INCIBE, ENISA.

Para realizar la búsqueda en las diferentes bases digitales, se ha establecido una cadena de búsqueda con palabras clave para la identificación de probables documentos que sean de utilidad para la presente investigación.

- Critical Information Infrastructure
- Critical Infrastructure
- Protection of Critical Infrastructure
- Critical Infrastructure Protection
- Critical Infrastructure Methodology
- Critical Infrastructure Good Practices
- National Cybersecurity Strategies
- Critical Infrastructure ENISA
- Critical Infrastructure INCIBE
- Critical Infrastructure NIST
- Critical Infrastructure ITU

Una vez realizada esta búsqueda se pudo encontrar diferentes marcos de referencia, buenas prácticas, guías de recomendaciones, estrategias nacionales de ciberseguridad, regulaciones, etc. Todos realizados durante la última década y desarrollados por países, personas u organizaciones encargadas de la investigación y la

protección de IC o estrategias para la implementación de políticas de ciberseguridad. A continuación, se presenta la Tabla 3 con los resultados y los documentos encontrados.

Tabla 3

Frameworks hallados en la investigación

Organización	Marco de Referencia	Año de publicación
ENISA	Methodologies for the identification of Critical Information Infrastructure assets and services Guidelines for charting electronic data communication networks	2014
ENISA	Good Practice Guide - Design and implementation of national cyber security strategies	2014
Department of Homeland Security USA	Homeland Security Presidential Directive 7	2015
CISA	Critical Infrastructure Sectors	2013
NIST	Framework for Improving Critical Infrastructure Cybersecurity Version 1.0	2014
NIST	Framework for Improving Critical Infrastructure Cybersecurity Version 1.1	2018

Para la selección de los frameworks que serán usados en esta investigación se procederá a realizar un primer descarte de acuerdo a metodologías que no tienen relación directa con la selección o identificación de infraestructuras críticas, a continuación, se detallan las guías que se desestiman y la razón de porque hacerlo.

- ENISA: Guía para el desarrollo de una política de ciberseguridad, porque es un documento orientado para el desarrollo de una política, pero no para el desarrollo de un catálogo de IC.
- CISA: Porqué no es una guía, metodología o marco de referencia que proponga un proceso de selección de IC.
- El decreto ejecutivo de Estados Unidos: porque es un decreto en el cual se establecen los lineamientos que deberán seguir los frameworks o guías para la detección de IC.
- Framework para detección de IC – NIST versión 1.1: porque a pesar de ser una nueva versión de la liberada en el año de 2014, aún no se ha definido como un estándar.

A continuación, en la Tabla 4, se presenta los marcos de referencia seleccionados de acuerdo a la necesidad de la presente investigación.

Tabla 4

Frameworks seleccionados para la investigación

Organización	**Marco de Referencia**	**Año de publicación**
ENISA	Methodologies for the identification of Critical Information Infrastructure assets and services Guidelines for charting electronic data communication networks	2014
NIST	Framework for Improving Critical Infrastructure Cybersecurity Version 1.0	2014

Los marcos de referencia definidos en la Tabla 4 cumplen con la necesidad de, detallar, explicar o sugerir procesos por medio de los cuales se pueda realizar una selección de las infraestructuras que puedan llegar a ser consideradas de vital importancia en el normal desempeño de un país, apoyando de esta manera en la seguridad de la sociedad civil y de cada una de las aristas que consideren críticas para su desempeño.

Análisis de marcos de referencia

Una vez realizada la fase de selección de marcos de referencia de selección de infraestructuras críticas, se procederá a realizar un análisis de las características y variables en común, con el propósito de realizar una comparación entre ellas. A continuación, se pretende plantear una taxonomía en la que se determinará características o variables que sirvan de base para una selección de IC.

Methodologies for the identification of Critical Information Infrastructure assets and services guidelines for charting electronic data communication networks

En “Methodologies for the identification of Critical Information Infrastructure assets and services” detallan la problemática de la identificación de Infraestructuras de Información Críticas en las redes de comunicación, el objetivo del estudio realizado por la ENISA es el de describir posibles mejoras en torno a posibles amenazas que afecten la información de los Estados Miembros de Europa, además aseguran los riesgos relacionados con las funciones vitales de la sociedad con respecto a la red de comunicación, estableciendo parámetros que identifican para la identificación de infraestructuras críticas en los estados miembros como por ejemplos, la colaboración

entre sectores público y privado, los criterios de criticidad para la identificación de activos críticos. (Mattioli et al., 2014).

Metodología

La metodología se ha basado en los siguientes puntos.

- Recopilación de Información
- Análisis
- Validación

Flujo de identificación de infraestructuras críticas y sectores críticos.

Figura 6

Flujo de identificación de infraestructuras críticas

Nota: Tomado de (Mattioli et al., 2014)

Sectores críticos según la Unión Europea

La lista de los siguientes sectores críticos ha sido expuesta en “Green Paper” del programa europeo para la protección de infraestructuras críticas.

- Energía.
- Tecnologías de la información y la comunicación (TIC).
- Agua.
- Comida.
- Salud.

- Financiero.
- Orden público y legal y seguridad.
- Administración civil.
- Transporte.
- Industria química y nuclear.
- Espacio e investigación.

Niveles de madurez

En función de la información recopilada se ha observado que existen diferentes niveles de madurez, por lo que se ha definido los siguientes niveles.

- Nivel 1: Ausencia de actividades relacionadas con la protección de IC de información.
- Nivel 2: Identificación del sector de las TIC como uno de los sectores críticos que deben abordarse.
- Nivel 3: Desarrollo de un marco metodológico general para la identificación de activos de CI.
- Nivel 4: Desarrollo de una definición de Información de Infraestructuras Críticas (CII) y establecimiento de criterios específicos para la identificación de activos de CII.

Stakeholders involucrados en la identificación de las IC

Recopilando la información encuestada a los estados miembros se ha logrado establecer a los interesados que podrían estar involucrados en la selección de los servicios considerados críticos.

- Operadores de Infraestructuras Crítica.
- Proveedores de TI.

- Autoridades Reguladoras Nacionales.
- Agencias de ciberseguridad.

Operadores de infraestructura crítica

Los operadores de las IC están expuestos a importantes riesgos que pueden afectar o perjudicar directa o indirectamente en la sociedad o en funciones esenciales que dependen de la misma, las consideraciones necesarias para las partes interesadas son:

- Los operadores aceptan hacerse cargo de operar y verificar sus infraestructuras, en varios estados miembros obligatoriamente deben realizar un análisis de riesgos y continuidad comercial.
- En ciertos sectores se deberá cumplir con regulaciones que podrían tener impacto en la operación.
- Deberán clasificar sus infraestructuras y procesos, así como también sus aplicaciones e información de soporte.
- Los operadores deberán aplicar diversos enfoques que permitan clasificar y priorizar de acuerdo a la importancia de los servicios.

Proveedores de TI

Los operadores de las IC deberán identificar los servicios y activos relacionados y gestionar su protección, incluyendo los contratos con proveedores y sus Acuerdos a Nivel de Servicio (SLA – Service Level Agreement), estos pueden renovarse en función de las necesidades del operador. Dentro de las consideraciones se espera:

- Una demanda creciente en soluciones de TI, basadas en tecnología en evolución.

- Deberán existir procesos para fortalecer y mejorar la seguridad y capacidades de la información de infraestructuras críticas, a la vez garantizar los servicios de las IC.
- Establecer requisitos en la etapa de adquisición de TIC.
- Considerar la evolución de los SLA relacionados con los IC con el fin de permitir una gestión fortalecida de SLA.
- Una automatización de procesos de aseguramiento con el objetivo de lograr una operación efectiva y eficiente de la IC.

Autoridades reguladoras nacionales

Las Autoridades Nacionales podrán tener el mandato de las IC dependiendo de la legislación nacional, el papel y las consideraciones que cumplen será:

- La selección de una infraestructura crítica podrá ser afectada por el tamaño de la población a la que está afectando y el impacto sectorial de la misma.
- Deben responder a directrices por lineamientos que pueden involucrar vulnerabilidades de IC o adquisición de IC.
- Deberán realizar auditorías anuales a operadores de IC se utilizan metodologías Ad-hoc o utilizando la ISO-27001.
- Manejo automatizado de incidentes que afecten a las IC mediante sistemas de información.
- Mantener una base de datos que mantenga entidades de servicio crítico, datos relevantes, operadores y responsables de las IC.

Agencias de ciberseguridad

Las Agencias nacionales de ciberseguridad tendrán un papel importante en la identificación de IC, dependiendo de su legislación podrán participar con:

- Desarrollo de leyes relacionadas con la identificación y protección de IC.
- Supervisión e implementación de la legislación.
- Auditoria relacionada a las partes involucradas.
- Investigación continua entre los activos críticos con referencia a alianzas público-privadas.
- Cooperación en la pérdida de información o activos de las IC.

Metodología para la identificación de IC

En la siguiente sección se detalla cada uno de los pasos en la identificación de servicios críticos desde la perspectiva de los estados miembros de la UE y desde los operadores de servicios. Los pasos son:

- Paso 1: Identificación del sector crítico.
- Paso 2: Identificación de los servicios críticos.
- Paso 3: Identificación de los servicios y activos de información crítica que respalden los servicios críticos.

Identificación del sector crítico

Como se ha identificado, los estados miembros de la UE han abordado el tema de la identificación de los sectores críticos, todos los miembros tienen un catálogo más largo o más corto dependiendo de su realidad, es decir se adecúan a las prioridades nacionales, las directivas comunitarias y las especificaciones de cada país.

Identificación de los servicios críticos

Una vez definidos los sectores críticos se tendrá que definir los servicios críticos, entre estos se puede apreciar dos enfoques desde los cuales definir los servicios que serán considerados críticos.

- Enfoque impulsado por el estado.
- Enfoque impulsado por un operador.

Enfoque impulsado por el estado

Todo el proceso de selección de servicios críticos debe estar guiado por agencias gubernamentales que deben ser las indicadas para impulsar la identificación y el cuidado de las infraestructuras críticas.

Estas agencias deben definir una lista de servicios que consideren críticos, después deben realizar un plan que se estará actualizando cada cierto periodo de tiempo en vista del continuo cambio debido a nuevas amenazas.

- Gobierno:
  - Selección de sectores críticos con su respectiva obligación.
  - Determinación de servicios críticos candidatos.
- Organizaciones de IC:
  - Emplear un método de puntuación de criticidad para seleccionar servicios críticos reales.
  - Notificar al operador de IC que opera el servicio crítico.
- Operador de IC:
  - Definición y selección de servicios críticos.
  - Definir un plan de protección de IC (seguridad y resiliencia).
  - Ejecutar el plan detallado.
- Organización de IC:

- Revisión del plan de protección y aprobación del mismo.
- Revisión constante de los servicios y operadores.
- Coordinación con operadores.

Identificación de los servicios y activos de información crítica que respalden los servicios críticos.

Este paso se considera el paso final en la protección y monitorización de servicios e información crítica que necesitan ser identificados.

Se debe realizar una descripción general de los métodos y las aplicaciones que se consideren relevantes para un servicio público, puede ser, agua, telecomunicación, transporte, etc. Se busca que todos los procesos involucrados al brindar un servicio crítico sean evaluados con el fin de proteger sus activos (información) y servicios.

Desafíos en la identificación de IC

Durante el proceso de evaluación de los estados miembros de la UE, fue posible encontrar que varios de ellos no han logrado encontrar un catálogo detallado de servicios críticos y comenzarlo desde cero es una tarea desafiante.

El sector privado y el público necesitan tener un proceso sistemático que les permita colaborar en la identificación de este catálogo. “La colaboración efectiva entre el sector público (Gobierno y agencias obligatorias) y el sector privado es fundamental para identificar y proteger los activos y servicios de la CII.” (Mattioli et al., 2014)

Identificación de sectores críticos

Mientras se ha realizado esta investigación, se ha identificado que varios estados no contemplan un catálogo de servicios críticos.

A continuación, se presenta la Tabla 5, que describe una lista de referencia de sectores y servicios críticos que un estado puede consultar y definir de acuerdo a su realidad y características geográficas.

Tabla 5

Sectores y servicios críticos

Sector Crítico	Subsector Crítico	Servicio Crítico.
Energía	Electricidad	Generación
		Transmisión y Distribución
		Mercado de electricidad
	Petróleo	Extracción
		Refinamiento
		Transporte
		Almacenamiento
	Gas Natural	Extracción
		Transporte y Distribución
		Almacenamiento
Tecnologías de la Información y Comunicación (TIC)	Tecnologías de la Información	Servicios Web
		Data Center / Servicios Cloud
		Software como servicio (SaaS)
	Comunicaciones	Voz / Comunicación de Datos
		Conexión a Internet
Agua	Agua Potable	Almacenamiento de agua
		Distribución del agua

Sector Crítico	Subsector Crítico	Servicio Crítico.
	Aguas Residuales	Aseguramiento de la calidad del agua Recolección y tratamiento de aguas residuales.
Alimentos		Agricultura / producción de alimentos Suministro de alimentos Distribución de comida Calidad / inocuidad de los alimentos
Salud		Asistencia sanitaria de emergencia Atención hospitalaria (pacientes hospitalizados y ambulatorios) Suministro de productos farmacéuticos, vacunas, sangre, suministros médicos. Control de infección / epidemia
Servicios Financieros		Banca Transacciones Bolsa
Orden Público y Seguridad		Mantenimiento del orden público y seguridad Sistema judicial y penal

Sector Crítico	Subsector Crítico	Servicio Crítico.
Transporte	Aviación	Servicios de navegación área
		Operación de aeropuertos
	Carretera	Servicio de autobús
		Mantenimiento de red vial
	Tren	Servicio Ferroviario
		Gestión de ferrocarril público
	Marina	Gestión de tráfico marítimo
Industria	Industrias Críticas	Empleo
	Industria Química y nuclear	Gestión de materiales peligrosos
		Seguridad de unidades industriales de alto riesgo
Administración Civil		Funciones Gubernamentales
Espacio		Protección de sistemas espaciales
Protección Civil		Servicios de emergencia y rescate
Ambiente		Control de la contaminación del aire

Nota: Tomado de (Mattioli et al., 2014)

Criterios de criticidad

De la misma manera que los servicios, los criterios de criticidad son una tarea engorrosa de definir, a continuación, se presenta la Tabla 6 que define los criterios que un estado puede tomar como referencia para definir los suyos.

Tabla 6

Criterios de criticidad

Criterio	Descripción
Población	El porcentaje de la población que se verá afectada por la falta del servicio
Concentración	La densidad poblacional dentro del área geográfica que se verá afectada por la falta del servicio
Impacto económico	El costo en términos de porcentaje de PIB por la falta del servicio
Confianza Pública	La confianza que genera el correcto funcionamiento del servicio hacia el gobierno
Relaciones Internacionales	El efecto que produce la interrupción del servicio en las relaciones con los demás países.
Orden Público	El efecto que produce la falta del servicio en el orden público
Impedimento en operaciones pública	Impedimento en operaciones diarias, como, transporte público, trabajo, agua potable, etc.
Servicios de Terceros	La interdependencia de servicios de otros estados / países, si es que llegan a afectarse.

Nota: Adaptado desde (Mattioli et al., 2014)

Framework for improving Critical Infrastructure cybersecurity.

En los Estados Unidos de Norteamérica la seguridad nacional y económica es uno de los tópicos más importantes y en lo que más se ha invertido durante la última década, en “Framwork for Improving Critical Infraestructure Cybersecurity” se busca implementar

un framework que regule el correcto funcionamiento y selección de infraestructuras críticas, asegurando que no se ponga en riesgo la seguridad, economía y salud pública de la nación. Se pretende reconocer los distintos riesgos de la seguridad cibernética dentro de los procesos de gestión de riesgos de una organización. El Marco ayudará a mejorar el enfoque que las actividades de ciberseguridad deberán tener en cuenta para los procesos de tolerancia y riesgo. (NIST, 2014).

Framework introduction

Dentro del marco de referencia se han establecido estándares y directrices las cuales facilitarán una taxonomía para que las organizaciones puedan:

- Establecer su realidad con respecto a ciberseguridad
- Establecer el target para la ciberseguridad
- Seleccionar y priorizar oportunidades para la mejora de un proceso continuo
- Revisar y analizar cuál es el progreso hacia el target establecido
- Tener una buena comunicación entre las partes interesadas sobre el riesgo de la ciberseguridad.

Resumen del Framework

El Marco de referencia se compone de tres partes:

- El Framework Core
- Los Niveles de Implementación
- Los Perfiles del Framework

Gestión del riesgo y ciberseguridad

La gestión del riesgo es un proceso continuo en el que una organización realiza una identificación de que ocurra un evento y cuyo resultado sea un impacto grave a la

funcionalidad de uno de sus activos, la evaluación y el análisis de los mismos comprenden una verdadera gestión de riesgos, de esta manera, se pretende minimizar o mitigar el riesgo o la tolerancia al mismo.

El Framework utiliza y pone en conocimiento de las organizaciones varios métodos de gestión de riesgos que permiten seleccionar y priorizar decisiones que conlleven un riesgo en torno a la ciberseguridad, el objetivo, es otorgar a las organizaciones el poder de identificar y mejorar la gestión de riesgos de las IC. Dentro de la gama de procesos de gestión de riesgos podremos encontrar:

- Organización Internacional de Normalización
    - (ISO) 31000: 20093, ISO / IEC 27005: 20114
- Instituto Nacional de Estándares y Tecnología (NIST)
    - Publicación Especial (SP) 800-395
- Subsector de Electricidad Gestión de Riesgos de Ciberseguridad Directriz (RMP)
    - RMP Guideline

Principios básicos

A continuación, se presentan los principios que ayudarán a entender y gestionar los riesgos de ciberseguridad para ambientes internos y externos. El objetivo principal es enfocar la correcta entrega de servicios críticos dentro de una organización.

Framework Core.

Dentro del núcleo del Framework se otorga una cierta cantidad de actividades con el objetivo de alcanzar resultados específicos en ámbitos de ciberseguridad. En la Figura 7 se presentan los cuatro elementos del núcleo, así como también la estructura del mismo:

- Funciones: el objetivo es planificar tareas del más alto nivel de ciberseguridad. Las funciones que se desarrollarán son:
    - Identificar
    - Proteger
    - Detectar
    - Responder
    - Recuperar
- Categorías: es la subdivisión de una Función, ejemplo de esta división puede ser:
    - Gestión de Activos
    - Procesos de detección
    - Control de Acceso.
- Subcategorías: división aún más específica sobre actividades técnicas o de gestión, ejemplos pueden ser:
    - Los datos se encuentran en reposo y están protegidos
    - Los sistemas de información externos están catalogados
- Referencias Informativas: sección específica para listar estándares, mejores prácticas, guidelines relacionados con cada sector de una Infraestructura Crítica.

Figura 7

Estructura del Framework Core

Nota: Tomado de (NIST, 2014)

A continuación, se presenta las cinco funciones principales del framework, estas se pueden ejecutar de forma simultánea, sin necesidad de realizar un proceso en serie de las mismas.

- Identificar: comprender a nivel organizativo la gestión del riesgo de ciberseguridad de los sistemas, ejemplos de resultados en esta categoría son:
    - Entorno de negocio
    - Evaluación de riesgos
    - Gestión de riesgos
    - Gobernanza
- Proteger: desarrollar aseguramientos que garanticen una correcta entrega de servicios de infraestructura crítica, ejemplo de resultados son:
    - Seguridad de datos

    - Procesos de protección de información
    - Mantenimiento
- Detectar: fomentar tareas de identificación de ocurrencias de eventos de ciberseguridad, como ejemplos podemos encontrar:
    - Anomalías y eventos
    - Monitoreo de seguridad
    - Procesos de detección.
- Responder: implementar tareas con el objetivo de tomar acciones frente a un evento de ciberseguridad que haya sido detectado, como ejemplos tenemos:
    - Análisis
    - Mitigación
    - Comunicación
- Recuperar: Desarrollo e implementación de procesos de remediación del servicio que haya sido afectado a causa de un evento de ciberseguridad, ejemplos:
    - Planificación de recuperación
    - Remediación.

Niveles de implementación

Los niveles de implementación del framework detallan el nivel de dureza y de complejidad de la gestión de riesgos de ciberseguridad y la manera en la que se integra con las necesidades de una organización.

Durante el proceso de identificación de nivel, la organización debe seleccionar aquel nivel que cumpla con los objetivos de la organización, mismo que será evaluado

tomando en cuenta las practicas actuales de gestión de riesgos, las amenazas, la misión del negocio y, sobretodo, sus limitaciones.

Los niveles se detallan a continuación.

- Nivel 1: Parcial
- Nivel 2: Riesgo Informado
- Nivel 3: Repetible
- Nivel 4: Adaptado.

Nivel 1: Parcial

- **Proceso de gestión de riesgos:** la gestión de riesgo se realiza de manera ad-hoc, no está formalizada.
- **Programa Integrado de gestión de riesgos:** la gestión de riesgos es implementada de forma irregular, la organización puede no tener un proceso donde se comparta información.
- **Participación externa:** no tiene procesos establecidos para colaboración con externos.

Nivel 2: Riesgo informado

- **Proceso de gestión de riesgos:** la gestión de riesgos esta formalizada pero no es una política dentro de la organización.
- **Programa Integrado de gestión de riesgos:** la gestión de riesgos no ha sido establecida a nivel de organización, la información se comparte con toda la organización.
- **Participación externa:** la organización es consciente de la importancia, pero no ha establecido aún procesos para compartir información con externos.

Nivel 3: Repetible

- **Proceso de gestión de riesgos:** la gestión de riesgos es aprobada formalmente y se expresa como política de la organización.
- **Programa Integrado de gestión de riesgos:** Toda la organización gestiona el riesgo de ciberseguridad, la gestión se centra en responder de manera eficaz al cambio.
- **Participación externa:** la colaboración se da en torno a la gestión de riesgos de la organización.

Nivel 4: Adaptado

- **Proceso de gestión de riesgos:** existe un proceso de aprendizaje por el cual se adoptan las prácticas de ciberseguridad que la organización adoptará.
- **Programa Integrado de gestión de riesgos:** toda la organización se enfoca en la ciberseguridad, existe una evolución constante debida al aprendizaje e información compartida desde fuentes externas.
- **Participación externa:** se comparte la información con fuentes externas con el fin de mejorar la ciberseguridad.

Coordinación para implementación del Framework

Existe un flujo común para la organización que detalla cada uno de los niveles dentro de la organización:

- Ejecutivo.
- Procesos de negocio.

- Implementación/Operación.

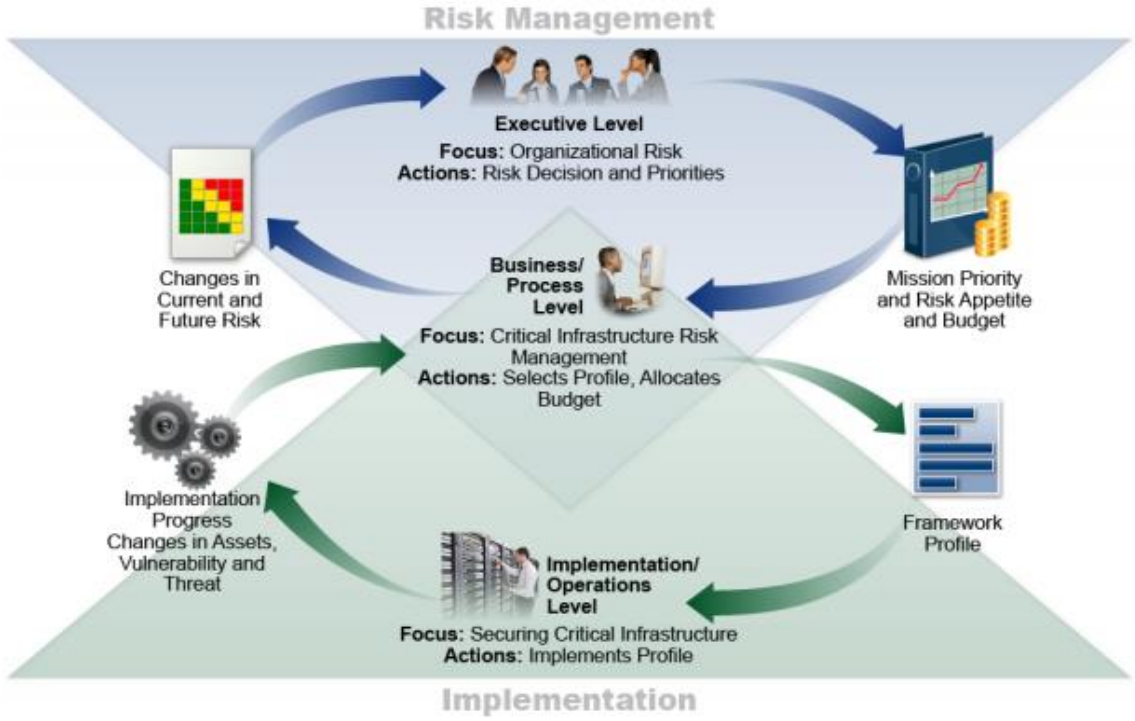
Los tres niveles trabajan a la par dentro de la organización del siguiente flujo:

- El ejecutivo hace partícipe de las prioridades y los recursos al nivel de proceso de negocio.
- El nivel Procesos de negocio emplea la información para el proceso de gestión de riesgos.
- Procesos de negocio colabora con el nivel Implementación/Operación para emitir las necesidades del negocio.
- Implementación/Operación notifica el progreso del desarrollo del perfil al nivel de Proceso de negocio.
- Proceso de negocio realiza una evaluación de impacto.
- Los resultados de la evaluación de impacto son entregados al nivel ejecutivo y al nivel de Implementación/Operación.
- El ejecutivo informa el proceso de gestión de riesgos de la organización.
- Implementación/Operación informa en impacto comercial.

En la Figura 8 se muestra el esquema del flujo de decisión dentro de una organización.

Figura 8

Flujo de implementación dentro de una organización



Nota: Tomado de (NIST, 2014)

Forma de usar el framework

El framework puede ser utilizado como una parte muy importante en el proceso de identificación y gestión de riesgos de ciberseguridad, ya que de esta manera una organización puede usar el framework para identificar los servicios y procesos críticos y su prestación.

Programas de ciberseguridad

A continuación, se presenta un flujo que una organización o nación debe seguir para crear un programa de ciberseguridad o mejorar el que posea, de esta manera, el framework se puede utilizar para mejorar de manera continua los procesos de ciberseguridad.

Paso 1. Priorizar y alcance

Se identifican los objetivos del negocio a fin de realizar una toma estratégica de decisiones con respecto a la ciberseguridad y el alcance de los servicios y activos que apoyen la línea de negocio, puede ser adaptado para cualquier necesidad de negocio.

Paso 2. Orientar

En este punto, la organización debe seleccionar los servicios y activos que tengan un enfoque de riesgo de ciberseguridad, una vez identificados los servicios se procede a determinar las amenazas y vulnerabilidades de los mismos.

Paso 3. Crear un perfil

Se debe desarrollar un perfil en el que se indiquen los resultados de las categorías y subcategorías del framework que se pretenden lograr.

Paso 4. Evaluación de riesgos.

Se debe realizar una evaluación de riesgos acorde a los procesos de la organización, se ejecuta un análisis de acuerdo al entorno de la organización para evaluar la posibilidad de que ocurra un evento de ciberseguridad.

Paso 5. Crear un perfil Objetivo.

Desarrollar un perfil Objetivo en el que se enfoque las Categorías y Subcategorías del framework en los cuales se detallan los resultados, en ciberseguridad, que la organización espera, también se pueden considerar a los stakeholders externos como socios comerciales, clientes o entidades del sector estratégico.

Paso 6. Determinar, analizar y priorizar brechas.

Se realiza un análisis entre el Perfil Actual y el Perfil Objetivo con el objetivo de identificar las brechas, a continuación, se desarrolla un plan de acción para afrontar estas brechas de acuerdo a los riesgos que puedan enfrentar en ciberseguridad. Luego, la organización debe seleccionar a los recursos que afrontaran estas brechas.

Paso 7. Implementar plan de acción.

Se debe determinar qué acciones tomar de acuerdo a las brechas identificadas en el paso anterior supervisando las prácticas de ciberseguridad del perfil objetivo, la organización debe identificar las directrices que mejor se acomoden al sector crítico y a las necesidades del negocio.

Stakeholders y los requisitos de ciberseguridad

Dentro del framework se detalla un lenguaje común por medio del cual se realiza la comunicación de los requisitos de ciberseguridad hacia los stakeholders, los cuales son los encargados de la entrega de los servicios a las infraestructuras críticas.

Por ejemplo, se puede:

- Utilizar el Perfil objetivo para gestionar los riesgos de ciberseguridad hacia un proveedor externo.
- Utilizar su perfil actual para informar es estado actual de ciberseguridad de una organización.
- Utilizar el perfil objetivo con el fin de comunicar las categorías y subcategorías de un servicio crítico de IC hacia un socio externo, siempre y cuando ese socio depende de la IC.
- Un sector de infraestructura crítica puede establecer su perfil objetivo de acuerdo a los componentes de un perfil actual.

Metodología para proteger la privacidad y libertades civiles

Esta sección describe la metodología para proteger la privacidad y la libertad civil de acuerdo a la Orden Ejecutiva emitida por los Estados Unidos en la misma que sea abordan operaciones de ciberseguridad.

Se pretende definir un conjunto de guidelines para que cada sector pueda abordar estas consideraciones por medio de implementaciones técnicas, de acuerdo a sus

necesidades se pueden desarrollar nuevos estándares técnicos o mejores prácticas para soportar dichas implementaciones.

Los siguientes procesos pueden considerarse como un intermedio para emprender las implicaciones referentes a libertad civil y privacidad.

Gobernanza del riesgo de ciberseguridad

- El programa de ciberseguridad considera el riesgo de ciberseguridad y las posibles respuestas a los mismos dentro de la organización.
- Los recursos asignados a responsabilidades de privacidad y que se relacionan con riesgos de ciberseguridad deberán ser capacitados de acuerdo a sus funciones.
- Se implementa un proceso que proteja la realización de los procesos de ciberseguridad junto con las leyes y regulaciones de privacidad.

Identificación y autorización de acceso a sistemas de la organización

- Existen procesos para abordar la privacidad y las medidas de control de acceso, siempre y cuando impliquen el uso de información personal.

Medidas de sensibilización y formación.

- Los recursos encargados de la ciberseguridad son sensibilizados de acuerdo a las políticas de privacidad de la organización.
- Los proveedores de servicios críticos relacionados con la ciberseguridad reciben información sobre las políticas de privacidad de la organización.

Detección de anomalías y monitoreo de activos

- Se debe realizar un proceso para la revisión de la privacidad sobre la detección de actividades anómalas y el monitoreo de ciberseguridad.

Actividades de respuesta y/o mitigación

- Se realiza un proceso para determinar la manera en la que se comparte la información fuera de la organización, en base a la cooperación de información de ciberseguridad.
- Se realiza una revisión de la privacidad en la gestión de mitigación de riesgos de la organización.

Definición de variables

Una vez realizada el análisis de los marcos de referencia que sirven de estudio para esta investigación, se pudo encontrar que existen variables en común las cuales permitirán precisar parámetros que son asociados a la selección de infraestructuras críticas y sus servicios críticos, de esta manera se podrá evaluar la eficacia de los marcos de referencia de selección de IC.

Definición de características

Al analizar los marcos de referencia seleccionados para la investigación se llegó a la conclusión que todas buscan el mismo objetivo, pero no todas siguen la misma estructura o tienen las mismas características.

De esta manera, se intenta clasificar las variables en grandes grupos que estén asociados a la estructura general de un framework de selección o identificación de infraestructuras críticas, entre los cuales tenemos:

- Identificar Sectores críticos de IC.
- Aplicación de criterios específicos a sectores críticos.
- Valoración de recursos críticos dentro de las IC.
- Evaluación de la dependencia de la IC.

- Análisis de Criterios Comunes de las IC.
- Análisis de Riesgos para las IC.

A continuación, se presenta una lista de Tablas en las que describe y detalla cada una de las variables pertenecientes a las características detalladas anteriormente junto con un código que permitirá la identificación de la misma en los posteriores análisis.

Identificación de sectores críticos

Tabla 7

Identificación de sectores críticos

Código	Característica	Descripción
CAR-1.1	Identificación de sectores y servicios de otros países	Se realiza un análisis de otros países que cumplen con una estructura geográfica, social y desarrollo tecnológico similar, identificando operadores de IC y los servicios que se considerarán críticos dentro del sector identificado.
CAR-1.2	Estudio analítico de selección de IC	Realizar un estudio analítico que contenga criterios y métodos sencillos, se puede emular los estudios realizados en otros países considerando las diferencias de los mismos.

Código	Característica	Descripción
CAR-1.3	Definir métodos detallados de identificación de IC	Realizar una metodología que cumpla con criterios de madurez para evaluar los sectores críticos, de esta manera se podrá decidir si una infraestructura es considerada crítica o no.

Aplicación de criterios específicos a sectores críticos

Tabla 8

Criterios específicos aplicados a sectores críticos

Código	Característica	Descripción
CAR-2.1	Selección de acuerdo a la participación del mercado	Se deberá realizar una primera selección de acuerdo a la capacidad del mercado y del transporte, por ejemplo, flujos de gas por segundo, importación y/o exportación, industria y población.
CAR-2.2	Restringir operadores de Infraestructuras Críticas	Con la primera selección se prevé realizar una restricción de operadores de IC, en caso de que existan múltiples para una IC
CAR-2.3	Establecer criterios cuantitativas y objetivos	Se debe procurar establecer criterios que sean cuantitativos y objetivos y no cualitativos y subjetivos con el propósito

Código	Característica	Descripción
		de ayudar en la siguiente etapa de identificación de IC.

Valoración de recursos críticos dentro de las IC

Tabla 9

Valoración de recursos críticos

Código	Característica	Descripción
CAR-3.1	Evaluar el carácter vital de la lista obtenida en la pre-selección	Es necesario realizar esta evaluación basándose en la definición de Infraestructura Crítica de cada país, es decir se debe conocer los servicios y los operadores de cada sector.
CAR-3.2	Evaluar los recursos críticos de otros países	Es importante tomar en cuenta que se puede adoptar ejemplos de los primeros pasos en otros países para identificar sectores y servicios, haciendo hincapié en las diferencias e interpretaciones de lo que será considerado crítico.

Evaluación de la dependencia de la IC

Tabla 10

Evaluación de dependencia de las IC

Código	Característica	Descripción
CAR-4.1	Identificar dependencias vitales de las IC	Los sectores de IC dependen de otros sectores y sus servicios críticos,
CAR-4.2	Identificar interdependencias entre IC	Es necesario identificar las dependencias entre sectores que pueden provocar un corte en cascada de los servicios
CAR-4.3	Determinar el número de IC	Es probable que el número de IC identificadas aumente una vez se hayan establecido las dependencias entre sectores y servicios de IC.

Análisis de criterios comunes de las IC

Tabla 11

Criterios comunes en las IC

Código	Característica	Descripción
CAR-5.1	Criterios sobre victimas	Se deberá evaluar criterios sobre posibles víctimas o heridos por el fallo de los servicios de la IC

Código	Característica	Descripción
CAR-5.2	Criterios de efectos económicos	Evaluar la importancia de posibles pérdidas y/o deterioro de los servicios de las IC, incluidos efectos al medio ambiente
CAR-5.3	Criterios de efectos públicos	Evaluar las repercusiones en la confianza de los ciudadanos incluyendo la afectación en la vida diaria
CAR-5.4	Criterios de repercusión	Se evalúa el ámbito afectado, puede ser local, nacional o internacional, a un solo sector o a múltiples sectores
CAR-5.5	Criterios de dependencia	Se evaluará los posibles efectos que produzca la falla o falta del servicio en otros servicios críticos, pueden ser fallos menores, moderados, importantes o incapacitantes.

Análisis de riesgos de las IC

Tabla 12

Análisis de riesgos en las IC

Código	Característica	Descripción
CAR-6.1	Identificación de riesgos	Identificación de amenazas técnicas y no técnicas, dentro de los servicios de IC seleccionados, se pueden utilizar

Código	Característica	Descripción
		herramientas que permitan la identificación
CAR-6.2	Evaluación de riesgos	Se debe medir el riesgo en base a la probabilidad de ocurrencia y el impacto que producirán las consecuencias en los activos de los servicios de IC
CAR-6.3	Gestión de riesgos	En base a la evaluación del riesgo se califica y gestiona, aceptándolo, evitándolo, mitigándolo o transfiriéndolo

Calificación de características

Una vez establecidas las características que están directamente relacionadas con la identificación y selección de Infraestructuras Criticas y sus servicios, se realizara una evaluación cuantitativa a los marcos de referencia analizados considerando si están presentes totalmente o si poseen algunas cláusulas que sean semejantes a la descripción de la característica. La calificación se realizará de la siguiente manera: si la característica analizada es considerada positiva se realizará una marca (X), al final se realizará un sumatorio de las características que han dado como positivas en cada etapa.

Identificación de sectores críticos

Tabla 13

Calificación – Identificación de sectores críticos

Framework	**Características**			**TOTAL**
	CAR-1.1	**CAR-1.2**	**CAR-1.3**	
ENISA	X	X	X	3
NIST	X	X		2

Aplicación de criterios específicos a sectores críticos

Tabla 14

Calificación – Criterios específicos a sectores críticos

Framework	**Características**			**TOTAL**
	CAR-2.1	**CAR-2.2**	**CAR-2.3**	
ENISA	X	X	X	3
NIST	X		X	2

Valoración de recursos críticos dentro de las IC

Tabla 15

Calificación – Valoración de recursos críticos

Framework	**Características**		**TOTAL**
	CAR-3.1	**CAR-3.2**	
ENISA	X	X	2
NIST		X	1

Evaluación de la dependencia de las IC

Tabla 16

Calificación – Dependencia de las IC

Framework	Características			TOTAL
	CAR-4.1	CAR-4.2	CAR-4.3	
ENISA	X		X	2
NIST	X			1

Análisis de criterios comunes de las IC

Tabla 17

Calificación – Criterios comunes de las IC

Framework	Características					TOTAL
	CAR-5.1	CAR-5.2	CAR-5.3	CAR-5.4	CAR-5.5	
ENISA		X	X	X	X	4
NIST		X	X	X		3

Análisis de riesgos de las IC

Tabla 18

Calificación – Riesgos de las IC

Framework	Características			TOTAL
	CAR-6.1	CAR-6.2	CAR-6.3	
ENISA	X			1
NIST	X	X	X	3

Calificación de características total

En las tablas 13, 14, 15, 16, 17 y 18 se procedió a evaluar las características de los dos frameworks analizados en esta investigación, se consideró una suma total de acuerdo a las características que se encuentran en cada uno de ellos y se realizara un recuento total que se visualiza a continuación en la Tabla 19.

Tabla 19

Calificación total de características

Framework	Suma Total Características
ENISA	15
NIST	12

Una vez realizado el proceso de sumatoria de las características evaluadas en las dos metodologías en la Tabla 19, podemos tener las siguientes conclusiones:

- El Framework que cumple con la mayoría de las características es el desarrollado por ENISA en el que se detallan la mayoría de los pasos para una selección o identificación de IC.
- Las características detalladas para la identificación de infraestructuras críticas son aptas para desarrollar un modelo de selección de IC dentro de un país en vías de desarrollo.

Criterios de comparación

Dadas las circunstancias de la investigación se procederá a depurar la lista de características obtenidas en la etapa de Definición de variables, con el objetivo clasificar y priorizar las características que tengan mayor relevancia dentro de un modelo de selección de IC.

Para poder realizar este análisis se utilizará una matriz de priorización que permitirá la clasificación de las características en base a la ponderación que se establecerá a continuación en la Tabla 20:

Tabla 20

Ponderación para matriz de priorización

Valor	Detalle
10	El criterio de la característica en la columna tiene más importancia que el criterio de la característica de la fila
5	El criterio de la característica en la columna tiene una importancia igual que el criterio de la característica de la fila
0	El criterio de la característica de la columna tiene una importancia menor que el criterio de la característica de la fila

El análisis se realizará en un proceso de comparación de todos versus todos enfrentando las características del lado vertical versus las del lado horizontal, de esta manera se espera primar las características con una mayor relevancia para la selección de IC.

Se realizará una sumatoria final de los pesos obtenidos de acuerdo a la ponderación detallada en la Tabla 20, con el objetivo de clasificar las características desde la que posea el mayor peso hasta la que tenga el menor peso de acuerdo al proceso de comparación.

A continuación, se presenta la Tabla 21 con la matriz de comparación de características para la selección de Infraestructuras Críticas.

Figura 9

Matriz de priorización

CÓDIGO DE CARACTERISTICAS	CAR-1.1	CAR-1.2	CAR-1.3	CAR-2.1	CAR-2.2	CAR-2.3	CAR-3.1	CAR-3.2	CAR-4.1	CAR-4.2	CAR-4.3	CAR-5.1	CAR-5.2	CAR-5.3	CAR-5.4	CAR-5.5	CAR-6.1	CAR-6.2	CAR-6.3	SUMATORIO
CAR-1.1		5	10	5	0	0	10	5	10	10	5	5	5	10	5	5	5	5	5	105
CAR-1.2	0		10	5	0	10	10	0	5	10	5	5	10	0	5	5	5	5	5	95
CAR-1.3	10	10		10	5	10	10	10	5	5	10	5	10	5	5	0	10	5	10	125
CAR-2.1	5	10	0		5	10	10	5	0	10	0	5	5	5	5	5	10	10	0	95
CAR-2.2	10	10	5	10		0	5	0	0	5	5	0	0	5	0	0	5	5	5	60
CAR-2.3	10	0	5	0	10		0	5	0	5	0	0	5	0	5	0	5	5	5	50
CAR-3.1	0	0	5	0	5	10		5	10	5	10	10	10	5	5	5	5	5	5	100
CAR-3.2	5	10	10	5	10	5	5		10	5	10	0	0	5	0	0	0	0	0	75
CAR-4.1	0	5	0	10	10	10	0	0		5	0	0	0	5	5	5	0	0	0	55
CAR-4.2	0	0	5	0	5	5	5	5	5		0	0	0	5	5	5	0	0	0	45
CAR-4.3	5	5	0	10	5	10	0	0	10	10		5	5	10	5	10	5	5	5	100
CAR-5.1	5	5	5	5	10	10	0	10	10	0	0		5	5	0	0	0	0	0	65
CAR-5.2	5	0	0	5	10	5	0	10	10	10	5	5		10	5	0	0	0	0	75
CAR-5.3	0	10	5	5	5	5	10	5	5	5	0	5	0		5	5	0	0	0	70
CAR-5.4	5	5	5	5	10	5	5	10	5	5	5	10	5	5		0	5	0	0	85
CAR-5.5	5	5	10	5	10	10	5	10	5	10	10	5	10	5	5		0	0	0	105
CAR-6.1	10	5	5	0	5	5	5	10	10	10	5	10	10	10	5	10		5	0	110
CAR-6.2	5	5	5	0	5	5	5	10	10	10	5	10	10	10	10	5	10		0	115
CAR-6.3	0	0	0	5	10	5	5	5	10	10	10	5	10	5	10	10	10	10		120

Una vez realizado el análisis de la matriz de priorización de acuerdo con la ponderación establecida en la tabla 20, definimos la columna Sumatoria, que representa la importancia que tendría la característica dentro de un modelo de selección o identificación de IC, a continuación, se presenta la Tabla 22, como un resumen y se filtra la columna desde la característica que tiene mayor importancia, hasta la que tiene menor importancia.

Tabla 21

Priorización de características de mayor a menor importancia

Código	Característica	Sumatorio
CAR-1.3	Definir métodos detallados de identificación de IC	125
CAR-6.3	Gestión de Riesgos	120
CAR-6.2	Evaluación de Riesgos	115
CAR-6.1	Identificación de Riesgos	110
CAR-1.1	Identificación de Sectores y servicios de otros países	105
CAR-5.5	Criterios de dependencia	105
CAR-3.1	Evaluar el carácter vital de la lista obtenida en la pre-selección	100
CAR-4.3	Determinar el número de IC	100
CAR-1.2	Estudio analítico de selección de IC	95
CAR-2.1	Selección de acuerdo a la participación del mercado	95
CAR-5.4	Criterios de repercusión	85
CAR-3.2	Evaluar los recursos críticos de otros países	75
CAR-5.2	Criterios de efectos económicos	75

Código	Característica	Sumatorio
CAR-5.3	Criterios de efectos públicos	70
CAR-5.1	Criterios sobre victimas	65
CAR-2.2	Restringir operadores de Infraestructuras Críticas	60
CAR-4.1	Identificar dependencias vitales de las IC	55
CAR-2.3	Establecer criterios cuantitativas y objetivos	50
CAR-4.2	Identificar interdependencias entre IC	45

Capitulo IV

Análisis de la evaluación de métodos de selección de infraestructuras críticas

En este capítulo se desarrolla el análisis de la evaluación de los documentos seleccionados referentes a modelos de selección de Infraestructuras Criticas, se detalla también el aporte de este trabajo de investigación mediante recomendaciones para el desarrollo de un modelo de selección de infraestructuras críticas que apoye al nacimiento de una política nacional de ciberseguridad.

Análisis comparativo por fases

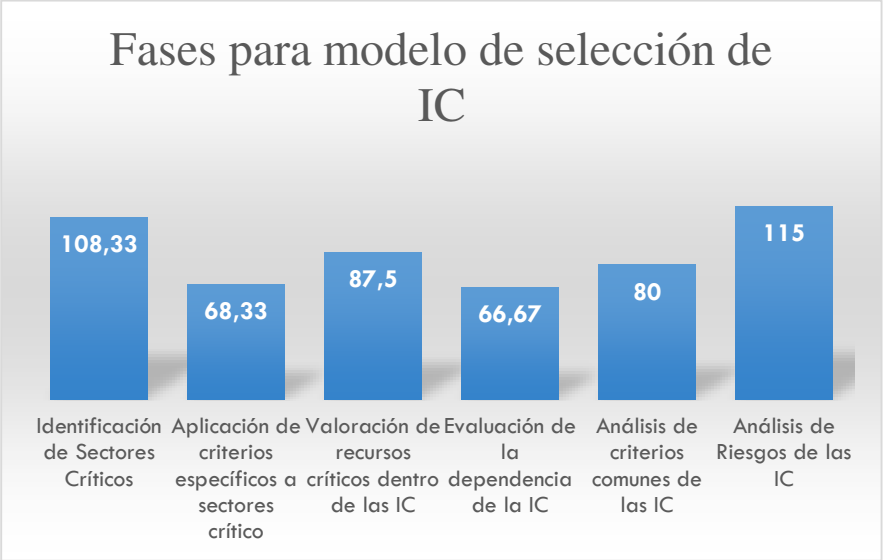
De acuerdo a las características planteadas y enfocándose en la Tabla 22, la matriz de priorización nos detalla los pesos que cada una de las características posee y cuán importante es su definición e implementación en un modelo de selección de infraestructuras críticas, a continuación, se presenta un resumen por fases y la importancia de las mismas en una implementación.

En la Figura 9, se establece que el Análisis de Riesgos de las IC es la fase más importante en el desarrollo de un modelo de identificación de las IC, en el que se deberá verificar las vulnerabilidades de cada uno de los sectores estratégicos que componen las infraestructuras críticas, así como también los servicios y stakeholders involucrados en los mismos, de la misma manera, se implanta como fase importante la Identificación de sectores críticos, lo cual tiene sentido, siendo esta la fase con mayor importancia del modelo, puesto que es en esta donde se deberá investigar en otros trabajos relacionados, tal como se menciona en los frameworks analizados, los sectores y servicios que pueden

ser considerados como críticos o no críticos, de acuerdo a la realidad social, económica y tecnológica del país.

Figura 10

Promedio de sumatoria por fases de modelo de selección de IC



También se indica que la Evaluación de la dependencia de las IC y la Aplicación de criterios especificas a sectores estratégicos son las fases que menos importancia pueden tener, pero eso no quiere decir que tengan que ser ignoradas, sino por el contrario, deben ser implementadas tomando en cuenta las características que deban ser aplicadas de acuerdo al análisis local y a los procesos que se desarrollen mediante la metodología que un país deba implementar para la definición de una IC y de sus servicios estratégicos.

Análisis comparativo por características

Como se ha revisado en esta investigación una característica elemental y que se ha usado en varios países es la cooperación, es decir, países considerados como

desarrollados pueden colaborar a otros países, considerados, en vías de desarrollo a realizar una definición de lo que serán las infraestructuras críticas, gracias a esto se puede desarrollar una lista preliminar que será depurada con el pasar del tiempo mientras se desarrolla la metodología necesaria para adaptar los conocimientos adquiridos en favor de la realidad situacional del país.

Detallando el análisis realizado en el capítulo anterior, en la Tabla 22, podemos encontrar que la característica con mayor importancia para la selección de infraestructuras críticas es la Definición de métodos detallados de identificación de IC, dándonos a entender que el grupo encargado de la identificación debe establecer una metodología que cumpla con criterios y procesos específicos reflejando la situación de país, mediante los cuales se pueda definir si una IC es crítica o no.

De igual manera, podemos encontrar que, una de las características importantes es la Gestión y Evaluación de Riesgos, en esta se definirá la identificación de amenazas técnicas y no técnicas relacionadas tanto a los servicios de las IC, como a los operadores de las mismas.

Por otro lado, también se determina que la Identificación de interdependencias entre las IC es la característica menos relevante del listado planteado, reconociendo que, es necesario identificar las relaciones entre IC y sus posibles consecuencias en caso de fallos, mas, sin embargo, la misma no es importante en un modelo de selección tomando en cuenta que debe existir una gestión del riesgo que detalle estos aspectos, a pesar de ello, es recomendable no omitir ninguna de las características planteadas en esta lista detallada en la Tabla 22.

Uno de los aspectos más importantes y que se visualiza en la priorización de las características son las vulnerabilidades y el nivel de impacto que puede llegar a afectar los riesgos en las IC, de esta manera, se debe establecer como esencial el hecho de

realizar una buena gestión de riesgos, en la que se deba identificar las vulnerabilidades en cada uno de los sectores estratégicos, así como también los servicios esenciales de los mismos incluyendo a los operadores y a todos los stakeholders involucrados con el objetivo de minimizar el nivel de impacto que tenga un error en una IC, teniendo en cuenta una evaluación sobre criterios para que se exponga el riesgo humano, social, económico y de dependencia sobre otras IC de países aliados o que tengan efecto sobre los mismos.

Las características correspondientes a la Aplicación de criterios específicos, de acuerdo al análisis realizado, pueden no ser de gran importancia, pero como se manifiesta en el punto 4.1 no deben ser ignoradas, características como la selección de la participación de acuerdo al mercado y la restricción de operadores de acuerdo a los servicios estratégicos serán de gran ayuda para la depuración de un catálogo de sectores críticos más robusto que permita la definición de la protección de servicios y la información de las IC.

La colaboración o la adopción de ejemplos sobre el desarrollo de una metodología con la que el país pueda definir los sectores críticos que se va a tomar como referencia para la protección de las IC, es de las características que debe tener mayor relevancia al momento de su elaboración, existen metodologías, como las estudiadas en esta investigación, que permiten adoptar sus estudios ajustando los mismo de acuerdo a las necesidades que requiera la situación social y civil, apoyándose también en políticas de ciberseguridad de países que compartan las mismas necesidades, teniendo en cuenta estudios realizados para países como Colombia, Perú o Chile.

La selección de infraestructuras debe darse en un margen amplio de estudios de investigación de los mercados a los cuales pueden afectar la falla o falta de los servicios que una IC provea, en Ecuador existen sectores estratégicos impuestos por el estado mediante la Constitución de la Republica, a partir de los mismos se deberá verificar su

importancia y al mismo tiempo priorizar los servicios que tengan un mayor impacto social y económico en la protección de su información. Sectores como las telecomunicaciones, energías, recursos naturales y no renovables, transportes y finanzas deberán ser estudiados y sus servicios deberán ser considerados como indispensables y críticos para el normal desarrollo de la sociedad ecuatoriana.

Como una característica de relevancia en el desarrollo de un modelo de selección de infraestructuras críticas, la depuración de stakeholders involucrados en el manejo de un servicio crítico es esencial, según los frameworks analizados, donde se requiere definir si los operadores de servicios de IC pueden ser compartidos entre diferentes servicios, se recomienda, en estos casos, definir si deben ser los mismos o, por el contrario, se necesita cambiarlos y definir nuevos.

Durante el proceso de desarrollo del modelo, se deberá incluir un estudio analítico sobre el impacto del fallo de un servicio estratégico sobre un sector estratégico, es recomendable, definir criterios de evaluación sobre posibles fallos clasificándolos por sectores teniendo en cuenta que los más importantes son:

Víctimas: en los que se debe analizar posibles heridos o víctimas mortales cuando el impacto de un posible riesgo en un servicio crítico de IC sea considerado alto, tomando en cuenta el análisis de riesgo realizado por la entidad encargada del mismo y el porcentaje de impacto que sea considerado para definir que el mismo sea alto.

Económico: en donde se refleje que, el impacto del fallo de un servicio crítico conlleve efectos que produzcan resultados negativos en la economía del país, en el mismo estudio se deberá incluir los impactos al medio ambiente y las posibles pérdidas en ámbitos financieros que el estado deberá asumir.

Social: se deberá analizar los impactos en la vida diaria del ciudadano común, sectores como transporte, agua, energía, son de vital importancia para el normal

desempeño diario del ciudadano, la falla en uno o varios de los servicios que otorgan las IC de estos sectores pueden provocar malestar y en determinados casos hasta víctimas fatales.

Dependencia: dado que se ha establecido que pueden y deberían existir dependencias de unos servicios con otros, es imperativo tener en cuenta los criterios de fallos ante posibles problemas en los servicios, esto con el propósito de evitar un posible fallo en cascada de los servicios afectados y que su efecto en términos de economía o social sean mermados por la gestión de riesgos que se realice, de acuerdo a la gestión de riesgos pueden existir fallos moderados, importantes o incapacitantes.

Repercusión: Si es el caso, se deberá evaluar si los servicios estratégicos de las IC identificadas, tienen relación con servicios prestados por el ámbito privado o por estados externos, de esta manera se reduce la repercusión que exista por los posibles fallos causados y la injerencia extranjera que pudiera ocasionar el impacto de los mismos.

Guías prácticas y recomendaciones para aplicar un modelo ecléctico adaptado a la realidad nacional

De acuerdo al análisis realizado durante el trabajo de investigación se ha consensuado una serie de buenas prácticas y recomendaciones las cuales se desarrollan con el objetivo de aplicar un modelo ecléctico que refleje la realidad social, económica y civil del Ecuador.

- Desarrollar un modelo ecléctico en base a diferentes modelos de selección de IC, enfocando el esfuerzo en el análisis de la situación actual y replicando sus resultados en el Ecuador.

- Replicar las características planteadas en esta investigación como base para el desarrollo del modelo de selección de IC, se puede partir sobre estas características para adoptar las mismas a la realidad del Ecuador.
- Identificar los servicios estratégicos en base a los sectores estratégicos identificados, una vez identificados, se debe hacer una depuración de los mismos en base a los procesos y modelos establecidos por la entidad encargada.
- Si se va a tomar como punto de partido los sectores y servicios estratégicos que forman parte de las IC mencionadas en este trabajo de investigación, se debe realizar un estudio de la situación actual para definir la importancia de cada uno de ellos y entender que nivel de importancia tiene en base a la realidad nacional.
- Trabajar de forma colaborativa de forma que los estudios y análisis realizados a países con similares realidades al Ecuador sirvan de modelo y sus procesos sean tomados como una pauta para el desarrollo del modelo de selección de infraestructuras críticas.
- Es importante realizar un análisis del mercado del Ecuador como parte del proceso de depuración de infraestructuras críticas, revisando niveles de optimización de servicios críticos que satisfagan las necesidades de cada uno de los involucrados en consumir estos servicios.
- Podrían existir alianzas con el ámbito privado que contribuyan con la implementación del modelo de selección IC y aporten con la gestión de la operación de las IC.

- Elaborar un plan de seguridad para los operadores de IC en el que se detallen las características de seguridad que la entidad encargada desarrolle de acuerdo con normas industriales enfocadas en la seguridad de la información y protección de infraestructuras críticas.
- El modelo de selección de IC debe evaluar criterios del impacto que puede provocar el fallo de uno o varios servicios de una infraestructura crítica, en consecuencia, de posibles pérdidas económicas, sociales y hasta humanas.
- Evaluar criterios de dependencia entre servicios de las IC, de manera que el impacto que produzca el fallo de cualquier servicio de un sector crítico pueda afectar al servicio de otro.
- Analizar los posibles riesgos a los que se atiene todos los servicios de una IC, de acuerdo con el nivel de tolerancia que la entidad encargada del desarrollo crea conveniente para poder gestionar los riesgos de una manera eficiente.
- Realizar una gestión de riesgos en base a normas de seguridad de la información como ISO 31000 e ISO 27001, se deberá detallar el nivel de tolerancia que puede ser permitido en los fallos de un servicio de IC.
- Tomar en cuenta normas como la ISO/IEC 27001 como base para la gestión de la seguridad de la información, procurando la preservación de la información de carácter sensible para el ámbito público.

Capítulo V

Conclusiones y recomendaciones

En esta sección se presentan las conclusiones sobre la investigación realizada. Se explica la importancia del desarrollo de un modelo de selección de infraestructuras críticas y las recomendaciones para su ejecución. Además, se define una línea en la que se continúe el trabajo realizado utilizando la investigación planteada y el análisis al cual se ha llegado por medio del estudio de los modelos abordados.

Conclusiones

El análisis realizado ha permitido encontrar las diferencias entre los procedimientos realizados a nivel mundial para la selección de servicios e infraestructuras críticas tomando en cuenta la realidad situacional del estado o país que lo quiera aplicar.

Existe una organización, en el Ecuador, encargada del desarrollo de un catálogo de infraestructuras críticas. Sin embargo, hasta el momento no se ha encontrado un modelo similar a los desarrollados en otros países, que cumpla con las características para su efectividad.

El proceso metodológico utilizado para este trabajo, permitió encontrar y clasificar las metodologías que han sido analizadas de acuerdo a las características planteadas, el proceso de selección y clasificación de las mismas fue evaluado y sus resultados son de gran ayuda para los resultados de esta investigación.

El análisis realizado permitió recabar información necesaria que servirá de base para el desarrollo e implementación de un modelo de selección de infraestructuras críticas que cumpla con los parámetros establecidos por otras metodologías utilizadas en países desarrollados.

No todas las características de los modelos analizados pueden ser aplicadas al Ecuador, especialmente por su realidad social y económica. No obstante, muchas de ellas pueden ser adoptadas y adaptadas, siempre y cuando se realice un análisis profundo de cada una y de su aplicabilidad.

Los modelos seleccionados para el desarrollo de la investigación han sido implementados con éxito. Sus características y lineamientos han sido probados y aplicados por las entidades regulatorias respectivas (ENISA – Unión Europea y NIST - Estados Unidos).

Las características y modelos analizados cumplen con los parámetros establecidos para la protección de la información de infraestructuras críticas. Las características de cada uno de los modelos implantan procesos de protección en ámbitos sociales, económicos y civiles.

Se ha desarrollado recomendaciones o guidelines basadas en una comparación de modelos exitosos en diferentes países y que el Estado puede adoptar como parte de un proceso de desarrollo de un modelo de selección de infraestructuras críticas.

Recomendaciones

Se recomienda realizar un análisis por sectores estratégicos para desarrollar un modelo nacional de selección de infraestructuras críticas, que refleje la gestión de protección de la información de los servicios críticos. Se debe considerar las recomendaciones planteadas durante la ejecución de este estudio.

Se recomienda realizar un análisis extenso de la situación actual de Ecuador en ámbito de seguridad de la información y de Ciberdefensa, con el objetivo de gestionar procesos que puedan ser incluidos dentro un modelo de selección de infraestructuras críticas.

Se recomienda revisar las experiencias en la selección de infraestructuras críticas implementadas en otros países. Existen modelos ejecutados con éxito en países como España, Chile, Colombia que pueden ser adaptados a la realidad del Ecuador y podrían servir de apoyo al desarrollo del modelo nacional de selección de infraestructuras críticas.

Se recomienda implementar el modelo de selección de infraestructura crítica que defina en el futuro, incorpore las características planteadas en la presente investigación, ya que han sido analizadas y probadas en modelos de selección implementados con éxito en países con desarrollo destacado en ciberseguridad.

Referencias bibliográficas

Anna, S., Konstantinos, M., European Union, & European Network and Information Security Agency. (2016). *Stocktaking, analysis and recommendations on the protection of CIIs*. Publications Office. http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Avast. (s/f). *Qué es el ciberdelito y cómo defenderse contra él*. Recuperado el 23 de septiembre de 2019, de https://www.avast.com/es-es/c-cybercrime?hsSkipCache=true&hs_ungate__cos_renderer_combine_all_css_disable=true

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.

Brechner, J. (2016, julio 24). *La historia de la guerra es la historia de la humanidad*. La Prensa. https://www.prensa.com/opinion/historia-guerra-humanidad_0_4535546463.html

Carrillo, M. R. (2015). *EL CIBERESPACIO Y LA CIBERSEGURIDAD: Consideraciones sobre la necesidad de un modelo jurídico*. *124*, 18.

Clemente, D. (2013). *Cyber security and global interdependence: What is critical?* Royal Institute of International Affairs. http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf

ENISA. (s/f). *About ENISA* [Page]. Recuperado el 26 de noviembre de 2019, de https://www.enisa.europa.eu/about-enisa/about-enisa

Franco Crespo, A. A. (2013). EL USO DE LA TECNOLOGÍA: DETERMINACIÓN DEL TIEMPO QUE LOS JÓVENES DE ENTRE 12 Y 18 AÑOS DEDICAN A LOS EQUIPOS TECNOLÓGICOS. *RIED. Revista Iberoamericana de Educación a Distancia*, *16*(2). https://doi.org/10.5944/ried.16.2.9908

Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*, *0*(31), 109. https://doi.org/10.16924/riua.v0i31.217

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Guerrero Fernando. (s/f). *Centro de Ciberseguridad Industrial*. La Ciberseguridad Industrial en Ecuador. Recuperado el 2 de mayo de 2019, de https://www.cci-es.org/web/cci/detalle-pais/-/journal_content/56/10694/445446

INCIBE. (s/f). *Modelo de Análisis de Riesgos Ligero de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB)*. 43.

ITU. (s/f). *Cybersecurity*. Recuperado el 9 de julio de 2019, de https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Materese, R. (2015, enero 5). *About NIST* [Text]. NIST. https://www.nist.gov/about-nist

Mattioli, R., Levy-Bencheton, C., European Union, & European Network and Information Security Agency. (2014). *Methodologies for the identification of critical information infrastructure assets and services: Guidelines for charting electronic data communication networks.* ENISA. http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Mendoza, M. (2015, junio 16). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Miró Linares, F. (2012). *El cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio*. 27.

Newmeyer, P. D. K. (2015). Ciberespacio, ciberseguridad y ciberguerra. *II Simposio Internacional de Seguridad y Defensa*, 20.

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology*, *1.0*, 41.

Pagnotta, S. (2017, enero 4). *Ataques a infraestructuras críticas, ¿modalidad inminente en 2017?* | *WeLiveSecurity*. WeLiveSecurity by ESET. https://www.welivesecurity.com/la-es/2017/01/04/ataques-a-infraestructuras-criticas-2017/

Qué es INCIBE. (2016, enero 27). INCIBE. https://www.incibe.es/que-es-incibe

Rabinad, M. G. (2008). *LA SOBERANÍA DEL CIBERESPACIO Algunas reflexiones sobre el concepto de Estado, soberanía y jurisdicción frente a la problemática que presenta Internet*. 23.

RAE. (s/f-a). *Definición de seguridad—Diccionario del español jurídico—RAE*. Diccionario del español jurídico - Real Academia Española. Recuperado el 9 de julio de 2019, de https://dej.rae.es/lema/seguridad

RAE. (s/f-b). *«Diccionario de la lengua española»—Edición del Tricentenario. Definición de Terrorismo*. «Diccionario de la lengua española» - Edición del Tricentenario. Recuperado el 17 de septiembre de 2019, de https://dle.rae.es/

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007

Ron, M., Fuertes, W., Bonilla, M., Toulkeridis, T., & Diaz, J. (2018). *Cybercrime in Ecuador, an exploration, which allows to define national cybersecurity policies*. 1–7. https://doi.org/10.23919/CISTI.2018.8399357

Samaniego. (2018, mayo 25). *Formación y prevención frente a la amenaza "hacker": Así es el Incibe*. Nobbot. https://www.nobbot.com/redes/que-es-el-incibe/

Sciallo, J. (2019, marzo 22). *Acerca del Instituto nacional de estándares y tecnología*. https://docs.vmware.com/es/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-BA190912-9136-4803-8F7D-46FDB682E007.html

Subijana, I. J. S. (2008). EL CIBERTERRORISMO: UNA PERSPECTIVA LEGAL Y JUDICIAL. *San Sebbastian*, *22*, 169–187.

Taddeo, M. (s/f). *An analysis for a just cyber-warfare*. 11.

Toulkeridis, T., Bernabé, M. A., Baile, D. S., Carreón, D., Cerca, M., Culqui, J., González, M. E., González, M., Gutiérrez, C., Gutiérrez, R., Herrera, G., Padilla, O., Pauker, F., Fabián Rodriguez, Rodríguez, G., Salazar, R., Vasco, C., & Zacarías, S. (2015). *Gestión de Riesgo en el Ecuador*. Imprenta ESPE. https://doi.org/10.13140/RG.2.1.4092.5845

Valarezo, L. C. C., Carrillo, J. J. M., Alexandra, M., Muñoz, D., & Andrade, G. V. P. (2016). *Análisis de Riesgos tecnológicos en la cooperativa de ahorro y crédito Calceta Limitada*. 14.

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