Diseño de un modelo de ciberseguridad basado en el marco de ciberseguridad v1.1 de la NIST alineado a COBIT 2019, para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del sector de las telecomunicaciones. Caso de estudio Área de Transmisiones – Corporación Nacional de Telecomunicaciones.

Tipán Oscullo, Darío Javier

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

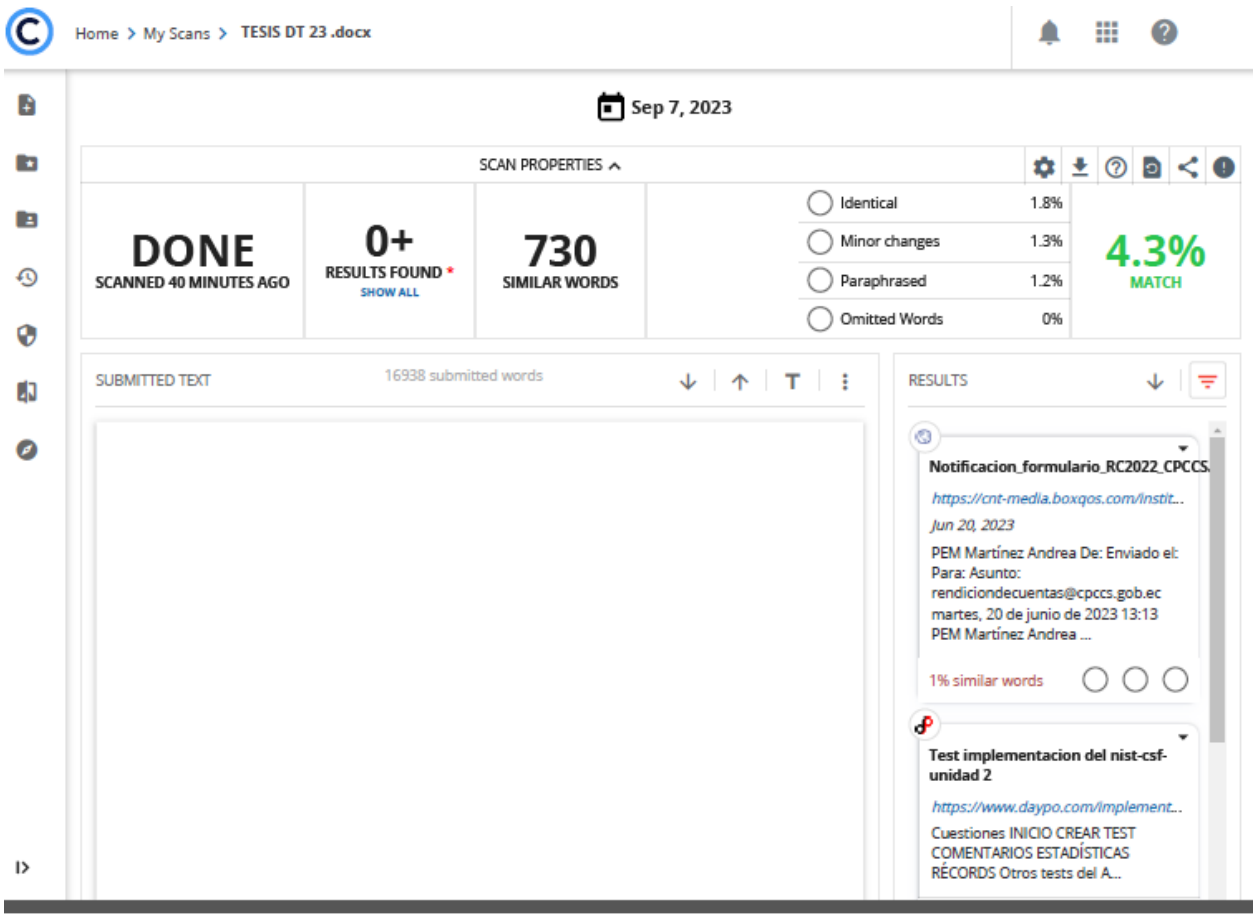
Centro de Posgrados

Maestría de Gerencia de Sistemas

Trabajo de titulación, previo a la obtención del título de Magíster en Gerencia de Sistemas

Msc. Ing. Pinto Auz, Diego Julián

23 Agosto 2023


Home > My Scans > TESIS DT 23 .docx
Sep 7, 2023
SCAN PROPERTIES
DONE
SCANNED 40 MINUTES AGO
0+
RESULTS FOUND *
SHOW ALL
730
SIMILAR WORDS
Identical 1.8%
Minor changes 1.3%
Paraphrased 1.2%
Omitted Words 0%
4.3%
MATCH
SUBMITTED TEXT
16938 submitted words
RESULTS
Notificacion_formulario_RC2022_CPCCS.
https://cnt-media.boxqos.com/instit...
Jun 20, 2023
PEM Martínez Andrea De: Enviado el: Para: Asunto: rendiciondecuentas@cpccs.gob.ec martes, 20 de junio de 2023 13:13 PEM Martínez Andrea ...
1% similar words
Test implementacion del nist-csf-unidad 2
https://www.daypo.com/implement...
Cuestiones INICIO CREAR TEST COMENTARIOS ESTADÍSTICAS RÉCORDS Otros tests del A...

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Certificación

Certifico que el trabajo de titulación: **"Diseño de un modelo de ciberseguridad basado en el marco de ciberseguridad v1.1 de la NIST alineado a COBIT 2019, para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del sector de las telecomunicaciones. Caso de estudio Área de Transmisiones – Corporación Nacional de Telecomunicaciones"**, fue realizado por el señor **Tipán Oscullo, Darío Javier**; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente

Sangolquí, 23 de agosto 2023.

DIEGO JULIAN PINTO AUZ

.....

Ing. Pinto Auz, Diego Julián, Mgtr.

Director

C.C.:1710807072

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Responsabilidad de Autoría

Yo **Tipán Oscullo, Darío Javier**, con cédula de ciudadanía n°1716195431, declaro que el contenido, ideas y criterios del trabajo de titulación: **Diseño de un modelo de ciberseguridad basado en el marco de ciberseguridad v1.1 de la NIST alineado a COBIT 2019, para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del sector de las telecomunicaciones. Caso de estudio Área de Transmisiones – Corporación Nacional de Telecomunicaciones,** 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, 23 de agosto 2023.

Firmado electrónicamente por:
DARIO JAVIER TIPAN OSCULLO

……..

Tipán Oscullo, Darío Javier.

C.C.:1716195431

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Autorización de Publicación

Yo **Tipán Oscullo, Darío Javier**, con cédula de ciudadanía n°1716195431, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Diseño de un modelo de ciberseguridad basado en el marco de ciberseguridad v1.1 de la NIST alineado a COBIT 2019, para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del sector de las telecomunicaciones. Caso de estudio Área de Transmisiones – Corporación Nacional de Telecomunicaciones** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 23 de agosto 2023.

Firmado electrónicamente por:
DARIO JAVIER TIPAN OSCULLO

……..

Tipán Oscullo, Darío Javier.

C.C.:1716195431

Dedicatoria

Al Señor Jesús, a mi amadísima Señora Virgen María y al Casto San José. A mi familia Jaime, Pilar y Lizbeth.

A la memoria de mis abuelitos Juan y Alfonso y de mis abuelitas Mercedes y Rosario, y de un gran amigo el Gral. Luis Duran.

A mi novia Silvia, quien me motivo para seguir hasta feliz término en la elaboración de la tesis.

A mi gran amigo Héctor Acosta, con quien hemos luchado por un sueño en común.

A mi gran amigo Eduardo Garcés, quien con sus consejos y ayuda, me enseñó que hay que perseverar en los estudios.

Darío Javier Tipán Oscullo

Agradecimiento

Al Ing. Diego Pinto por su compromiso, guía y paciencia durante el desarrollo de este proyecto.

Al Dr. Sang por su tiempo y comentarios de mejora para la elaboración de este trabajo.

Al Ing. Geovanny Ninahualpa por coordinar con mucha dedicación todos los trámites de la maestría.

A mis compañeros del área de transmisiones de la CNT, quienes fueron parte fundamental durante la elaboración de este trabajo.

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Resumen

El presente trabajo propone un modelo de ciberseguridad alineado a los objetivos empresariales de la Corporación Nacional de Telecomunicaciones (CNT) que permita minimizar el riesgo y aplicar gobernanza en un sistema de infraestructura crítica como caso de estudio el área de transmisiones de la CNT, la cual permite mantener la disponibilidad de conectividad e interconexión en el país. De esta manera, se ha planteado como objetivo: diseñar un modelo de ciberseguridad con el fin de evaluar e identificar procesos y controles que permitan mantener la integridad, disponibilidad y confidencialidad de la información a ser transportada en las redes de transmisión. La metodología empleada en este estudio se basó en la revisión bibliográfica y documental de estudios relacionados con temas de ciberseguridad alineados a la estrategia empresarial de un sistema de infraestructura crítica, utilización de marcos para análisis de riesgos, ciberseguridad y gobernanza. Los resultados de este diseño indican que seis objetivos de gobierno y gestión se alinean a los requerimientos de la alta dirección de la CNT, el nivel actual de ciberseguridad es riesgo informado y son necesarios 21 proyectos quick wins para optimizar los procesos con una inversión baja y de esta manera mejorar el nivel de ciberseguridad de la CNT. Este modelo propuesto es la base para que las actividades de gobierno y gestión generen valor a través del objetivo de asegurar la optimización del riesgo mediante un enfoque de mejora continua.

Palabras clave: modelo de ciberseguridad, riesgo, redes de transmisión, gobernanza

Abstract

The present work proposes a cybersecurity model aligned with the business objectives of the National Telecommunications Corporation (CNT) that allows minimizing risk and applying governance in a critical infrastructure system as a case study of the transmission area of the CNT, which It allows maintaining the availability of connectivity and interconnection in the country. In this way, the objective has been set: to design a cybersecurity model in order to evaluate and identify processes and controls that allow maintaining the integrity, availability and confidentiality of the information to be transported in the transmission networks. The methodology used in this study was based on the bibliographical and documentary review of studies related to cybersecurity issues aligned to the business strategy of a critical infrastructure system, use of frameworks for risk analysis, cybersecurity, and governance. The results of this design indicate that six governance and management objectives are aligned with the requirements of the CNT's senior management, the current level of cybersecurity is an informed risk and 21 quick wins projects are necessary to optimize processes with a low investment and in this way improve the level of cybersecurity of the CNT. This proposed model is the basis for governance and management activities to generate value through the objective of ensuring risk optimization through a continuous improvement approach.

*Keywords: c*ybersecurity model, risk, security networks, transmission, governance.

Capítulo I

Generalidades

En el primer capítulo se plantea el problema, el cual será el motivo de estudio durante el desarrollo del presente proyecto. Se definen los objetivos y se determina la justificación, importancia y alcance del mismo.

Antecedentes

El cibercrimen y la inseguridad cibernética en el top 5 de los riesgos globales según el Foro Económico Mundial (FEM), dejando al descubierto la necesidad de que las organizaciones desde su planeación estratégica incluyan proyectos de seguridad alineados a los objetivos de la gestión estratégica del negocio. (Deloitte, 2020). La emergencia sanitaria originada por el coronavirus ha evidenciado no solo la importancia de Internet como vehículo de conexión, información y comunicación de la sociedad, sino también la necesidad de disponer de redes de telecomunicaciones fuertes que los sustenten. La incertidumbre en esta crisis sanitaria, económica e incluso social se ha visto matizada, con cierto alivio por la seguridad que nos proporcionan unas infraestructuras de comunicaciones sólidas, fiables, estables y seguras. (Telefonica, 2020)

En el país, la conectividad y la interconexión de las instituciones públicas, educativas y operadores privados se la realiza a través de las redes de transmisión de la CNT, por lo que es necesario un modelo de ciberseguridad alineado un marco de gobernanza que permita mantener la disponibilidad de los servicios y permita a la empresa ser el principal socio tecnológico del país.

De acuerdo al informe correspondiente al índice global de ciberseguridad 2018 (ICG) de la Unión Internacional de Telecomunicaciones (UIT), el Ecuador se encuentra en el puesto 66 de 193 países a nivel mundial. El país está considerado por tener un nivel intermedio de compromiso con la seguridad cibernética, por la creación de un Centro de Respuestas a Incidente Informáticos (ECUCERT) (UIT, 2018), el cual debe complementarse con los procesos, políticas y controles que se apliquen en las empresas para mantener la integridad, disponibilidad y confidencialidad de la información que se transporta en las redes de interconexión.

Sin embargo, según (Ron, Rivera, Fuertes, & Toulkeridis, 2019), en el Ecuador varias compañías del sector público y privado no están seguras de la importancia de aplicar estándares de seguridad sobre su infraestructura de tecnologías de información (TI), a pesar que de acuerdo a (Kapersky, 2017), los sistemas de infraestructura critica han sufrido ciberataques en un 45%. Actualmente, el país recién cuenta con una estrategia nacional de ciberseguridad, la cual establece los lineamientos, políticas y controles para tener un ciberespacio seguro (Mintel, 2022)

Planteamiento del Problema

En Ecuador, de acuerdo a (Mintel, 2019a), se ha realizado la revisión de la madurez de la capacidad de ciberseguridad con el fin de permitir al gobierno ecuatoriano comprender su capacidad de ciberseguridad para priorizar estratégicamente la inversión en este sector y poder definir la estrategia de ciberseguridad.

Sin embargo, según (OEA, 2020), en el país todavía se tiene deficiencias en la identificación y organización de infraestructura critica, falta de políticas de seguridad cibernética y una baja resiliencia de la infraestructura del internet, lo cual se refleja en bajos índices de

confianza del usuario en el internet, servicios de gobierno electrónico y servicios de comercio electrónico. Según (CISA, 2018), las redes de transmisión de datos son un componente integral para la economía de un país, siendo la base para la operación de todos los negocios, organizaciones de seguridad nacional y gobierno.

En el país, la CNT a través de su plataforma tecnológica de transmisión interconecta y provee servicios para las instituciones del estado ecuatoriano, ejército, policía nacional, unidades educativas públicas e infocentros. (CNT, 2017). Por lo tanto, es necesario un modelo basado en el marco de ciberseguridad para infraestructuras criticas como el de la NIST v1.1 alineado a COBIT 2019, el cual permita generar valor a la CNT al optimizar el riesgo cibernético de la plataforma tecnológica de transmisión, se alinee a la estrategia de la empresa al mantener la disponibilidad del servicio de Internet y sea un complemento importante para las tareas de respuesta a incidentes del ECUCERT.

Objetivos del proyecto

Diseñar un modelo de ciberseguridad basado en el marco de ciberseguridad v1.1 para infraestructuras críticas de la NIST alineado a COBIT 2019 para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del sector de las telecomunicaciones, teniendo como caso de estudio al Área de Transmisiones de la Corporación Nacional de Telecomunicaciones

Justificación, importancia y alcance del proyecto

La presente propuesta será beneficiosa para los sistemas de infraestructura crítica del sector de las telecomunicaciones tal como la red de transmisiones de la CNT, debido a que al aplicar una norma específica de ciberseguridad para sistemas de infraestructura crítica como el

marco de ciberseguridad v1.1 de la NIST alineado a COBIT 2019, permitirá determinar el nivel de los procesos, políticas y controles definidos de acuerdo a un análisis de riesgos mediante la norma NIST 800-30. Esto permite que la ciberseguridad y la red de transmisión se constituyan en habilitadores importantes en el proceso de alcanzar y cumplir los objetivos empresariales, los cuales son alta disponibilidad de conectividad para los sectores de finanzas y educación, reducción del nivel de impacto económico y social de posibles ataques cibernéticos y concientización de implementar una cultura de ciberseguridad que se ajuste a los objetivos de la organización.

Cabe recalcar que el proyecto tendrá incidencia como aporte al establecer lineamientos a los sistemas de infraestructura crítica que se alineen a la estrategia nacional de ciberseguridad establecida, se implementen modelos de ciberseguridad de acuerdo al sector y sirvan para trabajar en conjunto con el ECUCERT, el cual se encarga de tareas reactivas en materia de ciberseguridad. Sin embargo, las fases de identificar, proteger, detectar y recuperar es responsabilidad de cada empresa y estas deben estar de acorde a los activos digitales de las mismas

En base a lo mencionado, el proyecto plantea el diseño de un modelo de ciberseguridad basado en el marco de ciberseguridad v1.1 de la NIST alineado a COBIT 2019 para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del sector de las telecomunicaciones tomando como caso de estudio al área de transmisiones de la CNT, la cual es la encargada de que la empresa sea el socio tecnológico de todo el país. En este diseño se realiza un análisis de riesgos cibernéticos y una propuesta de modelo de ciberseguridad alineado a la estrategia de la empresa para que la red de transmisiones permita mantener el nivel de interconexión y conectividad, reduzca el nivel de impacto económico y social de los ciberataques en el país.

Hipótesis de investigación

Si se diseñara un modelo de ciberseguridad utilizando un marco de ciberseguridad alineado a un marco de gobierno y gestión, se podría determinar perfiles de ciberseguridad en los cuales los procesos y controles tengan relación directa con los objetivos empresariales.

Categorización de las variables de investigación

Las variables que se manejan para este proyecto son independientes y dependientes.

Las variables independientes son:

- Norma NIST v1.1 ciberseguridad.
- COBIT 2019
- Activos

Las variables dependientes son:

- Nivel de interconexión y conectividad
- Nivel de impacto de ciberataques
- Riesgos
- Amenazas
- Vulnerabilidades

Marco teórico referencial

Se realiza la descripción de las definiciones más importantes que servirán como base para el desarrollo del siguiente proyecto:

Ciberseguridad: de acuerdo a (Leiva, 2015), la ciberseguridad se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información. Es decir, es donde los controles de ciberseguridad son eficaces y el ciberespacio es considerado confiable, flexible y seguro para los sistemas de infraestructura critica.

Infraestructuras Críticas: según (Aguirre, 2017), es el conjunto de activos tecnológicos indispensables, que interactúan entre sí para brindar servicios vitales a los habitantes de un país. Los activos pueden ser instalaciones físicas o virtuales, redes de datos, redes industriales, sistemas de información que permiten la prestación o el monitoreo de servicios esenciales para el bienestar de la población y el sostenimiento de la economía de un país.

Riesgo Cibernético: es catalogado como uno de los riesgos emergentes de impacto público y de prioridad estratégica para la industria y los gobiernos alrededor del mundo. (WoldEconomicForum, 2018)

Análisis de Riesgos: es un proceso sistemático que permite determinar con magnitudes los riesgos a los que está expuesta una organización. Se le conoce además como un proceso para comprender la naturaleza del riesgo. Se refiere también a la identificación de amenazas que acechan a los sistemas de información, determinando la vulnerabilidad y el impacto (MAGERIT, 2012).

COBIT: es un marco de gobierno, que es elemento vital para la formulación de la estrategia y el éxito de la transformación del negocio.

Cybersecurity Framework (CSF): es un marco de la NIST, el cual tiene un enfoque basado en el riesgo para gestionar la ciberseguridad. Está compuesto por el núcleo del marco, los niveles de implementación del marco y los perfiles del mismo. Cada componente del framework refuerza la conexión entre los impulsores del negocio y las actividades de ciberseguridad. (NIST, 2020).

Redes de comunicaciones: son un componente integral para la economía de un país, siendo la base para la operación de todos los negocios, organizaciones de seguridad nacional y gobierno, permitiendo la interconexión y conectividad a nivel nacional y mundial. (CISA, 2018)

Capítulo II

Revisión del Estado del Arte

De manera general, los sistemas de infraestructura critica son información interconectada e infraestructuras de comunicación esenciales para el mantenimiento de los servicios básicos de la sociedad (salud, seguridad, bienestar económico o social de las personas) cuyo daño o destrucción tendría serias consecuencias tales como pérdidas de vidas humanas y económicas (Meridian, 2016).

Estos sistemas tienen ciertas características entre las más destacables se encuentran la dependencia de las industrias a la infraestructura de red en sus procesos productivos, el software malicioso como una amenaza de primer nivel, la existencia de casos conocidos específicos para sistemas de control y el cibercrimen como servicio (INCIBE, 2019).

De acuerdo al reporte de ciberseguridad para América Latina del año 2020 realizado por la Organización de Estados Americanos (OEA, 2020), existe la necesidad de que las organizaciones desde su planeación estratégica incluyan proyectos de seguridad alineados a los objetivos de la gestión estratégica del negocio. Es importante diferenciar que la gestión de seguridad de la información es mucha más amplia y abarca información sin importar el formato, mientras que la ciberseguridad se enfoca en información digital y cualquier otro elemento que no sea información pero que se gestione, opere o maneje a través de tecnologías de información y comunicación.

En Ecuador, se tienen varios trabajos relacionados a seguridad de la información y ciberseguridad. En el ámbito educativo, se han elaborado proyectos en los cuales se analiza la situación actual de la ciberseguridad en el país (Aguirre, 2017), se evalúa las medidas de seguridad de la información que se han tomado hasta el 2018, en donde lo más sobresaliente

es la creación del ECUCERT (Ron, Bonilla, & Fuertes, 2016) . En cuanto a estudios sobre ciberseguridad en infraestructuras críticas, se observa que existe interés en determinar los retos que enfrenta el sector financiero mediante la identificación de potenciales riesgos a través de entrevistas estructuradas al personal directivo y la capacidad de respuesta que tienen las instituciones bancarias ante incidentes cibernéticos (Quintana, 2016). En lo que se refiere a ciberseguridad industrial aplicada al sector energético, no se ha encontrado trabajos relacionados realizados en el país.

En la Tabla 1, se muestran artículos de investigación referentes a modelos de ciberseguridad, análisis de riesgos y controles de ciberseguridad, en los cuales se describen el problema detectado, la solución aplicada y la metodología de ciberseguridad utilizada.

Tabla 1

Artículos de modelos de ciberseguridad

Artículo	**Problema**	**Solución**	**Metodología**
Lara Guijarra Elva Gioconda (2019) Diseño de un modelo de seguridad de la información para centros de educación	Falta de un modelo de seguridad de la información para centros de educación	Análisis de riesgos y diseño de un modelo bajo estándares internacionales.	OSSTMMv3, NIST SP800-30 e ISO 27001
Gómez Suarez Álvaro José (2019). Diseño de un programa de ciberseguridad de una empresa basado en el marco de trabajo de la NIST	Falta de una estrategia de seguridad cibernética bajo un marco especifico	Determinar los modelos normas y lineamientos que se ajusten a la empresa en lo relacionado a ciberseguridad	Marco de ciberseguridad de la NIST
Mendoza Silva Luis Fernando (2019). Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SISC.	Incapacidad de la empresa para detectar y responder a un evento de ciberseguridad	Identificar brechas de ciberseguridad para diseñar y proponer controles	Marco de ciberseguridad para infraestructuras criticas NIST V1.1.

Artículo	Problema	Solución	Metodología
Erreyes Pinzón Daysi Mireya (2017) Metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles	Falta de una guía práctica que permita seleccionar herramientas válidas para mejorar el nivel de protección	Diseño de una metodología bajo estándares de seguridad informática	ISO 27001, NIST SP800-30, COBIT 5 y OWASP
Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información.	Es frecuente que empresas de diversos sectores económicos reporten pérdidas debido a fallas y/o ataques sobre sus servicios de TI	Dos pilares fundamentales para realizar el análisis de riesgos: los estándares y normas, de un lado, y las metodologías, de otro	OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) [9] es una metodología desarrollada por el CERT/CC2 [11, 12] que tiene por objeto facilitar la evaluación de riesgos en una organización.

Nota. En la tabla se muestran los artículos sobre modelos de ciberseguridad. Recuperado de (Erreyes, 2017) (Gomez A. , 2019) (Gomez, Perez, & Donoso, 2010) (Mendoza, 2019).

En todos los trabajos mencionados, se evidencia el uso de metodologías de ciberseguridad. Sin embargo, se verifica que no existen trabajos que integren los mismos con marcos de gobernanza de TI como COBIT 2019.

De lo expuesto, se puede determinar que, en el país, no se han realizado trabajos de investigación sobre marcos de ciberseguridad alineados a marcos de gobernanza de TI en infraestructuras críticas del sector de las telecomunicaciones, que permitan establecer procesos y controles para mantener la confidencialidad, integridad y disponibilidad de la información y a la vez cumplir con los objetivos empresariales.

Capítulo III

Análisis de Riesgos

En el presente capítulo se realizará un análisis de riesgo utilizando la metodología del Instituto Nacional de Estándares y Tecnología de Estados Unidos NIST SP 800-30. Se selecciono esta metodología en razón de que cada fase tiene un objetivo específico y enumera todos los enfoques posibles para procesar los datos, a diferencia de otras metodologías como OCTAVE, CRAMM y FRAP, las cuales simplemente ofrecen descripciones de cada fase, ver Tabla 2.

Tabla 2

Fases de metodologías de riesgo

Metodología	Tipo	Fases
NIST 800-53	Cualitativa y Cuantitativa	Caracterización del sistema X Identificar amenazas Identificar vulnerabilidades Análisis de controles Determinación de probabilidad Análisis de impacto Determinación del riesgo Recomendaciones de control Documentación

Metodología	Tipo	Fases
OCTAVE	Cualitativa	Perfil de amenaza
		Vulnerabilidades de infraestructura
		Desarrollo de estrategia de seguridad y plan
FRAP	Cuantitativa	Reunión Pre-FRAP
		Sesión FRAP
		Proceso Post FRAP
CRAMM	Cualitativa	Identificación de activos
		Evaluación de amenazas y vulnerabilidades
		Selección de contramedidas y recomendación

Nota. En la tabla se muestra las fases de metodologías de riesgo. Recuperado de Risk Assestment Method: A review por N. Akaml, 2018, Universiti Teknikal.

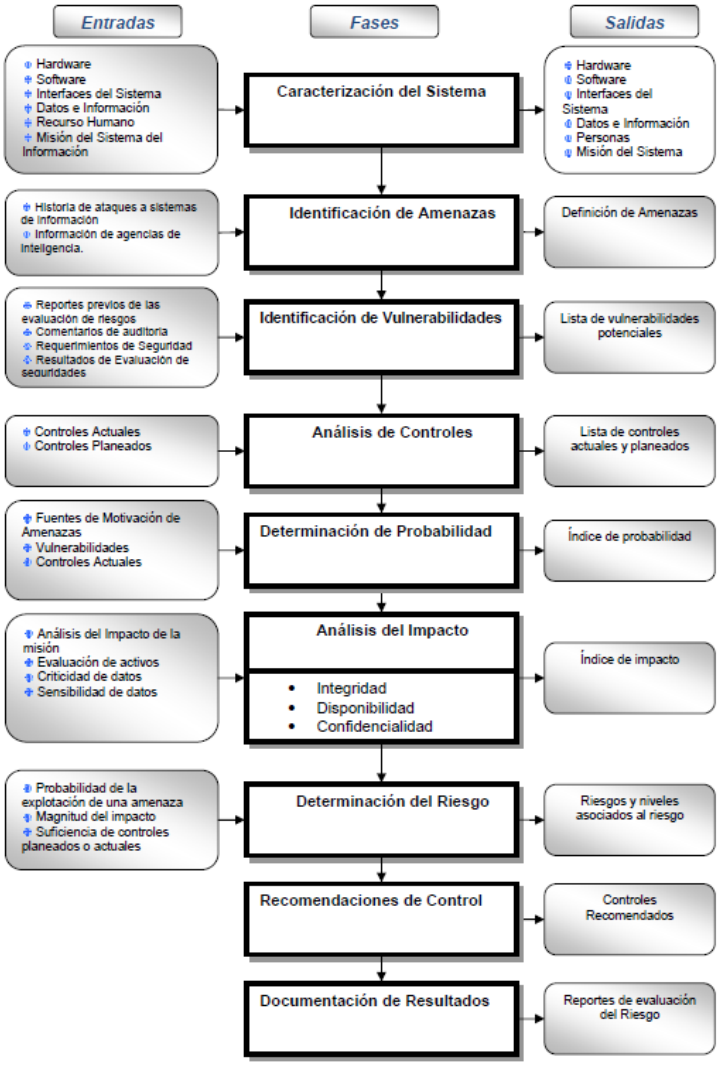
Además, esta metodología utiliza técnicas de obtención de información como entrevistas, cuestionarios para solicitar información relacionada al ambiente del sistema a analizar, así como también utiliza conclusiones y descubrimientos mencionados en documentación relacionada.

Esta metodología se enfoca en proteger los sistemas informáticos que almacenan, procesan y transmiten información al identificar sus activos, amenazas, vulnerabilidades y determinar el riesgo existente ante un posible impacto sobre el activo. De esta manera, se pueden tomar decisiones para identificar que controles y mecanismos de seguridad son necesarios para la organización teniendo en cuenta el factor riesgo inversión. (NIST, 2012)

La evaluación de riesgos comprende nueve fases las cuales son personalizadas para cada organización según las necesidades. Cada fase tiene entradas y salidas que se interrelacionan para elaborar la matriz de riesgos, como se muestra en la Figura 1.

Figura 1

Pasos metodología NIST Sp 800-30



Nota. El gráfico representa las fases de la metodología NIST 800-30. Tomado de guía NIST SP 800-30 por V. Avalos, 2007, NIST.

A continuación, se describen los pasos de la metodología de riesgos:

- **Caracterización del sistema**: define el alcance que va tener la evaluación de riesgos en la organización, los limites operacionales y proporciona información para definir el riesgo.
- **Identificación de Amenazas:** establecer las fuentes de amenazas potenciales y recopilar una lista de amenazas aplicables al sistema evaluado.
- **Identificación de vulnerabilidades:** desarrollar una lista de vulnerabilidades del sistema que pueden ser explotadas por las amenazas identificadas en el paso previo.
- **Análisis de controles:** verificar el funcionamiento de los controles establecidos o si es necesario establecer nuevos controles para reducir la probabilidad de que una amenaza aproveche una vulnerabilidad del sistema.
- **Determinación de la probabilidad:** analiza los factores principales tales como capacidad y motivación de la fuente de amenaza, naturaleza de la vulnerabilidad, existencia y eficacia de controles.
- **Análisis de impacto:** determina la magnitud o tipo de afectación en el escenario que la amenaza se ejecutará de manera exitosa en el sistema en términos de integridad, disponibilidad y confidencialidad.
- **Determinación del riesgo:** evalúa el nivel del riesgo considerando la probabilidad y magnitud de impacto de las amenazas identificadas.
- **Recomendaciones de control:** proporcionan los controles que pueden mitigar los riesgos identificados.

- **Documentación de resultados:** es un informe de evaluación de riesgos que permite a la alta dirección tomar decisiones para reducir y corregir pérdidas potenciales.

Caracterización del Sistema de Infraestructura Crítica -Sector Telecomunicaciones

Actualmente, la red de transmisiones es la encargada de permitir la interconexión y conectividad a sectores de la educación, salud, diferentes instituciones públicas y operadores privados de telecomunicaciones. Con el advenimiento de las redes 5G, el internet de las cosas y las redes definidas por intención, pueden surgir nuevas brechas de seguridad por lo que es necesario que las redes sean capaces de transportar la información de una manera segura, optimizando el nivel del riesgo antes las amenazas cibernéticas y manteniendo la disponibilidad del servicio de internet.

El propósito del análisis de riesgos es identificar las amenazas y vulnerabilidades de los sistemas de información del área de transmisiones de la CNT, que permiten realizar tareas de configuración y troubleshooting. Esto con el fin de salvaguardar los activos de información de ciberataques y realizar una correcta gestión de riesgos de ciberseguridad que permitan tomar decisiones alineadas a los objetivos de la empresa y mantener la disponibilidad de los servicios ofertados.

El área de transmisiones comprende todos los equipos administrados por el área de Fibra Óptica. Todo el tráfico de las redes IP/MPLS, redes de Acceso Móvil (3G HSPA+, LTE), redes de Acceso Fijo (DSLAM y GPON) se transporta por las redes de alta capacidad con tecnología de jerarquía digital sincrónica (SDH) y de multiplexación por división de longitud de onda (DWDM). Actualmente, sistemas de gestión permiten realizar tareas de configuración, obtener reportes de la alarmas y conexión remota a 676 equipos SDH, 1075 equipos DWDM y monitorea 10260 Km de fibra óptica a nivel nacional.

El personal encargado de la administración, configuración y tareas de mantenimiento utiliza los siguientes recursos:

- **Hardware**

El área de transmisiones se encuentra dividida en los siguientes departamentos a nivel de la zona Andina la cual corresponde a las provincias de la Sierra- Oriente y zona Pacífico la cual abarca todas las provincias de la Costa y región Insular, en las cuales se disponen los siguientes computadores portátiles para conectarse a los sistemas de gestión de los equipos y otros sistemas de la CNT, ver Tabla 3.

Tabla 3

Listado equipos portátiles

Departamento	**Zona**	**Equipos Portátiles**
Red Troncal	Andina / Pacífico	14
Anillos Metropolitanos	Andina / Pacífico	14
Unidad Fibra Óptica	Andina / Pacífico	8
Panamericano	Pacífico	5

Nota. En la tabla se muestra el listado de equipos portátiles.

De la misma manera, en los departamentos del área se disponen de los siguientes equipos tecnológicos tales como servidores físicos y virtualizados, teléfonos IP, switchs entre otros, los cuales permiten dar soporte a las tareas de configuración, interconexión con la red interna y externa de la empresa ver Tabla 4.

Tabla 4

Listado equipos tecnológicos

Equipos Tecnológicos	Modelo
Servidor primario físico Huawei	M4000
Servidor secundario físico Huawei	M4000
Servidor primario virtualizado Fiberhome	VMware ESXi 6.7
Servidor secundario virtualizado Fiberhome	VMware ESXi 6.7
Teléfonos IP	Cisco 7960
Switch	Cisco 2960 24 puertos
Router AP	Tplink 3 antenas
Firewall	Checkpoint VSX
Impresora	Canon MF634

Nota. En la tabla se muestra el listado de equipos tecnológicos.

- **Software**

El inventario de software detalla los programas informáticos que utilizan los funcionarios del área de transmisiones para cumplir con sus actividades diarias, ver Tabla 5.

Tabla 5

Listado Software

Software	Función
Sistema de gestión U2000 Huawei	Revisión, configuración y troubleshooting de enlaces DWDM y SDH
Sistema de gestión UNM2000 Fiberhome	Revisión, configuración y troubleshooting de enlaces DWDM
Sistema Remedy	Revisión, cambios y cierre de ordenes de trabajo
Sistema Sismac	Actualización de inventario de tarjetas y módulos equipos SDH y DWDM
Antivirus Panda	Revisión de archivos infectados con virus

Nota. En la tabla se muestra el listado de software.

- **Servidores**

De acuerdo a la Tabla 4, se indica que se tienen servidores físicos para la gestión de equipos Huawei y virtualizados para los equipos marca Fiberhome. En las tablas 6 y 7 se detallan las características de los servidores a nivel de hardware y software.

Tabla 6

Características servidores M4000 Huawei

Hardware	Software
Disco Duro de 51 GB	Sistema Operativo Sun OS 5.10
RAM 4 procesadores de 2.6 Ghz	NMS U2000 V200R016C060
Energía 110 V	Base de Datos MySQL
End of Service 2019	Veritas Cluster Server

Nota. En la tabla se muestra las características del servidor Huawei.

Tabla 7

Características servidores Fiberhome

Hardware	Software
Disco duro de 1 x 1.5TB + 1 x 1TB	Sistema operativo Windows Server 2012 R2
CPU 24 vCPU	Veritas Cluster Server 7.4.1
Memoria 96 GB	UNM200 V4R1M11
Hypervisor VMware ESXi 6.7	Symantec Endpoint Protection 12.0 Server

Nota. En la tabla se muestra las características del servidor Fiberhome.

Por lo tanto, el análisis de riesgos se realizará sobre los activos de información del caso de estudio área de transmisiones CNT, los cuales permiten la habilitación de servicios de altas capacidades para la conectividad de estas redes, considerando esquemas de protección efectivos que garanticen una alta disponibilidad de cada uno de los servicios para incrementar el nivel de satisfacción del cliente respecto a cobertura y calidad de los servicios que presta la CNT.

En esta fase de la metodología, como paso previo a la identificación de activos, es necesario definir la clasificación de los activos como primarios y de soporte. Los activos primarios son los procesos de negocio y la información de las actividades mientras que los de soporte son los elementos del sistema de información que frecuentemente tratan de ser vulnerados. Estos activos se etiquetarán de la siguiente manera, ver la Tabla 8.

Tabla 8

Clasificación de Activos

Grupo de Activo	Tipo de Activo	Descripción	Identificación
Primario	Dato	Información que se maneja en el área	INFO
Soporte	Tecnología	Hardware donde se procesa la información	HW
Soporte	Aplicación	Software que se utiliza para dar soporte a los procesos	SW
Soporte	Instalación	Lugar donde se encuentran los activos de información	INS
Soporte	Personal	Analistas que manejan los activos	PER
Soporte	Servicio	Servicios que brinda el área	SERV
Soporte	Redes	Interconexión con la red interna y externa	NET

Nota. En la tabla se muestra la clasificación de activos. Recuperado de Análisis y diseño de un sistema de gestión de la seguridad de la información para el GAD de Pujili, G. Orozoco, 2021, Universidad de las Fuerzas Armadas.

Identificación de Activos

La identificación de activos es un punto clave para la identificación de las amenazas y vulnerabilidades y determinar el nivel de riesgo o exposición de los activos y selección de controles para mitigarlos. (Mintel, 2019c).

El inventario de activos para el área de transmisiones se muestra en la Tabla 9, el cual es el resultado de levantar la información de manera física y lógica en las distintas dependencias de la CNT y clasificarlos de acuerdo al tipo de activo.

Tabla 9

Inventario de Activos

Nº	ID	Tipo	Activo	Descripción	Ubicación
1	INFO-001	Dato	Archivos de Datos	Carpetas de almacenamiento	Quito Centro Datacenter
2	INFO-002	Dato	Documentación Impresa	Ingenierías de direcciones IP y puertos	Quito Centro
3	INFO-003	Dato	Base de Datos	MySQL	Quito Centro Datacenter
4	HW-001	Tecnología	Servidores	Servidor M4000 Huawei y Virtualizado Firberhome	Quito Centro Datacenter
5	HW-002	Tecnología	Equipo multifuncional	Impresora / Copiadora	Quito Centro
6	HW-003	Tecnología	Teléfono	Cisco IP	Quito Centro
7	NET-001	Redes	Firewall	Checkpoint VSX	Datacenter
8	NET-002	Redes	Switch	Cisco 2960	Quito Centro
9	NET-003	Redes	Router AP	Tplink	Quito Centro
10	SW-001	Aplicación	Sistemas Operativos	Sun OS 5.1 Windows Server 2012 R12	Quito Centro Datacenter

Nº	ID	Tipo	Activo	Descripción	Ubicación
11	SW-002	Aplicación	Plataformas de Gestión Dwdm-Sdh	Sistema U2000 y Nnm2000	Quito Centro Datacenter
12	SW-003	Aplicación	Antivirus	Panda / Symantec Endpoint	Quito Centro
13	SW-004	Aplicación	Gestor Base de Datos	MySQL	Quito Centro Datacenter
14	SW-005	Aplicación	Clúster de Alta Disponibilidad	Veritas Cluster Server	Quito Centro Datacenter
15	SW-006	Aplicación	Licencias	Sistemas Gestión, OS, Bases de Datos, Veritas, Antivirus	Datacenter
16	SERV-001	Servicios	Configuración	Configuración de Enlaces para transmisión de datos e internet.	Todos los Nodos Cnt
17	SERV-002	Servicios	Soporte	Mantenimiento Preventivo y Correctivo	Todos los Nodos Cnt
18	PER-001	Personal	Técnicos	Analistas de Redes de Fibra	Quito Centro
19	PER-002	Personal	Responsable	Jefe de O&M Transmisión	Quito Centro

Nota. En la tabla se muestra el inventario de activos de acuerdo a su clasificación.

Una vez realizada la identificación de activos es necesario valorar los mismos, en términos de Confidencialidad, Integridad y Disponibilidad para determinar de manera cualitativa la criticidad de los distintos activos. (Mintel, 2020).

En la Tabla 10, se muestran las referencias para la valoración de los activos:

Tabla 10

Escalas para valoración de Activos

Criterio	Valor	Criticidad	Descripción
Confidencialidad (C)	1	Baja	El acceso y divulgación de información no autorizada del activo no afecta a las actividades del área.
	2	Media	El acceso y divulgación de información no autorizada del activo afecta limitadamente a las actividades del área.
	3	Alta	El acceso y divulgación de información no autorizada del activo tiene un efecto crítico sobre las actividades del área.
Integridad (I)	1	Baja	La modificación no autorizada del activo afecta levemente a las actividades del área.
	2	Media	La modificación no autorizada del activo afecta considerablemente a las actividades del área.
	3	Alta	La modificación no autorizada del activo tiene un efecto severo sobre las actividades del área
Disponibilidad (D)	1	Baja	La interrupción al acceso del activo afecta levemente a las actividades del área.
	2	Media	La interrupción al acceso del activo afecta considerablemente a las actividades del área.
	3	Alta	La interrupción al acceso del activo tiene un efecto severo sobre las actividades del área

Nota. En la tabla se muestra la escala para valoración de activos. Recuperado de Guía para la Gestión de Riesgos, por Mintel, 2020.

En la Tabla 11, se muestra la valoración de cada activo del área de transmisiones, teniendo en cuenta que el valor final es el promedio de los valores asignados en términos de

confidencialidad, integridad y disponibilidad, en un intervalo de 1 a 3, en el cual el valor de tres representa el nivel más alto de criticidad y el valor de uno el nivel más bajo.

Tabla 11

Valoración de Activos

ID	Activo	C	I	D	Valor	Criticidad
INFO-001	Archivos de Datos	2	2	3	2.33	Alta
INFO-002	Documentación Impresa	2	2	2	2	Media
INFO-003	Base de Datos	3	3	3	3	Alta
HW-001	Servidores	3	3	3	3	Alta
HW-002	Equipo multifuncional	0	1	2	1	Baja
HW-003	Teléfono	0	0	1	0.33	Baja
NET-001	Firewall	2	3	3	2.66	Alta
NET-002	Switch	2	2	3	2.33	Alta
NET-003	Router AP	1	2	3	2	Media
SW-001	Sistemas Operativos	2	2	3	2.33	Alta
SW-002	Plataformas de Gestión Dwdm-Sdh	3	3	3	3	Alta
SW-003	Antivirus	1	0	2	1	Baja
SW-004	Gestor Base de Datos	3	3	3	3	Alta
SW-005	Clúster de Alta Disponibilidad	3	3	3	3	Alta
SW-006	Licencias	2	2	3	2.33	Alta
SERV-001	Configuración	2	2	3	2	Media

ID	Activo	C	I	D	Valor	Criticidad
SERV-002	Soporte	2	2	2	2	Media
PER-001	Técnicos	2	2	2	2	Media
PER-002	Responsable	2	2	2	2	Media

Nota. En la tabla se muestra la valoración de activos.

Identificación de Amenazas/ Vulnerabilidades

Una amenaza es activar accidentalmente o explotar intencionalmente una vulnerabilidad especifica. El NIST establece como primer paso determinar los tipos de fuentes de amenaza que pueden aplicarse sobre los activos identificados con criticidad alta. (NIST, 2012). Los tipos de fuentes de amenazas se pueden clasificar como se muestra en la siguiente Tabla 12.

Tabla 12

Tipos de fuentes de amenaza

Tipo	Identificación	Descripción
Adversa	AD	Individuos, grupos, organizaciones o países buscan explotar la dependencia de la organización sobre los recursos cibernéticos.
Accidental	A	Acciones erróneas realizadas por el personal de la empresa sobre los activos al ejecutar sus actividades diarias.
Estructural	E	Falla de equipos, controles ambientales o software debido a el envejecimiento, agotamiento de recursos u otras, que exceden los parámetros óptimos.
Ambiente	AMB	Desastres naturales y fallas en los servicios de infraestructuras críticas de los cuales la empresa depende para su funcionamiento

Nota. En la tabla se muestra los tipos de fuentes de amenaza. Recuperado de Risk Assestment, por NIST, 2012

En la Tabla 13, se muestran los tipos, subtipos de fuentes de amenaza que son aplicables a los activos identificados.

Tabla 13

Tipos y subtipos fuentes de amenaza

Tipo	Subtipo	Fuente de Amenaza	Aplica
AD	Individuos	Agente Externo	Si
		Agente Interno	Si
	Grupo	Ad Hoc Investigadores	No
		Establecido	No
	Organización	Competidor	No
		Proveedor	No
		Socio	No
		Cliente	No
A	Humana	Usuario	Si
		Administrador	Si
E	Tecnología	Equipos de TI	Si
	Controles Ambientales	Temperatura / humedad	Si
	Software	Sistema Operativo	Si
		Redes	Si
		Aplicación de uso general	Si
AMB	Desastres Naturales	Fuego	No
		Inundación /Tsunami	No
		Huracán	No
		Terremoto	Si
	Falla de Infraestructura	Energía Eléctrica	Si

Nota. En la tabla se muestra los tipos de fuentes de amenaza.

El segundo paso es determinar los eventos que son originados por las fuentes de amenaza. La metodología NIST SP 800-30 establece posibles eventos de amenaza de acuerdo a los tipos de fuente de amenazas identificados, ver Tabla 14.

Tabla 14

Eventos de amenaza

Fuente de Amenaza	Evento de Amenazas
Agente Externo	Reconocimiento o escaneo de red perimetral.
	Rastreo de la red mediante sniffers para identificar componentes, recursos y protecciones.
	Obtención de información de la empresa utilizando fuentes abiertas.
	Reconocimiento de malware interno dirigido
	Ataques de pishing y de spear pishing
	Ataques específicos basados en los entornos de tecnologías de la información implementados.
	Aprovechar vulnerabilidades de zero day
	Deterioro o destrucción de componentes y funciones de sistemas de infraestructura critica
	Obtención de acceso no autorizado
Agente Interno	Divulgación de información crítica o sensible por parte de usuarios autorizados
	Instalar malware dentro de los sistemas críticos de información.
	Aprovechar Split tunneling conexiones al mismo tiempo hacia redes seguras y hacia conexiones remotas no seguras.
	Realiza Ingeniería social dentro de la empresa para obtener información
Usuario Administrador	Configuración incorrecta de privilegios
	Revela información sensible
	Ingeniería Social
	Mal manejo o pérdida de backups de configuración, alarmas y logs

Fuente de Amenaza	Evento de Amenazas
Equipos de TI	Falla de replicación de configuraciones
	Error de componentes
	Deterioro de equipos tecnológicos
	Daño de disco duros
Temperatura / humedad	Sobrecalentamiento de equipos
Sistema Operativo	Fallo del sistema por actualizaciones
Redes	Ataques de man in the middle
	Sniffing de las redes para obtener información sensible
	Falla de los equipos de transmisión.
Aplicación de uso general	Procesos corruptos
Terremoto	Daños graves locación de infraestructura critica
Energía Eléctrica	Ataques redes OT

Nota. En la tabla se muestra los eventos de amenaza.

El tercer paso es identificar las vulnerabilidades que pueden ser explotadas por las fuentes de amenaza. La metodología NIST SP 800-30 define a una vulnerabilidad como una falla o debilidad en los procedimientos de seguridad del sistema, el diseño, la implementación o los controles internos que pueden ser activados accidentalmente o explotados intencionalmente y resultar en una brecha o violación en las políticas de seguridad. (NIST, 2012).

Para este paso, como establece la metodología de evaluación de riesgos, se utilizará la información de fuentes externas e internas para determinar las vulnerabilidades aplicables a los activos del área. Se considera como fuentes externas al reporte de vulnerabilidades e incidentes reportados por el EcuCERT hacia los operadores de telecomunicaciones, en este caso a CNT. Estas vulnerabilidades están asociadas a las direcciones IP que corresponden a la infraestructura del prestador del servicio. (ARCOTEL, 2022)

Las fuentes internas se consideran a los resultados de las entrevistas estructuradas que se realizaron al personal del área de transmisiones, ver Apéndice 1 y documentación confidencial interna como informes de análisis de vulnerabilidades sobre los activos y reportes de riesgos.

En la Tabla 15 se muestran las vulnerabilidades que pueden ser explotadas por una o varias fuentes de amenaza.

Tabla 15

Vulnerabilidades

ID	Vulnerabilidad	Subtipo Fuente de Amenazas
V01	Falta de monitoreo de parámetros de operación de los servidores	Tecnología Humana Control Ambiental
V02	Falta de renovación de licencias de aplicativos, sistemas operativos y/o antivirus	Software Humana / Individuos
V03	Falta de actualización de parches en los sistemas operativos y aplicaciones	Software Humana / Individuos
V04	No se realiza revisiones de los eventos al momento de acceder a los sistemas	Software Humana / Individuos

ID	Vulnerabilidad	Subtipo Fuente de Amenazas
V05	No se realiza monitoreo de trafico de las aplicaciones	Software Humana / Individuos
V06	Insuficientes parámetros de autentificación para el ingreso a los aplicativos	Software Humana / Individuos
V07	Transferencia de archivos de configuración sin mecanismos de autenticación Open TFTP.	Software Humana / Individuos
V08	Obtención de información de gestión de equipos remotos sin encriptar Open Snmp	Software Humana / Individuos
V09	Puertos abiertos del servidor SQL sin restricción de Ips externas. Open Sql Server.	Software Humana / Individuos
V10	Problemas de sincronización para aplicaciones de database recovery	Software Humana / Individuos
V11	Conexiones a equipos remotos en texto plano. Open Telnet	Software Humana / Individuos
V12	Insuficiente capacitación para realizar evaluaciones de riesgo cibernético sobre nuevas implementaciones.	Humana / Individuos
V13	Insuficiente capacitación para realizar pruebas de conmutación de servidores.	Humana / Individuos
V14	Dependencia del know how del contratista para solucionar eventos sobre ataques cibernéticos en los servidores,	Humana
V15	Falta de políticas para generación de contraseñas	Humana / Individuos

Nota. En la tabla se muestran las vulnerabilidades.

Análisis de Controles

En este paso, se analizan los controles implementados y propuestos en el área de transmisiones mediante la verificación de documentación interna confidencial como el documento Controles de Seguridad para Activos de la CNT. (CNT, 2021)

Se validará el nivel de implementación de los controles mediante encuestas al personal del área de transmisiones, ver Apéndice 4.

Los niveles de implementación serán los siguientes, ver Tabla 16:

Tabla 16

Nivel de implementación controles

ID	Nivel de Implementación	Descripción
A	Avanzado	El personal del área conoce las políticas, normas y medidas, es capaz de ejecutarlas y monitorear el cumplimiento de las mismas
M	Medio	El personal del área conoce las políticas, normas y medidas. Depende del proveedor para ejecutarlas y monitorear el cumplimiento de las misma no es muy frecuente.
B	Bajo	El personal del área no conoce las políticas, normas y medidas. No tiene el conocimiento suficiente para ejecutarlas y no monitorea el cumplimiento de las mismas

Nota. En la tabla se muestran el nivel de implementación de controles.

En la Tabla 17, se muestra los resultados de la validación de los controles aplicables a los activos de información del área.

Tabla 17

Validación de controles

ID	Control	Nivel Implementación
C01	Implementar políticas y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares que realiza el teletrabajo	Medio
C02	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas	Medio
C03	Implementar políticas y medidas de seguridad para prevenir la divulgación, modificación o destrucción de información en medios de soporte.	Baja
C04	Medidas para asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios	Baja
C05	Medidas para que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	Baja
C06	Implementación de medidas para prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones.	Medio
C07	Implementar políticas y medidas de para registrar eventos y generar evidencia	Baja
C08	Implementar políticas y medidas para prevenir el aprovechamiento de vulnerabilidades técnicas.	Baja
C09	Medidas para asegurar la protección de la información, de las redes y sus instalaciones de procesamiento de información de soporte.	Medio
C10	Medidas para mantener la seguridad de la información transferida dentro del área y con cualquier entidad externa	Medio
C11	Implementar políticas y medidas para asegurar la protección de los activos de la organización que sean accesibles a los proveedores	Baja

Nota. En la tabla se muestra la validación de controles.

Determinación de probabilidad

En este paso, se determina la probabilidad de que los eventos de amenazas resulten en impactos adversos, considerando las fuentes de amenaza que pueden iniciar eventos y las vulnerabilidades identificadas. (NIST, Risk Assestment, 2012).

Para esta evaluación, se utilizó los niveles cualitativos de probabilidad establecidos por la metodología NIST 800-30, ver Tabla 18.

Tabla 18

Niveles cualitativos de probabilidad

Probabilidad	Descripción
Alta	Si un evento de amenaza se inicia u ocurre una vez a la semana o mes, es casi cierto que se tendrá impactos adversos.
Media	Si un evento de amenaza se inicia u ocurre una vez al año, es muy probable que se tendrá impactos adversos.
Baja	. Un evento de amenaza que no ha ocurrido, es poco probable que tendrá impactos adversos.

Nota. En la tabla se muestran los niveles cualitativos de probabilidad. Recuperado de Risk Assestment por NIST, 2012.

En este paso, se determina la probabilidad en función si el evento de amenaza es iniciado por un adversario o no y si resulta en impactos adversos, ver Apéndice 5.

En la tabla 19, se muestra el nivel de probabilidad total para cada evento de amenaza, el cual es el resultado de analizar la probabilidad de iniciación de un evento de amenaza versus probabilidad de los eventos de amenaza resultar en impactos adversos. En la tabla se tiene siete eventos de amenaza con nivel de probabilidad Alta, trece eventos con probabilidad Media y ocho eventos con probabilidad Baja.

Tabla 19

Probabilidad para eventos de amenazas

Evento de Amenazas	Probabilidad
Reconocimiento o escaneo de red perimetral.	Media
Rastreo de la red mediante sniffers para identificar componentes, recursos y protecciones.	Media
Obtención de información de la empresa utilizando fuentes abiertas.	Baja
Reconocimiento de malware interno dirigido	Media
Ataques de pishing y de spear pishing	Media
Ataques específicos basados en los entornos de tecnologías de la información implementados.	Media
Aprovechar vulnerabilidades de zero day	Alta
Deterioro o destrucción de componentes y funciones de sistemas de infraestructura critica	Baja
Obtención de acceso no autorizado	Media
Divulgación de información crítica o sensible por parte de usuarios autorizados	Baja
Instalar malware dentro de los sistemas críticos de información.	Media
Aprovechar Split tunneling conexiones al mismo tiempo hacia redes seguras y hacia conexiones remotas no seguras.	Baja
Realiza Ingeniería social dentro de la empresa para obtener información	Baja
Configuración incorrecta de privilegios	Alta
Revela información sensible	Baja

Evento de Amenazas	Probabilidad
Ingeniería Social	Media
Mal manejo o perdida de backups de configuración, alarmas y logs	Alta
Falla de replicación de configuraciones	Alta
Error de componentes	Media
Deterioro de equipos tecnológicos	Media
Daño de disco duros	Media
Sobrecalentamiento de equipos	Alta
Fallo del sistema por actualizaciones	Alta
Ataques de man in the middle	Media
Sniffing de las redes para obtener información sensible	Media
Falla de los equipos de transmisión.	Alta
Procesos corruptos	Media
Daños graves locación de infraestructura critica	Baja
Ataques redes OT	Baja

Nota. En la tabla se muestra la probabilidad para eventos de amenazas.

Análisis de Impacto

Para determinar los niveles de impacto, se utilizó la tabla de niveles cualitativos de la metodología NIST 800-30, ver Tabla 20.

Tabla 20

Niveles cualitativos de impacto

Nivel de Impacto	Descripción
Alto	El evento de amenaza puede resultar en tener un efecto adverso severo en las operaciones, activos entre otros, esto se traduce en pérdida de la capacidad de la misión en una medida y duración que la organización no puede realizar sus funciones principales, provocar daños importantes en los activos y resultar en una pérdida financiera importante.
Medio	El evento de amenaza puede resultar en tener un efecto adverso serio en las operaciones, activos entre otros, esto se traduce en degradación de la capacidad de la misión en una medida y duración que la organización puede realizar sus funciones principales, pero la efectividad de las funciones se reduce significativamente y provocar daños significativos en los activos y resultar en una pérdida financiera significativa.
Bajo	El evento de amenaza puede resultar en tener un efecto adverso limitado en las operaciones, activos entre otros, esto se traduce en degradación de la capacidad de la misión en una medida y duración que la organización puede realizar sus funciones principales, pero la efectividad de las funciones se reduce notablemente y ocasionar daños menores en los activos y resultar en una pérdida financiera significativa.

Nota. En la tabla se muestran los niveles cualitativos de impacto. Recuperado de Risk Assestment por NIST, 2012.

En este paso, se determina el nivel de impacto en función si el evento de amenaza tiene consecuencias sobre el área financiera, operaciones y disponibilidad de servicios al cliente, ver Apéndice 6. Esto se lo realizo mediante una encuesta de nivel de impacto de eventos de amenaza a personal de las áreas de financiero, transmisiones y monitoreo de la CNT.

En la tabla 21, se muestra el nivel de impacto resultante para los activos críticos de la empresa, en la cual se tiene once eventos de amenaza con nivel de impacto Alto, diecisiete eventos de impacto Medio y un evento con impacto Bajo.

Tabla 21

Nivel de Impacto de Evento de Amenazas

Evento de Amenazas	Impacto
Reconocimiento o escaneo de red perimetral.	Medio
Rastreo de la red mediante sniffers para identificar componentes, recursos y protecciones.	Medio
Obtención de información de la empresa utilizando fuentes abiertas.	Bajo
Reconocimiento de malware interno dirigido	Medio
Ataques de pishing y de spear pishing	Alto
Ataques específicos basados en los entornos de tecnologías de la información implementados.	Alto
Aprovechar vulnerabilidades de zero day	Alto
Deterioro o destrucción de componentes y funciones de sistemas de infraestructura critica	Alto
Obtención de acceso no autorizado	Medio
Divulgación de información crítica o sensible por parte de usuarios autorizados	Medio
Instalar malware dentro de los sistemas críticos de información.	Alto
Aprovechar Split tunneling conexiones al mismo tiempo hacia redes seguras y hacia conexiones remotas no seguras.	Medio
Realiza Ingeniería social dentro de la empresa para obtener información	Medio
Configuración incorrecta de privilegios	Alto
Revela información sensible	Medio

Evento de Amenazas	Impacto
Ingeniería Social	Medio
Mal manejo o pérdida de backups de configuración, alarmas y logs	Alto
Falla de replicación de configuraciones	Alto
Error de componentes	Medio
Deterioro de equipos tecnológicos	Medio
Daño de disco duros	Medio
Sobrecalentamiento de equipos	Alto
Fallo del sistema por actualizaciones	Medio
Ataques de man in the middle	Medio
Sniffing de las redes para obtener información sensible	Medio
Falla de los equipos de transmisión.	Alto
Procesos corruptos	Medio
Daños graves locación de infraestructura critica	Alto
Ataques redes OT	Medio

Nota. En la tabla se muestra el nivel de impacto de eventos de amenazas.

Elaboración de Matriz de Riesgo Cibernético

Para elaborar la matriz de riesgo cibernético, se utilizará el criterio de la metodología NIST 800-30, el cual determina el nivel del riesgo en función de la relación que existe entre la probabilidad de un evento de amenaza y su respectivo impacto, ver Tablas 22 y 23.

Tabla 22

Nivel de Riesgo

Nivel de Riesgo	Descripción
Inaceptable	El evento de amenaza puede resultar en tener un efecto adverso severo en las operaciones, activos, individuos, o el país.
Moderado	El evento de amenaza puede resultar en tener un efecto adverso serio en las operaciones, activos, individuos, o el país.
Aceptable	El evento de amenaza puede resultar en tener un efecto adverso limitado en las operaciones, activos, individuos, o el país.

Nota. En la tabla se muestra el nivel de riesgo. Recuperado de Risk Assestment por NIST, 2012.

Tabla 23

Mapa de Calor

		Nivel de Impacto		
		Bajo	**Medio**	**Alto**
PROBABILIDAD	**Alto**	Aceptable	Moderado	Inaceptable
	Medio	Aceptable	Moderado	Moderado
	Bajo	Aceptable	Aceptable	Moderado

Nota. En la tabla se muestra el mapa de calor. Recuperado de Implementación de un sistema de un sistema de gestión de seguridad de la información por R. Lema, 2018.

En la Tabla 24, se muestra la matriz de riesgo del área de transmisiones en función de la probabilidad de ocurrencia e impacto de los eventos de amenazas.

Tabla 24

Matriz de riesgo

Id Riesgo	Evento de Amenazas	Probabilidad	Impacto	Riesgo
R01	Reconocimiento o escaneo de red perimetral.	Media	Medio	Moderado
R02	Rastreo de la red mediante sniffers para identificar componentes, recursos y protecciones.	Media	Medio	Moderado
R03	Obtención de información de la empresa utilizando fuentes abiertas.	Baja	Bajo	Aceptable
R04	Reconocimiento de malware interno dirigido	Media	Medio	Moderado
R05	Ataques de pishing y de spear pishing	Media	Alto	Moderado
R06	Ataques específicos basados en los entornos de tecnologías de la información implementados.	Media	Alto	Moderado
R07	Aprovechar vulnerabilidades de zero day	Alta	Alto	Inaceptable
R08	Deterioro o destrucción de componentes y funciones de sistemas de infraestructura critica	Baja	Alto	Moderado
R09	Obtención de acceso no autorizado	Media	Medio	Moderado
R10	Divulgación de información crítica o sensible por parte de usuarios autorizados	Baja	Medio	Aceptable

Id Riesgo	Evento de Amenazas	Probabilidad	Impacto	Riesgo
R11	Instalar malware dentro de los sistemas críticos de información.	Media	Alto	Moderado
R12	Aprovechar Split tunneling conexiones al mismo tiempo hacia redes seguras y hacia conexiones remotas no seguras.	Baja	Medio	Aceptable
R13	Realiza Ingeniería social dentro de la empresa para obtener información	Baja	Medio	Aceptable
R14	Configuración incorrecta de privilegios	Alta	Alto	Inaceptable
R15	Revela información sensible	Baja	Medio	Aceptable
R16	Ingeniería Social	Media	Medio	Moderado
R17	Mal manejo o perdida de backups de configuración, alarmas y logs	Alta	Alto	Inaceptable
R18	Falla de replicación de configuraciones	Alta	Alto	Inaceptable
R19	Error de componentes	Media	Medio	Moderada
R20	Deterioro de equipos tecnológicos	Media	Medio	Moderada
R21	Daño de disco duros	Media	Medio	Moderada
R22	Sobrecalentamiento de equipos	Alta	Alto	Inaceptable
R23	Fallo del sistema por actualizaciones	Alta	Medio	Moderado
R24	Ataques de man in the middle	Media	Medio	Moderado

Id Riesgo	Evento de Amenazas	Probabilidad	Impacto	Riesgo
R25	Sniffing de las redes para obtener información sensible	Media	Medio	Moderado
R26	Falla de los equipos de transmisión.	Alta	Alto	Inaceptable
R27	Procesos corruptos	Media	Medio	Moderado
R28	Daños graves locación de infraestructura critica	Baja	Alto	Moderado
R29	Ataques redes OT	Baja	Medio	Aceptable

Nota. En la tabla se muestra la matriz de riesgo.

En la Tabla 25, se muestra el mapa de calor de riesgos, en el cual se determina que existen seis riesgos inaceptables, diecisiete moderados y seis aceptables. Esta matriz de riesgo es muy importante porque sirve de insumo para poder diseñar el modelo de ciberseguridad para optimizar los niveles de riesgo en la infraestructura crítica de telecomunicaciones.

Tabla 25

Mapa de calor de riesgos

		Nivel de Impacto		
		Bajo	**Medio**	**Alto**
PROBABILIDAD	**Alto**	……. .	R23, R28	R07, R14, R17, R18, R22, R26
	Medio	…….	R01, R02, R04, R05, R06, R09, R16, R19, R20, R21, R24, R25, R27	R11
	Bajo	R03	R10, R12, R13, R15, R29	R08

Nota. En la tabla se muestra el mapa de calor de riesgo.

Capítulo IV

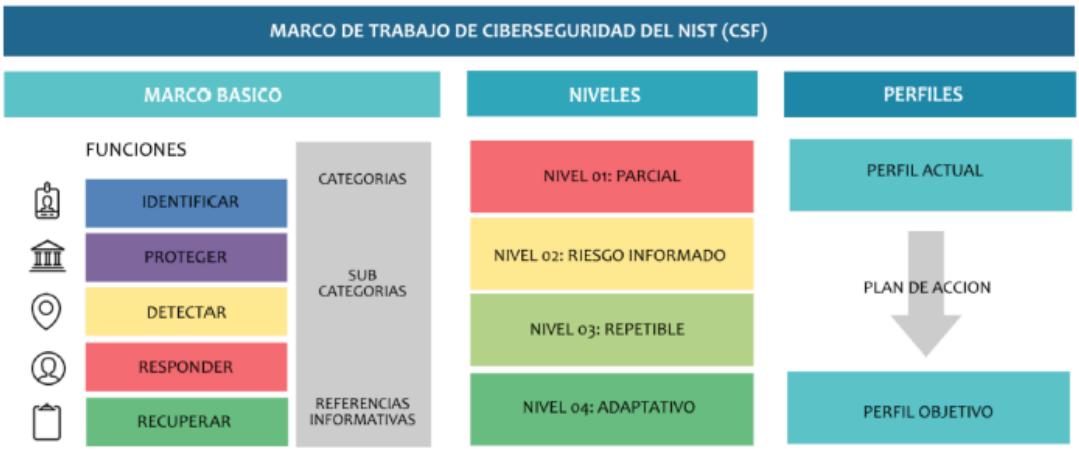
Diseño Modelo de Ciberseguridad

En el presente capítulo se realizará el diseño de un modelo de ciberseguridad mediante el uso del marco para la mejora de la seguridad cibernética en infraestructuras criticas (CSF, por sus siglas en inglés) versión 1.1 de la NIST alineado a COBIT 2019.

El marco de la NIST tiene un enfoque basado en el riesgo con el fin de reducir el riesgo de seguridad cibernética compuesto por tres partes, el núcleo, el perfil y los niveles de implementación (NIST, 2020), como se observa en la Figura 2.

Figura 2

Componentes marco de ciberseguridad



Nota. El gráfico presenta los componentes del marco de ciberseguridad. Tomado de Diseño de un programa de ciberseguridad por A. Gómez, 2019. Framework de Ciberseguridad v1.1

El primer elemento del marco es el núcleo del marco, el cual proporciona un conjunto de actividades para lograr resultados específicos de seguridad cibernética y hace referencia a ejemplos de orientación de cómo lograr dichos resultados.

Este consta de cuatro elementos que se pueden observar en la Figura 3 y se describen a continuación:

1. Funciones: organizan actividades de seguridad cibernética en su nivel más alto. Estas son Identificar, Proteger, Detectar, Responder y Recuperar.
2. Categorías: son subdivisiones de una función en grupos de resultados de seguridad cibernética estrechamente vinculados a las necesidades programáticas.
3. Subcategorías**:** dividen aún más una categoría en resultados específicos de actividades técnicas o de gestión.
4. Referencias Informativas: son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura critica que ilustran un método para lograr resultados asociados con cada subcategoría. (NIST, 2020).

Figura 3

Elementos núcleo del marco

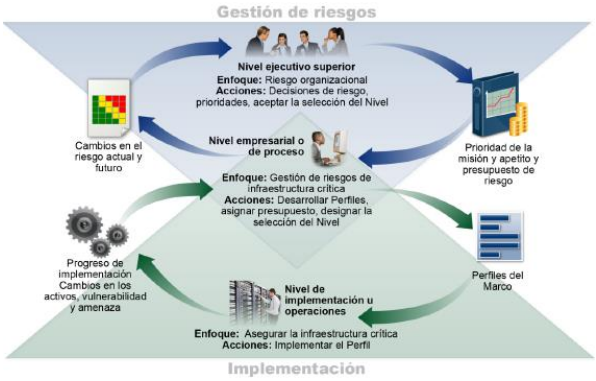
Nota. El gráfico presenta los elementos núcleo del marco. Tomado de Framework de Ciberseguridad v1.1 por NIST, 2020.

El segundo elemento son los niveles de implementación del marco, los cuales proporcionan un contexto sobre como una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo. Los niveles desde Parcial (Nivel 1) a Adaptable (Nivel 4) consideran las prácticas actuales de gestión de riesgos, el entorno de amenazas, objetivos empresariales, los requisitos de seguridad cibernética de la cadena de suministro y las limitaciones organizativas.

El tercer elemento son los perfiles del marco los cuales permiten alinear las funciones, categorías y subcategorías con los requisitos empresariales, la tolerancia al riesgo de los recursos de la organización. Además, se pueden utilizar para describir el estado actual o el estado objetivo deseado de actividades específicas de seguridad cibernética. En la Figura 4, se puede observar cómo los perfiles sirven como entradas en el proceso de gestión de riesgos a nivel ejecutivo, empresarial y de implementación.

Figura 4

Niveles del marco de ciberseguridad

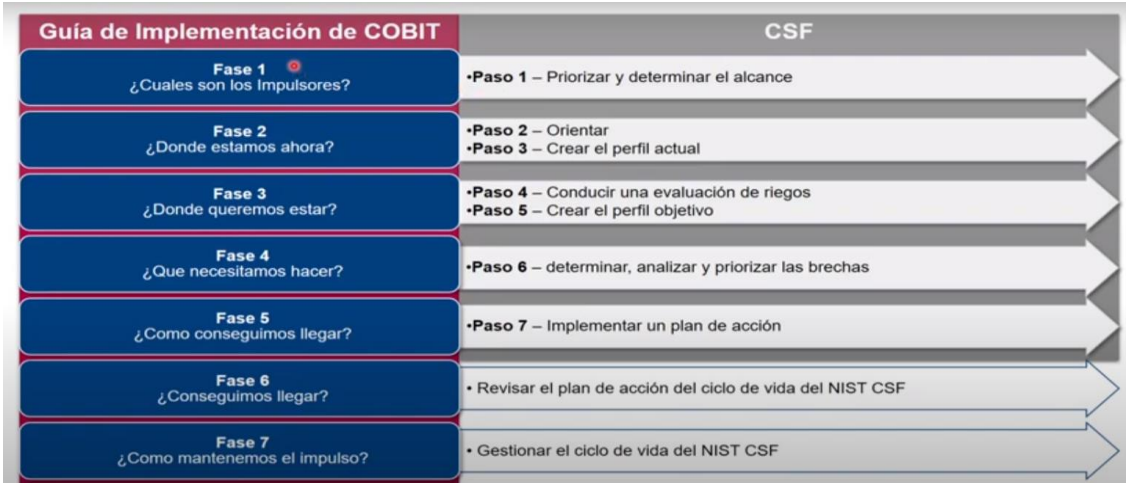


Nota. El gráfico presenta los niveles del marco de ciberseguridad. Tomado de Framework de Ciberseguridad v1.1 por NIST, 2020. Implementar el marco de ciberseguridad de la NIST utilizando COBIT 2019.

Para poder utilizar el marco CSF alineado a COBIT 2019 es necesario verificar las similitudes en los pasos que tienen en las correspondientes guías de implementación, como se observan en la Figura 5.

Figura 5

Relación pasos COBIT 2019 y CSF



Nota. El gráfico presenta la relación pasos COBIT 2019 y CSF. Tomado de Implementar el marco de ciberseguridad de la NIST utilizando COBIT 2019 por ISACA, 2019.

A continuación, se describen los pasos que deben seguirse para diseñar el modelo de ciberseguridad:

- **Paso 1- Priorización y Alcance: l**a organización identifica los objetivos de negocio / misión y prioridades organizacionales de alto nivel para tomar decisiones estratégicas con respecto a la implementación de ciberseguridad. Además, se determina el alcance de los sistemas y activos que dan soporte al negocio. Se utiliza la cascada de metas de COBIT 2019.

- **Paso 2- Orientación: i**dentifica los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general. Se consulta fuentes para identificar amenazas y vulnerabilidades aplicables a estos sistemas y activos.

- **Paso 3- Crear perfil actual: s**e desarrolla un perfil actual al indicar que resultados de Categoría y Subcategoría del Marco Básico se están logrando actualmente. Se realiza un análisis del componente procesos de los objetivos de gobierno y gestión seleccionados.

- **Paso 4- Evaluación de riesgo: i**dentifica riesgos y utiliza información sobre amenazas cibernéticas de fuentes internas y externas para obtener una mejor comprensión de la probabilidad y el impacto de los eventos de seguridad cibernética.

- **Paso 5- Crear perfil objetivo:** se centra en la evaluación de las categorías y subcategorías del marco alineados a los objetivos de gobierno y gestión de COBIT 2019 que describen los resultados de seguridad cibernética de la organización.

- **Paso 6- Determinar, analizar y priorizar brechas: s**e compara el perfil actual y objetivo para determinar brechas. El uso de perfiles alienta a la organización a tomar decisiones informadas sobre actividades de ciberseguridad.

- **Paso 7-Implementar plan de acción: s**e determina las acciones para abordar las brechas, evaluando la probabilidad de éxito e impacto positivo en el negocio.

Alcance del modelo alineado a los objetivos empresariales

El diseño del modelo de ciberseguridad alineado a COBIT 2019 inicia con la definición de la visión, metas, objetivos y estrategia empresarial de la infraestructura crítica de Telecomunicaciones:

- **Visión empresarial***:" Ser la empresa líder de telecomunicaciones y motor de la transformación digital del país, por la innovación tecnológica, la excelencia en la experiencia y calidad de los servicios que ofrece a sus clientes, que sea orgullo de los ecuatorianos".*
- **Misión empresarial:** *"Conectamos a los ecuatorianos con el mundo, a través de servicios de telecomunicaciones y TICs innovadores, de calidad y seguros, contribuyendo al desarrollo económico, productivo y tecnológico del país"*

Dentro de la planificación estratégica empresarial 2021-2025, la CNT tiene seis objetivos estratégicos que son aplicables para todas las áreas de la empresa, ver Tabla 26.

Tabla 26

Objetivos Estratégicos

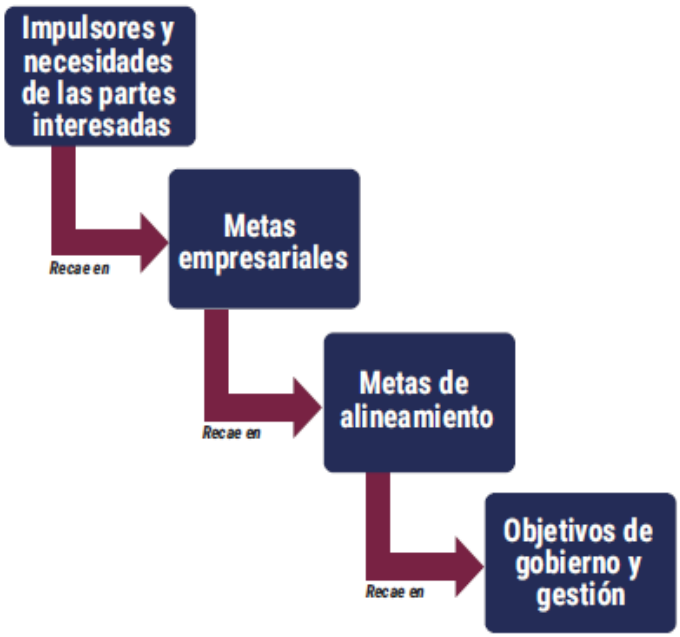
Id OE	Objetivo Estratégico	Estrategia Empresarial
OE1	Incrementar la cobertura y la base de clientes en las líneas de negocio de la empresa	Implementar, renovar y desplegar aceleradamente redes de telecomunicaciones de última generación para ampliar cobertura de servicios GPON, 4G, 5G.
OE2	Incrementar la conectividad de los ciudadanos mediante los servicios que brinda la CNT, tomando en cuenta la planificación territorial.	Ejecutar obras de infraestructura de telecomunicaciones tomando en cuenta la planificación territorial.
OE3	Incrementar la participación y competitividad de la CNT como principal proveedor de telecomunicaciones y TICs en el sector privado y público.	Entregar una experiencia de servicios simple, digital y de calidad al sector privado e instituciones públicas.
OE4	Incrementar productos y servicios de telecomunicaciones innovadores, convergentes, de calidad, seguros y con excelencia al cliente, desarrollando capacidades digitales que impulsen la constante transformación	Impulsar la transformación digital con seguridad.
OE5	Mantener el talento humano altamente capacitado, competente y comprometido con la organización.	Impulsar la cultura orientada al cliente y eficiencia del talento humano.
OE6	Incrementar la rentabilidad y crecimiento de ingresos de las líneas de negocio, asegurando la sostenibilidad financiera de la empresa.	Asegurar la inversión continua necesaria y oportuna en infraestructura de telecomunicaciones.

Nota. En la tabla se muestra los objetivos estratégicos.

Para priorizar y definir el alcance del diseño, se utiliza la cascada de metas y los factores de diseño de COBIT, dando como resultado final los objetivos de gobierno y gestión prioritarios alineados a los objetivos empresariales relacionados con la ciberseguridad, como se observa en la Figura 6.

Figura 6

Cascada metas de COBIT 2019



Nota. El gráfico muestra la cascada de metas de COBIT 2019. Tomado de Implementar el marco de ciberseguridad de la NIST utilizando COBIT 2019 por ISACA, 2019.

En este caso para la optimización del riesgo cibernético en los sistemas de infraestructura crítica del área de transmisiones de la CNT, se han escogido cuatro factores que tienen relación con riesgos y amenazas, ver tabla 27.

Tabla 27

Factores de Diseño COBIT 2019

Id FD	Factor de Diseño	Justificación
FD1	Estrategia Empresarial	Es necesario expresar la estrategia de la CNT en uno o varios arquetipos de estrategia propuestos de Cobit 2019 para optimizar el riesgo cibernético.
FD2	Metas Empresariales	Es fundamental determinar los objetivos alineados a Cobit 2019 que sirvan de soporte para alcanzar la estrategia empresarial
FD3	Perfil de Riesgo	Es importante identificar al tipo de riesgo al que está expuesta el área y verificar si esta dispuestas a alcanzar sus objetivos a pesar del margen de riesgo.
FD4	Panorama de Amenazas	Es esencial clasificar el panorama de amenazas sobre el cual opera el área.

Nota. En la tabla se muestra los factores de diseño de COBIT.

Factor de Diseño FD1 Estrategia Empresarial

En este factor es necesario verificar a que arquetipo de estrategia empresarial (EE) de COBIT 2019 corresponde la estrategia de la CNT, como se muestra en la Tabla 28.

Tabla 28

Relación EE y Arquetipos de COBIT

Id EE	Estrategia Empresarial	Arquetipo de Estrategia Cobit 2019
EE1	Implementar, renovar y desplegar aceleradamente redes de telecomunicaciones de última generación para ampliar cobertura de servicios GPON, 4G, 5G.	Innovación / Diferenciación

Id EE	Estrategia Empresarial	Arquetipo de Estrategia Cobit 2019
EE2	Ejecutar obras de infraestructura de telecomunicaciones tomando en cuenta la planificación territorial.	Crecimiento / Adquisición
EE3	Entregar una experiencia de servicios simple, digital y de calidad al sector privado e instituciones públicas.	Servicio al Cliente / Estabilidad
EE4	Impulsar la transformación digital con seguridad.	Innovación / Diferenciación
EE5	Impulsar la cultura orientada al cliente y eficiencia del talento humano.	Servicio al Cliente / Estabilidad
EE6	Asegurar la inversión continua necesaria y oportuna en infraestructura de telecomunicaciones.	Liderazgo de Costos

Nota. En la tabla se muestra la relación entre EE y arquetipos de COBIT.

También se desarrolla una matriz que tenga relación entre los arquetipos del primer factor de diseño de COBIT 2019 alineados a la estrategia de CNT y los objetivos de gobierno y gestión. Los posibles valores que se asignan a cada arquetipo se encuentran en el rango entre uno (1) a cinco (5), en donde 1 indica sin importancia y 5 muy importante. Esta asignación es realizada mediante un enfoque cuantitativo y en base a la experiencia del personal del área de transmisiones. En el Apéndice 2, se puede observar la matriz correspondiente al factor de diseño 1 Estrategia Empresarial, en la cual después de realizar las operaciones matriciales, se obtienen los objetivos más importantes para este factor.

Una vez realizado el análisis, los objetivos de gobierno y gestión que obtuvieron las calificaciones más altas se muestran en la Tabla 29.

Tabla 29

Resultados Objetivos FD1

Dominio	Objetivos Cobit 2019	Descripción	Calificación
Evaluar, Dirigir y Supervisar	EDM02	Asegurar la obtención de beneficios	34
	EDM03	Asegurar la optimización del riesgo	45
Alinear, Planear y Organizar	APO04	Gestionar la innovación	36
	APO09	Gestionar los acuerdos de servicios	43
	APO12	Gestionar el riesgo	33.5
	APO13	Gestionar la seguridad	46
	APO14	Gestionar los datos	33
Construir, Adquirir e Implementar	BAI08	Gestionar el conocimiento	36.5
	BAI09	Gestionar los activos	33
	BAI10	Gestionar la configuración	40
Entrega, Servicio y Soporte.	DSS04	Gestionar la continuidad	33.5
	DSS05	Gestionar los servicios de seguridad	36

Nota. En la tabla se muestran los resultados objetivos del FD1.

Factor de Diseño FD2 Metas Empresariales

Para este factor es necesario categorizar los objetivos estratégicos de la CNT en torno a las dimensiones del cuadro de mando integral propuesto por COBIT 2019 tales como metas Financieras, Aprendizaje y Crecimiento, Cliente e Interna, ver Tabla 30.

Tabla 30

Categorización Objetivos Estratégicos

Id OE	Objetivo Estratégico	Dimensiones Cobit 2019
OE1	Incrementar la cobertura y la base de clientes en las líneas de negocio de la empresa	Cliente / Interna
OE2	Incrementar la conectividad de los ciudadanos mediante los servicios que brinda la CNT, tomando en cuenta la planificación territorial.	Cliente / Interna
OE3	Incrementar la participación y competitividad de la CNT como principal proveedor de telecomunicaciones y TICs en el sector privado y público.	Cliente
OE4	Incrementar productos y servicios de telecomunicaciones innovadores, convergentes, de calidad, seguros y con excelencia al cliente, desarrollando capacidades digitales que impulsen la constante transformación	Interna
OE5	Mantener el talento humano altamente capacitado, competente y comprometido con la organización.	Aprendizaje y Crecimiento
OE6	Incrementar la rentabilidad y crecimiento de ingresos de las líneas de negocio, asegurando la sostenibilidad financiera de la empresa.	Financiera

Nota. En la tabla se muestra la categorización de objetivos estratégicos.

Una vez que los objetivos se encuentran categorizados a las dimensiones del cuadro de mando integral de COBIT 2019, se procede a determinar las metas empresariales más importantes mediante una tabla de relacionamiento entre los objetivos empresariales y las metas empresariales genéricas de COBIT, ver Figura 7.

En la tabla de relacionamiento, se utilizará la siguiente escala de calificación:

- **Primaria (P):** Cuando las metas de COBIT 2019 tienen una relación directa con los objetivos empresariales de la CNT. Se asigna el valor de cinco (5) para el análisis cuantitativo.
- **Secundario (S):** Cuando las metas de COBIT 2019 tienen una relación indirecta con los objetivos empresariales de la CNT. Se asigna el valor de uno (1) para el análisis cuantitativo.
- **Blanco:** Cuando las metas de COBIT 2019 no tienen ninguna relación con los objetivos empresariales de la CNT. Se asigna el valor de cero (0) para el análisis cuantitativo.

Figura 7

Tabla de Relacionamiento OE vs ME

	Metas Empresariales Cobit 2019												
	EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
	Portafolio de productos y servicios competitivos	Gestión del riesgo del negocio	Cumplimiento de leyes y regulaciones externas	Calidad de la información financiera	Cultura de servicio orientado al cliente	Continuidad y disponibilidad del servicio del negocio	Calidad de la información sobre gestión	Optimización de la funcionalidad de los procesos internos de negocio	Optimización de costas de los procesos de negocio	Habilidades, motivación y productividad del personal	Cumplimiento con las políticas internas	Gestión de programas de trasnformación digital	Innovación de productos y negocios
Objetivos CNT	Financiera				Cliente			Interna				Crecimiento	
OE1	S	P	P	S	S	P	P	P	S	S	P	P	P
OE2	S	P	P	S	P	P	P	P	S	S	P	P	P
OE3	P	P	P	S	S	P	S	S	S	S	P	P	S
OE4	P	P	P	S	P	P	S	P	S	S	P	P	P
OE5		S	S			S	S	S		P	S	P	S
OE6		P	P	P	S	S	S	S	P	S	P	S	S

Nota. El gráfico muestra la tabla de relacionamiento entre OE vs ME.

A partir de la sumatoria de los valores establecidos en la escala de calificación, se obtuvieron las metas empresariales de COBIT 2019 con mayor puntuación, ver Tabla 31.

Tabla 31

Metas Empresariales COBIT 2019

ID	Metas Empresariales para CNT
EG02	Gestión del riesgo del negocio
EG03	Cumplimiento de leyes y regulaciones externas
EG06	Continuidad y disponibilidad del servicio del negocio
EG11	Cumplimiento de las políticas internas
EG12	Gestión de programas de transformación digital

Nota. En la tabla se muestra las metas empresariales COBIT 2019.

A continuación, se debe realizar una tabla de relacionamiento entre las metas empresariales más significativas para la CNT y las 13 metas de alineamiento propuestas por COBIT 2019, ver Figura 8.

En la tabla de relacionamiento, se utilizará la siguiente escala de calificación:

- **Primaria (P):** Cuando las metas empresariales tienen una relación directa con las metas de alineamiento. Se asigna el valor de cinco (5) para el análisis cuantitativo.

- **Secundario (S):** Cuando las metas empresariales tienen una relación indirecta con las metas de alineamiento. Se asigna el valor de uno (1) para el análisis cuantitativo.

- **Blanco:** Cuando las metas empresariales no tienen ninguna relación con las metas de alineamiento. Se asigna el valor de cero (0) para el análisis cuantitativo.

Figura 8

Tabla de Relacionamiento ME vs AG

		Metas Alineamiento Cobit 2019												
		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		Cumplimiento y soporte de I&T para el cumplimiento del negocio con leyes y regulaciones externas	Gestión del riesgo relacionado con I&T	Beneficios obtenidos del portafolio de inversiones y servicios habilitados por I&T	Calidad de la información financiera relacionada con la tecnología	Prestación de servicios de I&T conforme los requisitos del negocio	Agilidad para convertir los requisitos del negocio en soluciones operativas	Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad	Habilidad y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología	Ejecución de programas dentro del plazo, sin exceder el presupuesto y que cumplen con los requisitos y estándares de calidad	Calidad de la información sobre gestión de I&T	Cumplimiento de I&T con las políticas internas	Personal competente y motivado con un entendimiento de la tecnología y negocio	Conocimiento, experiencia e iniciativas para la innovación empresarial
Metas Empresariales Cobit 2019		Financiera				Cliente		Interna					Crecimiento	
EG02	Gestión del riesgo del negocio	P	P	S	S	P	S	P	P	P	P	P	P	P
EG03	Cumplimiento de leyes y regulaciones externas	P	P	P	S	P	S	S		S	S	S		S
EG06	Continuidad y disponibilidad del servicio del negocio	P	P	P	S	P	S	P	S	P	P	P	P	S
EG11	Cumplimiento con las políticas internas		S	S	P	S	S	P	P	P	P	P	S	P
EG12	Gestión de programas de transformación digital	S	P	P	S	P	P	P	P	P	P	P	S	P

Nota. El gráfico muestra la tabla de relacionamiento entre ME vs MA.

A partir de la sumatoria de los valores establecidos en la escala de calificación, se obtuvieron las metas de alineamiento de COBIT 2019 con mayor puntuación, ver Tabla 32.

Tabla 32

Metas de Alineamiento COBIT 2019

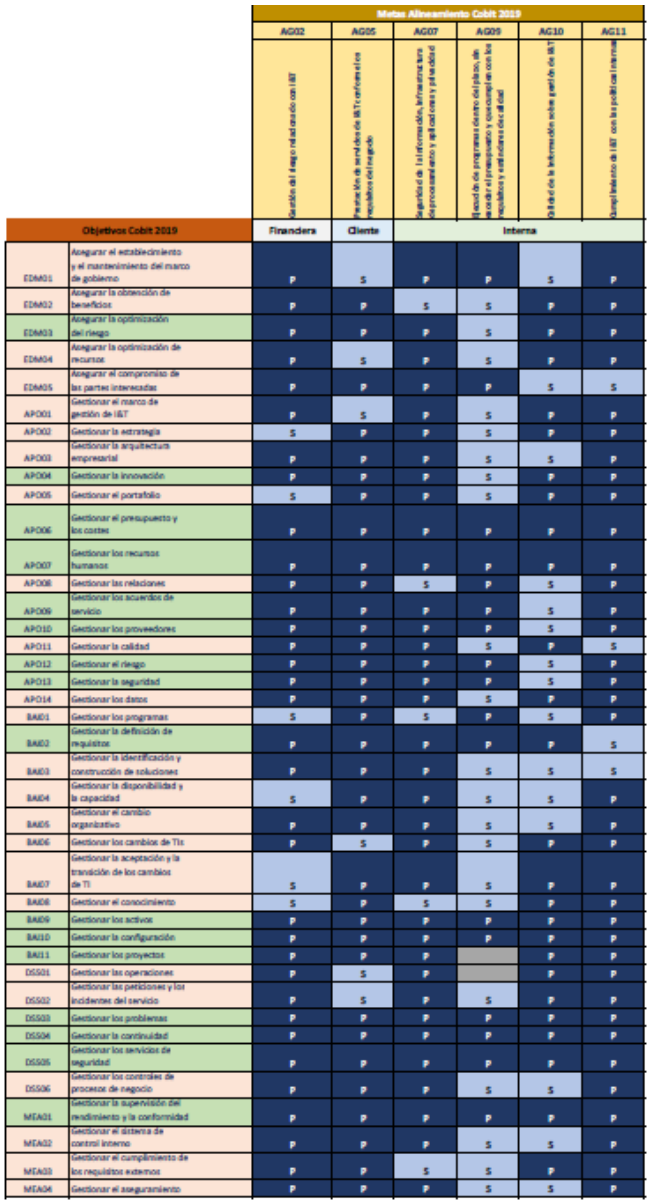
ID	Metas Alineamiento para CNT
AG02	Gestión del riesgo relacionado con I&T
AG05	Prestación de servicios de I&T conforme los requisitos del negocio
AG07	Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad
AG09	Ejecución de programas dentro del plazo, sin exceder el presupuesto y que cumplen con los requisitos y estándares de calidad
AG10	Calidad de la información sobre gestión de I&T
AG11	Cumplimiento de I&T con las políticas internas

Nota. En la tabla se muestra las metas de alineamiento COBIT 2019.

Para el segundo factor es necesario realizar una tabla de relacionamiento entre las metas de alineamiento más significativas para la CNT y los objetivos de gobierno y gestión de propuestos por COBIT 2019, ver Figura 9.

Figura 9

Tabla de Relacionamiento AG vs OGG



Metas Alineamiento Cobit 2019		AG02	AG05	AG07	AG09	AG10	AG11
		Gestión del riesgo relacionado con I&T	Prestación de servicios de I&T conforme a los requisitos del negocio	Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad	Calidad de programas dentro del plazo, de acuerdo al presupuesto y cumpliendo con los requisitos y estándares de calidad	Calidad de la información sobre gestión de I&T	Cumplimiento de I&T con las políticas internas
Objetivos Cobit 2019		Financiera	Cliente	Interna			
EDM01	Asegurar el establecimiento y el mantenimiento del marco de gobierno	P	S	P	P	S	P
EDM02	Asegurar la obtención de beneficios	P	P	S	S	P	P
EDM03	Asegurar la optimización del riesgo	P	P	P	S	P	P
EDM04	Asegurar la optimización de recursos	P	S	P	S	P	P
EDM05	Asegurar el compromiso de las partes interesadas	P	P	P	P	S	S
APO01	Gestionar el marco de gestión de I&T	P	S	P	S	P	P
APO02	Gestionar la estrategia	S	P	P	S	P	P
APO03	Gestionar la arquitectura empresarial	P	P	P	S	S	P
APO04	Gestionar la innovación	P	P	P	S	P	P
APO05	Gestionar el portafolio	S	P	P	S	P	P
APO06	Gestionar el presupuesto y los costes	P	P	P	P	P	P
APO07	Gestionar los recursos humanos	P	P	P	P	P	P
APO08	Gestionar las relaciones	P	P	S	P	S	P
APO09	Gestionar los acuerdos de servicio	P	P	P	P	S	P
APO10	Gestionar los proveedores	P	P	P	P	S	P
APO11	Gestionar la calidad	P	P	P	S	P	S
APO12	Gestionar el riesgo	P	P	P	P	S	P
APO13	Gestionar la seguridad	P	P	P	P	S	P
APO14	Gestionar los datos	P	P	P	S	P	P
BAI01	Gestionar los programas	S	P	S	P	S	P
BAI02	Gestionar la definición de requisitos	P	P	P	P	P	S
BAI03	Gestionar la identificación y construcción de soluciones	P	P	P	S	S	S
BAI04	Gestionar la disponibilidad y la capacidad	S	P	P	S	S	P
BAI05	Gestionar el cambio organizativo	P	P	P	S	S	P
BAI06	Gestionar los cambios de TIs	P	S	P	S	P	P
BAI07	Gestionar la aceptación y la transición de los cambios de TI	S	P	P	S	P	P
BAI08	Gestionar el conocimiento	S	P	S	S	P	P
BAI09	Gestionar los activos	P	P	P	P	P	P
BAI10	Gestionar la configuración	P	P	P	P	P	P
BAI11	Gestionar los proyectos	P	P	P		P	P
DSS01	Gestionar las operaciones	P	S	P		P	P
DSS02	Gestionar las peticiones y los incidentes del servicio	P	S	P	S	P	P
DSS03	Gestionar los problemas	P	P	P	P	P	P
DSS04	Gestionar la continuidad	P	P	P	P	P	P
DSS05	Gestionar los servicios de seguridad	P	P	P	P	P	P
DSS06	Gestionar los controles de procesos de negocio	P	P	P	S	S	P
MEA01	Gestionar la supervisión del rendimiento y la conformidad	P	P	P	P	P	P
MEA02	Gestionar el sistema de control interno	P	P	P	S	S	P
MEA03	Gestionar el cumplimiento de los requisitos externos	P	P	S	S	P	P
MEA04	Gestionar el aseguramiento	P	P	P	S	S	P

Nota. El gráfico muestra la tabla de relacionamiento entre AG vs OGG.

En la tabla de relacionamiento, se utilizará la siguiente escala de calificación:

- **Primaria (P):** Cuando los objetivos de gobierno y gestión tienen una relación directa con las metas de alineamiento. Se asigna el valor de cinco (5) para el análisis cuantitativo.
- **Secundario (S):** Cuando los objetivos de gobierno y gestión tienen una relación indirecta con las metas de alineamiento. Se asigna el valor de uno (1) para el análisis cuantitativo.
- **Blanco:** Cuando los objetivos de gobierno y gestión no tienen ninguna relación con las metas de alineamiento. Se asigna el valor de cero (0) para el análisis cuantitativo.

A partir de la sumatoria de los valores establecidos en la escala de calificación, se obtuvieron los objetivos de gobierno y gestión de COBIT 2019 con mayor puntuación, ver Tabla 33.

Tabla 33

Objetivos Gobierno y Gestión COBIT 2019 FD2

Objetivos Cobit 2019	Descripción	Calificación
EDM03	Asegurar la optimización del riesgo	26
APO04	Gestionar la innovación	26
APO06	Gestionar el presupuesto y los costes	30
APO07	Gestionar los recursos humanos	30
APO09	Gestionar los acuerdos de servicio	26
APO10	Gestionar los proveedores	26
APO12	Gestionar el riesgo	26

Objetivos Cobit 2019	Descripción	Calificación
APO13	Gestionar la seguridad	26
BAI02	Gestionar la definición de requisitos	26
BAI09	Gestionar los activos	30
BAI10	Gestionar la configuración	30
BAI11	Gestionar los proyectos	25
DSS03	Gestionar los problemas	30
DSS04	Gestionar la continuidad	30
DSS05	Gestionar los servicios de seguridad	30
MEA01	Gestionar la supervisión del rendimiento y conformidad	30

Nota. En la tabla se muestra los objetivos de gobierno y gestión FD2.

Factor de Diseño FD3 Perfil de Riesgo

En este factor se identifican los riesgos relevantes en base al impacto y probabilidad de ocurrencia de acuerdo a los escenarios de riesgo propuestos por COBIT 2019, ver Figura 10.

En la tabla de análisis del perfil de riesgo, se utilizará la siguiente escala de calificación:

- Los niveles de categorización de riesgo son Muy Alto color rojo, Alto color amarillo, Normal color verde y Bajo color negro.
- Los valores del impacto se encuentran en un rango desde sin importancia (uno) hasta crítico (cinco).
- La probabilidad de la ocurrencia del riesgo está en el rango entre improbable (uno) y muy probable (5).

Figura 10

Escenario de Riesgos

Categoría del escenario del riesgo	Impacto (1-5)	Probabilidad (1-5)	Escala de Riesgo
Toma de decisiones sobre inversiones en TI, definición y mantenimiento portafolio	3	3	
Gestión del ciclo de vida de los programas y proyectos	4	3	
Coste y Control de TI	3	3	
Comportamiento, habilidades y conocimiento de TI	4	4	
Arquitectura de la empresa TI	4	3	
Incidentes de infraestructura Operativa de TI	4	4	
Acciones no autorizadas	5	3	
Adopción de software, problemas de uso	3	3	
Incidentes de Hadware	5	4	
Fallo de software	5	3	
Ataque lógicos (hacking, malware, etc)	5	3	
Incidentes de terceros / proveedores	4	2	
Incumplimiento	4	4	
Problemas Geopolíticos	4	2	
Acción Industrial	3	3	
Actos de la naturaleza	4	2	
Innovación basada en la tecnología	3	2	
Medio Ambiente	3	3	
Gestión de datos e información	4	4	

Nota. El gráfico muestra el escenario de riesgos.

Una vez identificadas las categorías de riesgo para el área de transmisiones, los resultados de la categorización en base al nivel de riesgo se muestran en la Tabla 34.

Tabla 34

Nivel de riesgo categorías COBIT 2019

Nivel de Riesgo	Categoría Riesgo Cobit 2019	Descripción	Valor (Pxl)
Muy Alto	RISKCAT04	Comportamiento, habilidades y conocimiento de TI	16
	RISKCAT06	Incidentes de infraestructura operativa de TI	16
	RISKCAT07	Acciones no autorizadas	15
	RISKCAT09	Incidentes de hardware	20
	RISKCAT10	Fallo de software	15
	RISKCAT11	Ataques lógicos (hacking, malware, etc)	15
	RISKCAT13	Incumplimiento	16
	RISKCAT19	Gestión de datos e información	16
Alto	RISKCAT01	Toma de decisiones sobre inversiones en TI, definición y mantenimiento portafolio	9
	RISKCAT02	Coste y Control de TI	12
	RISKCAT03	Arquitectura de la empresa TI	9
	RISKCAT05	Adopción de software, problemas de uso	9
	RISKCAT15	Acción industrial	9
	RISKCAT18	Medio ambiente	9
Normal	RISKCAT12	Incidentes de terceros / proveedores	8
	RISKCAT14	Problemas geopolíticos	8
	RISKCAT16	Actos de la naturaleza	8
	RISKCAT17	Innovación basada en la tecnología	6

Nota. En la tabla se muestra el nivel de riesgos de categorías.

A continuación, es necesario desarrollar una matriz que tenga relación entre las categorías de escenarios de riesgo del tercer factor de diseño de COBIT 2019 y los objetivos de gobierno y gestión. Los cinco posibles valores que se asignan a cada escenario de riesgo se encuentran en el rango entre uno (1) a cinco (5), en donde 1 indica sin importancia y 5 muy importante. Esta asignación es realizada mediante un enfoque cuantitativo y en base a la experiencia del personal del área de transmisiones. En el Apéndice 2 se puede observar la matriz correspondiente al Factor de Diseño 3 Perfil de Riesgo, en la cual después de realizar las operaciones matriciales se obtienen los objetivos más importantes para este factor, ver Tabla 35.

Tabla 35

Objetivos COBIT 2019 FD3

Dominio	Objetivos Cobit 2019	Descripción	Calificación
Evaluar, Dirigir y Supervisar	EDM03	Asegurar la optimización del riesgo	706
Alinear, Planear y Organizar	APO06	Gestionar el presupuesto y los costes	320
	APO07	Gestionar los recursos humanos	366
	APO09	Gestionar los acuerdos de servicio	308
	APO10	Gestionar los proveedores	504
	APO12	Gestionar el riesgo	469
	APO13	Gestionar la seguridad	435
	APO14	Gestionar los datos	394
Construir, Adquirir e Implementar	BAI09	Gestionar los activos	399
Entrega, Servicio y Soporte.	DSS04	Gestionar la continuidad	400

Nota. En la tabla se muestra los objetivos COBIT 2019 FD3.

Una vez que se han determinado los objetivos de gobierno y gestión en base a cada uno de los factores de diseño previamente analizados, se muestra una tabla resumen con los objetivos que más se repiten entre los factores y que se consideran prioritarios, ver Tabla 36.

Tabla 36

Resumen Objetivos factores de diseño

Dominio	DF1	DF2	DF3	Prioritarios
Evaluar, Dirigir y Supervisar	EDM02			No
	EDM03	EDM03	EDM03	Si
	APO04	APO04		No
Alinear, Planear y Organizar		APO06	APO06	No
		APO07	APO07	No
	APO09	APO09	APO09	Si
		APO10	APO10	No
	APO12	APO12	APO12	Si
	APO13	APO13	APO13	Si
	APO14		APO14	No
Construir, Adquirir e Implementar		BAI02		No
	BAI08			No
	BAI09	BAI09	BAI09	Si
	BAI10	BAI10		No
		BAI11		No
		DSS03		No
Entrega, Servicio y Soporte.	DSS04	DSS04	DSS04	Si
	DSS05	DSS05		No

Nota. En la tabla se muestra un resumen de los objetivos de diseño.

Para perfeccionar el alcance del modelo alineado a los objetivos empresariales, se utiliza el factor de diseño panorama de amenazas y se relacionan con los objetivos prioritarios identificados.

Es necesario desarrollar una matriz que tenga relación entre los parámetros del cuarto factor de diseño de COBIT 2019 y los objetivos de gobierno y gestión. Los posibles valores que se asignan a cada categoría se encuentran en el rango entre uno (1) a cinco (5), en donde valores menores a cuatro indican un panorama de amenazas normal y valores mayores o iguales a cuatro corresponde a un panorama alto de amenazas. Esta asignación es realizada mediante un enfoque cuantitativo y en base a la experiencia del personal del área de Transmisiones, ver Apéndice 2 y Tabla 37

Tabla 37

Perfeccionamiento con FD4

Dominio	Objetivos Cobit 2019	Descripción	Calificación
Evaluar, Dirigir y Supervisar	EDM03	Asegurar la optimización del riesgo	4
Alinear, Planear y Organizar	APO09	Gestionar los acuerdos de servicio	4
	APO12	Gestionar el riesgo	4
	APO13	Gestionar la seguridad	4
	APO14	Gestionar los datos	4
Construir, Adquirir e Implementar	BAI09	Gestionar los activos	4
Entrega, Servicio y Soporte	DSS04	Gestionar la continuidad	4

Nota. En la tabla se muestra el perfeccionamiento del factor de diseño 4.

Por lo tanto, después de realizar el análisis respectivo de los 4 factores de diseño de COBIT 2019, se concluye que los objetivos de gobierno y gestión prioritarios para el área de transmisiones correspondientes a ciberseguridad en infraestructuras criticas para la optimización del riesgo son: EDM03, APO09, APO12, APO13, BAI09 y DSS04, dando así cumplimiento al Paso 1 de la guía de diseño de COBIT y del CSF.

Perfil Actual de Ciberseguridad

Un perfil de ciberseguridad es la alineación de las funciones, categorías y subcategorías con los requisitos empresariales, la tolerancia al riesgo y los recursos de la organización para describir el estado actual u objetivo deseado de actividades específicas de ciberseguridad. Este permite establecer una hoja de ruta para reducir el riesgo de seguridad cibernética considerando las mejores prácticas de la industria. (ISACA, 2019)

Para el caso del área de transmisiones, los objetivos de gobierno y gestión están enfocados a la optimización del riesgo cibernético. Por lo tanto, en el perfil actual se analizarán las funciones que permiten la consecución de estos objetivos. El análisis se realizará en las treinta y siete subcategorías del marco consideradas como de alta prioridad debido a que es necesario conocer el estado actual de las prácticas de ciberseguridad del área y estas forman la base para analizar las subcategorías restantes ya que el marco tiene un enfoque de mejora continua. (NTCA, 2021)

El paso previo a realizar el análisis es determinar el nivel de implementación del marco. Para este caso, el nivel de implementación del marco es Riesgo Informado, ver Tabla 38.

Tabla 38

Nivel de implementación del marco

Nivel	Aplica / No Aplica	Justificación
Tier 1- Parcial	No	La organización no implementa la gestión de riesgo de manera irregular
Tier 2- Riesgo Informado	Si	Las prácticas de gestión de riesgos no son establecidas como políticas de toda la organización.
Tier 3 -Repetible	No	Las prácticas de gestión de riesgos no son expresan como políticas y no se actualizan periódicamente
Tier 4 - Adaptable	No	Las prácticas de ciberseguridad no se basan en actividades previas y actuales de ciberseguridad

Nota. En la tabla se muestra el nivel de implementación del marco.

El primer paso consiste en evaluar las actividades correspondientes a cada una de las prácticas de COBIT 2019 que tienen relación a cada subcategoría del marco para determinar el nivel actual de ciberseguridad del área, ver Apéndice 3. La escala de nivel de implementación que se utiliza es la que se muestra en la Tabla 39.

Tabla 39

Escala nivel de implementación

ID	Descripción	% Cumplimiento
N	No Ejecutado	0 a < 15 %
P	Parcialmente Ejecutado	>15 a < 50%
L	Largamente Ejecutado	>50 a < 85%
F	Completamente alcanzado	>85 a < 100%

Nota. En la tabla se muestra la escala nivel de implementación del marco.

El resultado de la función Identificar determino que las subcategorías ID.AM-1 e ID.AM-2 se encuentran el nivel L y las subcategorías ID.AM-4, ID.GV-1, ID.GV-4, ID.RA-1, ID.RA-5 e ID.RM-1 tienen un nivel de implementación P, como se muestra en la Figura 11.

Figura 11

Nivel implementación función Identificar

					Nivel Implementación				
Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	N	P	L	F	Promedio
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	ID.AM-1	Los dispositivos y sistemas físicos dentro de la organización están inventariados.	BAI09.01			55		57,5
				BAI09.02			60		
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	ID.AM-2	Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	BAI09.05		47			47
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	ID.AM-4	Los sistemas de información externos están catalogados.	APO02.02		35			39
				APO10.01		43			
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	ID.GV-1	Se establece y se comunica la política de seguridad cibernética organizacional.	APO01.02		44			45,5
				APO13.01		47			
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	ID.GV-4	Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	EDM03.02		48			42,5
				DSS04.02		37			
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	ID.RA-1	Se identifican y se documentan las vulnerabilidades de los activos.	APO12.01		42			40,5
				APO12.03		39			
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	ID.RA-5	Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	APO12.02		44			44
1. IDENTIFICAR (ID)	5. Estrategia de gestión de riesgos (ID.RM)	ID.RM-1	Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	APO13.02		43			43
				BAI02.03		43			

Nota. El gráfico muestra el nivel implementación función Identificar.

El resultado de la función Proteger determino que las subcategorías PR.AC-3 y PR.PT-5 se encuentran el nivel L y las subcategorías PR.AC-1-2, PR.AC-5-6, PR.AC-7, PR.AT-1-2, PR.AT-5, PR.DS-1-2, PR.IP-4, PR.MA-2 y PR.PT-4 tienen un nivel de implementación P , como se muestra en la Figura 12.

Figura 12

Nivel implementación función Proteger

					Nivel Implementación				
Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	N	P	L	F	Promedio
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-1	Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	DSS05.04		49			45,5
				DSS06.03		42			
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-2	Se gestiona y se protege el acceso físico a los activos.	DSS01.04		49			45,5
				DSS06.03		42			
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-3	Se gestiona el acceso remoto.	BAI09.02			60		60
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-5	Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	DSS05.02		41			41
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-6	Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	DSS05.07		42			42
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de	PR.AC-7	Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor	DSS05.04		49			49
2. PROTEGER (PR)	2. Concienciación y capacitación (PR.AT)	PR.AT-1	Todos los usuarios están informados y capacitados.	APO07.03		48			48
2. PROTEGER (PR)	2. Concienciación y capacitación (PR.AT)	PR.AT-2	Los usuarios privilegiados comprenden sus roles y responsabilidades.	APO07.02		40			40
2. PROTEGER (PR)	2. Concienciación y capacitación (PR.AT)	PR.AT-5	El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	DSS06.03		42			42
2. PROTEGER (PR)	3. Seguridad de los datos (PR.DS)	PR.DS-1	Los datos en reposo están protegidos.	APO14.04		43			43
2. PROTEGER (PR)	3. Seguridad de los datos (PR.DS)	PR.DS-2	Los datos en tránsito están protegidos.	APO14.05		42			42
2. PROTEGER (PR)	4. Procesos y procedimientos de protección de la información	PR.IP-4	Se realizan, se mantienen y se prueban copias de seguridad de la información.	APO13.01		47			47
2. PROTEGER (PR)	5. Mantenimiento (PR.MA)	PR.MA-2	El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	DSS05.04		49			49
2. PROTEGER (PR)	6. Tecnología de protección (PR.PT)	PR.PT-4	Las redes de comunicaciones y control están protegidas.	APO13.01		47			47
2. PROTEGER (PR)	6. Tecnología de protección (PR.PT)	PR.PT-5	Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.	BAI04.01			50		50

Nota. El gráfico muestra el nivel implementación función Proteger.

El resultado de la función Detectar determino que las subcategorías DE.CM-1, DE.CM-2, DE.CM-4, DE.CM-7, DE.CM-8 y DE.DP-2 tienen un nivel de implementación P , como se muestra en la Figura 13

Figura 13

Nivel implementación función Detectar

					Nivel Implementación				
Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	N	P	L	F	Promedio
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-1	Se monitorea la red para detectar posibles eventos de seguridad cibernética.	DSS03.05		43			43
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-2	Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	DSS01.04		49			49
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-4	Se detecta el código malicioso.	DSS05.01		47			47
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-7	Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	DSS05.02		41			41
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-8	Se realizan escaneos de vulnerabilidades.	DSS05.07		42			42
3. DETECTAR (DE)	3. Procesos de Detección (DE.DP)	DE.DP-2	Las actividades de detección cumplen con todos los requisitos aplicables.	DSS06.03		42			42

Nota. El gráfico muestra el nivel implementación función Detectar.

El resultado de la función Responder determino que las subcategorías RS-RP-1, RS-CO-1, RS-CO-3, RS-CO-4, RS-AN-1, RS-MI-1, RS-MI-2 tienen un nivel de implementación P, como se muestra en la Figura 14.

Figura 14

Nivel implementación función Responder

					Nivel Implementación				
Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	N	P	L	F	Promedio
4. RESPONDER (RS)	1. Planificación de la Respuesta (RS.RP)	RS.RP-1	El plan de respuesta se ejecuta durante o después de un incidente.	APO12.06		45			45
4. RESPONDER (RS)	2. Comunicaciones (RS.CO)	RS.CO-1	El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	EDM03.02		48			48
4. RESPONDER (RS)	2. Comunicaciones (RS.CO)	RS.CO-3	La información se comparte de acuerdo con los planes de respuesta.	DSS03.03		41			41
4. RESPONDER (RS)	2. Comunicaciones (RS.CO)	RS.CO-4	La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	DSS03.04		47			47
4. RESPONDER (RS)	3. Análisis (RS.AN)	RS.AN-1	Se investigan las notificaciones de los sistemas de detección.	DSS02.04		43			43
4. RESPONDER (RS)	4. Mitigación (RS.MI)	RS.MI-1	Los incidentes son contenidos.	DSS05.03		47			47
4. RESPONDER (RS)	4. Mitigación (RS.MI)	RS.MI-2	Los incidentes son mitigados.	DSS05.07		42			42

Nota. El gráfico muestra el nivel implementación función Responder.

El resultado de la función Recuperar determino que la subcategoría RC-RP-1 tienen un nivel de implementación P, como se muestra en la Figura 15.

Figura 15

Nivel implementación función Recuperar

					Nivel Implementación				
Función	Categoría	Subcategoría	Descripción Subcategoría	Práctica Cobit 2019	N	P	L	F	Promedio
5. RECUPERAR (RC)	1. Planificación de la recuperación (RC.RP)	RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	APO12.06		45			45

Nota. El gráfico muestra el nivel implementación función Recuperar.

La creación del perfil actual da cumplimiento a los pasos 2 y 3 propuestos por el marco de ciberseguridad y que tienen correspondencia con COBIT 2019.

Perfil Objetivo de Ciberseguridad

El nivel de implementación objetivo para la creación del perfil se determina en base a lo siguiente:

- **Evaluación de Riesgos:** De acuerdo al mapa de calor de riesgos de la Tabla 25 del capítulo Análisis de Riesgos, se identifica la probabilidad y el impacto de las amenazas que pueden aprovechar una vulnerabilidad en los activos críticos de la CNT.
- **Nivel de Implementación de las Subcategorías del Perfil Actual:** El nivel de implementación de la mayoría de las actividades de COBIT 2019 correspondientes a las subcategorías es de P.
- **Nivel de Implementación del Marco Tier:** Actualmente, el nivel de implementación del marco es Tier 2 Riesgo Informado.

Por lo tanto, al tener en cuenta que el marco de ciberseguridad alineado a COBIT 2019 tiene un enfoque de mejora continua, se determina que el nivel de implementación objetivo es L: largamente ejecutada, debido a que las actividades de las prácticas se traducen en controles que permitan mitigar los riesgos identificados y subir al nivel Tier 3 para que las prácticas de riesgos se expresen como políticas y se actualicen periódicamente, ver Apéndice 3.

Análisis y Priorización de oportunidades y brechas detectadas

Para realizar el análisis y priorización de oportunidades y brechas detectadas es definir los criterios para la priorización de que actividades de las prácticas de COBIT 2019 correspondientes a las subcategorías del marco de ciberseguridad permiten optimizar los procesos de una manera rápida y con una inversión generalmente baja.

Los criterios para realizar el análisis y priorización son los siguientes:

- Se seleccionan las prácticas de COBIT 2019 que estén alineadas a los objetivos de gobierno y gestión determinadas en el Paso 1 Alcance del modelo alineado a los objetivos empresariales
- La probabilidad de éxito y el Impacto positivo en el negocio. La escala que se utilizará será Alto, Medio y Bajo, cada una con un valor de 3,2,1 respectivamente. El nivel de prioridad será el resultado de multiplicar los valores asignados de probabilidad e impacto y se seleccionaran los que tenga los valores más altos.
- Una vez definidos los criterios para priorizar las oportunidades y brechas, los resultados de las prácticas de COBIT 2019 seleccionadas que se alinean al marco de ciberseguridad y son proyectos quick wins que permiten optimizar procesos con una inversión baja, se muestran en la Tabla 40.

Tabla 40

Nivel prioridad Prácticas COBIT 2019

Subcategoría CSF	Práctica Cobit 2019	PE	IPN	Prioridad
ID.GV-4, RS.CO-1	EDM03.02 Act.4	2	3	6
ID.GV-4, RS.CO-1	EDM03.02 Act.5	2	3	6
ID-RA-1	APO12.01 Act.3	2	3	6
ID-RA-1	APO12.01 Act.7	2	3	6
ID-RA-5	APO12.02 Act.1	2	3	6
ID-RA-5	APO12.02 Act.3	2	3	6
ID-RA-5	APO12.02 Act.7	3	2	6
ID-RA-5	APO12.02 Act.8	2	3	6
ID-RA-1	APO12.03 Act.1	2	3	6
ID-RA-1	APO12.03 Act.2	2	3	6
RS.RP-1	APO12.06 Act.1	2	3	6
RS.RP-1	APO12.06 Act.2	3	2	6
ID.RM-1	BAI02.03 Act.3	2	3	6
ID.AM-2	BAI09.05 Act.1	3	2	6
ID.AM-2	BAI09.05 Act.3	3	2	6
ID.GV-4	DSS04.02 Act.2	2	3	6
ID.GV-4	DSS04.02 Act.5	3	2	6
ID.GV-4	DSS04.02 Act.6	3	2	6
ID.GV-4	DSS04.02 Act.7	3	2	6
DE.CM-4	DSS05.01 Act.3	2	3	6
PR.AC-5, DE.CM-7	DSS05.02 Act.1	2	3	6
PR.AC-5, DE.CM-7	DSS05.02 Act.4	2	3	6

Subcategoría CSF	Practica Cobit 2019	PE	IPN	Prioridad
PR.AC-5, DE.CM-7	DSS05.02 Act.5	3	2	6
PR.AC-5, DE.CM-7	DSS05.02 Act.7	2	3	6
PR.AC-5, DE.CM-7	DSS05.02 Act.8	3	3	9
RS.MI-1	DSS05.03 Act.5	2	3	6
RS.MI-1	DSS05.03 Act.9	2	3	6
PR.AC-1, PR.AC-7,PR.MA-2	DSS05.04 Act.5	2	3	6
PR.AC-1, PR.AC-7,PR.MA-2	DSS05.04 Act.6	2	3	6
PR.AC-1, PR.AC-7,PR.MA-2	DSS05.04 Act.8	3	3	9
PR.AC-6, DE.CM-8	DSS05.07 Act.3	2	3	6
PR.AC-1, PR.AT-5, DE.DP-2	DSS06.03 Act.1	2	3	6
PR.AC-1, PR.AT-5, DE.DP-2	DSS06.03 Act.4	3	3	9
PR.AC-1, PR.AT-5, DE.DP-2	DSS06.03 Act.6	2	3	6

Nota. En la tabla se muestra el nivel de prioridad prácticas COBIT 2019.

Elaboración del modelo de ciberseguridad alineado a Cobit 2019

El modelo de ciberseguridad alineado a COBIT 2019 consiste en identificar las soluciones de ciberseguridad, indicadores y responsables que darán soporte al cumplimiento de las prácticas de COBIT 2019 y a las categorías del marco de ciberseguridad de la NIST, las mismas que optimizarán los procesos de una manera rápida, ver Apéndice 3. (McAfee, 2018)

El resultado del modelo en la función Identificar determino que son necesarias tres soluciones de ciberseguridad, siete indicadores para las prácticas alineadas a las categorías del marco de ciberseguridad y dos responsables, como se muestra en la Figura 16.

Figura 16

Resultado modelo función Identificar

						Brechas				
Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Práctica	Subcategoría	Solución de Ciberseguridad	Indicadores	Responsables
1. IDENTIFICAR (ID)	1. Gestión de activos (ID.AM)	ID.AM-2	BAI09.05	47	L	Act.1		Herramientas de Gobernanza, Riesgo y Cumplimiento GRC	% licencias usadas vs compradas, % de licencias y productos que deben actualizarse	Gerencia Nacional Técnica, Jefatura de O&M Transmisión
1. IDENTIFICAR (ID)	3. Gobernanza (ID.GV)	ID.GV-4	EDM03.02	42.5	L	Act.4, Act.5		Gestor de Seguridad de la Información y Eventos	% de proyectos que consideran el riesgo cibernético, nivel de alineamiento entre el riesgo empresarial y el cibernético	
			DSS04.02			Act.2, Act.5, Act.7			% de stakeholders involucrados en evaluaciones de impacto del negocio	
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	ID.RA-1	APO12.01	40.5	L	Act.1, Act.3			Número de eventos con pérdidas y características principales	
			APO12.03			Act.1, Act.2		Gestor de Seguridad de Infraestructura de Red	% de procesos principales del negocio en el perfil de riesgo	
1. IDENTIFICAR (ID)	4. Evaluación de riesgos (ID.RA)	ID.RA-5	APO12.02	44	L	Act.1, Act.3, Act.7, Act.8			Número de escenarios identificados de riesgos	
1. IDENTIFICAR (ID)	5. Estrategia de gestión de riesgos (ID.RM)	ID.RM-1	BAI02.03	43	L	Act.3			% de requerimientos de riesgo no cubiertos por una acción de respuesta	

Nota. El gráfico muestra el nivel modelo función Identificar.

El resultado del modelo en la función Proteger determino que son necesarias seis soluciones de ciberseguridad, ocho indicadores para las prácticas alineadas a las categorías del marco y un responsable, como se muestra en la Figura 17.

Figura 17

Resultado modelo función Proteger

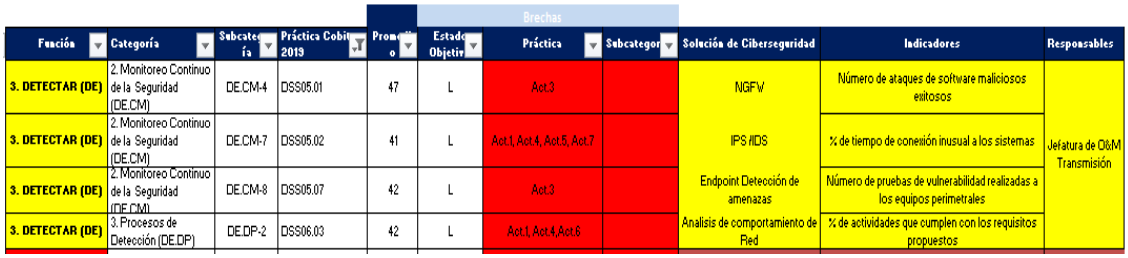
Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Brechas: Práctica	Brechas: Subcategoría	Solución de Ciberseguridad	Indicadores	Responsables
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-1	DSS05.04	45.5	L	Act.5, Act.6,Act.8		Next Generation Firewall	Promedio de tiempo entre cambio y actualización de cuentas	Jefatura de O&M Transmisión
			DSS06.03			Act.1, Act.4,Act.6			% de roles con derechos de acceso y niveles de autoridad	
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-2	DSS06.03	45.5	L	Act.1, Act.4,Act.6		Encripción de Discos	Número de incidentes por violación a los permisos de ingreso	
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-5	DSS05.02	41	L	Act.1, Act.4, Act.5, Act.7		Control de Acceso de Red NAC	Número de brechas en el firewall	
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-6	DSS05.07	42	L	Act.3		Control de Acceso de Usuarios Privilegiados	Número de cuentas vs Número de usuarios autorizados	
2. PROTEGER (PR)	1. Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-7	DSS05.04	49	L	Act.5, Act.6,Act.8			Número de incidentes relacionados a acceso no autorizado a la información	
2. PROTEGER (PR)	2. Concienciación y capacitación (PR.AT)	PR.AT-5	DSS06.03	42	L	Act.1, Act.4,Act.6		Encripción de datos basados en Roles	% de roles con clara separación de rutinas	
2. PROTEGER (PR)	5. Mantenimiento (PR.MA)	PR.MA-2	DSS05.04	49	L	Act.5, Act.6,Act.8		Aplication Delivery Controller	% de equipos actualizados a las últimas versiones	

Nota. El gráfico muestra el nivel modelo función Proteger.

El resultado del modelo en la función Detectar determino que son necesarias cuatro soluciones de ciberseguridad, cuatro indicadores para las prácticas alineadas a las categorías del marco de ciberseguridad y un responsable, como se muestra en la Figura 18.

Figura 18

Resultado modelo función Detectar



Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Brechas: Práctica	Brechas: Subcategoría	Solución de Ciberseguridad	Indicadores	Responsables
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-4	DSS05.01	47	L	Act.3		NGFW	Número de ataques de software maliciosos exitosos	Jefatura de O&M Transmisión
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-7	DSS05.02	41	L	Act.1, Act.4, Act.5, Act.7		IPS /IDS	% de tiempo de conexión inusual a los sistemas	
3. DETECTAR (DE)	2. Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-8	DSS05.07	42	L	Act.3		Endpoint Detección de amenazas	Número de pruebas de vulnerabilidad realizadas a los equipos perimetrales	
3. DETECTAR (DE)	3. Procesos de Detección (DE.DP)	DE.DP-2	DSS06.03	42	L	Act.1, Act.4,Act.6		Analisis de comportamiento de Red	% de actividades que cumplen con los requisitos propuestos	

Nota. El gráfico muestra el nivel modelo función Detectar.

El resultado del modelo en la función Responder determino que son necesarias cuatro soluciones de ciberseguridad, cuatro indicadores para las prácticas alineadas a las categorías del marco de ciberseguridad y un responsable, como se muestra en la Figura 19.

Figura 19

Resultado modelo función Responder

Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Brechas: Práctica	Brechas: Subcategoría	Solución de Ciberseguridad	Indicadores	Responsables
4. RESPONDER (RS)	1. Planificación de la Respuesta (RS.RP)	RS.RP-1	APO12.06	45	L	Act.1, Act.2			% de acciones ejecutadas vs las diseñadas en el plan de respuesta	Jefatura de O&M Transmisión
4. RESPONDER (RS)	2. Comunicaciones (RS.CO)	RS.CO-1	EDM03.02	48	L	EDM03.02 Act.4, Act.5		Endpoint Detección de amenazasy respuesta ETDR	% del personal que tiene conocimiento de sus funciones	
4. RESPONDER (RS)	4. Mitigación (RS.MI)	RS.MI-1	DSS05.03	47	L	Act.5, Act.9		Automatización de SOC	Número de Incidentes contenidos	
4. RESPONDER (RS)	4. Mitigación (RS.MI)	RS.MI-2	DSS05.07	42	L	Act.3		Herramientas de Inteligencia de Amenazas	Número de Incidentes mitigados	

Nota. El gráfico muestra el nivel modelo función Responder.

El resultado del modelo en la función Recuperar determino que son necesarias una solución de ciberseguridad, un indicador para las prácticas alineadas a las categorías del marco de ciberseguridad y un responsable, como se muestra en la Figura 20.

Figura 20

Resultado modelo función Recuperar

Función	Categoría	Subcategoría	Práctica Cobit 2019	Promedio	Estado Objetivo	Brechas: Práctica	Brechas: Subcategoría	Solución de Ciberseguridad	Indicadores	Responsables
5. RECUPERAR (RC)	1. Planificación de la recuperación (RC.RP)	RC.RP-1	APO12.06	45	L	Act.1, Act.2		Herramientas de DR y COOP	% de recuperación de operaciones del giro del negocio	Jefatura de O&M Transmisión

Nota. El gráfico muestra el nivel modelo función Recuperar.

Con la elaboración del modelo de ciberseguridad alineado COBIT 2019, se da cumplimiento a los 7 pasos correspondientes a las guías de diseño de COBIT 2019 y CSF.

Capítulo V

Conclusiones y Recomendaciones

Conclusiones

- La caracterización y valoración de los componentes de la red de transmisiones de la CNT determinó que la mayor parte de los activos con que se operan son críticos para el giro de negocio. De esta manera se logró establecer al área de Transmisiones como el núcleo de operaciones de la CNT y por lo tanto es una infraestructura critica para el país.
- Se realizó un análisis de riesgo basado en la metodología NIST 800-30, enfocado en identificar las fuentes de amenaza, eventos de amenaza y vulnerabilidades. En base a su frecuencia de ocurrencia y su nivel de impacto se determinó que seis riesgos son inaceptables, diecisiete son moderados y seis son aceptables Este análisis es la base para el diseño del modelo de ciberseguridad al identificar las brechas en los perfiles de ciberseguridad del marco de la NIST.
- Los factores de diseño y la cascada de metas de COBIT 2019 son elementos claves para determinar los seis objetivos de gobierno y gestión específicos alineados a la estrategia empresarial de esta infraestructura critica. Por lo tanto, COBIT 2019 se alinea a los requerimientos de la alta dirección de la CNT para optimizar el riesgo cibernético

- El marco de ciberseguridad para infraestructuras críticas de la NIST está compuesto por funciones, categorías y subcategorías, las cuales alineadas a las prácticas de COBIT 2019 determinaron que el nivel actual de ciberseguridad de la CNT es de Tier 2 Riesgo Informado y el nivel deseado en todas las prácticas de COBIT 2019 correspondientes a las subcategorías del marco es Largamente Ejecutado.
- Los criterios para el análisis, priorización de brechas y oportunidades tales como la probabilidad de éxito y el impacto positivo de negocio, definieron veinte y uno proyectos quick wins los cuales optimizarán los procesos con una inversión baja mejorando así el nivel de ciberseguridad de la empresa.
- El diseño del modelo de ciberseguridad alineado a COBIT y al CSF estableció que es necesario diecisiete soluciones de ciberseguridad, veinte y cuatro indicadores y una gerencia responsable. Por lo tanto, el modelo propuesto es la base para que las actividades de gobierno y gestión de la empresa generen valor a través de la optimización del riesgo cibernético con un enfoque de mejora continua.

Recomendaciones

- Planificar y ejecutar capacitaciones a todos los servidores del área de Transmisiones para la socialización de temas de marcos de trabajos para gobierno y gestión las tecnologías de información y de ciberseguridad en infraestructura críticas, con el propósito de implementar adecuadamente el modelo propuesto y dar inicio a la cultura corporativa empresarial con enfoque en ciberseguridad.
- Implementar las soluciones de ciberseguridad correspondientes a cada función del CSF, realizar un monitoreo continuo del rendimiento y un informe con los indicadores establecidos para justificar a la alta gerencia la inversión realizada en términos de amenazas y riesgos mitigados.
- Revisar el nivel de implementación de todas las categorías del marco de ciberseguridad periódicamente para determinar si están dando soporte a conseguir los objetivos empresariales o se necesita algún tipo de corrección en los procesos de las prácticas de COBIT 2019.
- Para mantener la disponibilidad de los servicios de manera interna y externamente a la empresa, se debe realizar un plan de mantenimiento preventivo y correctivo a todos los activos que están bajo la responsabilidad del área de Transmisiones de la CNT para la correcta gestión a nivel físico y lógico.

Bibliografía

Aguirre. (2017). Ciberseguridad en Infraestructuras Críticas. Universidad de Buenos Aires.

Aguirre, A. (2017). Ciberseguridad en Infraestructras Críticas. Universidad de Buenos Aires.

Arcotel. (2022). Reporte de Seguridad de Telecomunicaciones.

Avalos, V. (2007). Desarrollo de una aplicación para la gestión de riesgos utilizando la guia NIST SP 800-30.

CISA. (2018). Infraestructura Crítica Telecomunicaciones. Obtenido de https://www.cisa.gov/communications-sector

CNT. (2017). Memoria de Sostenibilidad. Obtenido de https://corporativo.cnt.gob.ec/wp-content/uploads/2017/12/Memoria-sostenibilidad.pdf

Cnt. (2021). Controles de Seguridad.

Deloitte, A. (2020). Estado Actual de la Ciberseguridad 2020. Obtenido de https://datta.com.ec/articulo/estado-de-la-ciberseguridad-en-ecuador

Erreyes, M. (2017). Metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles .

Gestión, O. d. (2019). 2019.

Gomez, A. (2019). Diseño de un programa de ciberseguridad de una empresa basado en el marco de trabajo de la NIST.

Gomez, R., Perez, D., & Donoso, Y. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información.

INCIBE. (2019). La importancia de la estrategia de ciberseguridad para la industria. Obtenido de https://www.incibe-cert.es/blog/importancia-estrategia-ciberseguridad-industria

ISACA. (2019). Implementar el marco de ciberseguridad de la NIST utilizando COBIT 2019.

Kapersky. (2017). Kapersky Lab Industrial Control System Cyber Emergency Response Team Report Latin America. Obtenido de https://securelist.lat/threat-landscape-for-industrial-automation-systems-in-h1-2017/85531/

Lara, E. (2019). Diseño de una modelo de seguridad de la información para centros de educación.

Leiva. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, págs. 161-176.

Lenma, R., & Donoso, D. (2018). Implementación de un sistema de un sistema de gestión de seguridad de la información.

MAGERIT. (2012). Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

McAfee. (2018). NIST Cybersecurity framework Mapping.

Mendoza, L. (2019). Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SISC.

Meridian. (2016). Guía para buenas prácticas de GFCE-MERIDIAN sobre protección de infraestructuras criticas de la informacion para responsables gubernamentales.

Mintel. (2019a). Libro Blanco Lineas de Investigación, Desarrollo e Innovación y Transferencia del Conocimiento en TIC. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/01/libro-blanco-lineas-de-investigación.pdf

Mintel. (2019b). Informe de Rendición de cuentas 2019. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2020/04/Informe-Rendicion-de-cuentas-2019.pdf

Mintel. (2019c). Acuerdo Ministerial No 025-2019.

Mintel. (2020). Guia para la Gestión de Riesgos.

Nist. (2012). Risk Assestment. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST. (2020). Framework de Ciberseguridad v1.1. Obtenido de https://ciberseguridad.blog/como-implantar-el-framework-nist/

NTCA. (2021). Guía para el Marco de Ciberseguridad.

OEA. (2020). Reporte Ciberseguridad 2020 para America Latina. Obtenido de https://www.oas.org

Orozco, G. (2021). Análisis y diseño de un sistema de gestión de la seguridad de la información para el GAD de Pujili.

Quintana, F. (2016). Cybersecurity Capabilities in a Critical Infrastructure Sector of a Developing Nation. Carnegie Mellon University.

Ron, Bonilla, Fuertes, Diaz, & Toulkeridis. (2018). Applicability of cybersecurity standards in Ecuador a field exploration. International Conference of Research Applied to Defense and Security.

Ron, M., Bonilla, M., & Fuertes, W. (2016). Applicability of cybersecurity standards in Ecuador-a field exploration.

Ron, Rivera, Fuertes, & Toulkeridis. (2019). Cybersecurity Baseline, An Exploration, which permits to delineate National Cybersecurity Strategy in Ecuador. International Conference on Information Technology & Systems.

Tejena, M. (2018). Análisis de riesgos en seguridad de la información. En Polo del Conocimiento (págs. 230-244).

Telefonica. (2020). El valor de la conectividad y el internet abierto. Obtenido de https://telos.fundaciontelefonica.com/el-valor-de-la-conectividad-y-del-internet-abierto/

UIT. (2018). Global Cybersecurity Index 2018. Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

WoldEconomicForum. (2018). The Global Risks Report. Obtenido de https://www.weforum.org/reports/the-global-risks-report-2018

Apéndices