DISEÑO DE UN FRAMEWORK DE CIBERSEGURIDAD, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA UN PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES EN UN AMBIENTE MULTIREGION

Ariel Nicolás Herrera Flórez
Jenny Carolina Tellez Monsalve

Departamento de ingeniería de Sistemas y Computación
Universidad de Los Andes
Noviembre 2021

RESUMEN

En este artículo se propone una metodología para la identificación y selección de uno o varios Framework de Ciberseguridad, Seguridad y Privacidad para un proveedor de servicios de Telecomunicaciones a lo largo de toda la región enfocado en clientes B2B (*Business to Business*) y B2C (*Business to Consumer*).

Para el desarrollo de este proyecto de investigación, revisamos literatura relacionada con los diferentes Frameworks de Ciberseguridad, Seguridad y Privacidad; y hemos trabajado con personal del área de Seguridad de la Información de la empresa, con el fin de identificar y seleccionar los frameworks más apropiados; aquellos que puedan apoyar de forma más efectiva el cumplimiento de los objetivos corporativos y la estrategia de seguridad del negocio, a pesar de la complejidad de la organización.

ABSTRACT

This article proposes a methodology for the identification and selection of one or more Cybersecurity, Security and Privacy Framework for a Telecommunications service provider company throughout the region focused on B2B (Business to Business) and B2C (Business to Consumer) customers.

For the development of this research project, we reviewed literature related to the different Cybersecurity, Security and Privacy Frameworks; and we have worked with personnel from the Information Security area of the company, to identify and select the most appropriate framework or frameworks; those that can most effectively support the fulfillment of the corporate objectives and the security strategy of the business, despite the complexity of the organization.

ÍNDICE DE TÉRMINOS

Telecomunicaciones, Framework, Ciberseguridad, Seguridad Digital, Privacidad.

I. CONTEXTO

Por ser una empresa líder en telecomunicaciones; con operaciones en diferentes países a nivel de toda la región, como lo son Colombia, Centro América y las islas del Caribe; la ciberseguridad, seguridad y privacidad son un punto clave en su estrategia al momento de priorizar los riesgos a los que la organización se encuentra expuesta.

Según (Onibere et al., 2017), "las organizaciones se encuentran expuestas en un entorno de amenazas a la seguridad sofisticadas y en evolución que expone su infraestructura de información a una serie de riesgos de seguridad". Lo que genera preocupación para la organización.

Para Nayia Barmpaliou (Reporte de Ciberseguridad 2020) "En los últimos cinco años, la noción de que la estrategia de ciberseguridad forma parte integral de la estrategia empresarial ha ganado más tracción e implementación real por parte de las empresas.", es un punto que ha venido tomando relevancia en las juntas directivas para la toma de decisiones, mostrando interés en las amenazas cibernéticas y los requerimientos legales y regulatorios que están adoptando los países, sobre todo en temas como la ciberseguridad y privacidad.

De acuerdo con lo anteriormente expuesto, cada vez más las organizaciones entienden que no solo con invertir en tecnología logran gestionar mejor sus riesgos, sino que necesitan bases más sólidas para gobernarlos. Esto se puede observar en los reportes del World Economic Forum (Principles for Board

Governance of Cyber Risk, March 2021) y (The Global Risks Report 2021).

Por otra parte, un plan para definir la estrategia y marco de trabajo de ciberseguridad, seguridad y privacidad requiere conocer de antemano las necesidades de la organización con respecto a su realidad, sin ser esto lo único que debería comprender, de modo que, dicha organización pueda ser más proactiva en la toma de decisiones al momento de proteger sus activos e información.

En este contexto, las normas y estándares tienen un papel clave en el gobierno de la ciberseguridad, seguridad y privacidad, ayudando a establecer una directriz de aplicabilidad de estas y tener definidas políticas y controles que están en sinergia con los objetivos y su tecnología, debido que algunas de sus operaciones se encuentran certificadas o alineadas con estándares nacionales e internacionales de seguridad de la información.

II. PROBLEMA

El problema identificado se ha resumido en una pregunta:

¿Cómo gobernar la ciberseguridad, seguridad y privacidad de la información de forma global y centralizada con el fin brindar los niveles adecuados de confianza digital para un proveedor de servicios de telecomunicaciones a lo largo de la región?

III. PROPUESTA DE SOLUCIÓN

Son varios factores que avalan la propuesta que surge a partir del problema planteado:

Por ser una empresa multirregión, la ciberseguridad, seguridad y privacidad es un punto muy importante, es una tarea que se fortalece y gana importancia en el negocio y cada vez más en el apoyo de sus operaciones.

La información propia y de sus clientes ha sido estimada como un activo estratégico para cumplir con sus objetivos corporativos. Preservar confidencialidad, integridad, disponibilidad, y privacidad; a través de un gobierno centralizado como herramienta facilitadora en el logro de los objetivos y gestión eficaz de los recursos y sus operaciones; es muy importante.

Sumado a lo anterior, la privacidad es un elemento importante, darle un tratamiento más transparente y confiable a los datos personales que recoge, sea de sus colaboradores, clientes o proveedores es un pilar importante del área de seguridad, su área legal y de cumplimiento. Por estar sometidos a distintos marcos regulatorios que rigen sus operaciones en la región, requiere una gestión y gobierno organizado en el tratamiento, procesamiento y/o transmisión de información personal por medio de las tecnologías de la información y/o las redes de comunicaciones.

En cuanto al crecimiento de los ciberdelitos, que hoy en día son cada vez más sofisticados y frecuentes, cabe destacar que los daños a gran escala causados por los ataques de ransomware a nivel internacional han venido aumentado. Según el informe de SonicWall (Mid-Year Update: 2021 SonicWall Cyber Threat Report), los ataques de ransomware en el primer semestre de 2021 incrementaron en un 151% en comparación al mismo periodo del año anterior. Esto es un punto importante para la empresa; la confidencialidad, disponibilidad, integridad, y privacidad de la información propia y de sus clientes, sus activos y servicios, hace necesario un modelo de gobierno y madurez de las medidas de protección implementadas, que le permita validar si son acordes a la realidad de los riesgos identificados y a la realidad global de los ataques informáticos, compensando así pérdidas financieras, tensiones reputacionales y/o inestabilidad en sus clientes.

Finalmente, el objetivo principal de la oficina de seguridad de la información, y por consiguiente del CISO (Chief Information Security Officer), es definir, implementar y mantener un gobierno de la seguridad y privacidad de la información global y centralizado, que le permita tener un mapa de ruta alineado a la estrategia corporativa, los recursos tecnológicos y el capital humano, para gestionar y responder de forma global los eventos inesperados, ya sean riesgos materializados y/o incidentes de ciberseguridad, en un ecosistema cambiante donde la infraestructura puede estar expuesta.

Esta estrategia permite generar valor al negocio, al disminuir la probabilidad de indisponibilidad en la prestación de los servicios, sufrir daños reputacionales o sanciones económicas, que puedan impactar la rentabilidad del negocio, debido a incumplimiento legal y regulatorio en alguna de sus operaciones. Contar con un framework permite seleccionar mecanismos que, alineados con los objetivos definidos

por la organización, y orientados a focalizar acciones en pro del beneficio de sus stakeholders, son un habilitador para el negocio.

Entre los beneficios de diseñar, definir e implementar el framework que apoye la gestión de la seguridad alineado a su visión y estrategia de negocio, se encuentran:

1. Proporcionar un entorno de confianza centrado en el negocio;
2. Proteger a los clientes, la marca y la reputación;
3. Satisfacer los requerimientos normativos, legales y regulatorios con respecto a la protección de información personal;
4. Medir la efectividad de los controles de ciberseguridad, seguridad y privacidad implementados;
5. Proporcionar una visión global del estado de la seguridad a nivel de las diferentes operaciones hacia el equipo ejecutivo desde la perspectiva del negocio por medio de tableros de control;
6. Optimizar la implementación de controles a nivel de las operaciones, debido a que desde una vista global puede manejarse un requerimiento local, reduciendo costos, y reduciendo esfuerzos del recurso humano de seguridad y de los equipos locales;
7. Monitoreo proactivo y centralizado por parte del Área de Seguridad de la Información;
8. Proporcionar una visión sistémica de los riesgos que la pueden afectar acorde con las situaciones que enfrenta;
9. Apalancar un modelo de gobierno de seguridad de la información apoyando la toma de decisiones basadas en los riesgos existentes.

Para el desarrollo del framework se plantean las siguientes fases:

Ilustración 1. Propuesta de Solución

Fuente: Elaboración propia.

Fase 1: Descubrir

El objetivo de esta fase se centró en determinar el estado actual de la gestión de la ciberseguridad, seguridad y privacidad de la información en la organización.

Para el desarrollo de la investigación se establecieron las técnicas para la evaluación de datos, considerando que al interior existen documentos útiles con información adecuada para diagnosticar el estado actual.

En el logro de cumplimiento de esta fase, se obtuvo acceso a información relevante, y alguna confidencial como la descrita a continuación:

a. Misión del área de seguridad;
b. Visión del área de seguridad;
c. Estrategia de Seguridad;
d. Estructura organizacional;
e. Política(s) de Seguridad de la Información;
f. Marco para la Gestión de Riesgos de ciberseguridad;
g. Estado de los riesgos y su mapa de calor;
h. Procesos de Seguridad;
i. Presupuesto asignado al área de Seguridad;
j. Proyectos en curso;
k. Presentaciones ejecutivas hacia los Stakeholders;
l. Requerimientos legales;
m. Test de seguridad;
n. Incidentes de seguridad;
o. Programa de entrenamiento y concientización en seguridad y privacidad.

Fase 2: Divisar

En esta fase se buscó comprender mejor los requisitos de los principios de ciberseguridad, seguridad y privacidad.

Se identificaron los framework que hacen parte de la propuesta de la Fase 3; para ello, se llevaron a cabo las siguientes etapas:

Etapa 1: Identificación de la población;
Etapa 2: Identificación de los Framework;
Etapa 3: Evaluación de los Framework.

Etapa 1: Identificación de la población

Para el desarrollo de esta etapa, se elaboró un instrumento de recolección de información, una encuesta tipo cuestionario, con el fin de identificar los Frameworks relevantes para la organización y sus operaciones. Los resultados obtenidos identifican los framework que hacen parte del análisis de la Etapa 2.

Con el fin de tener una visión holística de la ciberseguridad, se define la aplicación del instrumento de investigación a personal con roles estratégicos y operativos, involucrados en los procesos de ciberseguridad a nivel de todas sus operaciones.

Como resultado de esta visión global, se obtienen los siguientes frameworks para analizar:

a. ISO 27001;
b. PCI-DSS;
c. SOC 2;
d. NIST CSF;
e. ISO 31000;
f. ISO 27002.

Etapa 2: Identificación de los Framework

a. Criterios de Evaluación para la Selección del Framework

Los autores S. Donaldson, S. Siegel, C. Williams, A. Aslam (2018) indican, "… el programa de ciberseguridad de una empresa puede ser mapeado contra otros marcos de seguridad, y describe las razones para realizar dicho mapeo, como lo son:

- Muchos sectores están regulados y deben cumplir con normativas, leyes y regulaciones;
- De igual manera, los programas de ciberseguridad deben cumplir con los requisitos de ciberseguridad reglamentarios;
- El cumplimiento de dichas normativas y requisitos debe ser demostrable a los auditores independientes y a los reguladores;
- Las empresas necesitan informar sobre el estado de sus programas de ciberseguridad con respecto a los marcos externos para satisfacer a sus propios auditores u otros fines empresariales internos;
- Las empresas desean cotejar su programa de ciberseguridad con un marco externo para generar ideas para fortalecer la postura de ciberseguridad de la empresa."

De acuerdo con lo anterior, para el desarrollo del proyecto de investigación se han definido los siguientes criterios para para seleccionar el framework o los frameworks que más se adapten a las necesidades de la organización desde tres aristas de evaluación:

- Cumplimiento;
- Negocio;
- Evaluación.

Categoría	Criterios
Cumplimiento	Es un requerimiento contractual con o de terceras partes
	Es un requerimiento legal, normativo o regulatorio
	Por lo menos una operación está alineada o certificada
Negocio	Se alinea con la estrategia de seguridad y objetivos del negocio
	Genera una ventaja competitiva frente a los stakeholders (Partes interesadas)
	Se ajusta a los planes de mitigación de los riesgos identificados
Operación	Es un framework amplio con respecto a los controles de ciberseguridad, seguridad y privacidad
	Es un framework coherente, estructurado y con procesos definidos
	Es un framework certificable

Categoría	Criterios
	Se requiere habilidades y conocimiento específico del personal para la aplicación del framework
	Es un framework orientado a la gestión de riesgos integrada
	El framework apoya la gestión de la seguridad (Informes y Métricas)

Tabla 1. Criterios de Evaluación del Framework

Fuente: Elaboración propia, basada en la Figura 2. Characteristics of Popular Framework; Gartner, ID 441470.

A continuación, se realiza una breve explicación de cada uno de los criterios:

	Criterio	Descripción
CUMPLIMIENTO	Es un requerimiento contractual con o de terceras partes	El cumplimiento del framework puede estar ligado al contrato firmado por un Cliente para aceptar los servicios. El incumplimiento del framework puede llevar a pérdida de clientes o notas crédito relacionadas al incumplimiento.
	Es un requerimiento legal, normativo o regulatorio	El cumplimiento del framework se debe a requerimientos legales, normativos o regulatorios por ser un proveedor de servicios en alguna operación o en toda la organización.
	Por lo menos una operación está alineada o certificada	El cumplimiento del framework ya se encuentra en alguna operación certificada o alineada al mismo, siendo este un factor importante de selección, debido a la experiencia y madurez que se puede tener en la aplicación del framework y la madurez de sus controles.
NEGOCIO	El framework se alinea con la estrategia de seguridad y objetivos del negocio	El framework y su aplicación se alinea a la estrategia y objetivos de seguridad para soportar el negocio.
	Genera una ventaja competitiva frente a los stakeholders (Partes interesadas)	El cumplimiento del framework genera una ventaja competitiva frente a los demás competidores en el mercado, el cual puede hacer que genere mayores ingresos al aumentar sus clientes.
	El framework se ajusta a los planes de mitigación de los riesgos identificados	El framework y su aplicación se alinea a los planes de riesgos definidos para mitigar las posibles amenazas o vulnerabilidades a las se puede estar expuesta.
OPERACIÓN	Es un framework amplio con respecto a los controles de ciberseguridad, seguridad y privacidad	El framework contiene una lista completa de controles de ciberseguridad, seguridad, y privacidad tanto técnicos como de procedimiento, que pueden aplicarse. Esta lista abarca una amplia variedad de ámbitos aplicables al alcance del framework.
	Es un framework coherente, estructurado y con procesos definidos (Programa de Seguridad)	Una simple lista de controles no es suficiente para desarrollar un programa de seguridad. El framework proporcional un conjunto de procedimientos y gobernanza que, en conjunto, conforman un enfoque sistemático y riguroso de la aplicación de los controles.
	Es un framework certificable	El cumplimiento del framework puede ser certificable, en algunos casos es necesario y deseable esto.
	Se requiere habilidades y conocimiento específico del personal para la aplicación del framework	Cumplir o adherirse al framework de seguridad no es sencillo. Sin embargo, algunos framework requieren formación o certificación específica de las personas para apoyar su implementación.
	Es un framework orientado a la gestión de riesgos integrada	Seleccionar y gestionar los controles en función del riesgo para garantizar una mejor alineación y priorización de la asignación de recursos, por lo que utilizar un enfoque de gestión de riesgos evitará un gasto excesivo en la implementación de controles.
	El framework apoya la gestión de la seguridad (Informes y Métricas)	El framework contiene un proceso inherente para apoyar las métricas y la presentación de informes a los stakeholders y otras partes interesadas. Esta es una herramienta de comunicación fundamental para apoyar la eficacia de la gestión de riesgos y el soporte para la aprobación recursos y presupuestos.

Tabla 2. Explicación de los criterios de Evaluación

Fuente: Elaboración propia, basada en la Tabla 1. Comparison Criteria Explained; Gartner, ID 441470.

Etapa 3: Evaluación del Framework

a. Metodología de Evaluación

La evaluación de los frameworks con respecto a los criterios se realizó mediante el proceso de análisis jerárquico (AHP), desarrollado originalmente por Thomas L. Saaty (The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation), el cual está diseñado para resolver problemas complejos de criterios múltiples, transformando los aspectos cualitativos en cuantitativos, y estableciendo pesos de prioridad para las alternativas mediante la organización de objetivos, criterios y subcriterios en una estructura jerárquica.

Este método nos ayudó en la toma de decisión, teniendo en cuenta los objetivos de negocio y beneficios esperados, como también restricciones, riesgos y aspectos financieros.

b. Resultados de la Evaluación

Los resultados de la evaluación arrojaron los framework más aplicables a la organización.

A continuación, se muestra el resultado de los Framework propuestos:

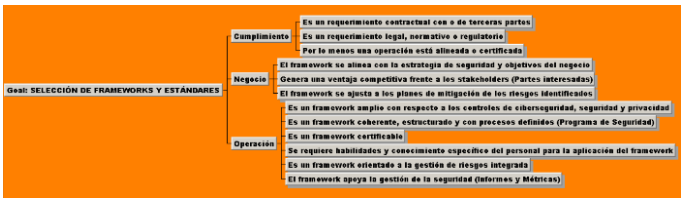

Ilustración 2. Criterios de Evaluación

Fuente: Elaboración propia – Herramienta

Para determinar el peso de cada criterio se utilizó la escala de Saaty, como se describe en la tabla descrita a continuación:

VALOR	DEFINICIÓN	COMENTARIOS
1	Igual importancia	El criterio A es igual de importante que el criterio B
3	Importancia moderada	La experiencia y el juicio favorecen ligeramente al criterio A sobre el B
5	Importancia grande	La experiencia y el juicio favorecen fuertemente el criterio A sobre el B
7	Importancia muy grande	El criterio A es mucho más importante que el B
9	Importancia extrema	La mayor importancia del criterio A sobre el B está fuera de toda duda
2,4,6 y 8	Valores intermedios entre los anteriores, cuando es necesario matizar	

Tabla 3. Escala de Saaty

*Fuente: Elaboración basada en **Thomas L.** Saaty (1980), The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation.*

De acuerdo con la metodología expuesta se obtuvo la representación de la jerarquía de criterios y sus pesos, como se puede observar a continuación:

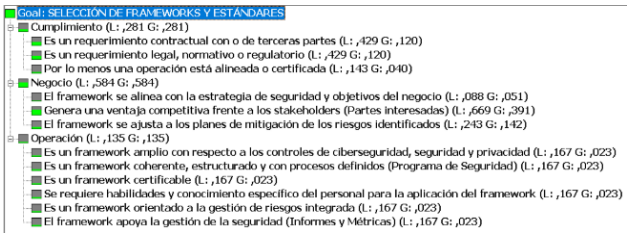

Ilustración 3. Jerarquía de criterios, pesos

Fuente: Elaboración propia – Herramienta

Una vez realizada las evaluaciones de nivel 1 y nivel 2, se obtuvieron resultados de las alternativas que nos ayudaron a escoger los framework y estándares a utilizar para este proyecto, como se puede ver en los análisis gráficos a continuación:

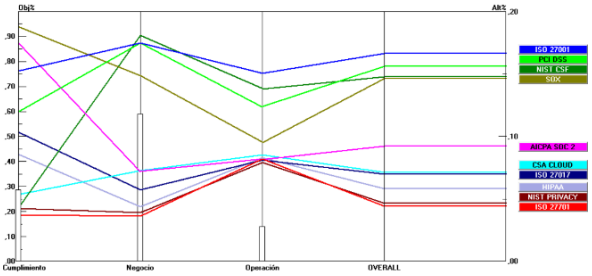

Ilustración 4. Análisis de Datos

Fuente: Elaboración propia – Herramienta

Análisis de sensibilidad

Se llevo a cabo un análisis de sensibilidad con el fin de evidenciar los cambios y la incertidumbre que generan otros valores de entrada para los criterios definidos, como también para predecir el resultado de la decisión con pesos diferentes a los de los juicios de los decisores.

Solución con las ponderaciones inferidas de los juicios de los decisores:

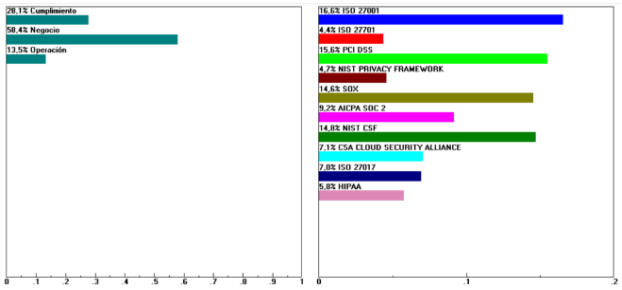

Ilustración 5. Análisis de Sensibilidad - juicios de decisores.

Fuente: Elaboración propia – Herramienta

Solución con una ponderación igual al 70% para el criterio de cumplimiento:

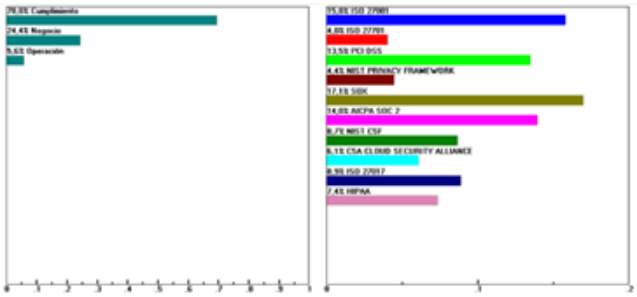

Ilustración 6. Análisis de Sensibilidad, Criterio: Cumplimiento

Fuente: Elaboración propia – Herramienta

Solución con una ponderación igual al 70% para el criterio de negocio:

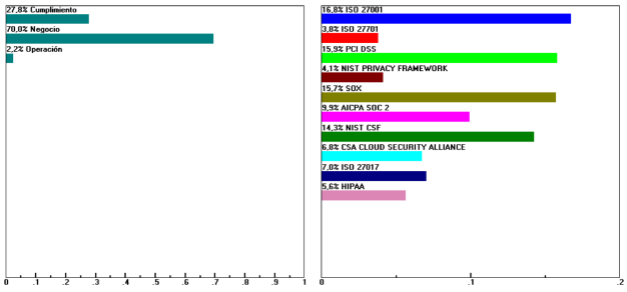

Ilustración 7. Análisis de Sensibilidad – Criterio: Negocio

Fuente: Elaboración propia – Herramienta

Solución con una ponderación igual al 70% para el criterio de operación:

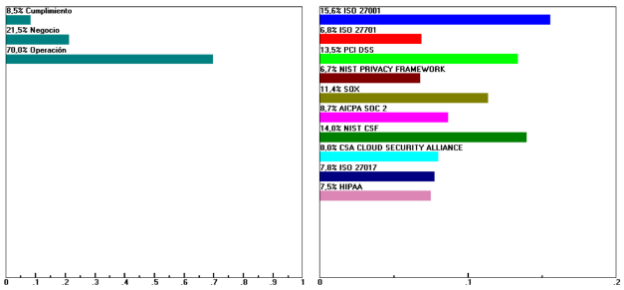

Ilustración 8. Análisis de Sensibilidad – Criterio: Operación

Fuente: Elaboración propia – Herramienta

Como se pudo observar en el análisis de sensibilidad, cambiando los pesos para cada criterio al 70% se constató que, considerando los criterios establecidos y ponderados para la elección de los framework y estándares, el resultado final indica que las alternativas más adecuadas son: ISO 27001, PCI DSS, NIST CSF y SOX.

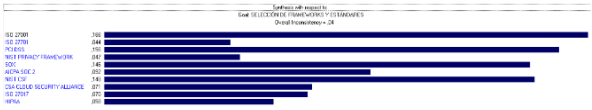

Ilustración 9. Selección del Framework

Fuente: Elaboración propia – Herramienta

Fase 3: Diseñar el Framework

En esta fase se desarrolló la herramienta con los framework seleccionados en la fase 2 (ISO 27001, PCI DSS, NIST CSF y SOX) con el fin de ayudar a la organización en el gobierno centralizado de la gestión de la seguridad, un marco de control global, el cual le permite identificar los controles que se comparten entre los diferentes framework.

Para el desarrollo de la herramienta, se tomó como base la NIST CSF, la cual se compone de buenas prácticas de otros Framework, tiene un lenguaje común y accesible, es adaptable a muchas tecnologías y se basa en el riesgo, lo que permite que pueda adaptarse más fácilmente; ya que como dice Gartner, ID: G00441470 (Security Frameworks: The What and Why, and How to Select Yours), "Los marcos de gestión de la seguridad, proporcionan un enfoque de gobernanza de la seguridad más amplio y formal para gestionar seguridad, en lugar de "sólo" una lista de controles".

Como se muestra en la tabla 4, el marco principal es la NIST CSF, sus funciones, categorías y subcategorías, las cuales han sido mapeadas con los otros framework seleccionados durante la Fase 2:

Function Grouping	NIST CSF Description				Framework		
	NIST CSF Domain	Control	NIST CSF #	Control Description	ISO 27001:2013	PCI-DSS v3.2.1	SOX
IDENTIFY (ID)	Asset Management (ID.AM)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1	Physical devices and systems within the organization are inventoried	A.8.1.1, A.8.1.2	2.4, 9.9, 11.1.1, 12.3.3	

Tabla 4. Framework

Fuente: Basado en la NIST CSF

Una vez desarrollada la primera fase de la herramienta, se desarrolla y propone un modelo de madurez (MIL – Maturity Indicator Level) basado en 4 niveles por cada uno de los controles. Este modelo se ha basado en el Cybersecurity Capability Maturity Model (C2M2).

Igualmente, se propone un Dashboard por Grupo de Función de la NIST CSF, como se puede observar en la Ilustración 10:

Ilustración 10. Dashboard

Fuente: Elaboración propia

Fase 4: Planificar

El objetivo de esta fase es definir y proponer un plan para la implementación del framework en la organización; este plan describe las actividades que deben seguirse, los recursos necesarios, los contactos claves, las actividades predecesoras y los hitos que deben tenerse en cuenta.

La organización será responsable de priorizar la implementación del framework en sus operaciones de acuerdo con su criticidad, complejidad, estructura, requerimientos legales, mercado e importancia para el negocio.

Fase 5: Evaluar y Aprobar

En esta fase, se presenta el Framework propuesto al Chief Information Security Officer (CISO) para su evaluación y aprobación.

IV. CONCLUSIONES

A. El framework es una propuesta que busca contribuir a la solución de la problemática identificada, se busca ayudar a disminuir los esfuerzos del capital humano en la implementación de controles de una manera más centralizada en todas las operaciones de la organización.
B. El diagnóstico de la situación actual con respecto a la ciberseguridad y privacidad de la empresa permitió responder a la pregunta al problema.
C. Las fases que se ejecutaron para la construcción y diseño del framework contribuyeron al cumplimiento de los objetivos enmarcados en el proyecto.
D. El framework está alineado con los objetivos y estrategia de negocio del proveedor de telecomunicaciones, generando valor en el negocio, y ayudando a los stakeholders en la toma de decisiones.
E. El framework aporta soporte en el cumplimiento legal, regulatorio y contractual del proveedor de telecomunicaciones, frente a sus clientes y terceros y reguladores.
F. Los criterios desarrollados para la definición del framework, permitieron a la organización realizar un análisis y selección objetiva de los frameworks que más se ajustaban al negocio.

V. REFERENCIAS

[1] Andrej Volchkov (2019), Information Security Governance. Framework and Toolset for CISOs and Decision Makers.
[2] Bell, J. (2002). Cómo hacer tu trabajo de investigación. Gedisa.
[3] BID, OEA Reporte de Ciberseguridad (2020). Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe.
[4] Capitán Gómez C. Carlos, May S. Luciano, Franco V. Carlos (2020). Análisis y estrategia de implementación de un marco de trabajo de ciberseguridad para la unidad de Ciberdefensa del Ejército Nacional. https://proyectosmaestrias.virtual.uniandes.edu.co/images/4SqhGgJEGI8iJbdVY3BhhR0moiYeph30Ke1tQv02.pdf
[5] Chris Moschovitis (2021). Privacy, Regulations, and cybersecurity.
[6] Cybersecurity Capability Maturity Model (C2M2).
[7] D. Blum (2020), Rational Cybersecurity for Business.
[8] Gartner, ID: G00441470 (2020), Security Frameworks: The What and Why, and How to Select Yours
[9] John Wiley & Sons, Inc. (2017), The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities.
[10] Krag Brotby (2009), Information Security Governance. A Practical Development and Implementation Approach.
[11] McGraw-Hill, Thomas L. Saaty (1980), The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation.
[12] Michele Bernasconi, Christine Choirat, Raffaello Seri (2010). The Analytic Hierarchy Process and the Theory of Measurement.
[13] Onibere, M., Maynard, S. B., & Ahmad, A. (2017). The chief information security officer and the five dimensions of a strategist.
[14] Portillo, E. (2015). Estrategia de innovación como marco para la adopción de un sistema de gestión de seguridad de la información.
[15] Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam (2018). Enterprise Cybersecurity Study Guide: How to Build a

Successful Cyberdefense Program Against Advanced Threats.
[16] S.H. von Solms, l R. von Solms (2009). Information Security Governance.
[17] SonicWall (2021). Mid-Year Update: 2021 SonicWall Cyber Threat Report. https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf
[18] SOX, ttp://www.sec.gov/about/laws/soa2002.pdf
[19] The Analytic Hierarchy Process: Structured Decisions. https://www.expertchoice.com/ahp-software
[20] William Stallings (2019). Effective Cybersecurity: Understanding and Using Standards and Best Practices.
[21] World Economic Forum (2021). Principles for Board Governance of Cyber Risk. http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf
[22] World Economic Forum (2021). The Global Risks Report 2021. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf