Ciberseguridad en redes NGN. Un análisis documental de los principales riesgos organizacionales y las estrategias de protección

Ingeniero Harol Stevens Araque Rojas

Asesor

Ingeniera Mónica Andrea Rico Martínez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Redes NGN

2025

Agradecimientos

La realización de este trabajo fue posible gracias al acompañamiento académico y a los recursos formativos brindados por la Universidad Nacional Abierta y a Distancia, UNAD, institución universitaria que ha promovido durante todo el proceso de la formación académica los espacios de aprendizaje que permitieron el desarrollo de esta monografía, fortaleciendo las diferentes competencias necesarias para el análisis y la comprensión desde la ciberseguridad.

De manera especial, se expresa un sincero agradecimiento a la ingeniera Mónica Andrea Rico por su valioso acompañamiento, orientación y aportes durante el proceso de elaboración de esta monografía. Su acompañamiento académico y sus observaciones oportunas contribuyeron de manera importante en la organización, el enfoque y la calidad del trabajo realizado.

Agradeciendo también a mi familia por el apoyo constante e incondicional, la comprensión y el ánimo brindado durante este importante proceso académico como profesional, los cuales fueron muy importantes para culminar satisfactoriamente este trabajo.

Resumen

Las Redes de Nueva Generación conocidas como NGN, representan actualmente un avance muy importante al permitir la convergencia en los servicios de voz, de datos y de video bajo una misma infraestructura basada en protocolos IP. Sin embargo, esta evolución tecnológica ha presentado desafíos en cuanto a la ciberseguridad, debido a la complejidad de los entornos digitales actuales, a la interconexión masiva de dispositivos y a la diversidad de servicios que operan en estas redes.

Actualmente el desarrollo de las Redes de Nueva Generación NGN, están caracterizadas por la integración de varios servicios en tiempo real sobre una infraestructura común basada en el protocolo IP. Estas redes permiten integrar voz, datos, video y otros servicios de valor agregado en tiempo real, brindando mayor eficiencia y flexibilidad en la gestión de las comunicaciones.

La presente monografía, tiene como objetivo analizar los principales riesgos organizacionales que están asociados a la ciberseguridad y que enfrentan las redes NGN, así como las diferentes estrategias y los marcos normativos actuales para su protección. Para ello, se realizó una revisión de literatura académica, de informes técnicos y estándares internacionales relacionados con la seguridad de la información y además la gestión en infraestructuras de telecomunicaciones basadas en las NGN.

Entre los hallazgos más importantes se identifican las vulnerabilidades propias de la convergencia tecnológica, la ausencia en la implementación de políticas organizacionales en cuanto a la seguridad, además de la necesidad de implementar arquitecturas seguras desde su diseño, el fortalecimiento de la cultura organizacional y la importancia de adoptar buenas prácticas como el cifrado, la autenticación robusta y también el monitoreo permanente.

Este trabajo de grado aporta una visión clara y además actualizada sobre la importancia de lograr fortalecer la ciberseguridad en entornos NGN, donde de promueva una gestión acorde de los riesgos y una cultura organizacional orientada a la protección de la información, en el que se garanticen la continuidad de los servicios. Sin embargo, esta transformación también ha incrementado los riesgos asociados a la seguridad de la información organizacional, al ampliar la superficie de ataque y exponer vulnerabilidades críticas que pueden ser explotadas por agentes malintencionados.

Palabras clave: Ciberseguridad, NGN, protección de red, riesgos organizacionales, seguridad de la información

Abstract

Next-Generation Networks (NGNs) represent a pivotal advance, enabling the convergence of voice, data, and video services over a single IP-based infrastructure. This evolution promises efficiency but introduces significant cybersecurity challenges due to digital complexity, device interconnection sprawl, and diverse service operations within these networks. NGN development is marked by real-time service integration of voice, data, video, and value-added services on shared IP platforms. This convergence enhances communication management flexibility but exposes critical vulnerabilities in technologically convergent environments lacking robust security policies from initial design stages onward.

Inadequate organizational safety cultures often fail in reinforcing encryption and strong authentication practices alongside constant monitoring protocols. These are often absent initially when deploying NGN infrastructures hastily without sufficient foresight into inherent risk factors tied with them long term. If not properly mitigated at onset during architectural planning phases and pre-deployment stages, breaches occur unchecked silently underneath surface layers. Unnoticed until too late, after damages are already done, irreversible harm may be inflicted beyond recovery capabilities available in post-compromise scenarios. Unfortunately, reality reflects that despite warnings issued beforehand repeatedly across various sectors, warning signs are ignored willfully or negligently by those highly responsible for maintaining proper order.

Either way, the end result is the same: compromised systems leak sensitive information outwards toward malicious actors exploiting weaknesses intentionally. They deliberately target weakest points systematically over time, gradually chipping away defenses layer-by-layer methodically until a breach is successfully achieved covertly. While external firewalls still hold firm, outwardly appearing secure, an illusion of stability persists deceitfully, convincing involved

parties nothing is amiss. Meanwhile, insiders might leak classified materials, colluding externally under payoff schemes hidden deep within organization charts until whistleblower tips finally surface.

Public scrutiny begins, and only then does action get taken seriously. Post-facto revelations make headlines and scandals unfold as media frenzies ensue. Culpability is assigned and accountability is held publicly. Success depends entirely on cooperation and truthfulness. Legal frameworks and binding obligations must be adhered to strictly with no exceptions allowed. Violations remain punishable by severe penalties imposed instantaneously upon detection, with authorities immediately notified once automated alerts are triggered today in our world.

Keywords: Cybersecurity, NGN, network protection, organizational risks, information security.

Tabla de Contenido

Lista de Tablas

Introducción

Actualmente el rápido desarrollo de las tecnologías de la información y las comunicaciones ha transformado la forma en que las organizaciones gestionan sus servicios y su información. En este proceso, se ha hecho cada vez más común la implementación de infraestructuras tecnológicas flexibles y orientadas a la integración de múltiples servicios (Velatia., 2021). De esta manera surgen las Redes NGN o Next Generation Networks las cuales permiten integrar servicios de voz, datos y video sobre una misma infraestructura, la cual está basada en protocolos IP, por lo cual las organizaciones han logrado optimizar recursos, mejorar la escalabilidad de sus servicios y facilitar la interoperabilidad entre redes fijas, móviles y entornos virtualizados, convirtiendo a las redes NGN en un componente importante para sectores como las telecomunicaciones, la banca, la salud y la administración pública (BPS., 2023).

Sin embargo, junto con estos beneficios también se presentan dificultades en materia de ciberseguridad, porque la alta interconectividad propia de las NGN, sumada a la virtualización de funciones de red, el uso de tecnologías como SDN y NFV, y además la dependencia de plataformas de gestión, ha ampliado las diferentes modalidades de ataques (Martínez., 2025). Como resultado, las organizaciones se enfrentan a amenazas cada vez más complejas, cuyos impactos también involucran aspectos organizacionales, normativos y de talento humano, ya que estas variables inciden directamente en la capacidad organizacional con el fin de prevenir, detectar y responder de manera oportuna a los incidentes de seguridad.

Por lo anterior, la ciberseguridad en redes NGN se convierten en un factor determinante, ya que de ellas dependen la protección de la información y la continuidad de los servicios en una organización. Garantizar la confidencialidad, la disponibilidad, la autenticidad y la confiabilidad de los datos se convierte en un objetivo prioritario para las organizaciones que operan sobre este

tipo de infraestructuras (Anías et al. , 2021). Si bien existen estándares y marcos de como lo son la ISO/IEC 27001, el NIST Cybersecurity Framework y las recomendaciones de la Unión Internacional de Telecomunicaciones o UIT, en la práctica muchas organizaciones presentan dificultades para su implementación, porque suelen estar relacionadas con la gestión del riesgo, la gobernanza de la seguridad y la consolidación de una cultura organizacional que este orientada en la protección de la información.

Bajo este escenario, el presente trabajo monográfico planteó la ciberseguridad en las Redes NGN y como bajo estas se pueden identificar y analizar los principales riesgos organizacionales que afectan este tipo de entornos tecnológicos. De igual manera, se examinaron las amenazas más recurrentes y las estrategias de protección propuestas en las investigaciones que se hicieron frente a la literatura académica y normativa, tanto a nivel internacional como nacional.

Este trabajo se centró en analizar la ciberseguridad en redes NGN desde distintos aspectos que influyen en su implementación dentro de las organizaciones. A lo largo del trabajo se consideró que la protección de la información no depende únicamente de controles tecnológicos, sino también de la forma en que se gestionan los procesos internos y se cumplen los lineamientos normativos. En ese sentido, el desarrollo del documento aportó elementos que pueden ser de gran apoyo para la toma de decisiones y para el fortalecimiento de prácticas orientadas en proteger la información y garantizar la continuidad de los servicios en entornos de redes NGN.

De acuerdo con estos propósitos, en la monografía inicialmente se describió el contexto tecnológico y normativo de las NGN; posteriormente, se identificaron y analizaron los principales riesgos y vulnerabilidades que afectaban la seguridad de la información en dichas

redes; y, finalmente, se documentaron estrategias y recomendaciones orientadas a fortalecer una gestión de ciberseguridad alineada con los estándares internacionales vigentes.

Objetivos

Objetivo General

Analizar, desde una revisión documental, los principales riesgos en ciberseguridad que están asociados a las NGN, considerando amenazas comunes como los ataques de denegación de servicio DDoS, spoofing, sniffing, vulnerabilidades en protocolos y fallos de gobernanza organizacional, junto con las estrategias normativas y técnicas propuestas en la literatura para su protección.

Objetivos Específicos

Identificar las amenazas más comunes que afectan la seguridad de las redes NGN según fuentes académicas y también técnicas actuales.

Describir los diferentes estándares internacionales y marcos legales vigentes que orientan en la protección de la información en entornos NGN.

Proponer estrategias de protección basadas en buenas prácticas y recomendaciones documentadas para fortalecer la ciberseguridad en redes NGN en el ámbito organizacional.

Justificación

Actualmente las redes de nueva generación representan uno de los ejes principales en cuanto a servicios que sostienen sectores estratégicos como lo son las telecomunicaciones, la banca, la salud y la administración pública. No obstante, la velocidad en su implementación tecnológica no siempre ha ido acompañada de una apropiación clara den cuanto, a sus riesgos en ciberseguridad, especialmente en entornos donde la normatividad existe, pero su adopción es dispareja o también limitada.

Este estudio se justificó en la necesidad de consolidar el conocimiento especializado, accesible y actualizado sobre las amenazas cibernéticas en redes NGN. Por medio de fuentes documentales, estándares internacionales y en legislación actual vigente. En lugar de realizar una investigación, esta monografía propone una revisión crítica de la literatura, que permita comprender el panorama global y nacional desde una perspectiva académica.

Como valor agregado este trabajo no se limitó a describir sobre los riesgos técnicos, puesto que se analizaron los riesgos organizacionales y su impacto en la ciberseguridad de las NGN, algo poco abordado en la literatura actual. Por lo cual, se incorporó la comparación entre marcos normativos y estrategias de protección, ofreciendo un enfoque que combina lo regulatorio con lo tecnológico.

De esta manera, este trabajo tiene como objetivo convertirse en un insumo útil para ingenieros, administradores de red, estudiantes de posgrado y en administradores en decisiones, quienes requieren contar con herramientas conceptuales y de normativas claras para lograr gestionar los riesgos tecnológicos de manera exitosa.

El análisis documental aquí propuesto aporta claridad sobre un tema complejo y a su vez dinámico, fomentando una cultura de seguridad informada y adaptable, clave para el desarrollo digital actual sostenible.

Generalidades del Proyecto

El presente trabajo se desarrolló como un estudio documental, con un de carácter analítico y descriptivo, que está orientado en examinar los principales riesgos organizacionales que están asociados a la ciberseguridad en las Redes de Nueva Generación NGN y en valorar más estrategias de protección adecuadas frente a los problemas de este entorno tecnológico y de las TIC.

El trabajo de grado se centró en comprender cómo los riesgos técnicos, de personal y normativos incidían en la gestión de la ciberseguridad en entornos NGN, caracterizados por su interconectividad y por la creciente virtualización de los servicios. Este análisis permitió establecer las diferentes relaciones entre la experiencia organizacional en materia de seguridad, su nivel de cumplimiento en cuanto a los marcos regulatorios internacionales y la efectividad real de las estrategias de mitigación implementadas.

En este primer capítulo se presenta el contexto que da origen al trabajo de grado sobre la ciberseguridad en las Redes de Nueva Generación conocidas como NGN, junto con el planteamiento del problema, la justificación, los objetivos generales y específicos el método de análisis utilizado. Este capítulo ofrece una comprensión clara del propósito del trabajo, la importancia de analizar los riesgos organizacionales vinculados a las NGN y la necesidad de fortalecer las estrategias de protección desde la normatividad y la gestión.

Planteamiento del Problema

Actualmente las amenazas cibernéticas son cada vez más sofisticadas y persistentes (Cyberark, 2025). Por estas razones, la protección de los servicios ofrecidos a través de las NGN se convierte en una situación prioritaria, debido a las fallas donde los mecanismos de seguridad pueden derivar en pérdidas de información confidencial, además de interrupciones del servicio,

sumado a ello en afectaciones económicas y en la pérdida de confianza por parte de los usuarios y de los clientes.

Sumado a esto, la ciberseguridad se ha convertido en una variable clave, que permite el garantizar la continuidad, la integridad y la confiabilidad de los servicios ofrecidos a través de las NGN (D'Andrea et al. , 2024). Y aunque existen actualmente estándares internacionales ampliamente reconocidos, como lo son la norma ISO/IEC 27001, que establecen las directrices para implementar Sistemas de Gestión de Seguridad de la Información (ISO, 2022)

O el NIST Cybersecurity Framework de los Estados Unidos, el cual propone buenas prácticas basadas en cinco funciones clave que son el identificar, proteger, detectar, responder y recuperar; muchas organizaciones no aplican estas herramientas de manera atenta y efectiva (NIST, 2024).

Además, la UIT ha emitido recomendaciones como la ITU-T X.805, la cual define una arquitectura de seguridad para redes de telecomunicaciones (ITU, 2003), incluyendo entornos con NGN. Pese a la existencia de estas normatividades, aún se presentan inconsistencias en la implementación de medidas de seguridad informática por parte de los operadores de red, especialmente en países en desarrollo como Colombia (Grajales et al. , 2025).

En el país el marco legal incluye normas como la Ley 1273 de 2009, que creó el tipo penal de delitos informáticos (CRC, 2009); la Ley 1581 de 2012, que regula la protección de datos personales (CRC, 2012); y las políticas públicas como el CONPES 3995 de 2020, que establece la Política Nacional de Confianza y Seguridad Digital (CONPES, 2023).

Sin embargo, la implementación oportuna y eficaz de estas disposiciones sigue siendo limitada en muchos entornos organizacionales, debido a la falta de conocimiento técnico, presentando por estas razones debilidades en la gestión de los riesgos en ciberseguridad.

De esta manera surgió la necesidad de realizar un análisis documental e investigativa que permitió identificar las principales amenazas y vulnerabilidades que enfrentan las redes NGN, así como las estrategias y los marcos regulatorios y de gestión actuales para su mitigación. Esta monografía tiene como propósito el generar una visión clara y actualizada sobre el estado actual de la ciberseguridad en NGN, resaltando su importancia en el fortalecimiento organizacional con el fin de garantizar la protección de la información. Lo que llevó a la siguiente pregunta de investigación:

¿Cuáles son los riesgos organizacionales que afectan la ciberseguridad en las Redes de Nueva Generación NGN y qué estrategias de protección, tanto normativas como técnicas, se pueden documentar y proponer para fortalecer la seguridad en las organizaciones?

Metodología

La investigación se desarrolló bajo el método cualitativo, con un diseño documental y de carácter analítico descriptivo. Su propósito metodológico fue recopilar, examinar y contrastar información académica, técnica y normativa que permitiera identificar los principales riesgos de ciberseguridad en las Redes de Nueva Generación NGN y evaluar las estrategias de protección propuestas en la literatura encontrada de acuerdo al tema de estudio y los marcos regulatorios internacionales.

Las NGN son un modelo de infraestructura que integra servicios de voz, datos y video sobre una arquitectura basada en el Protocolo IP, sustituyendo de manera gradual las redes tradicionales de conmutación de circuitos. Estas redes se caracterizan por su capacidad de transporte de manera unificada, la virtualización de funciones de red o NFV, el uso de redes definidas por software o SDN y la interoperabilidad entre redes fijas y móviles.

Por tanto, la investigación analizó las redes IP, redes de acceso fijo de banda ancha basada en fibra óptica, redes de acceso móviles 5G, así como las plataformas virtualizadas utilizadas en la gestión de servicios y seguridad la NFV y SDN.

El alcance del estudio se delimitó en la revisión documental de información publicada entre los años 2019 al 2024, 2025, seleccionada por su vigencia y relevancia académica. Con la aplicabilidad al contexto latinoamericano, con especial énfasis en Colombia. El estudio se centró en identificar amenazas como ataques de denegación de servicio DDoS, spoofing, sniffing, y vulnerabilidades de protocolo.

Dado el carácter documental al ser una monografía, no se realizaron pruebas experimentales, simulaciones ni análisis de tráfico real; por tanto, los resultados correspondieron a un análisis desde lo investigado y comparado con las buenas prácticas en cuanto a la ciberseguridad dentro de las NGN.

El proceso metodológico se desarrolló en tres fases, la primera la compilación de la información, donde se consultaron bases de datos académicas como IEEE Xplore, ScienceDirect, SpringerLink, así como repositorios institucionales y documentos normativos emitidos por la UIT, ISO, NIST y el MinTIC, entre otros. Priorizando en las publicaciones que trabajaron con temas de ciberseguridad, gestión del riesgo, estándares internacionales y regulación nacional aplicable a las redes NGN.

La siguiente fase fue la clasificación y el análisis de la información encontrados, por medio de los documentos compilados que fueron organizados en cuatro categorías; los riesgos técnicos como las fallas de infraestructura, interoperabilidad, vulnerabilidades IP, los riesgos organizacionales en cuanto a las debilidades en la gestión, capacitación, respuesta a incidentes y cultura de seguridad. Los marcos normativos estándares internacionales como la ISO/IEC 27001,

la UIT-T X.805, NIST SP 800-53 y la normativa nacional como el Decreto 620 de 2020, Política Nacional de Ciberseguridad de Colombia.

Y estrategias de protección como medidas de mitigación, buenas prácticas y mecanismos de gobernanza aplicados a las NGN. Se aplicó el análisis de contenido para identificar variables, vacíos conceptuales y coincidencias en los enfoques de seguridad adoptados por diferentes organismos y autores encontrados.

A partir del análisis de la información compilada, se construyó un marco comparativo de riesgos y estrategias, en las cuales se contrastaron las principales amenazas identificadas en las NGN con las medidas de mitigación propuestas por distintos marcos normativos y autores encontrados. Donde se fortaleció la comprensión de la gestión organizacional en ciberseguridad, integrando los resultados en un marco teórico y conceptual que sustenta las conclusiones y recomendaciones finales de este estudio.

Marco Teórico

Frente a los Modelos y Estándares de Seguridad

La NIST Cybersecurity Framework 2.0 (2024), presenta un enfoque estratégico y además organizativo para madurar procesos de seguridad, con énfasis en resiliencia, gestión de cadenas de suministro y gobierno corporativo (NIST, 2024).

Además de los estándares internacionales como la ISO 27001, para la gestión de seguridad de la información. Estudios recientes en el sector financiero demuestran mejoras en lo que es la gestión de riesgos, respuesta a incidentes y de cultura organizacional (Kuzankah et al. , 2024).

Junto a la ITU -T X.805, el cual es el marco de seguridad para las redes de telecomunicaciones, incluyendo aspectos como la confidencialidad, la autenticación y el control de acceso, y que puede ser plenamente aplicables a infraestructuras de NGN (ITU, 2003).

En cuanto a la seguridad en redes NGN y 5G, autores como Sahni et al. (2022), explican por medio de una revisión sistemática sobre seguridad en 5G, la complejidad del ecosistema, la aparición de nuevos vectores de ataque y el uso de IA y SDN para la detección y la defensa (Sahni et al , 2022).

Por su parte Damir et al. (2022), presentaron un nuevo protocolo de autenticación, de acuerdo con claves para 5G, con cifrado resistente en ataques cuánticos, que mejoraron la seguridad de 5G AKA tradicional (Damir et al. , 2022).

Otros autores como el caso de Ghafoor & Bazai (2022), analizaron el uso de machine learning para la detección de intrusiones en redes 5G, alcanzando una precisión del 99.7 % en datasets NSL-KDD (Ghafoor et al. , 2022).

Holtrup et al. (2022), clasificaron las amenazas en función de STRIDE y recomendaron controles específicos para el núcleo y el radio, tanto en despliegues NSA como en SA (Holtrup et al. , 2021)

Y, por último, un estudio de International Technological University (2025) por el autor Mehrab, evaluaron los riesgos en slicing y virtualización SDN/NFV en 5G, señalando vulnerabilidades como la interoperabilidad, la segmentación y los ataques al plano de control (Mehrab, 2025).

Modelos de Protección

El ZTA, conocido como Zero Trust Architecture o arquitectura de confianza 0, por medio de la NIST desde el año 2020, tiene como principio central: Never trust, always verify, en español nunca confiar, siempre verificar (NIST, 2020), en especial en redes interconectadas y virtualizadas como las NGN. La misma NIST explica que en este documento que la implementación de operadores en telecomunicaciones, con el fin de gestionar accesos frente a los riesgos organizacionales.

Otro modelo conocido es el MITRE ATT&CK Framework, siendo una herramienta importante que permite el clasificar tácticas y también técnicas de ataque en infraestructuras de seguridad complejas. Fortinet resalta su valor para los Security Operations Centers o SOC's (FORTINET, 2024) cómo se explicó en el marco conceptual, ya que esta misma permite identificar patrones de intrusión y además en fortalecer las defensas proactivas (Scapicchio, 2024).

Frente a los Riesgos Organizacionales

Un estudio realizado por Merchán Castillo (2024), explica que por medio de network slicing o de segmento virtual de la red, donde se trabaja sobre la complejidad a la segmentación de redes como las 5G, y las vulnerabilidades que pueden surgir en la implementación.

Entre los riesgos están los ataques dirigidos a planos de control, los cuales afectan en la gestión y coordinación de los recursos de red, junto con los problemas que derivan de la separación inadecuada entre slices; lo que daría accesos no autorizados, incidentes de seguridad por medio de segmentos que, en principio, deberán estar aislados (Merchán , 2024).

Un análisis de estas amenazas aparece en estudios recientes sobre redes 5G/6G, de Alnaim(2024), que incluyen amenazas como la denegación del servicio, también la manipulación de slicing y la falta de aislamiento entre entornos virtuales (Alnaim, 2024).

Sumado a esto, las redes 5G y Wi-Fi, hacen que existan vulnerabilidades particulares que no se observan en entornos aislados, por ejemplo, problemas de autenticación compartida y de control de acceso en niveles físicos y de protocolo. Lo que implica desafíos regulatorios y de gobernanza significativos (Ramezanpour et al. , 2022).

Marco Conceptual

Redes de Nueva Generación

Las NGN son aquellas infraestructuras que permiten la transmisión de voz, datos y video a través de redes IP. Su diseño se basa en la separación entre servicios y red de transporte, permitiendo flexibilidad y convergencia de múltiples servicios en una misma plataforma (RedesTelecom, 2023).

Según Oliveira (2024), esta arquitectura, aunque eficiente, presenta desafíos en cuanto a la protección de red y la gestión de seguridad, al ser más propensa a vulnerabilidades por su alto grado de interconexión y virtualización (Oliveira , 2024).

Ciberseguridad

Se define como el conjunto de herramientas, políticas, directrices y prácticas diseñadas con el fin de proteger la integridad, la confidencialidad y la disponibilidad de los activos digitales frente a amenazas internas y externas (Lindemulder et al. , 2024).

El NIST Cybersecurity Framework 2.0 (2024), estructura la gestión de la ciberseguridad en cinco funciones que son: Identificar, Proteger, Detectar, Responder y Recuperar, promoviendo una cultura preventiva y además resiliente (NIST, 2024).

Seguridad de la Información

Va más allá de lo técnico, puesto que se refiere a la protección de los datos frente a los accesos no autorizados, pérdida o de modificación. Que incluye elementos organizativos, normativos y en recursos humanos (MINTIC, 2022). La ISO/IEC 27001:2022 establece los requisitos para un Sistema de Gestión de Seguridad de la Información o SGSI, y su norma complementaria ISO 27002:2022 ofrece un catálogo de controles para asegurar la información en diferentes situaciones (ISO, 2022), incluyendo redes NGN.

Amenazas Cibernéticas

Las amenazas en las redes NGN pueden clasificarse en ataques de denegación de servicio o DDoS, la suplantación de identidad o Spoofing, la intercepción de tráfico o sniffing (Radware, 2023).

La inyección de código malicioso en servicios IP según Mojan et al. (2021), la virtualización en NGN mediante tecnologías como SDN y NFV introduce nuevas puertas de entrada para actores maliciosos, especialmente en redes 5G (Mojan et al. , 2022).

Protección de Red

Esta implica implementar mecanismos para prevenir, detectar y mitigar ataques. En redes NGN, esto incluye la autenticación multifactor, Firewalls inteligentes NextGen, sistemas detección de intrusos o IDS/IPS, la segmentación con Network Slicing en redes 5G (Casquero et al. , 2020).

Nigam (2024) destaca que el uso combinado de inteligencia artificial y de machine learning en protección de redes 5G y NGN mejora la capacidad de respuesta ante amenazas dinámicas (Nigam, 2024).

Riesgos Organizacionales en Ciberseguridad

Son aquellos que afectan los procesos, activos y operaciones de una organización, García (2020), en su trabajo Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo de la Universidad Piloto de Colombia, explica que en las organizaciones se tiende a subestimar o malinterpretar los riesgos de ciberseguridad, afectando la toma de decisiones (García , 2020).

Riesgos Técnicos

La infraestructura de las NGN se compone de protocolos IP y de arquitecturas virtualizadas, lo que aumenta su superficie de ataques. Por ejemplo, errores en protocolos y software pueden generar graves vulnerabilidades, según la ITU-T, con base a la recomendación Y.2701, 2022, que analiza los requisitos de seguridad específicos en NGN (UIT-T, 2007).

Riesgos Humanos

Es uno de los factores más débiles en ciberseguridad, esto en cuanto a estudios como el de Coker (2025), el cual describe que el 95% de las filtraciones en datos se deben a errores humanos, y que apenas el 8 % del personal es responsable del 80% de estos incidentes (Coker, 2025).

Otro autor como O'Flaherty (2025) explica que el 89 % de las empresas considera el error humano como su principal obstáculo de seguridad, destacando la falta de capacitación y hábitos de los usuarios (O'Flaherty, 2025).

Reporte del año 2023, como el de la empresa tecnológica Kaspersky, informa que casi el 25 % de los incidentes de alta gravedad incluyeron intervención del personal directamente, especialmente en sectores críticos de las organizaciones como los de contabilidad (Woburn, 2024).

Riesgos de Normatividad y de Cumplimiento

Dado el Foro Económico Mundial o WEF por sus siglas en inglés en este 2025, advierten que el vacío que se presenta en habilidades cibernéticas y la falta de regulaciones fuertes amplían la superficie de ataque (WEF, 2025); especialmente en entornos críticos como los de NGN

La falta de implementaciones en marcos normativos como la ISO/IEC 27001, NIST CSF o Cybersecurity Framework (2018) y reglamentos como el GDPR (2016) generan vacíos en la gestión de seguridad, lo cual incrementa en los riesgos organizacionales.

Human-Machine Identity Blur

Janani (2025) realizó un estudio de cómo la creciente integración de identidades humanas y máquinas crea nuevas superficies de ataque. Por lo cual propuso un Unified Identity

Governance Framework, que está basado en la verificación continua y en los principios de confianza cero, lo que mejoró la respuesta ante incidentes en un 62 % (Janani, 2025).

Centros de Operaciones de Seguridad, SOC

Encargados de supervisar, analizar y dar respuesta a incidentes de ciberseguridad. Permitiendo mitigar en los riesgos como malware, intrusiones, vulnerabilidades, pishing, errores operativos, entre otros (Scapicchio, 2024). En riesgos normativos el incumplimiento de marcos regulatorios como lo son la ISO 27001 o la NIST CSF Marco de Seguridad Cibernética (NIST , 2024).

Estado del Arte

Antecedentes Internacionales

Farris et al. (2019) realizaron una encuesta sobre los mecanismos de seguridad SDN y NFV para sistemas IoT, analizando que las amenazas más complejas están relacionadas con la manipulación de controladores, el tráfico malicioso entre funciones virtualizadas y la vulnerabilidad de las API abiertas (Farris et al., 2019).

Otro estudio de la King Faisal University de Saudí Arabia, explican que los ataques dirigidos a la segmentación y virtualización de redes 5G se han convertido en uno de los principales problemas en cuanto a la de seguridad global, al comprometer tanto la infraestructura física como los servicios en la nube (Alnaim, 2024).

Por su parte, Shi et al. (2024) en su trabajo *Physical layer security techniques for data transmission for future wireless networks,* proponen la adopción de mecanismos de cifrado en capa física y generación de claves dinámicas como solución complementaria para las NextG Networks (Shi et al. , 2022), mientras que un estudio de la Universidad Dalhousie de Canadá, explican sobre el estado actual de la eficiencia energética y la automatización como factores que

deben integrarse a la seguridad desde el diseño de las tecnología de redes inteligentes (Kiasari, 2024).

Desde la gestión organizacional, Bernardo, Malta y Magalhães (2025) desarrollaron un marco de evaluación de madurez en la ciberseguridad alineado con el NIST Cybersecurity Framework CSF, explicando la importancia de medir la gestión institucional y no solo la capacidad técnica. sino también la eficacia de los procesos institucionales en la gestión del riesgo digital.

De igual forma, Abdiukov (2023) y Babatunde et al. (2022) demostraron que la implementación combinada de los estándares ISO/IEC 27001 y el CMMI-Security permiten mejorar la gobernanza y la cultura de protección en organizaciones con infraestructuras distribuidas, que promueven una cultura de protección proactiva y optimiza la toma de decisiones en organizaciones con infraestructuras distribuidas y entornos altamente virtualizados.

Antecedentes Nacionales

El desarrollo de las redes NGN se encuentra de alguna manera vinculado con las políticas de Transformación Digital y Conectividad Inteligente impulsadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, la Comisión de Regulación de Comunicaciones y la Agencia Nacional del Espectro. Las cuales vigilan y promueven redes seguras, interoperables y sostenibles, pero a su vez enfrentan problemas relacionados con la ciberseguridad organizacional y la gestión de riesgos en entornos convergentes.

Un estudio de la Universidad Externado de Colombia realizó un diagnóstico sobre la adopción de redes IP de nueva generación en entidades públicas, encontrando problemas en la implementación de controles de ciberseguridad y en la capacitación del personal técnico (Salazar, 2024).

La revista ciberespacio, tecnología e innovación (2024) analizaron las vulnerabilidades en la infraestructura de telecomunicaciones, destacando la necesidad de aplicar marcos internacionales como la ISO/IEC 27001 y el NIST CSF para mejorar la protección de la información de universidades públicas del país (Carreño, 2024)

Por su parte, Ortiz (2024) propuso un modelo red industrial NGN para medidores de energía e integración con software para gestión de energía y análisis de consumo en Diaco planta Tuta, implementando una infraestructura híbrida que combino el cableado Ethernet y fibra óptica bajo estándares internacionales

Finalmente, la Política Nacional de Confianza y Seguridad Digital, CONPES 3995, 2020 fortalecen la protección cibernética, aunque la implementación práctica de estos marcos aún presenta debilidades en coordinación interinstitucional y evaluación de riesgos (Cremades et al. , 2024).

Vacíos Identificados

El análisis de los antecedentes permitió evidenciar varios vacíos tanto conceptuales y prácticos en la literatura relacionada con la ciberseguridad en las Redes de Nueva Generación NGN. Predomina una orientación técnica en la mayoría de los estudios, centrada en aspectos como los protocolos de comunicación, la virtualización de funciones de red o NFV, las redes definidas por software o SDN y los mecanismos de control del tráfico. Y aunque estas investigaciones fueron un soporte para la comprensión de las vulnerabilidades estructurales, existe una escasa atención hacia la gestión organizacional del riesgo, la gobernanza institucional y la gestión de los procesos internos, los cuales determinan la efectividad de la ciberseguridad en el ámbito corporativo.

También se observa una débil integración entre los marcos normativos internacionales y las estrategias operativas aplicadas en entornos NGN. La literatura revisada muestra que las organizaciones tienden a adoptar parcialmente estándares como ISO/IEC 27001 o el NIST Cybersecurity Framework, pero sin implementarlos de manera consistente con las políticas de gestión del riesgo, la cultura organizacional o la capacitación del talento humano. Y que no permite medir las gestiones organizacionales en materia de ciberseguridad, lo que dificulta la implementación de modelos de mejora continua.

Finalmente, se identifica la ausencia de investigaciones nacionales con base a las NGN, pero de carácter comparativo que documenten cómo las empresas de telecomunicaciones en Colombia implementan y adaptan los estándares internacionales en la gestión de la ciberseguridad en NGN.

Los pocos estudios existentes trabajan los aspectos tecnológicos o regulatorios generales, sin ofrecer evidencias sobre las prácticas, dificultades y niveles de madurez de las organizaciones nacionales. Lo que representa una oportunidad para fortalecer la comprensión de los problemas entre el marco normativo, la operación y la gestión organizacional del riesgo nacional.

Aporte del Estudio

A partir de los vacíos anteriormente identificados, el presente trabajo vinculo los factores tecnológicos con la gestión organizacional del riesgo. Su contribución principal, analizar la relación entre las vulnerabilidades de las NGN, el nivel de gestión institucional y la aplicación de marcos de referencia como la ISO/IEC 27001, NIST CSF y las políticas nacionales de ciberseguridad.

La revisión de los estudios recientes del 2019 al 2025, permitió comparar y evidenciar que es importante fortalecer la capacidad institucional y los modelos de gestión del riesgo y

promover buenas prácticas que garanticen una protección efectiva de los servicios avanzados de voz, datos y multimedia propios de las NGN.

Caracterización de las Amenazas que Afectan la Seguridad en Redes NGN

Actualmente el desarrollo de las Redes de Nueva Generación o NGN, han transformado la manera en que las organizaciones gestionan sus servicios de comunicación. Ya que estas redes no solo integran voz, datos y video en una infraestructura unificada basada en IP, sino que además dependen de la virtualización de funciones y la automatización para optimizar la prestación de los servicios (RedesTelecom, 2023). Sin embargo, esta integración ha aumentado la complejidad operativa y los problemas que están asociados a la ciberseguridad de las infraestructuras organizacionales digitales.

En este capítulo, se analizaron tres dominios principales dentro de las NGN, por un lado, las redes troncales IP, por otra parte, las redes de acceso fijo y móvil, y por último las plataformas que soportan la gestión de los servicios. Donde cada una de ellas se ve afectada por amenazas que impactan directamente los principios de confidencialidad, de integridad, disponibilidad y de autenticidad, que son las bases de la seguridad de la información según la norma ISO/IEC 27001, NIST Cybersecurity Framework CSF.

Amenazas en las Redes Troncales IP

Son el eje central del transporte en las redes NGN, ya que por estas redes troncales circulan la mayor parte del tráfico entre los sistemas y los servicios. Debido a esto, suelen verse afectadas por amenazas que buscan interrumpir el funcionamiento general de la red, a su vez de alterar el enrutamiento o reducir en la disponibilidad de los servicios que dependen de esta infraestructura (Anías et al. , 2021)

Entre sus principales amenazas se encuentran los ataques de denegación de servicio o DDoS, porque estos ataques sobrecargan la capacidad de procesamiento de los nodos en la red, afectando además en la disponibilidad de los servicios y generando interrupciones críticas en

entornos virtualizados (FORTINET, 2024). Su efecto se extiende más allá de lo tecnológico, pues afecta no solo la gestión, sino también la disponibilidad de los servicios y la confianza del usuario.

Junto con la amenaza de manipulación del enrutamiento conocido como BGP Hijacking, los cuales son atacantes que manipulan o anuncian rutas falsas, desviando el tráfico hacia destinos incorrectos o permitiendo la interceptación de la información sensible en tránsito (CloudFlare., 2025).

Otra amenaza es el Packet injection, el cual se encarga de enviar por medio de paquetes alterados o diseñados enlaces que afectan la estabilidad o provocar caídas en la red troncal (De los Llanos., 2024). Por último, la vulneración en los routers de backbone, los cuales se presentan cuando los equipos centrales operan con un firmware desactualizado, con protocolos sin mecanismos de protección y presentando configuraciones débiles que facilitan accesos no autorizados y fallos críticas que comprometen la estabilidad de la red (FORTINET., 2025).

Amenazas en las Redes de Acceso Fijo y Móvil

Las redes de acceso fijo y móvil representan el punto más cercano entre los usuarios y los servicios que ofrece una red NGN. Por esta razón, suelen ser una amenaza en escenarios frecuentes de ataques que buscan aprovechar configuraciones débiles, prácticas inseguras de los usuarios o por el nivel de accesibilidad pública que presentan algunas tecnologías de acceso (CISA., 2024).

Entre sus principales amenazas se encuentran la intercepción de tráfico, conocida como Sniffing, la cual es una amenaza para las redes NGN, porque permite el acceso no autorizado de información sensible cuando las comunicaciones no están cifradas adecuadamente, vulnerando la confidencialidad de los datos. Silvestre y De Ocampo (2023) presentaron en un estudio que

incluso herramientas de análisis de red como Wireshark pueden ser utilizadas con propósitos de espionaje, lo que resalta la necesidad de implementar controles preventivos y políticas de seguridad que regulen su uso en entornos corporativos.

En redes Wi-Fi, LTE o de fibra, la captura de paquetes permite obtener datos sensibles como credenciales, sesiones o información personal. Por tanto, esta amenaza no solo exige controles a nivel técnico como cifrado extremo, segmentación y filtrado, sino también políticas organizacionales que contemplen auditorías continuas, monitoreo en tiempo real y protocolos de gestión de incidentes adaptados al entorno de las NGN (Silvestre et al. , 2023).

Otra amenaza es la suplantación de identidad o Spoofing, la cual es utilizada para engañar a los sistemas de autenticación, con el fin de obtener acceso no autorizado, comprometiendo la autenticidad y la trazabilidad de las comunicaciones (Kaspersky Lab, 2025). Este tipo de ataque suele presentarse por fallas en la configuración de los servicios de la red y la falta de procesos eficaces para validar el origen del tráfico, lo que facilita la manipulación de direcciones IP o dominios falsificados (Morrás, 2022).

Amenazas en las Plataformas de Gestión y Servicios

Representan el núcleo administrativo y operativo de las redes NGN, donde su función es coordinar, supervisar y asegurar el correcto funcionamiento de los servicios, por lo que cualquier vulnerabilidad en estos sistemas tiene un efecto inmediato en la estabilidad y continuidad de la red (Gunawardena et al. , 2023).

Entre sus principales amenazas están las vulnerabilidades en los protocolos, donde su funcionamiento depende de la correcta configuración e integración entre sistemas (Aslan et al. , 2023). Estas fallas se originan en el uso de protocolos inseguros, versiones obsoletas o implementaciones incorrectas que no contemplan sistemas actualizados de autenticación o de

cifrado. Entre los protocolos utilizados para estas vulnerabilidades están los SIP o Session Initiation Protocol, BGP o Border Gateway Protocol y DNS Domain Name System, los cuales pueden ser utilizados para redirigir el tráfico, interceptar sesiones y gestionar el flujo de información en tiempo real (Owoko, 2024).

Por último, los fallos en la gobernanza organizacional se presentan por la ausencia de una estructura de gestión en la ciberseguridad, políticas desactualizadas o de carencia en la capacitación continua del personal (Interact, 2025). Estos factores aumentan la exposición al riesgo, a su vez dificultan la toma de decisiones y debilitan la capacidad de respuesta organizacional frente a incidentes (Almanza, 2024). El autor explica que la falta de liderazgo estratégico y de coordinación entre los objetivos tecnológicos y las políticas de seguridad, dificulta que una organización pueda contar con capacidad de adaptación y de respuesta ante incidentes de ciberseguridad.

Resumen de la Caracterización de Amenazas en NGN

El análisis desarrollado a lo largo de este capítulo permitió identificar que las redes NGN si bien han transformado la forma en que se prestan y gestionan los servicios de telecomunicaciones, sino que también presentan un conjunto de amenazas que pueden comprometer la operación de los servicios y la protección de la información en una organización. Estas amenazas se presentan en distintos niveles de la infraestructura NGN, desde las redes de acceso y transporte hasta las plataformas de gestión y control, afectando principios como la confidencialidad, la integridad, la disponibilidad y la autenticidad de los datos.

Por lo anterior, es importante conocer los principales riesgos identificados, junto con sus impactos y las medidas de prevención más importantes, con el fin de ofrecer al lector una visión clara de los hallazgos. Por esta razón, a continuación, se presenta una tabla que resume las

amenazas más frecuentes en las redes NGN, su impacto en una organización y las estrategias de prevención recomendadas, las cuales responden a las buenas prácticas y los principales estándares que son utilizados en la gestión de ciberseguridad.

Tabla 1

Amenazas y Estrategias de Mitigación en Redes NGN

Tipo de amenaza	Clasificación, principio de seguridad afectado	Descripción	Afectación	Estrategias de prevención
Ataques DDoS	Amenazas en las Redes Troncales IP	Saturación de recursos que interrumpen la disponibilidad en los servicios	Interrupción de las diferentes operaciones y áreas, dentro de una organización	La implementación de firewalls inteligentes, detección temprana de anomalías, y uso de CDN o red de distribución de contenido en una Cloudfare, Google Cloud CDN, entre otros
Spoofing	Amenazas en las Redes de Acceso Fijo y Móvil	Es la suplantación de IP o de credenciales para obtener acceso ilegítimo	La alteración frente al compromiso en la autenticidad e integridad de la información transmitida. El cual facilita el acceso fraudulento y la suplantación de identidad	Autenticación multifactor, filtros de tráfico o BCP 38, que tienen como objetivo evitar que se envíen paquetes de datos con direcciones IP de origen falsas se aplica en los routers o gateways de una red para verificar que los paquetes que ingresan provengan realmente de direcciones válidas dentro del rango permitido (Kaspersky, 2024)

Tipo de amenaza	Clasificación, principio de seguridad afectado	Descripción	Afectación	Estrategias de prevención
Sniffing	Amenazas en las Redes de Acceso Fijo y Móvil	Intercepción de tráfico no cifrado entre dispositivos o en servidores	Exposición de información confidencial en una organización	Cifrado extremo a extremo por medio de protocolos TLS/IPSec, donde TLS protege la capa de aplicación, y la IPSec protege la capa de red. Los dos evitan que la información sea interceptada o alterada durante su transmisión, junto con la segmentación de red (CloudFlare, 2025)
Vulnerabilidades en protocolos	Amenazas en las plataformas de gestión y servicios	El uso inadecuado de los protocolos SIP, BGP, DNS	Al no contar con procesos de autenticación o de cifrado adecuados, pueden ser vulnerados con el fin de interceptar, redirigir o manipular el tráfico de red. Para afectar la seguridad y disponibilidad de los servicios en las NGN.	Mantener actualizados los sistemas, validar la autenticidad del enrutamiento del tráfico. Fortalecer los servicios para garantizar la seguridad de las NGN.
Fallos de gobernanza	Amenazas en las plataformas de gestión y servicios	Falta de políticas o de cultura	Los fallos de gobernanza generan una afectación directa en la	Implementar estándares como la ISO/IEC 27001, NIST

Tipo de amenaza	Clasificación, principio de seguridad afectado	Descripción	Afectación	Estrategias de prevención
		en la seguridad organizacional	estabilidad de la organización, al presentar debilidades en la gestión estratégica de la ciberseguridad	CSF, con capacitaciones y auditorías

Nota. Se describe brevemente el resumen de los diferentes tipos de amenazas y estrategias de mitigación en redes NGN

Estándares Internacionales y Marcos Legales Vigentes que Orientan la Protección de la Información en Entornos NGN

La implementación y uso de redes NGN, actualmente se ha vuelto más común en organizaciones que requieren manejar grandes volúmenes de información y servicios interconectados. A medida que estas redes implementan distintos protocolos, equipos y plataformas, también se presentan inconvenientes para mantener la seguridad de los datos y asegurar que todo funcione de manera continua y confiable.

Por esta razón, los estándares internacionales y la normativa nacional vigente se convierten en referentes importantes para orientar en el manejo de las buenas prácticas, además de establecer responsabilidades e implementar medidas que permitan reducir riesgos en el uso de tecnologías avanzadas.

En este capítulo se presentan los estándares internacionales más reconocidos en materia de seguridad de la información, a su vez las normatividades y políticas que actualmente rigen en Colombia. También se incluyó una tabla comparativa que reúne los puntos más importantes de estos marcos, con el propósito de explicar de manera sencilla qué plantea cada estándar y también de qué manera aporta en el fortalecimiento de la seguridad y el funcionamiento confiable de las redes NGN.

Estándares Internacionales de Ciberseguridad

Las redes NGN, por su arquitectura y nivel de interconexión, presenta enfoques de seguridad que se deben gestionar en situaciones de riesgo. En este sentido, los estándares internacionales de ciberseguridad se convierten en referentes importantes, ya que reúnen prácticas que orientan en los procesos de protección de la información y la continuidad de los servicios. La aplicación de estos estándares en las organizaciones facilita el orden de los procesos

de seguridad, el tratamiento de las amenazas y la implementación de medidas que se trabajen con las necesidades reales de infraestructuras como las redes NGN.

ISO/IEC 27001:2022. Sistema de Gestión de Seguridad de la Información

Este estándar internacional se compone de cláusulas que permiten establecer los requisitos para un SGSI. En las que se incluyen la situación de la organización, el liderazgo y el compromiso de la alta dirección, junto con la planificación del SGSI basada en la gestión del riesgo, el soporte, es decir, los recursos, las competencias y la documentación, con la operación del sistema y la evaluación del desempeño con procesos de seguimiento, auditorías internas y revisión por la alta dirección y de mejora continua.

Se divide en 10 secciones cada una hace referencia a la sección Nro.01 alcance la cual define los límites de la aplicación del SGSI dentro de una organización, la sección Nro.02 explica las referencias normativas en las que se identifican los documentos indispensables para su correcta interpretación y la sección Nro.03 que trata sobre los términos y definiciones que se deben establecer en un lenguaje común con el fin de asegurar la comprensión del estándar. En la sección Nro.04 que trata sobre el contexto de la organización explica la identificación de variables internas y externas que influyen en la seguridad de la información.

La Sección Nro.5 explica el liderazgo y resalta la responsabilidad sobre la alta dirección en la asignación de roles, de políticas y de compromisos; junto con la Sección Nro.06 que trata sobre la planificación y se centra en la gestión del riesgo y en la definición de objetivos de seguridad en una organización. Por su parte, la Sección Nro.07 explica el apoyo que contempla los recursos, las competencias, la capacitación y el control documental necesarios para operar el SGSI.

La sección Nro.08 funcionamiento regula la ejecución de los procesos definidos; la Sección Nro.09 es la evaluación del rendimiento, la cual establece los diferentes procesos de seguimiento, de medición, de auditoría y de revisión por la dirección; y finalmente, la Sección Nro.10 mejora, promueve la corrección de desviaciones y el fortalecimiento continuo del sistema, asegurando su vigencia y efectividad en entornos tecnológicos como lo son las redes NGN.

La norma tiene como objetivo la implementación de sistemas de gestión de seguridad, el cual define un conjunto de requisitos que permiten identificar riesgos, definir controles, establecer políticas y evaluar continuamente el desempeño del sistema de gestión, así como definir diferentes controles, políticas y procedimientos acordes con las necesidades del entorno tecnológico en una organización (ISO/IEC., 2022).

Su importancia en las redes NGN es proporcionar una estructura ordenada que permita proteger la confidencialidad, la integridad y la disponibilidad de la información, independientemente de la tecnología utilizada, lo que promueve la adopción de controles actualizados y la mejora continua, con el fin de gestionar adecuadamente los diferentes incidentes, vulnerabilidades y requisitos regulatorios que afectan directamente a la operación segura de estas redes (CINTEL., 2020).

ISO/IEC 27002:2022. Controles de Seguridad

El estándar presenta una estructura organizada por dominios de control, agrupados en diferentes controles como lo son los controles organizacionales, los controles de personas, controles físicos, controles tecnológicos

Cada control incluye su propósito, directrices de implementación y de atributos que facilitan su clasificación y alineación con otros marcos de ciberseguridad y que permite aplicar los controles de manera confiable según el contexto tecnológico y los riesgos de la organización.

Cuenta con ocho (8) secciones que orientan en la selección y aplicación de controles de seguridad de la información, para la Sección Nro.01 Alcance, se define el objetivo del estándar como una guía para la implementación de controles de seguridad en distintos tipos de organizaciones. La Sección Nro.02 Referencias normativas identifica los documentos necesarios para su correcta aplicación, mientras que la Sección Nro.03 Términos, definiciones y abreviaturas establece un marco conceptual que facilita la interpretación del estándar, para la Sección Nro.04 estructura del documento explica la organización interna de la norma y la lógica de agrupación de los controles y atributos que permiten su comprensión con otros marcos y estándares de ciberseguridad.

A partir de la Sección Nro.05 controles organizacionales, se desarrollan los controles asociados a la gobernanza, las políticas de seguridad y la gestión del riesgo, en la sección Nro.06 controles de personas se analizan las responsabilidades, las competencias y la capacitación del personal; para la Sección Nro.07 controles físicos se presentan la protección de instalaciones, equipos y activos; y la Sección Nro.08 controles tecnológicos, reúne las medidas técnicas orientadas a la protección de sistemas, redes y servicios de información, las cuales son muy importantes en entornos como las redes NGN.

Mientras la ISO/IEC 27001 establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información o SGSI, la ISO/IEC 27002:2022 funciona como una guía práctica la cual describe cómo aplicar los controles de seguridad que fortalecen el sistema de gestión. Este estándar organiza los controles en diferentes categorías como lo son los

controles organizacionales, de personal, físicos, tecnológicos y operativos. Cada control cuenta con objetivos, lineamientos y recomendaciones para su implementación, facilitando la implementación a distintos entornos e industrias (ISO/IEC., 2022).

Para las redes NGN permite la gestión de accesos remotos, algo importante para la interconexión de varios servicios y plataformas, la seguridad en las operaciones, con sus correspondientes procedimientos de respaldo, la gestión de cambios y el manejo seguro de la información. Junto con la protección de las diferentes plataformas, lo cual es indispensable en infraestructuras que combinan servicios de voz, datos, movilidad y además virtualización (Ikusi. , 2022).

NIST Cybersecurity Framework. NIST CSF 2.0

Es el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología de los EE. UU, y es uno de los más trabajados desde la práctica, porque su estructura se organiza en cinco funciones que son el identificar, proteger, detectar, responder y recuperar, las cuales permiten analizar e implementar la gestión en seguridad como un proceso continuo. Cada función trabaja por medio de categorías y subcategorías que permiten la orientación en la implementación de los diferentes controles, la priorización de riesgos y la toma de decisiones en cualquier tipo de organización. Esto facilita que las empresas puedan evaluar su nivel de madurez, reconocer debilidades y planear mejoras de manera progresiva.(IBM., 2023).

Este marco no solo permite identificar y proteger los activos de una organización, sino también responder y recuperarse ante incidentes, asegurando la continuidad de los servicios. Su estructura con 5 secciones, la primera el Overview, el cual presenta los objetivos y el alcance de la NIST, explicando la necesidad de un enfoque de la gestión de riesgos en ciberseguridad, ya

que esto permite que las organizaciones puedan definir estrategias claras para proteger la información y garantizar la estabilidad operativa de redes como las NGN.

La segunda sección o introduction to the CSF Core, describe el núcleo del marco, organizado en cinco funciones como se describieron al principio el identificar, proteger, detectar, responder y recuperar. Cada función incluye categorías y subcategorías que orientan la implementación de controles específicos y que facilitan un enfoque frente a las diferentes amenazas que se puedan presentar. Para las redes NGN, esto asegura que la interconexión de servicios de voz, datos y video se mantenga confiable y segura.

La tercera sección o introduction to CSF Profiles and Tiers, explica los perfiles y niveles conocidos como tiers, los cuales permiten a las organizaciones evaluar su estado actual en temas de ciberseguridad, además definir metas de madurez y priorizar acciones frente a los riesgos. Para el caso de las redes NGN, esto contribuye a establecer un plan progresivo de mejoras, priorizando en los servicios y la complejidad de la infraestructura.

La cuarta sección o Introduction to Online Resources That Supplement the CSF, describe que el marco ofrece recursos en línea que facilitan la actualización continua, la integración con otros estándares y la capacitación del personal. Por lo que esto fortalece la capacidad de implementación de las organizaciones ante nuevas vulnerabilidades y tecnologías presentes en las redes NGN.

Por último, el Improving Cybersecurity Risk Communication and Integration, explica la importancia de implementar la ciberseguridad en los procesos organizacionales y mejorar la comunicación del riesgo entre áreas técnicas, operativas y directivas. En las redes NGN, donde la coordinación entre plataformas y servicios en parte es compleja, esta sección de la NIST permite

responder de manera más efectiva ante incidentes y mantener la continuidad de los servicios en una organización.

Para el caso de las redes NGN, permite la gestión de riesgos con la respuesta operativa ante los diferentes incidentes que se puedan presentar. Para el caso de la función Detectar, por ejemplo, ayuda a estructurar capacidades de monitoreo continuo en redes troncales o en plataformas de gestión. La función Responder aporta lineamientos para lograr establecer protocolos frente a incidentes como ataques DDoS, secuestro de rutas o de accesos indebidos. Finalmente, la función Recuperar es importante porque permite restablecer los servicios y minimizar en el impacto en los usuarios, lo cual es vital en redes que soportan servicios VoIP, movilidad y aplicaciones en la nube (NIST., 2024).

ISO/IEC 22301:2019. Sistemas de Gestión de Continuidad del Negocio

Se clasifica en cláusulas que están orientadas en la gestión de la continuidad del negocio, que comprenden la comprensión del contexto organizacional, el liderazgo y planificación de la continuidad, el análisis de impacto al negocio o BIA, la evaluación de riesgos, la definición de estrategias de continuidad, la implementación de planes de respuesta y recuperación y las pruebas, ejercicios y mejora continua.

Este estándar se compone de diez (10) cláusulas que trabajan los aspectos que son muy necesarios para la implementación de un SGCN exitoso, la cláusula Nro.01. Alcance el cual define los límites y aplicabilidad del sistema de continuidad, la cláusula Nro.02 referencias normativas que establece los documentos que respaldan la implementación, la cláusula Nro.03 términos y definiciones que aseguran un lenguaje común para la interpretación correcta del estándar, la Nro.04 contexto de la organización la cual identifica los diferentes factores internos y externos que pueden afectar la continuidad del negocio, la cláusula Nro.05 que es el liderazgo, en

donde se destaca la responsabilidad de la alta dirección y el compromiso con la adaptabilidad organizacional (ISO 22301., 2019).

La cláusula Nro.06 planificación, incluye el análisis de impacto al negocio o BIA con y la evaluación de riesgos, que son importantes para priorizar recursos y estrategias, la cláusula Nro.07 apoyo, la cual trabaja sobre los recursos, las competencias y la comunicación necesaria para sostener el SGCN. Junto con la cláusula Nro.08 operación, que define los procesos y procedimientos de respuesta, recuperación y mantenimiento de los servicios. La cláusula Nro.09 que es la evaluación del rendimiento, que permite monitorear, medir y auditar la efectividad del sistema de continuidad y finalmente la cláusula Nro.10 mejora la cual establece los mecanismos de revisión y actualización continua para adaptarse a cambios y nuevas amenazas.

Aunque no sea un estándar exclusivo en el tema de la ciberseguridad, su aplicación es muy importante en las redes NGN, puesto que establece un conjunto de requisitos para que las organizaciones puedan prepararse, responder y recuperarse frente a eventos complejos que puedan afectar en la operación. El objetivo de este estándar es el análisis de impacto al negocio, conocido como BIA, junto con la identificación de funciones principales, con la definición de estrategias de continuidad y la puesta en marcha de planes de recuperación. Con el fin de que una organización logre mantener sus servicios operativos incluso ante fallas tecnológicos, como desastres naturales, errores del personal o incidentes cibernéticos (ISO 22301., 2019).

Desde las redes NGN, la ISO 22301:2019 es importante debido a que estas redes trabajan con servicios que no pueden detenerse, como las comunicaciones corporativas, la interconexión de plataformas, los servicios móviles y aplicaciones que dependen del tiempo real. La norma orienta a prever escenarios como caídas de nodos troncales, interrupciones por ataques DDoS,

fallas masivas en centros de datos o afectaciones en la infraestructura de acceso (CINTEL., 2020).

ITU-T X.805. Arquitectura de Seguridad para Sistemas de Comunicaciones Extremo a Extremo

Identifica las diferentes amenazas para cada plano de la operación en la administración, el usuario y el control, a su vez propone mecanismos para mitigarlas, con el fin de garantizar que los servicios de voz, datos y multimedia funcionen sin interrupciones ni vulneraciones. Asimismo, establece los dominios de seguridad que deben protegerse como el acceso, el transporte, la operación, las aplicaciones y los usuarios, lo que facilita la segmentación de los riesgos y su vez la aplicación de controles según la complejidad de cada área (UIT-T., 2003).

Este estándar se compone de tres capas que son la capa de infraestructura de red la cual protege los elementos físicos y virtuales de la red, incluyendo servidores, nodos y enlaces de comunicación, tres planos y ocho dimensiones de seguridad, la capa de servicios que asegura que los servicios de voz, datos, video y aplicaciones operen de manera confiable y sin interrupciones; junto con la capa de funciones de usuario la cual protege las actividades y la información de los usuarios finales, garantizando privacidad y control de acceso.

Se compone además de tres planos que son el plano de usuario que está centrado en la interacción y los derechos de los usuarios dentro de la red, junto con el plano de control el cual asegura la gestión, la supervisión y la administración de la red de forma segura y el plano de gestión el cual analiza las operaciones administrativas, políticas y procedimientos para mantener la seguridad y continuidad de la red.

Y finalmente se compone de ocho dimensiones de seguridad las cuales incluyen la confidencialidad, la integridad, la disponibilidad, la autenticación, la autorización, no

repudiación, la privacidad y confidencialidad, los cuales abarcan todos los aspectos necesarios para proteger la información y las operaciones de la red de amenazas como la destrucción, la corrupción, la eliminación, la difusión y la interrupción (Estándar X.805., 2003).

Para el caso de las NGN, este estándar es muy importante, porque permite la orientación en la creación de arquitecturas de seguridad que sean capaces de resistir ataques dirigidos a diferentes puntos de la infraestructura (Montoya et al., 2020).

Esta define una arquitectura de seguridad que se compone de tres variables como son los planos de operación como el usuario, el control y la gestión, los dominios de seguridad como el acceso, el transporte, las aplicaciones, los usuarios, entre otros. Junto con los requisitos de seguridad como la confidencialidad, la autenticación, el control de acceso, la disponibilidad, etc. Además, permite analizar y proteger la seguridad de las comunicaciones de extremo a extremo, identificando amenazas y controles según el componente específico de la red (UIT-T., 2003).

Estándares Nacionales de Ciberseguridad

Para el caso a nivel nacional, la protección de la información y la gestión de riesgos cibernéticos se presentan como un conjunto de estándares, políticas y leyes que permiten orientar a las organizaciones para que logren implementar las buenas prácticas en seguridad. Los siguientes estándares nacionales permiten comprender el cómo establecer responsabilidades, además de promover la implementación de medidas organizacionales, y fortalecer las capacidades institucionales frente a las actuales amenazas digitales. Para el caso de las redes NGN, donde la interconexión y el manejo de grandes volúmenes de información aumentan la exposición a riesgos, la aplicación de estas normas permite asegurar no solo la confidencialidad, sino además la seguridad y la disponibilidad de los datos, con el fin de garantizar al mismo tiempo la continuidad y confiabilidad de los servicios.

Política Nacional de Seguridad Digital. CONPES 3995 de 2020

El CONPES se organiza de acuerdo con el diagnóstico del estado de la seguridad digital en el país con base a los principios, objetivos estratégicos, líneas de acción, actores responsables y procesos de implementación organizacional, a su vez orienta la formulación de planes, programas y acciones para fortalecer las capacidades nacionales frente a los riesgos digitales.

El CONPES 3995 del año 2020, establece los principios, objetivos y líneas de acción que orientan en el fortalecimiento de las capacidades institucionales frente a riesgos cibernéticos. Entre sus objetivos centrales, está el de promover la gestión del riesgo digital, además del desarrollo de una infraestructura segura, la implementación de buenas prácticas internacionales, junto con la creación de un trabajo colaborativo entre el sector público, privado y académico. También impulsa en la formación del talento humano especializado, reconociendo que la ciberseguridad requiere competencias avanzadas y actualización constante (DNP et al., 2020).

Esta política se compone de 5 secciones, en la primera se presentan los antecedentes y la justificación donde se puede identificar los problemas actuales en el país, por ejemplo, las debilidades en capacidades de seguridad digital tanto de ciudadanos como del sector público y privado, así como la necesidad de un marco de gobernanza actualizado, lo que permite analizar la política frente a las exigencias de un entorno tecnológico cada vez más complejo y conectado. Para la segunda sección explica el marco conceptual el cual establece los principios, definiciones y conceptos principales que orientan la política, asegurando que las acciones posteriores se fundamenten en un entendimiento común de los riesgos digitales y las estrategias de prevención.

La tercera sección es el diagnóstico, el cual analiza tres áreas en especial que son la falta de capacidades adecuadas en seguridad digital, la debilidad del marco de gobernanza y la necesidad de adoptar estándares y modelos internacionales aplicables a nuevas tecnologías, con

el fin de priorizar acciones y asignar recursos de manera óptima. La siguiente sección explica la definición de la política la cual presenta el objetivo general que busca consolidar la seguridad digital nacional y los objetivos específicos orientados a fortalecer las capacidades, actualizar la gobernanza y además promover la implementación de estándares y marcos de trabajo para analizar y trabajar en los diferentes desafíos de la Cuarta Revolución Industrial o 4RI. Para cada objetivo se complementa un plan de acción el cual debe describir las medidas concretas, responsables y plazos, asegurando que las estrategias sean ejecutables y medibles.

Por último, las secciones de seguimiento y financiamiento establecen mecanismos para evaluar el avance de la política, garantizar su sostenibilidad y coordinar la participación del sector público, privado y académico. En conjunto, esta política proporciona una guía para la implementación de medidas de seguridad digital, que fomenta en la confianza, la capacidad y la preparación del país frente a amenazas cibernéticas, especialmente para entornos tecnológicos como las redes NGN.

Para proyectos basados en tecnologías de redes NGN, esta política permite la orientación de la implementación de medidas organizacionales para garantizar la seguridad, la disponibilidad y la confidencialidad de los servicios. El CONPES también explica en la necesidad de fortalecer los procesos de monitoreo y de respuesta ante incidentes, lo cual es muy importante en entornos de redes NGN por su alto nivel de interconectividad. En este sentido, el CONPES 3995 de 2020 proporciona directrices para que las instituciones alineen sus planes, además de sus estrategias y procedimientos de seguridad con los objetivos nacionales de protección digital (MinTIC., 2020).

Decreto 1377 de 2013 y Ley 1581 de 2012. Sobre la Protección de Datos Personales

La Ley 1581 de 2012 se basa en la protección de datos personales en Colombia, la cual establece los principios, los derechos y las obligaciones que deben cumplir las organizaciones al

tratar información personal (CRC., 2012). Sin embargo, fue necesario contar con una norma que precisara cómo aplicar esos lineamientos a la práctica. Por lo cual se reglamenta el Decreto 1377 de 2013, el cual se basa en aspectos operativos como lo es la obtención de la autorización del titular, la implementación del aviso de privacidad, los procedimientos para el tratamiento de datos y las obligaciones asociadas a las políticas internas de protección de datos (CRC., 2013).

Su cumplimiento es especialmente importante en infraestructuras como las redes NGN, debido a los grandes volúmenes de información con los que se trabaja bajo esta red, por lo cual se exige que las organizaciones implementen medidas administrativas y jurídicas que permitan garantizar la privacidad, la seguridad y el tratamiento responsable de los datos (ITU-T, 2019).

El Decreto 1377 de 2013 complementa la ley mediante disposiciones operativas relacionadas con la autorización del titular, el aviso de privacidad, las políticas de tratamiento y los procedimientos para la gestión de datos personales.***Modelo de Seguridad y Privacidad de la Información, MSPI del MinTIC***

El MSPI del MinTIC se basa en componentes que trabajan con el gobierno de la seguridad de la información, la gestión de riesgos, la implementación de controles de seguridad, el monitoreo, evaluación y mejora continua. El cual establece lineamientos mínimos para que las entidades públicas gestionen la seguridad y privacidad de la información de forma sistemática

Es una guía desarrollada por el Ministerio de las TIC, con el fin de orientar a las entidades públicas en la implementación de controles de seguridad de la información. Este modelo implementa prácticas de la gestión como lo es la clasificación de activos, el análisis y el tratamiento del riesgo, la protección de infraestructura tecnológica, los controles de acceso y los diferentes procedimientos con el fin de garantizar la continuidad de los servicios. Además, establece los criterios mínimos para la implementación de políticas de seguridad, la definición de

funciones y roles, junto con la creación de procesos internos para el monitoreo y evaluación continua (MinTIC., 2021).

Se compone de cuatro (4) fases las cuales permiten a las a las entidades públicas gestionar la seguridad y la privacidad de la de acuerdo con la fase 1 planificación establece la situación organizacional, identifica necesidades y expectativas de los interesados, y define el alcance del modelo. Además, permite integrar el liderazgo, las políticas de seguridad, las funciones y las responsabilidades, junto con la identificación de activos y la valoración de riesgos, que permitan asegurar que la organización tenga claridad sobre qué proteger y cómo priorizar los esfuerzos de seguridad.

La fase Nro.02, permite la planificación en acciones concretas, es decir, mediante la implementación de controles, la ejecución del plan de tratamiento de riesgos y la definición de indicadores de gestión que permiten evaluar la efectividad de las medidas que sean implementadas. Esto garantiza que la seguridad de la información no sea solo teórica, sino aplicada a los procesos y servicios de la organización.

En la fase 3 que es la evaluación de desempeño, se realizan seguimientos, mediciones, auditorías internas y revisiones por la dirección de la organización, lo que proporciona una retroalimentación sobre la eficiencia de los controles y además permite identificar oportunidades de mejora continua.

Finalmente, para la fase Nro.04 que es el mejoramiento continuo se asegura que las organizaciones respondan de manera oportuna a incidentes, a no conformidades y a nuevas amenazas, que permitan fomentar en la adaptación de los procesos en seguridad y en la privacidad frente a los cambios tecnológicos y regulatorios.

Para el caso de las redes NGN, facilita la implementación de controles en este tipo de redes las cuales son altamente convergentes y distribuidas, a su vez asegura que la información y los servicios se mantengan protegidos frente a amenazas externas e internas. Por lo cual, el MSPI contribuye a que las entidades operen con criterios que garanticen un mayor nivel de seguridad en ciberseguridad (CINTEL., 2020).

Ley 1273 de 2009. Sobre los Delitos Informáticos

Esta ley permite la tipificación y sanción de los delitos cometidos contra la confidencialidad, seguridad y disponibilidad de los datos y sistemas informáticos. Entre las conductas penalizadas se encuentran el acceso abusivo a un sistema informático dado el artículo 269A, la obstaculización ilegítima de sistemas o redes en su artículo 269B, la interceptación de datos informáticos dado el art. 269C, el daño informático y alteración de datos en su artículo 269D y 269, el uso de software malicioso o destinado a vulnerar sistemas en el artículo 269F, la violación de datos personales en su artículo 269G, junto con la suplantación de sitios web para capturar datos dado el artículo 269H de esta misma ley. Esta ley a su vez protege los activos digitales tanto en el ámbito público como privado, y constituye un soporte jurídico muy importante frente al aumento de los delitos cibernéticos (CRC., 2009).

Desde el aspecto de las redes NGN, donde la infraestructura es más compleja, al estar distribuida y expuesta a diferentes vectores de ataque, esta ley permite que las organizaciones cuenten con un respaldo legal para denunciar y enfrentar incidentes que afecten la operación de sus servicios informáticos. Permitiendo que en las organizaciones se implementen medidas preventivas, como el monitoreo continuo, los controles de acceso, la segmentación de la red y los procesos de autenticación con el fin de minimizar el riesgo de que estas conductas afecten la seguridad del sistema (MinTIC et al., 2021).

Tabla Comparativa de los Principales Lineamientos Internacionales y Nacionales Investigados y Aplicables a la Ciberseguridad en Redes NGN

Con el propósito de facilitar la comprensión de los estándares internacionales y los marcos normativos nacionales analizados en el numeral 3.2, a continuación, se presenta una tabla comparativa que analiza los principales lineamientos aplicables a la ciberseguridad en redes NGN. La cual permite identificar el enfoque de cada norma y marco de referencia, además de su alcance y de su aporte específico frente a la protección de la información y la continuidad de los servicios en entornos de redes NGN.

Asimismo, la comparación permite evidenciar cómo estos instrumentos se complementan entre sí, lo que permite orientar a las organizaciones en la implementación de buenas prácticas y en el fortalecimiento de sus estrategias de ciberseguridad.

Tabla 2

Comparación de Estándares y Marcos Legales Vigentes Investigados

Estándar o normatividad	Objeto de regulación o estandarización	Principales lineamientos	Aportes a la seguridad en redes NGN
ISO/IEC 27001:2022	Sistema de Gestión de Seguridad de la Información-SGSI	Implementación de políticas, análisis de riesgos, controles, auditorías y mejora continua	Garantiza la protección de la confidencialidad, seguridad y disponibilidad de la información manejada en infraestructuras unificadas con las de NGN
ISO/IEC 27002:2022	Controles de seguridad	Controles organizacionales, además de tecnológicos, físicos y operativos;	Permite implementar controles clave como son los accesos remotos, la seguridad operativa, el

Estándar o normatividad	Objeto de regulación o estandarización	Principales lineamientos	Aportes a la seguridad en redes NGN
		análisis de los diferentes lineamientos para su aplicación	respaldo, la gestión de cambios y la protección de plataformas en NGN
NIST Cybersecurity Framework, CSF	Marco de gestión de la ciberseguridad	Entre sus funciones está el identificar, proteger, detectar, responder y recuperar; categorías y subcategorías para mejorar en los procesos de ciberseguridad	Facilita el monitoreo continuo, la respuesta a incidentes que se puedan presentar y a la recuperación ante fallas o ataques como lo son DDoS o intrusiones en redes NGN
ISO/IEC 22301:2019	Sistema de Gestión de Continuidad del Negocio	Permite el análisis de impacto o BIA, junto con las diferentes estrategias de continuidad y planes de recuperación	Garantiza la operación continua de servicios en redes NGN como lo son voz, datos, movilidad e interconexión de plataformas
ITU-T X.805	Arquitectura de seguridad extremo a extremo	Dominios de seguridad, amenazas por plano es decir usuario, control, administración y procesos de mitigación	Segmenta riesgos y define controles por áreas, reforzando la protección de servicios convergentes en NGN
CONPES 3995 de 2020	Política Nacional de Seguridad Digital	Se gestiona el riesgo digital, además de la infraestructura segura, el talento humano e infraestructura multiservicio	Permite trabajar con proyectos como el de redes NGN y las diferentes directrices nacionales de seguridad digital, con el fin de fortalecer en el monitoreo y la respuesta

Estándar o normatividad	Objeto de regulación o estandarización	Principales lineamientos	Aportes a la seguridad en redes NGN
Ley 1581 de 2012 y Decreto 1377 de 2013	Sobre la protección de los datos personales	Principios de tratamiento de datos personales, derechos del titular, avisos de privacidad, autorización y políticas internas	Exige el tratamiento adecuado, seguro y responsable de los datos que circulan por las redes NGN, donde por lo general se manejan grandes volúmenes de información sensible
Modelo de Seguridad y Privacidad de la información MSPI MinTIC	Lineamientos de la seguridad y privacidad de la información para entidades públicas	Clasifica activos, análisis y tratamiento del riesgo, controles de acceso, continuidad y monitoreo	Aporta controles con el fin de asegurar la información y las diferentes plataformas distribuidas en las redes NGN
Ley 1273 de 2009	Sobre los delitos informáticos	Tipificación como el acceso abusivo, la interceptación, el daño informático, el malware y la violación de datos junto con la suplantación	Brinda un soporte jurídico ante los diferentes ataques a redes NGN y promueve medidas preventivas como lo son el monitoreo, la segmentación y la autenticación

Nota. Se presentan las correspondientes y diferentes estándares nacionales e internacionales dado los aportes que brindan en la seguridad de las redes NGN

Estrategias para Fortalecer la Ciberseguridad en Redes NGN en el Ámbito Organizacional

Las buenas prácticas en ciberseguridad son el conjunto de principios, procedimientos, controles y lineamientos que permiten proteger los activos de la información frente a amenazas internas y externas en una organización (MinTIC., 2021). Estas prácticas trabajan bajo los estándares internacionales sustentados en el capítulo anterior, junto con los marcos normativos, el análisis de riesgos que orientan de manera segura y consistente el operar sistemas tecnológicos dentro de una organización.

Para el caso de las redes Next Generation Networks, consideradas infraestructuras tecnológicamente avanzadas y de alta demanda, las buenas prácticas se vuelven indispensables. Porque su importancia radica en que estas redes integran varios servicios como VoIP, datos, aplicaciones en la nube y movilidad frente a plataformas distribuidas que requieren un alto nivel de disponibilidad y además de seguridad. El implementar buenas prácticas permite establecer controles, promover la gestión de los riesgos, garantizar la protección de los datos y reducir vulnerabilidades asociadas a la interconexión funcional de múltiples componentes tecnológicos. (Almanza, 2024).

Las estrategias que hacen parte de las buenas prácticas incluyen la gestión del riesgo tecnológico, la implementación de controles de seguridad basados en normas internacionales, el monitoreo continuo de actividad y detección temprana de incidentes, la gestión segura de identidades, accesos y privilegios, la protección de datos personales y sensibles, la respuesta ante incidentes y continuidad del negocio, la capacitación permanente del talento humano junto con la evaluación constante de vulnerabilidades.

Con el fin de cumplir con el último objetivo específico, en este capítulo se plantean diferentes estrategias desde el ámbito organizacional, que se recomienda tener en cuenta.

Estrategia Nro.01. Implementar un Sistema de Gestión de Seguridad de la Información o SGSI Basado en la ISO/IEC 27001:2022

Esta estrategia permite integrar la seguridad de la información dentro de los procesos internos, permitiendo que la protección de los activos de información sea gestionada de manera formal, documentada y acorde con los objetivos de una organización.

Al implementar este SGSI, se pueden identificar riesgos, a la vez de definir controles, evaluar amenazas y mejorar continuamente en cada uno de los procesos de una organización. Implementando a su vez políticas institucionales de seguridad, con el fin de clasificar los activos asociados a las redes NGN, implementar controles específicos con base al Anexo A de la ISO/IEC 27001.

Ello garantizará una gestión de los riesgos, controlando de forma ordenada los procesos asociados a plataformas que trabajan con redes NGN.

Estrategia Nro.02. Fortalecer la Gestión del Riesgo en Infraestructuras de Redes NGN

Esta estrategia permite identificar y reconocer los diferentes riesgos que afectan a las redes NGN, considerando su complejidad y el nivel de interconexión, con el propósito de anticipar escenarios que puedan comprometer la operación de los servicios en una organización.

Puesto que la gestión del riesgo es un proceso que permite garantizar que las redes NGN operen de manera segura y confiable. Ya que no se trata únicamente de identificar problemas, sino de comprender cómo estos pueden afectar la disponibilidad, la seguridad y la confidencialidad de los servicios, a su vez de anticipar escenarios que podrían comprometer la operación de la infraestructura tecnológica. Porque fortalecer la gestión del riesgo implica

además establecer un proceso que permita a las organizaciones reconocer las amenazas y a su vez las vulnerabilidades de manera temprana, evaluando la probabilidad y el impacto. Con las cuales se puedan diseñar medidas efectivas para disminuirlas.

Para el caso de las redes NGN, la complejidad y la interconexión de varios servicios, como los de VoIP, datos móviles, aplicaciones en la nube y plataformas virtualizadas, hacen que cada fallo pueda tener consecuencias si no se gestionan de manera adecuada. Y este proceso se inicia creando un inventario de activos actualizado, donde se deben incluir tanto el hardware, como el software, además de servicios y flujos de datos. Con la identificación anticipada de vulnerabilidades, es posible asegurar la continuidad y la disponibilidad de los servicios asociados a redes NGN.

Esto con el fin de aplicar metodologías de análisis y valoración de riesgos con base a la ISO 27005, MAGERIT o NIST, de priorizar amenazas que estén relacionadas con servicios y fallas de señalización, riesgos asociados a la cadena de suministro digital e interconexión funcional con terceros por ejemplo Roaming, con vulnerabilidades en VoIP, ataques DDoS y fallas en routers.

Lo que permitiría a la organización prepararse, reaccionar y recuperarse frente a cualquier tipo de incidente, además el implementar este tipo de gestión en redes NGN contribuye a generar confianza en los servicios ofrecidos, en reducir la probabilidad de interrupciones críticas y a su vez en garantizar que la operación tecnológica se mantenga alerta frente a las diferentes amenazas que cada vez son más sofisticadas. Por último, el fortalecer la gestión del riesgo no solo protege la infraestructura y los datos, sino que también asegura la continuidad de los servicios y la confianza de los usuarios y los stakeholders es decir los empleados, los clientes, proveedores, accionistas y todo lo que corresponde y hace parte de una organización.

Estrategia Nro.03. Implementación de Controles Especializados para Redes NGN

Esta estrategia busca adaptar las medidas de seguridad a las características propias de las redes NGN, con el fin de asegurar que la protección de los servicios y la infraestructura responda a la forma en que estas redes operan y se relacionan.

Es importante explicar que los controles de seguridad son medidas que se implementan para proteger los activos de información, con el fin de garantizar la continuidad de los servicios y su vez de minimizar la exposición a riesgos y amenazas. Estos se constituyen de varios tipos como los controles preventivos, los cuales buscan evitar que ocurra un incidente, como la autenticación, segmentación de red o cifrado de datos. Los controles detectivos, que como su nombre lo indica, identifican y alertan sobre incidentes, como sistemas de monitoreo, IDS/IPS o auditorías (Berti., 2025).

Además de los controles correctivos, es decir, que permiten controlar el impacto de un incidente, por ejemplo, procedimientos de recuperación, restauración de datos y aplicación de parches. Los anteriores controles están diseñados específicamente para responder a la complejidad, a la interconexión y a los servicios únicos de estas infraestructuras que permiten segmentar la red por niveles de acceso, de distribución y de núcleo, esto recordemos según los principios de la ITU-T X.805, con el fin de fortalecer el control de acceso de plataformas de señalización SIP, IMS y VoIP.

Esta estrategia permitiría implementar procesos avanzados como firewalls de aplicación, IDS/IPS, la autenticación y el cifrado de extremo a extremo. aplicando parches y actualizaciones de manera controlada. Lo que permitiría la reducción directa de riesgos de intrusión, de fraude, de manipulación de tráfico y de ataques frente a la denegación de servicio.

Estrategia Nro.04. Gestión de Incidentes y Respuesta Rápida

Esta estrategia de gestión es el conjunto de procedimientos y acciones que son coordinadas en una organización con el fin de identificar, analizar y responder a eventos de seguridad, esto con el fin de minimizar su impacto sobre los servicios, los usuarios y la infraestructura tecnológica. En el caso de las redes NGN, donde los servicios de voz, datos, aplicaciones en la nube y movilidad se encuentran interconectados, la capacidad de reacción rápida es muy importante con el fin de mantener la continuidad operativa y la confianza de los usuarios.

También esta estrategia permitiría estructurar un proceso que permita detectar incidentes de manera temprana, para responder de manera oportuna y además de recuperar los servicios afectados. Esta implementación es posible implementarla por medio del NIST Cybersecurity Framework CSF, utilizando sus funciones de Detect, Respond y Recover. Y esto implica definir las diferentes rutas de escalamiento, matriz de responsabilidad en el caso del personal y las áreas que hagan parte de la organización, junto con los tiempos máximos de respuesta y los diferentes protocolos de comunicación interna.

Además, la coordinación con entidades externas como el CSIRT Colombia permitiría a las empresas estar atentos frente a la respuesta ante amenazas complejas o de alcance nacional, lo que permitiría garantizar la rápida contención de los incidentes que podrían comprometer la infraestructura de las redes NGN, la estrategia incluye simulacros de ciberataques, que permitirían evaluar la efectividad de los procesos establecidos, además de identificar puntos débiles y capacitar al personal para que actúe con rapidez y precisión.

Esto aseguraría que, frente a eventos como ataques DDoS, intentos de acceso no autorizado o fallas en las plataformas de señalización, la organización pueda lograr reducir los

tiempos de inactividad, controlar los daños y restaurar los servicios de manera controlada, fortaleciendo la capacidad y la seguridad de la red.

Estrategia Nro.05. Desarrollar un Plan de Continuidad y Recuperación ante Desastres

Es un conjunto basado en políticas, procedimientos y acciones que permiten a una organización mantener o restaurar sus operaciones ante eventos inesperados, ya sean fallas tecnológicas, desastres naturales, ataques cibernéticos o errores del personal. Su propósito es garantizar que los servicios principales no se vean interrumpidos y que la organización pueda recuperarse de manera ordenada y controlada, minimizando pérdidas económicas, de información y de confianza (MinTIC., 2021).

Además de la mano del Sistema de Gestión de Continuidad del Negocio como lo es la ISO 22301:2019, que permita desarrollar un Análisis de Impacto al Negocio, conocido como BIA específico para servicios en redes NGN. A su vez, diseñar planes de contingencia para caídas de nodos troncales, la interrupción del transporte o fallas en la interconexión funcional, con ataques DDoS. En el cual se logren realizar pruebas mensuales de recuperación. Esto garantizaría la operación ininterrumpida de servicios corporativos y comunicaciones de una organización.

Además, un plan de continuidad exitoso incluye la definición de roles y a su vez de responsabilidades, procedimientos de recuperación escalonados, rutas de comunicación durante incidentes y a su vez la realización de pruebas mensuales de recuperación, que permiten validar su eficacia y ajustar los procesos según las lecciones aprendidas. Con la realización de simulacros y ejercicios se fortalecería la capacidad de respuesta del personal y se aseguraría que las plataformas puedan restablecerse rápidamente sin afectar a los usuarios finales.

Estrategia Nro.06. Cultura Organizacional y Capacitación Continua al Talento Humano de la Organización

El diseño e implementación de programas de formación en ciberseguridad para todo el personal, junto con la capacitación específica para los ingenieros y administradores de las redes NGN. Con el desarrollo de campañas de concientización sobre phishing, ingeniería social y manejo seguro de la información. Con el fin de que se presente una disminución de errores humanos, el cual es uno de los principales factores de ataque en plataformas NGN implementadas.

Tener una capacitación continua al talento humano, donde se reconoce el objetivo del talento humano en cuanto a la seguridad de las redes NGN, promoviendo una cultura organizacional que debe estar orientada a la prevención, el uso responsable de la información y la adopción de buenas prácticas.

Estrategia Nro.07. Asegurar el Cumplimiento de la Ciberseguridad en las Organizaciones

Esta estrategia busca garantizar que todas las acciones relacionadas con la seguridad de la información en redes NGN se desarrollen con base al marco legal, normativo y de buenas prácticas vigentes, presentadas en este trabajo dado el capítulo 3 (véase lista de tablas: Tabla 2. Comparación de estándares y marcos legales vigentes investigados), esto con el fin de que se pueda fortalecer la responsabilidad institucional y generando confianza en los usuarios. Por ejemplo, para aplicar y demostrar el cumplimiento de la Ley 1581 de 2012. Protección de Datos Personales, en la gestión de servicios de redes NGN, e implementar los lineamientos de ciberseguridad emitidos por el MinTIC y su MSPI. Con el fin de establecer protocolos que aseguren el reporte oportuno de incidentes al CSIRT y a las autoridades competentes, cumpliendo con los requerimientos legales vigentes.

Junto con la Ley 1273 de 2009 sobre delitos informáticos, la cual establece los delitos relacionados con accesos no autorizados, manipulación de datos, ataques frente a la denegación de servicio y otras conductas que vulneran la seguridad de la información. Su inclusión frente a esta estrategia permitiría que la organización contemple acciones preventivas y correctivas frente a los diferentes incidentes que puedan constituirse como delitos cibernéticos, garantizando un respaldo legal y además la capacidad de respuesta ante situaciones de ciberseguridad.

Además del CONPES 3995 de 2020, el cual define la Política Nacional de Seguridad Digital, y que como se explicó en el numeral 3.2.1 del capítulo 3, proporciona una guía de directrices estratégicas con el fin de fortalecer las capacidades de la organización frente a los riesgos digitales, con el fin de que se logre la coordinación entre el sector público, privado y el académico. Porque el implementar este marco en la presente estrategia aseguraría que las acciones de la organización estuviesen alineadas con los objetivos nacionales de protección digital, promoviendo la colaboración y el cumplimiento de estándares de seguridad que son reconocidos a nivel nacional.

A su vez trabajar con los estándares internacionales como la ISO/IEC 27001:2022 para la implementación de Sistemas de Gestión de Seguridad de la Información o SGSI les permitiría que el cumplimiento normativo no se presente solo como aspectos legales, sino que se trabaje en procesos organizados, documentados y sujetos a mejoras continuas, que fortalezcan la gestión de riesgos, controles y auditorías internas. Y de manera complementaria, trabajando con la ISO/IEC 22301:2019, donde su objetivo es la continuidad del negocio, con el fin de asegurar que las medidas legales y de seguridad se logren integrar en los procesos de seguridad y de recuperación ante desastres para el funcionamiento de las redes NGN.

Finalmente, los lineamientos del Modelo de Seguridad y Privacidad de la Información conocido como MSPI del MinTIC establecen criterios muy importantes de implementación como lo son controles de monitoreo y de reporte de incidentes, esto con el fin de garantizar que la organización pueda demostrar de manera tangible el cumplimiento de la normativa y de las buenas prácticas de ciberseguridad, lo que permitiría contribuir en la protección de la información, la continuidad de los servicios y muy importante de la confianza organizacional es decir, la percepción con la cual la empresa gestionará la información de manera segura, responsable y transparente, de manera que los usuarios, los clientes y socios confíen en que los servicios, datos y procesos no serán vulnerados ni manipulados.

En términos de ciberseguridad, implica que la entidad ha implementado controles, protocolos, políticas y procedimientos confiables, que cumplen con la normatividad vigente y con las buenas prácticas, y que además podrá responder de manera eficiente a los incidentes para mantener la continuidad de los servicios. En una red NGN, esto es importante porque los usuarios confían en que sus comunicaciones, datos y servicios digitales funcionen de manera segura, continua y protegida frente a amenazas internas o externas. Por ello, la confianza organizacional no es solo reputación, sino además una garantía de que la seguridad de la información está resguardada y respaldada de manera óptima en la operación cotidiana de la organización.

Conclusiones

Las redes NGN presentan complejidad y un nivel de interconexión que las hace vulnerables frente amenazas como ataques DDoS, spoofing, sniffing, vulnerabilidades en protocolos y además de fallos de gobernanza organizacional. Este trabajo monográfico permitió investigar, analizar y verificar que estas amenazas no solo comprometen la disponibilidad y continuidad de los servicios, sino que también impactan directamente en la confianza de los usuarios y en la operación exitosa de las organizaciones. Donde el reconocer estos riesgos constituye un primer paso y muy importante para que las organizaciones implementen medidas de protección efectivas y además estratégicas.

Los estándares internacionales como la ISO/IEC 27001, 27002, 22301, la NIST CSF, ITU-T X.805 y los marcos nacionales como el CONPES 3995, la Ley 1581, el MSPI se presentan como referentes muy importantes que permiten guiar en cuanto a la protección de la información en entornos de redes NGN. Además de que su implementación en una organización permitiría establecer procesos formales de gestión de seguridad, a su vez en definir controles como los presentados en el capítulo Nro.04 en la estrategia Nro.05, con el fin de garantizar el cumplimiento normativo y estructurar la gestión de riesgos. El trabajar en conjunto con las buenas prácticas internacionales y con la normatividad nacional, fortalecerían en cada uno de los procesos de la organización y su vez asegurarían la operación de los servicios.

Además, la implementación de estrategias, como los SGSI, los controles, la gestión de incidentes, los planes de continuidad y recuperación, con la estrategia de formación continua del talento humano, permitirían que las organizaciones puedan anticipar y controlar estos riesgos, reduciendo la probabilidad de interrupciones y de pérdidas de información. Estas acciones no

solo fortalecerían la protección tecnológica, sino que también consolidarían una cultura de seguridad orientada en la prevención y en la responsabilidad de las organizaciones.

Por último, el fortalecimiento de la ciberseguridad en redes NGN influyen directamente en la confianza organizacional, entendida como la certeza de los usuarios y de los actores internos descritos en el capítulo Nro.04, sobre la capacidad de las organizaciones para que logren proteger sus activos, además de garantizar la continuidad de los servicios y de cumplir con las obligaciones legales. Una gestión de la seguridad que se trabaje de manera coherente y transparente generaría además de la credibilidad, la reducción de riesgos frente a errores que se puedan cometer por parte del personal y su vez mejoraría en los procesos de seguridad ante los clientes, los colaboradores y los socios estratégicos de las organizaciones.

Recomendaciones

Es importante que en las organizaciones se cuente con un inventario detallado de los diferentes activos, además de que se identifiquen vulnerabilidades y prioricen amenazas, con el objetivo de integrar los estándares presentados y explicados en este trabajo; como lo son la ISO 27005, MAGERIT o NIST. Esto permitirá una gestión óptima frente a los riesgos en las redes NGN.

Se sugiere además coordinar estos estándares internacionales y marcos legales vigentes nacionales, con el fin de que se implementen los controles a las características propias en las redes NGN como lo son la segmentación de la red, la autenticación, el cifrado y los diferentes procesos de monitoreo continuo, los cuales deben ser parte de un sistema de seguridad formal y actualizado.

También es muy importante diseñar y probar de manera semanal o mensual planes de contingencia y de recuperación ante amenazas y desastres, esto con el fin de asegurar que los servicios de la organización se mantengan operativos incluso ante las fallas, ataques cibernéticos o interrupciones externas que se puedan presentar. Por esta razón se recomienda implementar programas de formación para todo el personal, que estén enfocados en comprender y saber sobre los riesgos, prácticas de seguridad y protocolos internos, esto porque una cultura organizacional responsable fortalecería la prevención de los incidentes y la responsabilidad compartida en la protección de la información.

Referencias Bibliográficas

Almanza. (2024). *El problema de la ciberseguridad, parece ser resolver problemas.* Obtenido de Linkedin: https://es.linkedin.com/pulse/el-problema-de-la-ciberseguridad-parece-ser-resolver-almanza-junco-vp1be?trk=public_post

Alnaim. (2024). *Securing 5G virtual networks: a critical analysis of SDN, NFV, and.* Obtenido de Department of Management Information Systems, School of: https://link.springer.com/article/10.1007/s10207-024-00900-5

Alnaim. (2024). *Securing 5G virtual networks: a critical analysis of SDN, NFV, and network slicing security.* Obtenido de International Journal of Information Security: https://link.springer.com/article/10.1007/s10207-024-00900-5

Anías et al. . (2021). *Amenazas y defensas de seguridad en las redes de próxima generación.* Obtenido de Politécnico José Antonio Echeverría: https://www.researchgate.net/publication/320715817_Amenazas_y_defensas_de_seguridad_en_las_redes_de_proxima_generacion

Aslan et al. . (2023). *A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions.* Obtenido de https://www.mdpi.com/2079-9292/12/6/1333

Carreño. (2024). *Cybersecurity model for the protection of critical information at Colombian.* Obtenido de Revista Ciberespacio, Tecnología e Innovación: https://share.google/j8ZDmuaLgnBsSnhNE

Casquero et al. . (2020). *Descubriendo los desafíos técnicos para la seguridad en las redes 5G.* Obtenido de https://www.realinstitutoelcano.org/analisis/descubriendo-los-desafios-tecnicos-para-la-seguridad-en-las-redes-

5g/#:~:text=Network%20slicing%20El%20network%20slicing%20('segmentaci%C3%B3n%20de,cubrir%20las%20necesidades%20individuales%20de%20cada%20client

CINTEL. (2020). *NGN, Competitividad y Desarrollo Social.* Obtenido de RCT. Revista Colombiana de Telecomunicaciones: https://cintel.co/wp-content/uploads/2013/05/RCT_56.pdf

CISA. (2024). *ENFOQUES MODERNOS PARA LA SEGURIDAD DEL ACCESO A LA RED.* Obtenido de Agencia de Ciberseguridad y Seguridad de la Infraestructura : https://www.cisa.gov/sites/default/files/2024-10/joint-guide-modern-approaches-to-secure-network-access-security-508c_ES.pdf

CloudFlare. (2025). *¿Qué es IPsec? | Cómo funcionan las VPN IPsec.* Obtenido de https://www.cloudflare.com/es-es/learning/network-layer/what-is-ipsec/

CloudFlare. (2025). *¿Qué es el secuestro de BGP?* Obtenido de https://www.cloudflare.com/es-es/learning/security/glossary/bgp-hijacking/

Coker. (2025). *95% of Data Breaches Tied to Human Error in 2024.* Obtenido de Reed Exhibitions Ltd: https://www.infosecurity-magazine.com/news/data-breaches-human-error/#:~:text=Human%20error%20contributed%20to%2095,accounting%20for%2080%25%20of%20incidents.

CONPES. (2023). *CONPES 3995.* Obtenido de Política Nacional de Confianza y Seguridad digital: https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

CRC. (2009). *Congreso de la República de Colombia* . Obtenido de Ley 1273: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

CRC. (2012). *Congreso de la República de Colombia.* Obtenido de Ley 1581: https://www.google.com/search?q=la+Ley+1581+de+2012%2C+que+regula+la+protecci%C3%B3n+de+datos+personales%3B&oq=la+Ley+1581+de+2012%2C+que+regula+la+protecci%C3%B3n+de+datos+personales%3B&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzIyN2owajSoAgCwAgA&sourceid=chrome&

CRC. (2009). *Ley 1273.* Obtenido de Congreso de la República de Colombia: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

CRC. (2012). *Ley 1581.* Obtenido de Congreso de la República: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CRC. (2013). *Decreto 1377.* Obtenido de Congreso de la República de Colombia: http://funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Cremades et al. . (2024). *Revisión del estado actual de la ciberseguridad en ColombiaReview of the Current State of Cybersecurity in Colombia.* Obtenido de Revista Estudios en Seguridad y Defensa: https://www.researchgate.net/publication/389412235_Revision_del_estado_actual_de_la_ciberseguridad_en_ColombiaReview_of_the_Current_State_of_Cybersecurity_in_Colombia

Cyberark. (2025). *2025 Identity Security Landscape.* Obtenido de https://www.cyberark.com/threat-landscape/?utm_source=google&utm_medium=paid_search&utm_term=threat_landscape_report_nam_spanish_mx_cr_co&utm_content=threat_landscape_report&utm_campaign=identity_security&gclid=CjwKCAjwg7PDBhBxEiwAf1CVuxRkWjhEkZ1ES6O0Lnyq

Damir et al. . (2022). *A Beyond-5G Authentication and Key Agreement Protocol.* Obtenido de Cornell University: https://doi.org/10.1007/978-3-031-23020-2_14

D'Andrea et al. . (2024). *Cómo garantizar la integridad de los datos.* Obtenido de Keeper: https://www.keepersecurity.com/blog/es/2024/09/30/how-to-ensure-data-integrity/#:~:text=Es%20posible%20garantizar%20la%20integridad,adoptando%20controles%20de%20acceso%20estrictos.

De los Llanos. (2024). *Packet Injection: Entendiendo la Amenaza.* Obtenido de Minery Report: https://mineryreport.com/blog/packet-injection-entendiendo-la-amenaza/

DNP et al. (2020). *Documento CONPES* . Obtenido de POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL : https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

Farris et al. (2019). *A survey on emerging SDN and NFV security mechanisms for IoT systems.* Obtenido de Sejong University: https://www.researchgate.net/publication/326758128_A_survey_on_emerging_SDN_and_NFV_security_mechanisms_for_IoT_systems

FORTINET. (2024). *¿Qué es el marco MITRE ATT&CK ?* Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/mitre-attck

FORTINET. (2024). *Tipos de ciberataques: ataque DDoS, ransomware y más.* Obtenido de http://fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks

FORTINET. (2025). *Vulnerabilidades de seguridad de red.* Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/network-security-vulnerability

García . (2020). *Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo.* Obtenido de Universidad Piloto de Colombia:

https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9545/Ciberseguridad%20en%20las%20organizaciones%2C%20el%20personal.pdf?sequence=1&isAllowed=y

Ghafoor et al. . (2022). *Implications of Network Security in 5G Network and Detection of Cyber Attacks.* Obtenido de University of the Punjab: https://www.researchgate.net/publication/368416756_Implications_of_Network_Security_in_5G_Network_and_Detection_of_Cyber_Attacks

Grajales et al. . (2025). *Colombia tiene una ciberseguridad y ciberdefensa estatal vulnerables ante los ataques.* Obtenido de Periódico UNAL: https://periodico.unal.edu.co/articulos/colombia-tiene-una-ciberseguridad-y-ciberdefensa-estatal-vulnerables-ante-los-ataques

Gunawardena et al. . (2023). *Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Galle 80000, Sri Lanka.* Obtenido de https://doi.org/10.3390/telecom4030025

Holtrup et al. . (2021). *5G System Security Analysis.* Obtenido de Cornell University: https://doi.org/10.48550/arXiv.2108.08700

IBM. (2023). *¿Qué es el Marco de Ciberseguridad del NIST?* Obtenido de https://www.ibm.com/es-es/think/topics/nist

Ikusi. . (2022). *Redes de nueva generación: El camino hacia la conectividad del futuro.* Obtenido de https://www.ikusi.com/mx/blog/redes-de-nueva-generacion-el-camino-hacia-la-conectividad-del-futuro/

Interact. (2025). *Falta de gobernanza y los riesgos que amenazan la sostenibilidad del negocio.* Obtenido de https://www.interactsolutions.com/es/falta-de-gobernanza-y-los-riesgos-que-amenazan-la-sostenibilidad-del-negocio/

ISO. (2022). *ISO/IEC 27001:2022.* Obtenido de ISO: https://www.iso.org/es/norma/27001

ISO 22301. (2019). *Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos.* Obtenido de http://iso.org/standard/75106.html

ISO/IEC. (2022). *27002:2022.* Obtenido de https://www.iso.org/es/contents/data/standard/07/56/75652.html

ISO/IEC. (2022). *ISO/IEC 27001:2022.* Obtenido de Information security, cybersecurity and privacy protection — Information security management systems — Requirements: https://www.iso.org/es/norma/27001

ITU. (2003). *X.805.* Obtenido de https://www.itu.int/rec/T-REC-X.805-200310-I/en

ITU-T. (2019). *La seguridad de las telecomunicaciones y las tecnologías de la información.* Obtenido de Sector de Normalización de las Telecomunicaciones de la UIT: https://www.itu.int/dms_pub/itu-t/opb/hdb/t-hdb-sec.03-2006-pdf-s.pdf

Janani. (2025). *The Human-Machine Identity Blur: A Unified Framework for Cybersecurity Risk Management in 2025.* Obtenido de https://arxiv.org/abs/2503.18255

Kaspersky. (2024). *Tipos de suplantación de IP.* Obtenido de https://latam.kaspersky.com/resource-center/threats/ip-spoofing

Kaspersky Lab. (2025). *¿Qué es la suplantación? Definición y explicación.* Obtenido de https://latam.kaspersky.com/resource-center/definitions/spoofing

Kiasari. (2024). *A comprehensive review of the current state of smart grid technologies for renewable energy integration and future trends: The role of machine learning and energy storage systems.* Obtenido de Dalhousie University , Canada: https://www.virtualpro.co/articulos/revisi-n-exhaustiva-del-estado-actual-de-las-tecnolog-

as-de-redes-inteligentes-para-la-integraci-n-de-energ-as-renovables-y-tendencias-futuras-el-papel-del-aprendizaje-autom-tico-y-los-sistemas-de-almacenamiento-de-ener

Kuzankah et al. . (2024). *ISO 27001 IN BANKING: AN EVALUATION OF ITS IMPLEMENTATION AND EFFECTIVENESS IN ENHANCING INFORMATION SECURITY.* Obtenido de https://www.researchgate.net/publication/377420098_ISO_27001_IN_BANKING_AN_EVALUATION_OF_ITS_IMPLEMENTATION_AND_EFFECTIVENESS_IN_ENHANCING_INFORMATION_SECURITY

Lindemulder et al. . (2024). *¿Qué es la ciberseguridad?* Obtenido de IBM: https://www.ibm.com/es-es/topics/cybersecurity

Mehrab. (2025). *Network Security in 5G -Threats, Vulnerabilities, and Mitigation Strategies.* Obtenido de International Technological University: https://www.researchgate.net/publication/391343907_Network_Security_in_5G_-Threats_Vulnerabilities_and_Mitigation_Strategies

Merchán . (2024). *Desafíos y vulnerabilidades asociados con la seguridad informática en las redes de generación (NGN) móviles 5G.* Obtenido de UNAD: https://repository.unad.edu.co/jspui/bitstream/10596/63765/1/jamerchanc.pdf

MINTIC. (2022). *MINTIC Colombia* . Obtenido de Conceptos clave Seguridad de la Información - Gobierno digital: https://gobiernodigital.mintic.gov.co/692/articles-272875_Conceptos_clave_Seguridad.docx

MinTIC et al. (2021). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.* Obtenido de https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

MinTIC. (2020). *Política de Seguridad Digital.* Obtenido de https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital

MinTIC. (2021). *¿Qué es el MSPI?* Obtenido de Modelo de Seguridad y Privacidad de la Información : https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

Mojan et al. . (2022). *Cyber Security Threats for 5G Networks.* Obtenido de Conference: 2022 IEEE International Conference on Electro Information Technology (eIT): https://www.researchgate.net/publication/361855139_Cyber_Security_Threats_for_5G_Networks

Montoya et al. (2020). *REDES DE NUEVA GENERACIÓN (NGN), SEGURIDAD EN SD-WAN REDES DE CONECTIVIDAD BASADAS EN SOFTWARE* . Obtenido de UNAD: https://repository.unad.edu.co/bitstream/handle/10596/36765/rjimenezo_smmontoyaar.pdf?sequence=1&isAllowed=y

Morrás. (2022). *Spoofing, qué es, tipos y soluciones.* Obtenido de https://veridas.com/es/que-es-spoofing/

Nigam. (2024). *El papel de la inteligencia artificial y el aprendizaje automático en la mejora de la ciberseguridad contra el ciberdelito.* Obtenido de https://www.eccouncil.org/cybersecurity-exchange/network-security/role-of-ai-ml-in-enhancing-cybersecurity-against-threats/

NIST . (2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST.* Obtenido de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

NIST. (2020). *T SP 800-207.* . Obtenido de ZERO TRUST ARCHITECTURE: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

NIST. (2024). *The CSF 1.1 Five Functions.* Obtenido de https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

NIST. (2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST.* Obtenido de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

O'Flaherty. (2025). *Human error in cybersecurity: how leaders can prevent avoidable attacks.* Obtenido de ITPRO: https://www.itpro.com/security/human-error-in-cybersecurity-prevent

Oliveira . (2024). *Análisis Integral de Seguridad en Dispositivos IoT.* Obtenido de Universitat Oberta de Catalunya: https://openaccess.uoc.edu/server/api/core/bitstreams/11bd741d-8e1b-4f18-b467-779b78b5f9ce/content

Owoko. (2024). *Security schemes for the next-generation networks: A survey.* Obtenido de Jaramogi Odinga Oginga University of Science and Technology 40601, Bondo, Kenya: https://gsconlinepress.com/journals/gscarr/sites/default/files/GSCARR-2024-0446.pdf

Radware. (2023). *¿Qué es la suplantación de dirección IP en DDoS?* Obtenido de https://www.radware.com/security/ddos-knowledge-center/ddospedia/ip-spoofing/

Ramezanpour et al. . (2022). *Security and Privacy vulnerabilities of 5G/6G and WiFi 6: Survey and Research Directions from a Coexistence Perspective.* Obtenido de ResearchGate: https://www.researchgate.net/publication/361655868_Security_and_Privacy_vulnerabilities_of_5G6G_and_WiFi_6_Survey_and_Research_Directions_from_a_Coexistence_Perspective

RedesTelecom. (2023). *NGN: Red de siguiente generación.* Obtenido de https://www.redestelecom.es/infraestructuras/ngn-red-de-siguiente-generacion/

Sahni et al . (2022). *A Systematic Literature Review on 5G Security.* Obtenido de Cornell University: https://doi.org/10.48550/arXiv.2212.03299

Salazar. (2024). *Ciberseguridad y gestión de riesgos en infraestructuras críticas del sector de las tecnologías de la información y telecomunicaciones: fundamentos y recomendaciones regulatorias.* Obtenido de Universidad Externado de Colombia: https://bdigital.uexternado.edu.co/entities/publication/70a3534e-f5b1-4c48-b9eb-f877456bcd9e

Scapicchio. (2024). *¿Qué es un SOC?* Obtenido de IBM: https://www.ibm.com/es-es/topics/security-operations-center

Shi et al. . (2022). *Physical layer security techniques for data transmission for future wireless networks.* Obtenido de School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing,: https://sands.edpsciences.org/articles/sands/full_html/2022/01/sands20210003/sands20210003.html

Silvestre et al. . (2023). *Packet Sniffing in the Cyber Threat Landscape: Examining Wireshark Capabilities, Misuse, and Policy Options in the Philippines.* Obtenido de https://rsisinternational.org/journals/ijriss/articles/packet-sniffing-in-the-cyber-threat-landscape-examining-wireshark-capabilities-misuse-and-policy-options-in-the-philippines/

UIT-T. (2007). *Y.2701.* Obtenido de SECTOR DE NORMALIZACIÓN DE LAS TELECOMUNICACIONES DE LA UIT: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-Y.2701-200704-I!!PDF-S&type=items

UIT-T. (2003). *X.805.* Obtenido de SECTOR DE NORMALIZACIÓN DE LAS TELECOMUNICACIONES DE LA UIT: https://share.google/8VT8aAw4pM0roi1a2

WEF. (2025). *El 72 % de los líderes en ciberseguridad ve riesgos crecientes. Así responden gobiernos y empresas.* Obtenido de World Economic Forum: https://es.weforum.org/stories/2025/05/el-72-de-los-lideres-en-ciberseguridad-ve-riesgos-crecientes-asi-responden-gobiernos-y-empresas/#:~:text=Se%20observa%20un%20uso%20creciente,alto%20nivel%20gubernamental%20e%20industrial.

Woburn. (2024). *Kaspersky experts: 2023 saw more than two critical cyber incidents per day.* Obtenido de https://usa.kaspersky.com/about/press-releases/kaspersky-experts-2023-saw-more-than-two-critical-cyber-incidents-per-day