REDES DE QUINTA GENERACIÓN: ESTÁNDARES Y NORMATIVAS QUE CONTRIBUYEN EN LA CONSOLIDACIÓN DE UN ENTORNO DIGITAL SEGURO EN EL USO DE DISPOSITIVOS DE COMUNICACIÓN MÓVIL EN COLOMBIA

ROBERTO AGUSTIN TIRADO ROMERO
JOHN WILLMAR ROMERO MORERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PROYECTO DE SEGURIDAD INFORMATICA II
BOGOTA D.C.
2022

REDES DE QUINTA GENERACIÓN: ESTÁNDARES Y NORMATIVAS QUE CONTRIBUYEN EN LA CONSOLIDACIÓN DE UN ENTORNO DIGITAL SEGURO EN EL USO DE DISPOSITIVOS DE COMUNICACIÓN MÓVIL EN COLOMBIA

ROBERTO AGUSTIN TIRADO ROMERO
JOHN WILLMAR ROMERO MORERA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Msc. Katerine Márceles Villalba
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PROYECTO DE SEGURIDAD INFORMATICA II
BOGOTA D.C.
2022

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

PROYECTO DE SEGURIDAD INFORMATICA II

BOGOTA D.C.

2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., Mayo 23 de 2022

DEDICATORIA

Este trabajo está dedicado principalmente a Dios, por permitir se materialicen los sueños además de la fortaleza para lograr obtener el título como especialista en seguridad informática; a nuestra familia por el apoyo y sacrificio incondicional en el trascurso de nuestra formación académica en todos estos años, lo que nos ha permitido avanzar y poder alcanzar este logro, que es reflejo del esfuerzo, dedicación y disciplina.

AGRADECIMIENTOS

Agradecer a Dios por la vida y por guiarnos a lo largo de nuestra existencia, por bendecirnos y darnos fortaleza en los momentos de dificultad; también manifestamos el más sincero agradecimiento a la universidad por la oportunidad al hacer parte de la formación académica a través del programa de Especialización en Seguridad Informática; asimismo, agradecer al cuerpo de docentes por el apoyo y acompañamiento en todo momento, por los valores y principios inculcados durante el proceso de formación, lo cual ha permitido llegar a la meta.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

APLICACIONES: En la industria del desarrollo de software se utiliza este nombre para referirse a las diferentes soluciones tecnológicas basadas en el desarrollo de algoritmos para construir aplicaciones bien sea web o móviles.

ATAQUES INFORMATICOS: Los ataques informáticos son aquellos que llevan a cabo los ciberdelincuentes aprovechando las vulnerabilidades que pueda tener una infraestructura informática a través de ataques cibernéticos

COMUNICACIONES MÓVIL: En la nueva era de las tecnologías y las comunicaciones se define la comunicación móvil

DESARROLLO: Es el término en la industria informática que se utiliza para la construcción de algoritmos referentes a desarrollar aplicaciones web, móviles entre otras.

FIRMWARE: Este es un software que realiza el control de la parte electrónica de los circuitos de los dispositivos, hace parte como componente del hardware por lo general está siempre integrado en la parte electrónica

IoT: Internet de las cosas, de esta manera se les ha nombrado a los dispositivos que se conectaran a internet en la nueva era digital, estos dispositivos como lo son la nevera, la licuadora lo cual se darán lugar con la red de nueva generación 5G

MALWARE: Los Malware son softwares maliciosos que infectan un dispositivo con el fin de escalar privilegios para tomar control de la máquina, extraer información, o generar daños a una organización

NORMATIVIDAD: Son las directrices que enmarcan los lineamientos para ejercer determinada actividad bajo la supervisión de las normas definidas.

REVOLUCIÓN INDUSTRIAL 4.0: Se le llama 4.0 a la cuarta revolución industrial, la cual promete generar nuevos cambios tecnológicos en la industria y la tecnología que se utiliza en las diferentes áreas laborales, comerciales, educativas entre otras.

SEGURIDAD DIGITAL: Dentro de la seguridad informática se establece la seguridad digital que se basa en utilizar los entornos digitales de manera segura aplicando los cuidados que se deben tener a la hora de utilizar las tecnologías

SMARTPHONE: Este es un depósito de comunicación móvil el cual tiene la capacidad de realizar conexiones a internet, hacer uso de aplicaciones, transmisión de paquetes, hacer pagos en línea entre otros atributos funcionales a nivel tecnológico.

TELECOMUNICACIONES: Es el sistema actual que nos permite interactuar por medio de diferentes dispositivos haciendo posible la trasmisión de datos a distancia

VULNERABILIDADES: Las vulnerabilidades en los sismas informáticos se refiere a las falencias que tienen los dispositivos, como, por ejemplo: la falta de parches o actualizaciones de sistemas operativos entre otros.

REDES DE QUINTA GENERACION 5G: Se le llama 5G a las redes de quinta generación, la cual se está proyectando poner en funcionamiento para mejorar la conectividad, ya que esta promete una latencia muy baja lo que mejora la transferencia de información.

RESUMEN

El presente trabajo de monografía tiene como objetivo realizar una investigación sobre redes de quinta generaciones 5G, para hacer la investigación se consultaron diferentes bases de datos como diversos documentos relacionados con la normatividad, entornos digitales seguros, ciberseguridad, principales vulnerabilidades de la red 5G, utilización de los dispositivos móviles conectados a la red de quinta generación, La seguridad digital del desarrollo de aplicaciones en entorno 5G, principales riesgos y amenazas asociados a los dispositivos conectados a la res 5G entre otros temas que fueron relevantes para documentar este trabajo.

Sobre las redes de quinta generación a nivel internacional los países más desarrollados se enfrentan en una disputa geopolítica por saber quién será el país dominante de la tecnología del futuro, la cual es muy prometedora en el ámbito económico. Los países de Estados Unidos y China se ven envueltos en disputas por esta nueva tecnología que desencadena todo un desarrollo a nivel global incluyendo la cuarta revolución industrial, esto ha dado lugar a que Estados Unidos realice acusaciones al País de China, por incluir puertas traseras a los dispositivos que comercializa para la implementación de esta red, por este motivo acusa al gigante Chino como lo son Huawei y ZT de emplear este método en los equipos, por lo que se considera un peligro para la seguridad nacional, en virtud de eso se han adoptado medidas en materia de ciberseguridad para mitigar los riesgos a nivel tecnológicos a través de normativas que conlleven a un entorno digital seguro.

Sobre la implementación en la Unión Europea la situación es más enfocada al tema de normatividad que a su mismo despliegue de esta nueva tecnología, se han creado mesas de trabajo para estudiar los posibles casos de ciberseguridad y entornos digitales seguros lo que hace más sólido su implementación, dado que los

operadores prestadores de servicio tendrán unos lineamientos soportados por las normas que regirán el funcionamiento e implementación y puesta en marcha los servicios de telecomunicaciones que estarán fundamentados en normas que respalden el uso de la red 5G para los usuarios finales como lo son: las empresas y la tecnología que adoptaran para aumentar su producción en el mercado; así como también los usuarios independiente que tendrán el acceso a nuevos aplicativos que darán lugar a entornos digitales enmarcados y soportados por las normas de la Comisión Europea. Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE. Bruselas, 2020.

La situación en América Latina sobre las redes de quinta generación y su despliegue se ve más sumido en la brecha tecnológica, pese a que para hacer esta implementación los costos son bastantes elevados. Los proyectos para la nueva tecnología ya se encuentran en marcha, los países como: México, Brasil, chile entre otros, ya están realizando pruebas pilotos para su implementación además de la creación de nuevas normas para los operadores que serán finalmente quien presten el servicio de esta nueva tecnología, los avances en materia de ciberseguridad aún no se encuentran bien definidos, para lo cual ya se han creado mesas de trabajo con diferentes métodos para llegar a crear normas cimentadas en un entorno digital seguro.

En Colombia ya se encuentran realizando las pruebas pilotos para la implementación de las redes 5G, el Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), ha creado una mesa de trabajo de acuerdo a la proyección por el Departamento Nacional de Planeación a través del documento CONPES 3995, donde se estipulan las normas y marcos jurídicos para la implementación de la red de quinta generación en un entorno digital seguro en las redes de telecomunicaciones y operadores que estarán al frente de esta nueva era

de la revolución industrial como se le conoce por su innovación tecnológica y el impacto que tendrá en diferentes sectores.

ABSTRACT

The objective of this monograph work is to carry out an investigation on 5G fifth generation networks, to carry out the investigation different databases will be consulted, such as various documents that contain related information regarding the part of regulations, secure digital environments, among others. topics that are relevant to documentary this work.

On the fifth generation networks at the international level, the most developed countries face a geopolitical dispute to know who will be the dominant country of the technology of the future which is very promising in the economic field, the countries of the United States and China are seen involved in disputes over this new technology that triggers a global development including the fourth industrial revolution, this has led to the United States making accusations to the country of China of including back doors to the devices it markets for the implementation of this network , for this reason accuses the Chinese giant such as Huawei and ZT of using this method in the equipment which is considered a danger to national security, for this reason cybersecurity measures have been adopted to mitigate the risks at the technological level through regulations that lead to a secure digital environment.

Regarding the implementation in the European Union, the situation is more focused on the issue of regulations than on its deployment of this new technology, work tables have been created to study possible cases of cybersecurity and secure digital environments, which makes its implementation more solid. , since the service provider operators will have guidelines supported by the standards that will govern the operation and implementation and start-up of telecommunications services that will be based on standards that support the use of the 5G network for end users such as companies and the technology that they will adopt to increase their production in the market as well as independent users who will have access to new applications

that will give rise to digital environments framed and supported by these previously created standards.

The situation in Latin America regarding the fifth generation networks and their deployment is more plunged into the technological gap, despite the fact that the costs are quite high to carry out this implementation, the projects for the new technology are already underway, the countries such as Mexico, Brazil, Chile, among others, are already conducting pilot tests for its implementation in addition to the creation of new regulations for the operators that will ultimately be the ones who provide the service of this new technology, advances in cybersecurity are not yet well defined. , for which work tables have already been created with different methods to create standards based on a safe digital environment.

In Colombia they are already conducting pilot tests for the implementation of 5G networks, the Ministry of Information Technologies and Communications (MinTIC), has created a work table according to the projection by the National Planning Department through of the document CONPES 3995, which stipulates the rules and legal frameworks for the implementation of the fifth generation network in a secure digital environment in the telecommunications networks and operators that will be at the forefront of this new era of the industrial revolution as it is known for its technological innovation and the impact it will have on different sectors.

INTRODUCCIÓN

El contenido del presente documento está enfocado en la red de quinta generación, donde se pretende dar a conocer los principales aspectos de esta tecnología, así como sus ventajas frente al mundo tecnológico en Colombia.

Para realizar un análisis sobre un entorno digital seguro en la red de quinta generación en distintos entornos se ha realizado una búsqueda de información en los diferentes motores de bases de datos que contienen documentos relacionados con la red de quinta generación, la cual es objeto de estudio en este documento, con los datos obtenidos se pretende tener un panorama global sobre los avances que adelantan a nivel mundial con esta tecnología además de conocer aspectos tales como: las normatividad que se aplican en países desarrollados como lo son Estados Unidos, China, la Unión Europea entre otros.

Asimismo, se pretende conocer por medio de esta documentación consultada, cuál es el panorama que se vive en América Latina respecto a la llegada de la red de quinta generación frente a un entorno digital seguro, conocer las políticas que regirán para el despliegue e implementación y puesta en funcionamiento de los servicios y productos que se ofrecerán con base a la tecnología 5G, la cual se encuentra en el marco de la cuarta revolución industrial por el alto impacto que promete en el ámbito tecnológico y comercio digital. Por otro lado, y no menos importante, se busca conocer cuáles son las gestiones en materia de normatividad que Colombia plantea frente a esta cuarta revolución industrial para masificar y conectar con este auge tecnológico además de proporcionar un entorno digital seguro que brinde la tranquilidad a los usuarios conectados a la red 5G y el uso de dispositivos de comunicación móvil, la normatividad que demarca este despliegue en todo el territorio nacional en materia de ciberseguridad.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La llegada de la red de quinta generación trae diferentes aspectos que se deben analizar puntualmente para que se logre su implementación y despliegue logrando mantener entornos digitales seguros, la utilización de dispositivos de comunicaciones móvil es sin lugar a duda la herramienta que marcará la diferencia en la tecnología de 5G, ya que su masificación se enfrenta a diversas vulnerabilidades con las que deben lidiar los usuarios y empresas del sector público y privado.

En este mismo sentido, el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC[1]. Le ha dado importancia al tema de la ciberseguridad dirigido a las tecnologías y sistemas de información más que en el tema de las redes e infraestructuras de los proveedores de servicios. Es en esta parte donde se identifica una oportunidad similar a la que están aplicando en Estados Unidos y Europa con la llegada de las redes 5G.

Por otro lado, en 2011 se emitió el Documento CONPES 3701 donde se consignan los Lineamientos de Política para la Ciberdefensa y ciberseguridad, el cual su objetivo es emitir directrices de política en Ciberdefensa y ciberseguridad dirigido al desarrollo de estrategias a nivel nacional que logre mitigar el aumento de las amenazas en aspectos informáticos que puedan afectar de una manera significativa al país. En 2016 se aprobó el Documento emitido por el Consejo Nacional De

[1] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES MINTIC. Plan 5G Colombia El Futuro Digital es de Todos. Bogotá D.C.: 2019. p. 57.

Política Económica y Social (CONPES 3854) Política Nacional de Seguridad Digital cuyo objetivo va enfocado al fortalecimiento de capacidad sobre las diferentes partes que muestran interés para gestionar, identificar, mitigar y tratar los diferentes riesgos de seguridad en un entorno digital en las diferentes actividades socioeconómicas en el sector digital, enmarcado en un ambiente de cooperación, colaboración y asistencial. Todo esto, para lograr la proyección del crecimiento en el sector económico digital en todo el territorio nacional, logrando de esta manera impulsar un mayor aumento en el sector económico y social en el todo país[2].

Teniendo en cuenta estas disposiciones emitidas en el marco regulatorio es fundamental en Colombia para afrontar el despliegue e implementación en las redes de quinta generación dando lugar a la utilización bajo criterios estandarizados en la nueva era de las tecnologías.

Por consiguiente, el auge de la red de quinta generación es de suma importancia que se comiencen a tomar medidas sobre la seguridad informática en Colombia, ya que las redes 5G impactan de una manera significativa al desarrollo de la economía, de la salud, educación, entre otros aspectos que da lugar en la era digital; es por esto que Colombia se debe preparar en esta área para fortalecer los pilares fundamentales de la seguridad informática como son: Integridad, Confidencialidad y Disponibilidad[3].

[2] Ibid., p.57.

[3] Ibid., p. 56-57.

1.2 FORMULACIÓN DEL PROBLEMA

Es fundamental conocer el impacto a nivel tecnológico que puede traer esta nueva tecnología en las distintas áreas que se ven inmersos diversos sectores, pero; ¿Cómo la normatividad y los estándares que rigen en Colombia las redes de quinta generación, contribuyen en la consolidación de un entorno digital seguro en el uso de dispositivos de comunicación móvil?

2. JUSTIFICACIÓN

Con el desarrollo de este trabajo se busca brindar un enfoque más amplio sobre la implementación de las redes de quinta generación en Colombia basados en las normativas y estándares aplicables que puedan favorecer a ésta. De esta manera, llegar a generar protección de la información, la cual es de suma importancia teniendo en cuenta las falencias que teóricamente acompañan esta evolución de las redes; así mismo, se pretende involucrar al sector público y privado para que en conjunto se tenga inclusión de la evolución tecnológica que impacte de forma positiva sacando provecho en el sector industrial, educativo, medicinal, agrario entre otros campos que se pueden impulsar a través de la tecnología de una manera exponencial.

Para las compañías y el sector privado es de vital importancia implementar los mejores esquemas para protección de la información, acordes con la normatividad establecida, como son el Sistema de Gestión de Seguridad de la Información SGSI a la luz de las Normas ISO/IEC 27001/2013, ISO/IEC 27002:2013 e ISO/IEC 27005:2018 y los últimos estándares internacionales; ya que en el mundo digital el intercambio de información juega un papel fundamental en un ambiente cada vez más globalizado y competitivo y la información es considerada uno de los activos más valiosos. Para lograr este objetivo, se requiere evaluar periódicamente los riesgos que constantemente amenazan los activos informáticos y que por ende afectan la continuidad en la prestación de los servicios tecnológicos informáticos que apoyan su normal funcionamiento e implementar los controles de seguridad necesarios para mitigar el riesgo tecnológico llevando a la consolidación de un entorno digital seguro.

Por lo anterior, es necesario elaborar un informe de controles y medidas orientado en asegurar la Disponibilidad, Integridad y Confidencialidad de la información y de

los componentes tecnológicos, buscando hacer el mejor uso de la nueva tecnología Informática 5G; establecer los lineamientos para el comportamiento que debe tener cada uno de los funcionarios responsables de la información; llevar a cabo también procesos de gestión de riesgo y evaluaciones de impacto en los proveedores de servicio, operadores y fabricantes, con el fin de identificar y mitigar nuevos riesgos de la nueva red de quinta generación[4]. Sobre este tema el Consejo Nacional De Política Económica y Social se ha manifestado emitiendo directrices en el documento 3854 que habla sobre lo siguiente;

> En el año 2016 fue aprobado el documento CONPES 3854 denominado "Política Nacional de Seguridad Digital, el cual busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsara una mayor prosperidad económica y social en el país"[5].

Asimismo, se ha publicado el Decreto 1078 del 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, el cual establece los principios para desarrollar la Política de Gobierno Digital, encontrándose entre ellos el de la Seguridad de la Información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la Confidencialidad, Integridad y Disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

---

[4] AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. Introducción a las tecnologías 5G y sus riesgos para la privacidad. Madrid. 2020. p. 11.

[5] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES MINTIC. Op. cit., p. 57.

Finalmente, con este documento se pretende hacer una contribución sobre las recomendaciones al buen uso de las redes de quinta generación en los entornos digitales seguros, la ciberseguridad de las redes de quinta generación, hacer un uso adecuado de las redes de quinta generación al utilizar los dispositivos móviles, conocer y aplicar recomendaciones en los diferentes sectores tales como: el sector financiero, medicina, educativo, agricultura, comercial entre otros, es fundamental acatar las diferentes medidas, dado que, esta nueva generación de las redes también trae consigo vulnerabilidades a las cuales están expuestos los usuarios al momento de incorporar diversos medios tecnológicos en su cotidianidad, como por ejemplo, cuando se vinculan a la parte laboral en las empresas.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar los estándares y las normativas que contribuyen en la consolidación de un entorno digital seguro en el uso de dispositivos de comunicación móvil en Colombia mediante una revisión documental, con el fin de proponer recomendaciones que gestionen el riesgo.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar una revisión documental referente al entorno de seguridad digital que establecen las redes de quinta generación (5G) respecto al uso de dispositivos de comunicación móvil en Colombia.

- Establecer las principales vulnerabilidades, amenazas y riesgos Informáticos a los que se encuentran expuestos los dispositivos de comunicación móvil que se encuentran conectados en una red de quinta generación (5G).

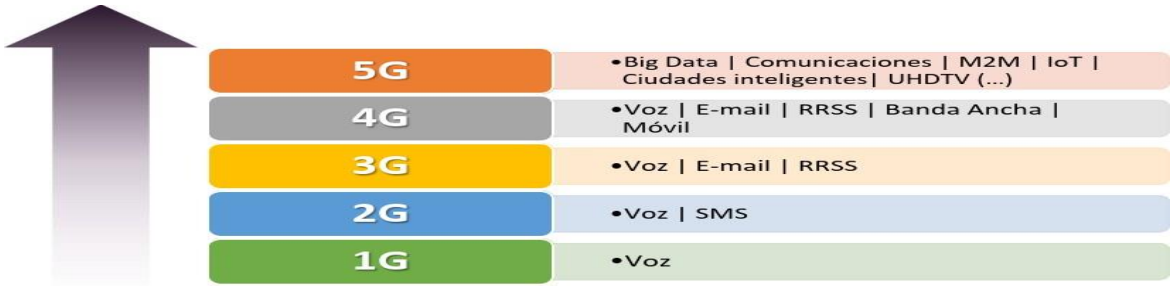
- Construir un documento soportado por la normatividad y los estándares establecidos en Colombia, que proporcione recomendaciones para la mejora de un entorno digital seguro en dispositivos de comunicación móvil.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Apara abordar el tema de la red de quinta generación, es primordial dar a conocer el proceso evolutivo de las redes móviles como lo muestra el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC[6]. Estas son: la red de Primera generación, Segunda generación Tercera generación y Cuarta generación. Que al igual que las otras generaciones lo que buscan es el espacio para ofrecer los servicios con más capacidad que los anteriores referentes a las redes, como: ampliar la conectividad e implementar en esta nueva era las máquinas inteligentes y la automatización, entre otros servicios. Esto dirigido a los usuarios finales, entregando bajas latencias además de una mejor calidad en los servicios. Como se describe en la Figura 1. se observa un ejemplo de la evolución de las tecnologías móviles.

Figura 1 Evolutivo de generaciones de redes móviles.



Fuente: MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Plan 5G Colombia El Futuro Digital es de Todos. 2019. p. 9.

[6] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Plan 5G Colombia El Futuro Digital es de Todos. 2019. p.9-10.

4.1.1 **Evolutivo de generaciones de redes móviles.** Estas son:

Primera Generación (1G) Nació a finales de los 70's y se popularizo desde los 80's. Fue una tecnología que permitió la llegada de teléfonos celulares al mercado.

Segunda Generación (2G) Primera de las tecnologías móviles digitales. Abrió paso a los teléfonos Inteligentes en los que había más servicios que solo las llamadas. Su producto estrella fueron los SMS (Mensajes De Texto) con los que los operadores llenaron sus bolsillos.

Tercera generación (3G) La llegada del 3G multiplico la velocidad de conexión de forma drástica pasando, en promedio, de 64 Kilobytes por segundo a 4 Megabytes por segundo (aunque seguro se operador dice que le ofrece más velocidad de navegación), con lo cual abrió servicio a los servicios de valor agregado como la descarga de archivos y aplicaciones, el streaming de música y video, la trasmisión de voz IP (Skype, viber facetime audio, etc.) e incluso las videoconferencias desde celular.

Cuarta Generación (4G) Fue la evolución del 3G y HSPA+ que logra velocidades de conexión hasta de 100 Mbps (Teóricamente, porque hasta el momento, en Colombia no he conocido el primer operador que en condiciones normales ofrezca este tipo de velocidades), con lo cual, un usuario puede reproducir video hasta en resolución Ultra HD o 4 k y acelerar tareas empresariales relacionadas con el uso de la nube.

Quinta Generación (5G) Desde diciembre del 2017, en Colombia, se está en proceso de estandarización el uso de estas nuevas tecnologías de trasmisión de datos móviles 5G, enfocadas en el consumo de contenidos digitales, aplicaciones empresariales y conectividad masiva para internet de las cosas (IoT). A inicios del

2019 se realizaron las primeras pruebas de la quinta generación de tecnologías de trasmisión móviles, pero aún falta camino para tener la versión comercial andando y con usuarios finales[7].

4.1.2 Tecnologías Inalámbricas Sobre 5G. 5G no se trata solo de teléfonos inteligentes rápidos como un rayo. El ideal a largo plazo afectará todo, como autos autónomos hasta robots para cirugía remota. Eso incluye todos los aparatos conectados a internet que sirven para quienes se quedan a vivir en sus casas durante la vejez, como cámaras que te permiten monitorear la entrega de paquetes, refrigeradores inteligentes que te alertan cuando queda poca leche, o termostatos con conexión wifi que aprenden tus horarios.

En algunas zonas más rurales, las redes 5G pueden convertirse en una alternativa inalámbrica fija, de banda ancha en el hogar, a internet de gigabit. El servicio inalámbrico fijo conecta un lugar a internet a través de una antena fija, por lo que una empresa que provee internet no necesita una línea de fibra óptica más cara. Pero en muchos lugares, las tecnologías de 5G e internet de gigabit tienen más probabilidades de ser complementarias y no necesariamente hacer la competencia. El entusiasmo por las redes 5G ha pasado de largo la realidad. En los primeros días del lanzamiento, todavía quedan varias preguntas sobre la cobertura, los dispositivos y los precios.

Según el autor Edward Baig[8], 5G es una complicación técnica en evolución que parece aún más compleja, debido a los esfuerzos de mercadeo de las compañías,

---

[7] TECHECETERA; 5G: historia y algunas verdades; [Sitio web]. [Consulta: 20 de octubre 2021]. Disponible en: https://techcetera.co/historia-y-verdades-acerca-del-5g/

[8] BAIG, Edward C. Qué son las redes inalámbricas 5G y de gigabit. Washington. 2020. Vol. 2, No. 1. p. 1.

que a veces son confusos, afirma Avi Greengart, presidente y analista principal de Techsponential, una empresa de investigación y asesoramiento tecnológico en el norte de Nueva Jersey.

4.1.3 La tecnología 5G ésta caracterizada por 8 especificaciones. Estas 8 especificaciones que tiene la tecnología 5G son:

1. Una tasa de datos de hasta 10Gbps - > de 10 a 100 veces mejor que las redes 4G y 4.5G.
2. Latencia de 1 milisegundo.
3. Una banda ancha 1000 veces más rápida por unidad de área.
4. Hasta 100 dispositivos más conectados por unidad de área (en comparación con las redes 4G LTE).
5. Disponibilidad del 99998%.
6. Cobertura del 100%.
7. Reducción del 90.0% en el consumo de energía de la red
8. Hasta 10 años de duración de la batería en los dispositivos IoT (Internet De Las Cosas) de baja potencia[9].

4.1.4 **Beneficios De La Tecnología 5G.** La tecnología 5G promete hacer aportes significativos en diferentes áreas a través de las tecnologías impulsando por medio de esta los sectores tales como: el comercio, la masificación del comercio digital, la cuarta revolución industrial, el sector de la agricultura, la educación, telemedicina, robótica, desarrollo de la tecnología 3D, automatización entre otros sectores como el de *Internet of Things (IoT).*

[9] 4NET NETWORKING. ¿qué es 5g? ¿qué tan rápido es 5g? [Sitio web]. Miami Florida: 4NET. [Consulta: 17 de septiembre 2021]. Disponible en: http://www.4netonline.com/ws/5g-lo-que-debes-saber/

4.1.5 Radio Cognitiva. Son las comunicaciones inalámbricas, que tienen como propósito la inteligencia artificial a los dispositivos de telecomunicaciones para lograr la capacidad de escanear el espectro completo y de esta manera realizar tareas como la identificación de las secciones de espectro libre y la asignación de tráfico a dichos espacios del espectro, lo cual logra garantizar la comunicación de alta velocidad y la interconexión de muchos más dispositivos.

4.1.6 Administración Avanzada De Interferencia. Esta es la interferencia co-canal que se presenta en la tecnología actualmente en servicio 4G LTE, con base en estas limitaciones se proponen soluciones futuras como:

- Receptor avanzado y programa conjunto que desde la trasmisión y desde el dispositivo final se implementen técnicas para reducir la afectación de las interferencias.
- Interferencias co-canal causadas por un canal contiguo, es este caso, la interferencia que causa una BS sobre un equipo en el área de otra BS.
- Receptor avanzado es capaz de decodificar tanto la información deseada como la interferencia para de esta manera retirarla[10].

4.1.7 Internet Móvil Personal y más allá. describe tres requisitos fundamentales: La capacidad de ampliar la red con el fin de tener la capacidad de albergar el creciente número de dispositivos que acceden a la red con el fin de intercambiar información, haciendo especial hincapié en las comunicaciones M2M *(Machine to Machine)*, dado el crecimiento casi exponencial de los diferentes dispositivos portátiles, sensores actuadores que se dispone en la actualidad b) los usuarios no

[10] JARAMILLO NÉSTOR, William Páez, *et al.* Tecnología 5G. Bogotá D.C.: Revista Ingeniería, Matemáticas y Ciencias de la Información, 2017. p. 41-42.

deben acceder a la red para alcanzar la información de internet, sino que el internet vendrá a ellos c) tener una red lo suficientemente rápida para garantizar periodos de latencia muy bajos[11].

4.1.8 Densificación De Las Redes Inalámbricas. Son un reto, ya que deben converger aspectos tan importantes como el cambio total de infraestructura y la evolución de los actuales dispositivos de recepción, por lo que debe existir una reorganización de las redes y un manejo más eficaz de las interferencias entre celdas, todo esto soportado por una densificación de Backhuaul red de retorno (porción de red dentro una estación base que se encuentra entre el núcleo (Core) y las subredes presentes, receptores capaces de realizar procesos de cancelación de interferencia[12].

4.1.9 Tecnologías Cloud Para Acceso a Redes De Radio Flexibles 5G. Se incorpora a sus servicios móviles nuevos y más complejos dispositivos operados por humanos y también dispositivos que se comunicaran con otros dispositivos, estos totalmente automatizados (máquina a máquina, M2M). Dejando claro la gran importancia de la nube y el papel esencial que cumple, integrándolo a objetos de uso cotidiano, como automóviles, electrodomésticos, textiles y aplicaciones críticas para la salud[13].

[11] Ibid., p. 42.

[12] Ibid., p. 42.

[13] Ibid., 42.

4.2 MARCO LEGAL

A continuación, se presentan las acciones encaminadas a la actualización de las políticas públicas sobre el marco normativo y regulatorio asociado al despliegue y operación de las redes 5G. Estas disposiciones son emitidas por las autoridades nacionales del sector de tecnologías, Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC) consignado en el programa denominado Plan 5G y el Consejo Nacional De Política Económica y Social (CONPES 3995) en su documento más reciente sobre las políticas de seguridad digital enfocado en las redes de quinta generación denominado

Política Nacional De Confianza Y Seguridad Digital donde se dictan estas medidas las cuales reglamentan jurídicamente la forma en que se deben utilizar las redes de quinta generación además de un entorno de desarrollo de industria que habilite y facilite la masificación de esta tecnología en todo el país. De igual forma, se definirán las características técnicas y de calidad que deben ser ofrecidos por los servicios 5G. A continuación, se relacionan algunos lineamientos importantes que se deben tener en cuenta para el despliegue e implementación de las redes de quinta generación definidas por el Ministerio de Tecnologías de la Información y las Comunicaciones en el documento denominado Plan 5G Colombia.

Lineamiento de acción 1. Se deben definir los modelos de administración de espectro. El Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC) cuenta con el apoyo de la Agencia Nacional del Espectro (ANE) en la parte técnica asesorando los procesos para evaluar y definir los nuevos patrones para administrar el espectro referente a la asignación de este recurso, ya que los interesados en esta tecnología son diferentes actores (Proveedor de Redes y Servicios de Telecomunicaciones, empresas de diferentes áreas, academia, etc.).

Todo esto con la finalidad de estar preparados para los diferentes avances en el sector tecnológico y técnico además de la gran demanda que exigen las redes de quinta generación 5G. para el segundo trimestre del año 2021 se debe tener finalizada esta acción.

Lineamientos de acción 2. Determinar técnicamente las características para los servicios de telecomunicaciones móviles. Conociendo el resultado que proporcione el diagnóstico sobre el estado que se encuentran las redes móviles en la actualidad, el cual se encargara de elaborar la Comisión de regulación de Comunicaciones (CRC), este deberá hacer un estudio que proporcione los insumos y bases para lograr la actualización de las directrices sobre la calidad de los servicios ofrecidos a los usuarios de telefonía móvil, sobre la protección que se le debe brindar al usuario entre otras que se consideren relevantes. Se debe tener en cuenta en esta actualización que en el entorno de redes de quinta generación 5G, cuando se refiere a usuarios no solo va dirigido a las personas, también incluye dispositivos de *Internet of Things (IoT)* tales como drones, vehículos, maquinas inteligentes entre otros dispositivos.

Lineamientos de acción 3. Actualizar el espacio total del espectro para el despliegue de las redes de quinta generación en todo el territorio nacional. El Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC) cuenta con el apoyo de la Agencia Nacional del Espectro (ANE), estudiara los techos del espectro radioeléctrico en la actualidad para redactar una propuesta sobre su actualización, esto enfocado al despliegue de la nueva tecnología de las redes de quinta generación en todo el territorio nacional, para esto es primordial tener presente el estado del mercado en la actualidad, la demanda en cuanto al crecimiento de servicios proyectados, la disponibilidad de bandas del espectro, entre otros. Teniendo esta información se elaborará un documento que definirá los

topes del espectro radioeléctrico con disponibilidad para la implementación de los servicios móviles.

Lineamientos de acción 4. Actualización y divulgación de las estrategias para deponer los obstáculos al despliegue de la infraestructura para la tecnología de las redes de quinta generación 5G. La Comisión de regulación de Comunicaciones (CRC), actualizará y revisará el código de buenas prácticas para el despliegue de redes de comunicaciones. Mencionado código se utilizará como material de consulta para los administradores locales con el fin de impulsar y facilitar el adecuado despliegue de infraestructura para las redes de quinta generación 5G en todo el territorio nacional.

El Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), en conjunto con la de la Agencia Nacional del Espectro (ANE), y la Comisión de regulación de Comunicaciones (CRC), realizarán actividades de capacitación y divulgación a los diferentes organismos territoriales, particularmente en temas que se relacionan con las tecnologías móviles y su funcionamiento, los límites de exposición que deben tener en cuenta las personas en campos electromagnéticos. De igual manera, se vincularán a otros entes del Estado Colombiano como; Ministerio de Protección Social, de Medio Ambiente y Desarrollo Sostenible, de Salud y de Comercio, el Ministerio de Cultura, Industria y Turismo, y el de Transporte con el fin de conseguir una mayor armonización en todo el territorio nacional en cuanto al despliegue e implementación del ecosistema digital en las redes de quinta generación 5G.

Lineamientos de acción 5. Actualizar y revisar periódicamente la regulación y normatividad. El Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), periódicamente debe hacer revisiones de las normas vinculadas al espectro radioeléctrico para la tecnología de quinta generación 5G, además de la

implementación y masificación de las redes de quinta generación 5G. De igual manera, El Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), o el ente que tenga la responsabilidad, deberá hacer la actualización de las normas que puedan estar obstruyendo o dilatando la implementación y masificación de la tecnología de quinta generación 5G.

El Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), en conjunto con la Agencia Nacional del Espectro (ANE), con la información técnica, establecerá los mecanismos para hacer las pruebas técnicas a través de experimentos, ensayos, evidenciar o aprobar funcionalidades sobre los dispositivos de radio, redes de telecomunicaciones. De esta manera se pretende validar la funcionalidad y futuras ofertas en el sector comercial de las redes de quinta generación 5G.

Se debe realizar un análisis y actualizaciones del régimen actual referente a las contraprestaciones para la utilización del espectro en las pruebas antes mencionadas, haciendo exequible el acceso a este recurso a todos los sectores que sea de su interés.

La Comisión de Regulación de Comunicaciones (CRC), incorporará en todo el periodo de mejora regulatoria como también los análisis expost hechos a la regulación emitida, perspectiva para evaluar aspectos relacionados a la eliminación de obstáculos y la implementación de las redes de quinta generación 5G. En particular, se debe tener en cuenta todo aquello que se encuentre asociado con el continuo seguimiento a los distintos niveles de calidad en los diferentes servicios, el debido cuidado y protección de los usuarios, Convalidación de equipos y la implementación de infraestructura en todo el territorio nacional. Los siguientes resultados se tendrán en cuenta para su actualización, siempre y cuando así se requiera.

La Agencia Nacional del Espectro (ANE), actualizará y revisará las normas sobre las personas expuestas a los campos electromagnéticos, teniendo presente la particularidad de los nuevos sitios radioeléctricos utilizados para las redes de quinta generación 5G. Se debe considerar también, las definiciones de los métodos y variables para la evaluación y supervisión con el fin de cumplir con los límites a los que deben estar expuestos los seres humanos a los campos electromagnéticos[14].

[14] MINTIC. Op. cit., p. 71-73.

5. DESARROLLO DE LOS OBJETIVOS

A continuación, se presenta el desarrollo de los objetivos propuestos en la presente monografía, se realiza una definición de cada uno de los conceptos relacionados en los diferentes objetivos los cuales serán abordados de una manera puntual y objetiva.

5.1 REVISIÓN DOCUMENTAL REFERENTE AL ENTORNO DE SEGURIDAD DIGITAL QUE ESTABLECEN LAS REDES DE QUINTA GENERACIÓN (5G) RESPECTO AL USO DE DISPOSITIVOS DE COMUNICACIÓN MÓVIL EN COLOMBIA

5.1.1 Seguridad Digital en las redes de quinta generación. La tecnología de quinta generación será la que de paso al desarrollo de (IoT) internet de las Cosas, las impresiones en 3D, la autónoma conducción, la telemedicina, la industria 4.0, la avanzada robótica, el Big Data en su uso masivo y la realidad virtual como otras sin nombrar dentro de la economía digital. Se estima que la Unión Europea (EU) en 2020 todos los países deben tener una disponibilidad por lo menos de una ciudad de las principales con la tecnología de quinta generación con un acceso comercial proyectando una cobertura total en 2035. Según la comisión Europea el despliegue tendrá un aporte al PIB de 910.000 millones de euros adicionales además de generar alrededor de unos 1,3 millones de empleos de aporte a la economía de estado.

Si no se realiza un esfuerzo para hacer esta inversión no es posible lograr un mercado digital único lo que puede ocasionar que Europa quede por detrás de China y los Estados Unidos en el afán por dominar tecnológicamente el mundo. La competencia real se traduce en la protección digital, en la desconfianza sobre si se cumplen las normas sobre la propiedad y privacidad de algunos fabricantes en el

ámbito industrial, al igual sobre algunas denuncias que la tecnología de quinta generación traiga consigo puertas traseras lo que puede incurrir en algunos comportamientos no deseados en los sistemas de componentes de los integrados en las relevantes infraestructuras para la seguridad nacional[15].

En esta nueva tecnología se beneficiarán algunos sectores más que otros tales como: las industrias, seguridad, automoción, salud, defensa, entretenimiento y medios de comunicación, transporte, energía además del sector financiero. Para realizar este despliegue es necesario requisitos económicos y técnicos. En la mayoría de los países el modelo seleccionado para la implementación de la red de quinta generación y tener una seguridad que sea económicamente viable, se basa en dejar que se realicen acuerdos voluntarios entre operadores entre sí para la colocación, distribución y compartir el uso de las infraestructuras teniendo en cuenta su alto costo.

Por lo anterior, es necesario saber, que adicional a la infraestructura de tecnología 4G que ya está instalada, se deben instalar más fibras, además de los cientos de *small cells* para cubrir centenares de metros en el territorio. Cabe mencionar, que se debe hacer una correcta gestión por parte de las administraciones públicas del espectro radioeléctrico, el cual es de administración pública, con el objetivo de asegurar la disponibilidad de ancho de banda[16].

5.1.2 Contexto en las redes de comunicación y geopolítica a nivel mundial.

Lo más importante de este tema que aparenta ser solo tecnológico, es lo que recién

---

[15] El despliegue de las redes 5G, o la geopolítica digital [en Línea]. Madrid España: Real Instituto Elcano, 2019. [Fecha de consulta: 23 noviembre 2021]. Disponible en: https://www.realinstitutoelcano.org/analisis/el-despliegue-de-las-redes-5g-o-la-geopolitica-digital/

[16] Ibid., p. 2-3.

se conoce por dichos acontecimientos sucedidos a nivel internacional, es lo que está más allá de la utilización correcta de las grandes oportunidades que brinda la nueva era tecnológica para el mejoramiento de los procesos. También la tecnología y su preponderancia se encuentran en juego, la cual se convierte en una disputa geopolítica en las potencias grandes. De esta manera lo entienden las grandes potencias como lo son China y Estados Unidos, estos países se encuentran en una competencia para ver quien logra tecnológicamente la supremacía en una competencia abierta en el ámbito geopolítico, esta competencia que básicamente consiste en tecnología, economía y comercio, causa traumatismo a lo que es la seguridad nacional.

Los sistemas y la tecnología otorgan la prevalencia al que consigue posicionarse tener una ventaja a nivel de competencia indudablemente al momento de imponer geopolíticamente los intereses comerciales, económicos e incluso cultural. Por esta razón, es que la seguridad nacional se encuentra relacionada directamente en todos los países y no solamente en las potencias mundiales, por que depender tecnológicamente u optar por un sistema que se prefiera estratégicamente son opciones que pueden condicionar el desarrollo en el futuro a dichos países[17].

Asimismo, la tecnología de quinta generación se ha convertido en un motivo de conflicto por lo que las potencias están compitiendo comercialmente, hasta el punto de utilizar argumentos de seguridad nacional lo que posiblemente incorpora una buena intención para proteger las empresas locales además de saber quién gana la confrontación de imponer la tecnología del futuro. No es de sorprendernos que dicha confrontación se intensifico en los últimos años teniendo en cuenta que es bastante lo que se encuentra en juego.

[17] Ibid., p. 3.

Se relaciona con una disputa bastante amplia y abierta sobre los microchips. Son considerados como el nuevo petróleo, lo que hace que este combustible tenga utilidad son los chips considerados como los motores que mueven este combustible. Como primera medida tecnológicamente se manifiesta en lo que se relaciona a la parte de seguridad y defensa, la cual consume de una manera masiva los microchips los cuales son una pieza fundamental en todos los sistemas. En la estrategia de seguridad nacional de EEUU se manifestó con gran preocupación recientemente dicha información[18].

La elaboración de *small cells* será relevante en el proceso de implementación de las redes 5G, y constituirán la parte principal de la arquitectura de este tipo de tecnología. Actualmente, son 5 los principales fabricantes de estos elementos, los cuales son: ZTE, Huawei, Samsung, Ericsson y Nokia, las dos primeras son empresas chinas, por esta razón precisamente es que utilizar las tecnologías de las empresas ZTE y Huawei han dado pie a graves controversias de tipo político y comercial entre China y EEUU[19].

Por otro lado, esta diferencia geopolítica hace referencia particularmente a la posibilidad de que las empresas chinas que fabrican *small cells* incorporen en estos elementos, dispositivos que tengan la capacidad de enviar de una manera encubierta información, o también que exista la posibilidad que no se pueda ejercer el control absoluto por parte de los operadores que gestionan estos equipos, lo cual representa una amenaza a la seguridad, confidencialidad e integridad en los sistemas.

[18] Ibid., p. 3.

[19] Ibid., p. 4.

En estados Unidos el ente de inteligencia en 2012 dió a conocer que Huawei y ZTE pueden ser una amenaza para la seguridad nacional. Hay más manifestaciones de preocupación frente al tema, como, por ejemplo: Nueva Zelanda ha prohibido por parte del gobierno a una empresa de telecomunicaciones y redes llamada Spark, advirtiendo sobre el uso de los equipos de la empresa china Huawei para la implementación de la red de quinta generación.

De esta manera el tema tecnológico se va tornando en un asunto de seguridad nacional, de esta misma manera estados Unidos y Australia se oponen para que no sea integrado los equipos de este fabricante a sus redes de telecomunicaciones. Alemania también se ha sumado a esta restricción de los equipamientos de las empresas chinas para la implementación y despliegue de las redes de quinta generación motivado por razones de amenazas de ciberseguridad. Es por esta razón que el proveedor chino dice que Estados Unidos ejercen presión sobre sus aliados para impulsar su participación en lo que se ha denominado la nueva guerra basada en la tecnología[20].

5.1.3 Implementación y despliegue de las redes de quinta generación en la Unión Europea en materia de ciberseguridad. Sobre este tema la Unión Europea ha desarrollado un informe evaluando el riesgo sobre la ciberseguridad en las redes de quinta generación. Este informe contiene las amenazas principales y los agentes de riesgo, los puntos principales y los activos más sensibles o vulnerables, de carácter técnico o de otro aspecto que pueden generar afectación en las redes de quinta generación. Teniendo esto en conocimiento el informe es basado en diversas categorías de los riesgos más importantes estratégicamente desde la óptica de la Unión Europea. Esto basado en escenarios concretos de riesgos que muestran

[20] Ibid., p. 4

combinaciones de los diferentes parámetros como son los agentes de riesgo, amenazas y vulnerabilidades relacionado con los diferentes activos.

La European Unión Agency for Cybersecurity (ENISA), ha complementado el informe teniendo en cuenta ciertas amenazas de forma específica, en el cual se refleja detalladamente un análisis de carácter técnico basándose más que todo en los componentes de red y las posibles amenazas que estos pueden tener, la Unión Europea centra su informe evaluando los riesgos centrándose en una variedad de aspectos de las redes de quinta generación los cuales se citan concretamente[21].

a) Tecnológicamente se vienen diversos cambios que serán insertados por las redes de quinta generación 5G. Incrementará la cantidad de ataques de una manera general además de potenciales puntos de ingreso para los ciberdelincuentes. las funciones mejoradas en la red especialmente en los equipos de borde y una arquitectura no tan centralizada como usualmente estaba en anteriores generaciones de redes móviles que comprometen algunas funcionalidades básicas que se pueden integrar en diferentes lugares de las redes, lo que hace más vulnerables los equipos correspondientes.

La función más importante del software en los equipos de quinta generación 5G involucra el incremento de riesgos asociados a los procesos de actualización y desarrollo de software, establece nuevas exposiciones de errores en las configuraciones y crea un rol más importante en el análisis de seguridad a las opciones seleccionadas por cada operador de servicio de redes móviles en la fase de implementación y despliegue de la red.

[21] COMISIÓN EUROPEA. Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE. Bruselas, 2020. p. 3.

b) Las nuevas características tecnológicas tendrán más que ver con la confianza de los operadores de redes móviles en proveedores externos y su rol en la cadena de suministro en las redes de quinta generación 5G.

Esto, por lo tanto, aumentará el número de vías de ataque que pueden sacar provecho los actores de riesgo y, en particular, los de países no pertenecientes a la UE o que tengan el apoyo debido a su capacidad (recursos e intención) para atacar las telecomunicaciones. redes de los Estados miembros de la UE y la posible gravedad de las consecuencias de tales ataques.

A la luz de la creciente amenaza de ataques de proveedores externos, el perfil de riesgo de cada proveedor será particularmente importante, especialmente si tienen una presencia significativa en redes o en ciertas áreas.

c) Depender demasiado de un proveedor aumenta la visibilidad y las consecuencias de la falla de un proveedor. También exacerba el impacto potencial de las debilidades o vulnerabilidades y su posible uso por parte de los actores del riesgo, especialmente cuando se utiliza un proveedor de alto riesgo.

d) Si algunos de los casos nuevos de uso de las redes de quinta generación 5G pronosticados llegan a materializarse, las redes de quinta generación 5G se convertirán en una parte indispensable de la cadena de suministro para muchas aplicaciones de TI críticas, no solo afectando los requisitos de privacidad y seguridad, sino que también, transformará la disponibilidad e integridad de las redes en mención principal para la seguridad nacional además de un gran desafío de seguridad importante para la UE[22].

[22] Ibid., p. 4.

5.1.4 La Ciberseguridad de las redes de quinta generación en la Unión Europea.

La Unión Europea ha desarrollado una caja de herramientas donde describe y enumera una variedad de restricciones estratégicas además de técnicas que están ligadas a unas medidas para apoyarse con el objetivo de aumentar su eficiencia al momento de reducir los riesgos que se logren observar.

También se contemplan las medidas de una forma estratégica teniendo en cuenta suministrar a las administraciones más disposiciones reglamentarias para poder supervisar las contrataciones y las implementaciones de las redes de quinta generación, especificando las medidas que se van abordar, relacionando los riesgos o vulnerabilidades que no sean técnicas y algunas iniciativas para incentivar el valor en la cadena de suministro de las redes de quinta generación y su sostenibilidad y diversidad para prevenir los riesgos comunes derivados de esta a un determinado tiempo. Las medias preventivas técnicamente se basan en reforzar la parte de seguridad de las infraestructuras de las redes y los equipamientos 5G teniendo en cuenta los derivados riesgos de las tecnologías, el factor humano y físico además de los procesos.

La denominada caja de herramientas de la Unión Europea, la cual es acordada en materia de seguridad por el grupo de cooperación Redes y Sistemas de Información (SRI) hacen las recomendaciones basadas en una serie de medidas puntuales las cuales todos los integrantes de los estados deberán llevarla a cabo además de la comisión, estas son:

- Requisitos de seguridad mejorados para los operadores de redes móviles (por ejemplo, estricto control de acceso, supervisión de seguridad y normas de funcionamiento, límites a la subcontratación de determinadas funciones, etc.);

- Evaluar los perfiles de riesgo de los proveedores y, en consecuencia, hacer cumplir las restricciones que se aplican a los proveedores que se consideran de alto riesgo, incluidas las necesarias para reducir el riesgo de manera efectiva. UE (por ejemplo, funciones de la red central, funciones de coordinación y gestión de la red y funciones de coordinación de la red). red de acceso).

- Asegúrese de que cada operador tenga una estrategia consistente basada en múltiples proveedores que evite o limite cualquier dependencia significativa de un solo proveedor (o proveedores con perfiles de alto riesgo). considerado de alto riesgo; También significa evitar situaciones de contención para un solo proveedor, lo que, entre otras cosas, promueve una mayor interoperabilidad de los dispositivos.

La Comisión Europea, junto con los Estados miembros, debería ayudar a:

Mantener una cadena de suministro de las redes de quinta generación 5G sostenible y diversa para evitar circunstancias de dependencia a largo tiempo, para esto, entre otros aspectos: o se hará uso total de los instrumentos y herramientas de la UE que ya existen, en particular, por medio del control de las potenciales inversiones de otros países que puedan afectar a los activos estratégicos de las redes de quinta generación 5G. El mercado de suministro de 5G debido a posibles actividades de dumping o subsidio; Se reforzará la capacidad de la UE en tecnologías 5G y post-5G con la ayuda de la financiación y los programas adecuados de la UE.

Posibilitar las coordinaciones entre los Estados miembros respecto a la normalización para conseguir objetivos de seguridad más específicos y desarrollar uno o varios sistemas que certifiquen de forma relevante a nivel de la UE para promocionar procesos y productos más seguros.

Para proveer las garantías que este enfoque coordinado resista la prueba del tiempo, se debe ampliar la misión del Grupo de Colaboración Redes y Sistemas de Información SRI y la colaboración con otras agencias y entidades relevantes, en particular:

Realizar la revisión periódica, con el apoyo de la Comisión y La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), las evaluaciones de riesgo de la UE y del país sobre la seguridad de la red de quinta generación 5G y posterior a 5G, preparar y adaptar la siguiente metodología de evaluación y perfeccionarla para adaptarla al desarrollo de la tecnología de quinta generación 5G;

Llevar a cabo una evaluación y un seguimiento detallados periódicamente de la aplicación de la denominada caja de herramientas con base en informes realizados por parte de Estados miembros;

Apoyar y coordinar la implementación de medidas de apoyo que necesiten cooperación dentro de la UE, en particular cuando se trata de brindar asesoramiento e intercambiar mejores prácticas sobre diferentes medidas;

Brindar apoyo a una posible coordinación ulterior al interior de la Unión Europea (UE), en especial para conseguir una mayor convergencia orientada a los requisitos de la seguridad técnica y organizada para los operadores de redes[23].

5.1.5 Etapas evolutivas del sistema móvil de telefonía. Desde 1980 referente a la telefonía móvil cada década se ha incrementado la evolución de esta tecnología de una manera significativa, la cual se ha conocido de una forma generacional lo que ha llevado a que en mencionadas generaciones se incluyan funcionalidades nuevas permitiendo que aparezcan amenazas que ponen en peligro la privacidad de los usuarios[24]. A continuación, se describen las etapas evolutivas de la telefonía móviles.

1G: Comenzando la década de los ochenta se encuentran los primeros dispositivos móviles los cuales tenían una capacidad muy limitada logrando solamente hacer llamadas. Para esa época la funcionalidad era primordial y no se tenía en cuenta la

[23] Ibid., p. 5-7.

[24] AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. Op. cit., p. 4.

privacidad de los datos, teniendo en cuenta que su uso era excepcional, las llamadas entre los usuarios no eran tan privadas como las personas pensaban.

2G: En el año de 1991 llamada la 2da generación la cual ya era digital, incorpora la función de los mensajes de texto entre usuarios, en la segunda generación se incorporan algunos cifrados lo cual mejoraba la parte confidencial en las comunicaciones, en la parte de autenticidad siguen quedando vacíos sin resolver. Se ven inmersos los usuarios a vulnerabilidades como lo fue el SPAM además de interceptar sus comunicaciones por medio de estaciones falsas que utilizaban los delincuentes.

3G: En el año dos mil (2000) se dan a conocer los primeros teléfonos 3G los cuales ya tenían incorporado funciones multimedia, podían tener conectividad a televisión e internet, estos dispositivos traían consigo las primeras vulnerabilidades conocidas de codificación maliciosa, poder localizar por GPS, entre otras.

4G: En el año dos mil diez (2010) tomo fuerza la telefonía de cuarta generación, con la cual se podía tener conectividad a internet con una alta velocidad, esto obligo a la implementación de cifrados de más complejidad, como esta era red basada en el protocolo de internet las amenazas comunes existentes en las redes de área local se incorporaron a la tecnología de dispositivos móviles tales como: DDoS, APTs, virus, entre otros. Además de las vulnerabilidades vinculadas a la parte de la privacidad[25].

5.1.6 Las novedades principales en la red de quinta generación en la telefonía móvil.

La telefonía móvil de quinta generación promete cambios sustanciales referente a las anteriores generaciones. Entre esos cambios está la de utilizar cierto

[25] Ibid., p. 5.

hardware tradicionales utilizados en la telefonía, para cambiar a la utilización de equipamiento de una forma general, los cuales no son diferentes a los que se pueden identificar en los centros de datos TIC (Tecnologías de la Información y las Comunicaciones), pero con la diferencia que se implementa la virtualización como tecnología, a nivel de costos, implementación y flexibilidad, esto refleja ciertas ventajas, de igual manera permite a la infraestructura ser interoperable de fácil acceso desde internet por los equipos.

Se pueden clasificar en tres características las cuales permiten definir la red de quinta generación tecnológicamente de cambios en lo que ya conoce conceptualmente de redes referente a la comunicación móvil: localización, virtualización y Edge computing; agregando los cambios significativos de la seguridad[26].

5.1.6.1 Localización. Para la implementación de las redes de quinta generación se tiene pensado utilizar las frecuencia más altas de transmisión (Banda 26GHz), que son las utilizadas en la actualidad en el sistema de telefonía móvil, esto dará lugar a tener una mayor velocidad en las tasas de transmisión, asimismo tendrá una limitante que es la señal la cual se torna más limitada en los campos abiertos además de la sensibilidad ante muros, paredes que obstaculicen la transmisión de señal e incluso en partes internas.

Para este inconveniente en particular se ha diseñado una solución que consiste en hacer instalaciones de access point de una forma densa en las partes externas sumado a la implementación de access point de la tecnología móvil en las partes internas de edificios y en elevadas edificaciones públicas de mayor afluencia.

[26] Ibid., p. 5.

En conclusión, es necesario un acceso a la red más sólido, con más access point y entre ellos menos distancia. Esta solides en la red les facilitara a los operadores, la veracidad de hacer una localización del dispositivo de un usuario teniendo mayor exactitud a la que se tiene actualmente, logrando ubicaciones bastante exactas que pueden ser menos de un metro, a diferencia de las anteriores generaciones de 5G, se incluye una localización de 3 dimensiones. Es por esto que la expectativa en los servicios fundamentados en la localización (Location Based Services) se desarrollen innovando este sistema[27].

5.1.6.2 Seguridad. Desde una perspectiva de seguridad, las especificaciones técnicas de 5G incluyen, en comparación con las generaciones anteriores, las medidas de seguridad se han mejorado significativamente, En el acceso de la red y la central [28].

Algunas de ellos son:

- La novedad de la organización del identificador de usuario permanente, además, Cifrado para prevenir que se transmita sin cifrar, así como en Algunas situaciones en las otras generaciones pasadas de 5G.
- Con la introducción de 5G-AKA, el mecanismo de autenticación ha mejorado, la principal mejora es la red del operador y El servicio (red doméstica) es un servicio que autentica el terminal del usuario y la red.

  Donde el dispositivo móvil tiene la intención de conectarse al servicio de la red no descifre la clave de comunicación hasta que esté autenticada en red doméstica también tiene diversas formas para controlar el fraude.
- Protección de la integridad de los datos del usuario en la interface de radio, sumado a la que ya se ha proporcionado a la protección de confidencialidad de 4G.
- Autorizar el ingreso desde las redes que no sean 3GPP mediante la creación del cifrado de un túnel con la clave que proporcionan los operadores.

---

[27] Ibid., p. 8.

[28] Ibid., p. 9.

- Cuenta con el cifrado de *(Transport Layer Security),* permitiendo la comunicación entre las funcionalidades de la red Core.
- Incorporación de diversas opciones de seguimiento que permiten registrar las operaciones para hacer auditorías a la red en temas de seguridad[29].

Es posible que existan riesgos potenciales en materia de seguridad cuando la implementación de la red sea bastante deficiente y se acceda a este servicio en condiciones no seguras de funcionamiento de la mismas en la telefonía móvil. La ideología de continuar teniendo compatibilidad con las generaciones anteriores de telefonía móvil en cuento a los protocolos en las redes de quinta generación permite que ciertas vulnerabilidades existentes en estos se prolonguen en las tecnologías venideras.

5.1.6.3 Computación De Borde *(Edge Computing).* *Cloud computing* o computación en la nube, es fundamentada en gigantes centros de procesamiento de datos, en localizaciones que se encuentran distribuidas en todo el mundo, y su función es el almacenamiento y procesamiento de enormes volúmenes de datos. Actualmente, en los dispositivos móviles existen una forma de este servicio a través del uso de aplicaciones (Apps), logrando hacer un intercambio de información a través de internet por medio de servidores sin la gestión de los usuarios, por mencionar, físicamente su ubicación.

En diversos casos esta tecnología es de gran utilidad, pero no siempre es posible hacer uso de ella debido a su alta latencia, en ocasiones incierta, esto limita la utilización en tiempo real de ciertas aplicaciones. La utilización de hardware para uso general para el almacenamiento de virtualización de servicios de operadores da paso para implementar componentes que son novedosos en la red de quinta generación, estos son los llamados (*Multi-Access Edge Computing). Edge*

[29] Ibid., p. 9.

computing es la tecnología que hará posible el desplazamiento del centro de gravedad, que hace el tratamiento de los datos en los servidores a las zonas más cerca de los dispositivos móviles y usuarios, cuando exista la necesidad. En conclusión, se puede establecer una afluencia de servicios e información en ubicaciones diferentes que previamente los operadores se han puesto de acuerdo.

Poniendo en funcionamiento la computación ubicada muy cerca al usuario, la red de quinta generación lograra disminuir la latencia en la comunicación de tal manera que se acercara a lo que es tiempo real, esto es muy importante en el sector industrial, tal como:

- Realidad aumentada
- Oficinas y hogares conectados
- Videojuegos
- Automotores como vehículos
- La automatización en las industrias
- Las asistidas cirugías remotas[30].

En conclusión, las redes de quinta generación son el motivo de disputas de las grandes potencias mundiales teniendo en cuenta el gran potencial que hay en el despliegue de esta tecnología que abarca muchos sectores con un futuro prometedor el cual se inclina por el crecimiento y dominio de la nueva economía global, esto a su vez genera discordias en el ámbito geopolítico donde enmarca acusaciones en materia de seguridad nacional lo que conlleva a diferencias mostradas como aparente política.

Se evidencian más al marco económico y dominio de intereses comerciales. Por otro lado, la Unión Europea toma medidas en materia de ciberseguridad

[30] Ibid., p.8.

adelantándose a lo que conlleva la implementación y despliegue de las redes de quinta generación en los sectores económicos que se potenciarán con la llegada de 5G, se adoptan medidas de seguridad en la parte técnica siendo más selectiva con el despliegue de equipos, tecnología y normatividad que regula a los operadores que van a ofrecer estos servicios manteniendo la gobernabilidad en el sector tecnológico[31].

5.1.7 Las redes de quinta generación asociados a dispositivos de comunicación móvil. La revolución industrial 4.0 se desprende este concepto al inicio de la 3ra revolución en la industria, debido a la incorporación de medios tecnológicos y digitales que tienen origen a mediados del pasado siglo compuesta por conceptos conocidos como la unión de tecnologías desapareciendo las líneas que dividen las partes digitales, biológicas y físicas. Asimismo, se destaca la tecnología de comunicación móvil la cual ha tenido una gran relevancia en el avance de industrialización de esta tecnología, la cual proyecta clientes para el año dos mil trece en la tecnología 4G. Superiores a los mil trecientos millones al término del año dos mil dieciocho sumado a la proyección de conectividad de usuarios a la red de 5G.

Por otro lado, la comisión económica para américa latina, se pronunciaba sobre la importancia que tenía la red 4G en la conectividad de la industria con el consumidor final, generando variedad de oportunidades en el ámbito de compras en internet o comercio electrónico. El gran volumen de dispositivos móviles ha unificado la

[31] Ibid., p.8.

comercialización de productos con la industria avanzando a una velocidad bastante rápida, todo esto debido a los avances de las tecnologías y su conectividad[32].

Por otro lado, referente a las innovaciones digitales en la parte económica, el (WEF) Foro Económico Mundial dió a conocer en el reporte general sobre la competitividad en el año dos mil diecinueve (2019), indicaba que América Latina mostraba ciertos atrasos comparado con algunas economías, seleccionando en el listado a Chile de la región como el primer país en el lugar número 33, basado en lo expuesto, los propósitos de esta investigación son varios, el primero se basa en el análisis de la falta de elaboración documental científica enfocada a las comunicaciones móviles en la 4ta revolución industrial en América Lanita; segunda, dar a conocer el estado emitido por (WEF) en su reporte y el de la diferencia digital emitido por la comisión económica para américa latina y el caribe sobre el volumen de publicaciones realizadas de carácter científico, tercera, encontrar las estrategias y oportunidades que impulsen de una manera competitiva con relación a la conectividad en la región y sus países[33].

De igual manera, con esta investigación se busca afianzar las hipótesis encaminadas a las estrategias en el marco empresarial enfocadas en el sector de tecnologías, teniendo presente que la industria cuatro puntos cero (4.0) abarca una serie de tecnologías que facilitan desarrollar las cadenas de valores, un producto con mejor calidad, ser más eficaz en la comunicación con los clientes además de la mejora organizacional en el desempeño. Para dar cumplimiento a lo propuesto, se dan a conocer principalmente varios conceptos referente a la 4ta revolución de la industria, sus componentes, su desarrollo desde el punto de vista de los gobiernos

---

[32] CORZO, German D. y ALVAREZ-AROS, Erick L. Estrategias de competitividad tecnológica en la conectividad móvil y las comunicaciones de la industria 4.0 en Latinoamérica. En: Revista Información Tecnológica, Vol. 3, No. 6. p. 184.

[33] Ibid., p. 184.

además del impacto socioeconómico, posteriormente se hace por medio de metodologías enfocadas de una manera cualitativa, por medio de un inductivo proceso, haciendo uso de un estudio bibliométrico obteniendo metadatos de scopus una base de datos, entre otros métodos de recolección de información y cuantificación.

Lo cual ha permitido identificar parcialmente los posibles orígenes y sus variantes de las falencias externas referentes a los demás países e internas en los países de América Latina, por otro lado, se alcanza a visibilizar las crecientes oportunidades referentes a desarrollar e investigar en el sector de las comunicaciones móviles se realizan recomendaciones que tienden a direccionar tecnológicamente las estrategias de América Latina en la conectividad[34].

América Latina se está encaminando a la red de quinta generación, así como la vinculación de todos los países miembros de esta región, aunque algunos más que otros, esto debido a diversas razones que limitan en algunos casos al despliegue de esta nueva tecnología como la inclusión de las telecomunicaciones y dispositivos móviles para el esparcimiento y avance de esta interconexión, algunos países destacados en el avance de esta nueva tecnología son: México, Brasil, chile entre otros[35].

5.1.8 Estrategias establecidas en México para la cuarta revolución industrial 4.0. En México, el gobierno ha establecido alianzas con el sector privado y con las academias con el fin de elaborar las políticas públicas para impulsar la evolución de la revolución industrial 4.0, el secretario del sector económico señaló que el sector público está comprometido, en alianza con el sector privado es reducir las brechas

[34] Ibid., p. 184.

[35] Ibid., p. 185.

que existen en las grandes, medianas y pequeñas empresas, referente a los cambios en la tecnología. Uno de los objetivos prioritarios que México tiene respecto a la industria 4.0 es optimizar la parte de recursos humanos.

Los emprendedores del país en un 44% dicen que no es fácil conseguir personal con conocimiento adecuado para los que se necesita y en el mercado laboral el 40% de los emprendedores no se sienten preparados en los retos de la actualidad, asimismo se dio a conocer que se amerita invertir en la parte de desarrollo e investigación sea aumentada, ya que los recursos que se están destinando no alcanzan a cubrir los costos, en la actualidad solo se invierte el 0.6% del producto interno bruto de la nación, comparado con el 2,4% promediado que hacen los países con las economías más desarrolladas. Se requiere dar los estímulos necesarios para crear centros de innovación e investigación en alianza del gobierno y la industria en compañía de las academias[36]. México ha establecido 4 aspectos fundamentales en los que deben enfocarse para continuar con la evolución de la implementación de la revolución industrial 4.0

- Desarrollar el capital humano: se enfoca en dar las capacitaciones necesarias a las personas que laboran en las instituciones de educación y empresas centradas en las principales habilidades que se requieren en la industria 4.0.

- La Innovación: promover y apoyar del rubro en el desarrollo de las empresas.

- Clúster: promover el desarrollo de las alianzas adecuadas que conlleven a el éxito en el trabajo.

[36] VEGA BENAVIDEZ, Adriana Marcela. Industria 4.0 en los países desarrollados y países de Latinoamérica. Santiago de Cali: Universidad Cooperativa de Colombia. 2021, p. 29-30.

- Adoptar Nuevas Tecnologías: incentivar a las Pymes con el fin de que incorporen nuevas tecnologías para crecer exponencialmente sus ventajas de competitividad en los mercados[37].

5.1.9 Brasil y sus avances en la industria 4.0. En el año dos mil diecinueve (2019) en Brasil se hicieron estudios para evaluar el nivel de preparación que tienen las empresas, en la industria 4.0 en el sector de fabricación, en este estudio se detalla el proceso que permiten tener una preparación respecto a la nueva revolución industrial.

En primer lugar, para hacer un estudio de evaluación del nivel de preparación de las compañías referente a la cuarta revolución industrial es determinar las condiciones del sector de tecnologías, teniendo en cuenta que esta es la parte fundamental para desarrollar la parte tecnológica de la industria 4.0, estas tecnologías también llamadas habilitadoras, como lo son:

El Big Data, El Internet de Las Cosas (IoT), Almacenamiento en la nube, La conectividad al internet, Realidad aumentada, Robótica industrial entre otras. Después de esto se debe evaluar con el fin de conocer cuál es el nivel que tienen las compañías, sabiendo que hay desde la industria uno punto cero hasta 4.0, lo que permite hacer un estudio de este caso para poder determinar algunos factores, estos pueden ser su infraestructura referente a la tecnología, el nivel económico con el que cuentan para seguir con el proceso a la industria 4.0[38].

5.1.10 Chile y a cuarta revolución industrial. La industria 4.0 ha influido de una manera significativa en diversos cambios, sin embargo, aproximadamente un 20%

[37] Ibid., p. 26.

[38] Ibid. p. 31-32.

de los habitantes del planeta no cuentan con servicio de internet o en su defecto a energía eléctrica, el resultado de esto es que países de bajos recursos se les dificulta poder llegar a la industria 4.0.

Los Smartphone o también llamada telefonía inteligente se han apoderado del mercado de la comunicación aboliendo la telefonía tradicional dado que, por medio de un dispositivo como estos, se puede establecer el envío de datos, una comunicación ágil, pagos en línea, una mayor eficiencia sumado a que este dispositivo es uno de los elementos más importantes de las personas en la actualidad.

La industria 4.0 ha tenido un gran auge y crecimiento bastante alentador, pero también demanda que el personal que se una en esta, tengan un conocimiento amplio sobre la misma, que cuenten con capacitación además de preparadas en el tema para la administración de esta tecnología logrando un óptimo desarrollo y uso[39].

5.1.11 Políticas de carácter público para el despliegue de la tecnología 4.0 en Chile. Sobre las políticas de carácter público en Chile aún no hay una que impulse el desarrollo de la industria 4.0, que sea llamativo para el comercio a diferencia de otros países, este factor crea afectaciones tanto al comercio como a los demás sectores que también son fundamentales tales como: educación, industrial, salud, empresarial entre otros, por este motivo a chile no le permite hacerse cargo de los retos que la industria 4.0 trae respecto a los avances tecnológicos[40].

[39] Ibid., p. 37-38.

[40] Ibid., p. 39.

Se puede deducir que en el país de chile aún no se cuenta con una política pública para afrontar la llegada de la industria 4.0, esto genera atraso para hacer provecho de la industria 4.0 lo que afecta y el desarrollo en todos los ámbitos además de no estar a la vanguardia de los países desarrollados para fortalecer los convenios de mercadeo entre naciones.

Pese a esta situación, la subsecretaría de Telecomunicaciones (SUBTEL), en supervisión del Ministerio de Transporte y Telecomunicaciones a considerado prioridad motivar el despliegue de las redes y los servicios de la quinta generación en el país de chile, debido a que mundialmente se habla de los grandes beneficios que esta nueva tecnología ofrecerá en la parte económica y social bastantes significativos, por esta razón se decidió hacer una consulta, la cual tiene como finalidad reunir información y propuestas importantes referente a los temas importantes sobre el desarrollo de la red 5G, se considera importante que se haga participe y contribuciones de la ciudadanía, academias, empresas, el sector público y en general toda la sociedad[41].

5.1.12 Situación del despliegue de la red de quinta generación en Colombia. El principal problema con el despliegue de la tecnología de quinta generación (5G), en Colombia es que todavía existen regiones en el país, en las que no se ha completado la cobertura de la red 4G. Colombia aún cuenta con una población aproximadamente de 10 millones que solo utilizan las tecnologías de las redes 3G y 2G, lo que es una situación de prioridad y fundamental darle solución, ya que debido a esto existe una brecha en cuanto a la conectividad de este sector de usuarios.

Aproximadamente más de 20 millones de usuarios del país se ven afectados, para

[41] Ibid., p. 40-41.

esto se debe antes establecer las normas que enmarquen y regulen las actividades de las redes de quinta generación en Colombia, ya que esta tecnología es muy reciente en su uso he implementación en todo el mundo lo que la hace carente de reglamentación, protocolos, para que su funcionamiento sea óptimo y seguro con el usuario final.

A causa de la emergencia sanitaria actualmente en Colombia y en el mundo, es primordial superarlo en el aspecto económico y para seguir avanzando.
El gobierno nacional mantiene optimista, ya que, por parte de la ministra de las tecnologías de la Información y las comunicaciones, manifestó, en todo Latinoamérica el único país que ya se está introduciendo en las tecnologías de quinta generación (5G) es Colombia, mediante el evento que se realiza virtual Colombia 5G, presentado por *Digital Policy Law* (Ley de política digital).

El ministerio resaltó el llamado Plan 5G Colombia El Futuro Digital es de Todos, el cual fue aprobada en el mes de junio del 2019, logro que los operadores de telecomunicaciones se interesaran con el fin de incluirse en los proyectos que se colocaran a su disposición tres mil quinientos Mega Hertz para la transición a las redes de quinta generación (5G), sumado a esto se hizo el anuncio que ya se cuenta con la preparación en el país para una etapa de implementación y despliegue para masificar el sector de tecnologías.

Debido a que el país está entre los primeros del continente en conjunto con estados unidos, en hacer una presentación de la estrategia integra para la implementación de la red de quinta generación, la ministra, dió a conocer que en la actualidad se han hecho más de diez pruebas de ensayo enfocadas en esta tecnología en partes distintas de la geografía colombiana[42].

[42] MINTIC. Op. cit., p. 71.

Teniendo en cuenta la importancia de la implementación y despliegue de la tecnología de quinta generación que abre paso a la industria 4.0 en los diferentes países se aborda de una manera diferente en los países desarrollados, se enfoca este sector de acuerdo a la magnitud e impacto que genera en la parte financiera así como estratégica además de la parte política y dominio de la globalización en los países menos desarrollados, esto conlleva a una competencia de potencias por quien dominará la red del fututo; no obstante, cabe resaltar los grandes ingresos económicos que deja esta nueva tecnología a los que logren ejercer su dominio, la influencia que tendrían a los dependientes de sus equipos de infraestructura.

Los países latinoamericanos por su parte, aún se encuentran en una etapa de estudio y de prueba en la parte de implementación de las redes de quinta generación, es fundamental establecer políticas de seguridad que deben regir esta nueva tecnología, ya que los operadores de telecomunicaciones serán los prestadores de servicio a los usuarios finales y a su vez responsables del manejo del Big Data que esta tecnología manejara de una forma masiva.

La mayoría de los países de América latina, se enfrentan a la falta de recursos para establecer una red como ésta, la cual es bastante costosa su implementación, pero más allá de ponerla en funcionamiento la parte legal sobre el uso e implementación son las bases que darán lugar a las nuevas herramientas tecnológicas de una manera segura a los usuarios finales, ya que son éstos los que consumirán las capacidades tecnológicas que ofrece las redes 5G y su auge en los diferentes sectores.

Por otro lado, en Colombia el ministerio de las Tecnologías de la Información y las Comunicaciones, ya ha diseñado un plan para el despliegue e implementación para las redes de quinta generación en el territorio colombiano, se han diseñado algunas políticas de seguridad digital publicadas en el documento del Consejo Nacional De

Política Económica y Social (CONPES 3995), denominado Política Nacional De Confianza Y Seguridad Digital que buscan fortalecer y cimentar frente a los operadores de telecomunicaciones el uso tecnológico que se ofrecerá al público y sectores que se benefician de este auge tecnológico.

Dado que se prevé que el impacto al sector económico será bastante grande en los sectores de; educación, medicina, teletrabajo, desarrollo tecnológico, nuevas tecnologías, la agricultura, la realidad aumentada, el sector industrial con la automatización y la robótica, a diferencia de otros países en el continente. Colombia es uno de los países más adelantado en cuanto a la parte de normatividad y en pruebas piloto sobre el despliegue e implementación de las redes de quinta generación.

5.1.13 La seguridad digital en las redes de quinta generación frente al uso de dispositivos móviles en Colombia. En el año 2011 se elabora el documento CONPES 3701, el cual tiene como objetivo afianzar y fortalecer al estado en capacidad para mitigar las amenazas en la parte cibernética, generando de esta las condiciones que se necesitan para suplir la protección en el ciberespacio. Este documento contiene las estrategias para mitigar las amenazas que interfieren a la seguridad y la defensa del estado que están enfocadas a la ciberseguridad y Ciberdefensa, dando lugar a la creación de centros dedicados a este sector, como lo son:

centro cibernético policial (CECIP), Teniendo en cuenta la importancia de la seguridad digital, un gran logro referente a generar confianza en la era digital es la ley creada para la protección de datos personales que estarán expuesto en el mundo cibernético la cual se relaciona a continuación. Ley 1581 del año 2012. El objetivo de esta ley es impulsar el derecho constitucional que han adquirido todos los ciudadanos, ratificar y actualizar su información de carácter personal, en este

mismo aspecto, se ha desarrollado un marco jurídico que contiene el reconocimiento de la información de los datos personales como bien jurídico tutelado[43].

En el año 2016 se elabora el documento CONPES 3854, donde se habla sobre la Política Nacional de Seguridad Digital, su principal objetivo era hacer un fortalecimiento de las capacidades de las diferentes partes de interés para gestionar, identificar mitigar y tratar los diferentes riesgos en cuanto a la seguridad digital. Sobre esto, el aporte significativo de esta política fue desarrollar las estrategias que definieron un marco en cuento a la seguridad digital enfocada a la gestión de riesgo de igual manera también dio lugar a la creación de condiciones que admitieran que las diferentes partes de interés hicieran gestión del riesgo en lo concerniente a la seguridad digital, con el fin de hacer más fuerte la seguridad de los usuarios y a su vez la del estado, también la soberanía y defensa nacional en el marco digital[44].

Decreto 1008 publicado en el año 2018, que trata sobre las directrices generales de lo que es la Política de Gobierno Digital. En este decreto se consigna sobre la seguridad de la información, es uno de los elementos principales que dan paso para desarrollar el Gobierno Digital. Adicional a esto, también busca esta política preservar la integridad, disponibilidad, confidencialidad y privacidad de todos los datos, asimismo se incluyó en el Manual de Gobierno Digital, elaborado por el Ministerio de tecnologías de la Información y la Comunicaciones.

Se estipulan las directrices que deben adoptar el sector público para implementar la Política de Gobierno Digital, además de aplicar el Modelo de Seguridad y Privacidad

---

[43] LÓPEZ MARTÍN, Tatiana y HERNÁNDEZ, Karol Violeta. El Contrato de Seguro Cibernético. Bogotá D.C.: Universidad Santo Tomás. 2020, p. 30.

[44] Ibid., p. 7.

de la Información (MSPI), debido a que sus directrices permiten determinar el nivel que tiene de madurez en la parte de la seguridad digital para el sector público. Cabe destacar que este manual está alineado con las normas de buenas prácticas. Ley 1712 de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional) y con la Ley 1581 de 2012 que trata de la Protección de Datos Personales

En el año 2019 se publicó la ley 1955 donde se expide el Plan Nacional de Desarrollo 2018-2022 Pacto por Colombia, Pacto por la Equidad. Puntualmente en el capítulo séptimo. Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento, se quiere que Colombia sea encaminado con dirección a que la sociedad sea más digital y en dirección de la Industria 4.0, por medio de la generación en la parte digital y desarrollo en estrategias enfocada en la seguridad digital en el territorio nacional. Por otro lado, el capítulo referente al Pacto por la legalidad: seguridad efectiva y justicia transparente para que todos vivamos con libertad y en democracia, se define como una opción para suscitar el control integro terrestre, marítimo, fluvial, aéreo ciberespacial y espacial que fortalezca el gobierno nacional robustecer los alcances de Ciberdefensa y ciberseguridad para asegurar lo de interés nacional[45].

Plan TIC 2018-2022 El Futuro Digital es de Todos, con las propuestas del área TIC, diversos de estos están ligados a la seguridad digital, se pueden destacar entre ellos las generaciones con habilidades dirigidas a la igualdad de géneros, crear e impulsar los emprendimientos femeninos, asimismo que fortalecer las capacidades de carácter nacional para promover la transición digital del estado.

Para finalizar en el mes de noviembre del año 2019 se publicó CONPES 3795 Política Nacional para la Transformación Digital e Inteligencia Artificial. La cual tiene

[45] Ibid., p. 8.

como objetivo es aportar a la generación de un mayor valor en la economía y la sociedad por medio de la transformación digital en el área del sector privado y público, para que el país logre hacer provecho de las diversas oportunidades y asumir los retos que trae consigo la cuarta revolución industria 4.0, esta política, aparte de ser la que rige los temas sobre la digitalización en el país, también incluye en su accionar, los lineamientos de políticas públicas enfocadas en la ciberseguridad para elevar las capacidades de Colombia sobre el tema.

Según El Consejo Nacional de Política Económica y Social[46]. Por medio de esta política es que se puede ver que en el año 2019 es que ha surgido políticas que incluyan de forma más extensa la generación de la confianza digital además de las mejoras en el área de la seguridad digital con la mira a los ciudadanos y otras áreas del país.

Figura 2. Reglamentación y políticas de seguridad.

Fuente: CONPES 3995. Política Nacional de Confianza y Seguridad Digital. 2020. p. 10.

En conclusión, en el marco de reglamentación y políticas de seguridad, a través de la documentación consultada, se puede deducir que Colombia a través del

[46] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. CONPES 3995. Política Nacional de Confianza y Seguridad Digital. Bogotá D.C. 2020. p. 13.

Ministerio de Tecnologías de la Información y las Comunicaciones tiene un avance significativo sobre los demás países de América Latina, revisando los avances de los países como lo es México, Chile y Brasil, referente a los países desarrollados como lo es Estados Unidos, china y La unión Europea hay una alineación sobre en las políticas de seguridad digital, pero en la Unión Europea se evidencian avances notorios los cuales buscan tener una mayor seguridad en la red de 5G respecto a la telefonía móvil.

Además de la revolución industrial que viene de la mano de esta tecnología, definiendo de una manera puntual las alianzas entre el sector público y privado en el despliegue e implementación que se debe adoptar en el marco jurídico que regirá a los operadores de las redes de telecomunicaciones buscando proteger los intereses nacionales como la seguridad digital de los usuarios quienes finalmente serán los consumidores masivos de esta nueva tecnología.

Por esta razón la Unión Europea ha desarrollado un informe evaluando el riesgo sobre la ciberseguridad en las redes de quinta generación. Este informe contiene las amenazas principales y los agentes de riesgo, los puntos principales y los activos más sensibles o vulnerables, de carácter técnico o de otro aspecto que pueden generar afectación en las redes de quinta generación. Teniendo esto en conocimiento el informe es basado en diversas categorías de los riesgos más importantes estratégicamente desde la óptica de la Unión Europea. Esto basado en escenarios concretos de riesgos que muestran combinaciones de los diferentes parámetros como son los agentes de riesgo, amenazas y vulnerabilidades relacionado con los diferentes activos.

La ENISA ha complementado el informe teniendo en cuenta ciertas amenazas de una forma específica en los cual se refleja detalladamente un análisis de carácter técnico basándose más que todo en los componentes de red y las posibles

amenazas que estos pueden tener, la Unión Europea centra su informe evaluando los riesgos centrándose en una variedad de aspectos de las redes de quinta generación los cuales se citan concretamente en este informe.

Pese a las diferentes políticas que ha implementado el gobierno colombiano, es fundamental realizar los estudios más a fondo sobre las vulnerabilidades del riesgo en las redes de quinta generación adoptando medias para mitigar las falencias que trae la cuarta revolución industrial, teniendo en cuenta que Colombia tiene una política de seguridad digital se deben reforzar para dar garantías del uso de la red de quinta generación y las vulnerabilidades que esta trae consigo.

5.2 PRINCIPALES VULNERABILIDADES, AMENAZAS Y RIESGOS INFORMÁTICOS A LOS QUE SE ENCUENTRAN EXPUESTOS LOS DISPOSITIVOS DE COMUNICACIÓN MÓVIL QUE SE ENCUENTRAN CONECTADOS EN UNA RED DE QUINTA GENERACIÓN (5G)

5.2.1 Las vulnerabilidades amenazas y riesgos informáticos relacionados a las redes de quinta generación.

La piratería es un tema muy grave a nivel mundial y la preocupación es la seguridad en la red es bastante grande e involucran muchos dispositivos que se conectan a las redes 5G, estos aspectos ponen en riesgo a los consumidores gobiernos y a nivel mundial a todos los países, se tiene menos riesgos y desventajas en las redes anteriores a 5G, más ancho de banda afectará sin duda alguna el monitoreo de la seguridad actual en cualquier país del mundo.

Por otra parte, las vulnerabilidades toman una amplia variedad cómo los ataques de botnet los cuales controlan una red de dispositivos conectados para manipular un ataque masivo. También los ataques de negación de servicio para sobrecargar la red o un sitio web y desconectarla. Si bien las redes actuales tienen una velocidad y capacidad limitada esto ayuda a los proveedores a monitorizar la seguridad de

todos los dispositivos en móviles en tiempo real los beneficios de una red 5G pueden dañar la seguridad cibernética.

Esto que traerá consecuentemente desafíos a los equipos de seguridad para crear nuevos métodos sobre las nuevas amenazas la falta de cifrado al principio del proceso de la conexión puede ser utilizado para ataques y esto realmente ayuda a los piratas informáticos para saber exactamente qué dispositivos están conectados en una red y poder perpetrar sus ataques con más precisión[47]. Los ataquen *Man-in-the-Middle* (MiTM) interceptan y cambian silenciosamente las comunicaciones entre 2 partes. El seguimiento en la ubicación y la interceptación de las llamadas se pueden que se puedan realizar si alguien sabe incluso una pequeña cantidad sobre los protocolos de búsqueda de difusión[48].

Por otra parte, la telefonía móvil e incluso los satélites se comunican mediante radiofrecuencia. La frecuencia se mide en Hz y las frecuencias de radio tienden a operar en un rango de GHz, según los informes la red 5G transmitirá sus datos en un rango de alrededor de 6 GHz. Pero este rango de radiofrecuencia está lleno por otros enlaces o señales como los satélites, por lo cual este hacinamiento de señales y cuando las personas transmitan sus señales de datos a esta frecuencia habrá problemas para enviar y recibir señales[49].

Las tecnologías anteriores de telefonía móvil 3G cubrirá un territorio inmenso relativamente con pocas celdas ahora cuando comenzó a avanzar la tecnología 4G las personas notaron que su cobertura se caía con frecuencia, a medida que se despliegue la red 5G esta tendencia continuará mucho más, ya que se necesitan

[47] GONZÁLEZ. Op. cit.

[48] Ibid.

[49] Ibid.

muchas torres de telefonía móvil para producir este inmenso ancho de banda porque las celdas no pueden cubrir tanto espacio como una celda 3G o 4G[50].

5.2.2 Principales riesgos y amenazas asociados a los dispositivos móviles que se encuentran conectados a una red de quinta generación. Existen pocos mecanismos de ciberseguridad de acuerdo a estudios, los ciberataques a teléfonos móviles crecen día a día de forma exponencial, se han contabilizado más de 14 millones de intentos para subvertir el funcionamiento de un teléfono móvil, esto sin tener en cuenta la inmensa mayoría de dispositivos móviles que no instala ninguna herramienta de ciberseguridad que permita restringir las amenazas que diariamente se ven sometidos todos estos dispositivos.

Es bastante preocupante la seguridad móvil ya que encabeza una gran lista de preocupaciones para la mayoría de las empresas de todo el mundo que acceden a dispositivos inteligentes, desde la llegada de la pandemia la gran cantidad de personas interactúan aún mayor proporción en un 60% y las cifras sigue aumentando, a continuación, se relaciona algunas áreas subestimadas donde se encuentra varios riesgos y amenazas[51].

5.2.3 Ingeniería social. Una de las tácticas que es muy preocupante es el Phishing el cual se ha multiplicado por 6 con la pandemia del COVID-19 claramente los dispositivos ahora son el objetivo principal de los ciberdelincuentes los cuales saben de lleno que las personas trabajan desde sus hogares todo el día mediante teletrabajo y estos no toman todas las precauciones que tienen los dispositivos o

---

[50] Ibid.

[51] CIO MÉXICO. Ocho amenazas preocupantes para la seguridad móvil. [Sitio web]. México: CIO. [Consulta: 13 de septiembre 2021]. Disponible en: https://cio.com.mx/ocho-amenazas-preocupantes-para-la-seguridad-movil/

equipos tradicionales. El 92% de los delitos cibernéticos empiezan desde el correo electrónico y se basan en suplantación de identidad[52]. Es de resaltar que, en un mundo interconectado, los riesgos tienden a incrementarse, para una red de quinta generación se convierte en una potencial amenaza ya que la convergencia de datos es mucho más rápida lo que le facilita a un ciberdelincuente la intrusión a un sistema de una manera fraudulenta cuando no se tienen en cuenta medias de seguridad por parte de los usuarios.

5.2.4 Fuga de datos. En este apartado los problemas o decisiones que toman los usuarios son erróneas y se requiere la implementación de aplicaciones con las cuales se pueden intercambiar información segura. El principal desafío es la verificación de aplicaciones que no abrumen al administrador y no frustren a los trabajadores. En un entorno de las redes de quinta generación, son diversos los aplicativos y dispositivos inteligentes que estarán conectados, es de suma importancia que como medida de seguridad estos dispositivos se encuentren con los sistemas operativos actualizados a la última versión, instalar una solución de antivirus además que los usuarios desarrollen los hábitos de utilizar contraseñas solidas lo cual mitigara en determinados casos la intrusión de ciberdelincuentes exponiéndose a la fuga de datos.

5.2.4 Interferencia de WiFi. Los dispositivos móviles son tan seguros como la red a través de la cual transmite datos. principalmente donde la mayoría de las personas a nivel mundial están conectados constantemente redes en las cuales no están protegidas de una manera óptima, ya sean que estén en sus hogares o no, nuestra información no está tan protegida como creemos. Según las investigaciones los celulares o dispositivos móviles utilizan wifi casi 3 veces más que los datos de operadoras, y casi 1/4 parte se conectan a redes abiertas donde se exponen.

[52] Ibid.

potencialmente a hackers y Ciberdelincuentes[53], empezando por la actualización de los dispositivos de red inalámbrica que cuenten con la debida actualización en su sistema operativo, mitigando con esto las vulnerabilidades por falta de parches en su actualización, lo que provoca que un ciberdelincuente puede aprovechar esta brecha para ingresar de una manera fraudulenta a los dispositivos que se conectan a la red de quinta generación por medio de un equipo inalámbrico.

5.2.5 Dispositivos obsoletos. Una gran cantidad de dispositivos obsoletos representa un gran riesgo de seguridad empresarial, por lo general los equipos corporativos cuentan con actualizaciones de software oportunas y continuas, pero esto no pasa en el mundo Android, la gran mayoría de fabricantes no son tan eficientes para mantener sus móviles y dispositivos actualizados[54]. Es un gran riesgo lo cual expone a dispositivos móviles obsoletos conectados a la red de quinta generación a ser atacados con malware logrando robar sus datos personales además de contraseñas entre otra información de valor para los ciberdelincuentes.

5.2.6 Higiene deficiente de las contraseñas. La gran mayoría de personas utilizan contraseñas en múltiples cuentas, pero casi 1/3 de personas no utiliza el doble factor de autentificación y solo 1/4 parte de personas lo activa por lo que esto quiere decir que la gran mayoría de personas no tienen contraseñas seguras[55]. Exponiéndose ataque de diccionario descifrando las contraseñas para utilizarlas en los diferentes sitios digitales que utiliza el usuario como lo es en la parte financiera entre otros sitios útiles para los ciberdelincuentes en cuando a fraude.

---

[53] Ibid.

[54] Ibid.

[52] Ibid.

5.2.7 Fraude publicitario móvil. Se estima que en el futuro la publicidad genere millones de dólares en ganancias esto lo saben claramente los ciberdelincuentes y por ello buscan maneras para desviar el dinero hacia fuentes de ingresos publicitarios, este tipo de fraude publicitario tiene varias formas, pero la más común es el malware el cual genera clics en anuncios que parecen provenir de usuarios legítimos logrando su cometido y engañando a la víctima[56].

Por este motivo los dispositivos móviles que no estén preparados para una conexión de quinta generación donde todo va mucho más rápido, puede ser secuestrado en una Bots para ser utilizados involuntariamente para ser parte de estos fraudes publicitarios.

5.2.8 Principales riesgos y amenazas asociados a los dispositivos móviles que se encuentran conectados a una red de quinta generación. Esta quinta generación de redes móviles es una gran oportunidad en cuanto a los avances que contiene y trae a nivel global, el desarrollo de tecnologías como IoT (Internet of Things) tendrá un gran impacto ya que crecerá mucho, hace más de una década empezó su fabricación y finalmente los operadores móviles están implementando 5G.

Esto supondrá la integración de servicios en la red 5G lo que dará lugar a muchos desafíos de seguridad en las redes móviles de quinta generación 5G, es preocupante porque son muchos los aspectos de seguridad que se deben considerar debido a factores como lo son:

- Lectura abierta basada en IP de la 5G.
- Diversidad de las tecnologías de red de acceso subyacente del sistema 5G.

---

[52] Ibid.

- la plétora de dispositivos de comunicación interconectados, que también serán muy móviles y dinámicos.
- La heterogeneidad de los tipos de dispositivos en cuanto solo escena miento energía y memoria.
- Los sistemas operativos de los dispositivos.
- El hecho de que los dispositivos interconectados normalmente van a ser operados por usuarios no profesionales en cuestiones de seguridad.

Por ende, los sistemas de comunicaciones de quinta generación tendrán que abordar amenazas mucho más fuertes que los actuales sistemas de comunicaciones móviles existentes, no se tiene claro que amenazas a futuro serán las más graves, ni que qué elementos de la red serán objeto de mayor atención con el fin de dar garantía y mayor seguridad en las próximas generaciones de sistemas de comunicación móvil[57].

Con la llegada de las redes de quinta generación 5G, se logran identificar diferentes vulnerabilidades a las que algunas de ellas ya son comunes en las redes de cuarta generación 4G, lo que alerta sobre posibles transiciones heredados de vulnerabilidades y riesgos que se deben enfrentar en esta nueva era digital, es muy importante tener en cuenta estas diferentes falencias tecnológicas para en un futuro se mitiguen estos riesgos que amenazan la seguridad de los dispositivos móviles conectados a la red de quinta generación 5G.

5.2.9 Vulnerabilidades de la red de quinta generación. DDoS es el principal ataque hacia las redes 5G, según el informe; autos conectados o sistemas de ciudades inteligentes pueden ser el objetivo de hackers. Así como global de seguridad en telecomunicaciones, divulgó hoy el informe Redes de señalización 5G

[57] GONZÁLEZ. Op. cit.

problemas del pasado que siguen presentes que proporciona una visión general del estado actual de la seguridad en las redes móviles y previsiones para la seguridad de las emergentes redes 5G.

Este es el primero de una serie de cuatro informes sobre seguridad de las telecomunicaciones, que analizará las pruebas de Positive Technologies en las redes SS7, Diameter y GTP, incluyendo detalles de ataques reales realizados por hackers y qué pueden hacer las operadoras para protegerse. De acuerdo con *Positive Technologies*, es necesario revisar algunos conceptos, como que el 5G no será afectado por las vulnerabilidades de seguridad existentes en las redes móviles actuales, por ejemplo. Para mostrar este hecho, el informe expone cuestiones clave, como:

Se puede enfatizar que los riesgos del pasado permanecen presentes, principalmente porque las redes 5G interactúan con otras redes móviles, Giovani Henrique, director general de Positive Technologies para América Latina.

A causa de esta dependencia de la infraestructura heredada, los hackers pueden realizar ataques entre protocolos explorando las vulnerabilidades del Número del sistema de señalización. *Signalling System Number 7* (SS7) y *Diameter*, por ejemplo, como parte de un único ataque. Un ataque a una red de 5ta generación puede comenzar con la exploración de vulnerabilidades en las redes 3G para obtener identificadores de suscriptores *International Mobile Subscriber Identity* (Identidad Internacional del Abonado Móvil) (IMSI), por ejemplo. Es por eso que proteger las generaciones de redes anteriores es crucial para la seguridad 5G. El informe también analiza nuevas amenazas del 5G. Además de los riesgos heredados de las redes anteriores, están surgiendo amenazas adicionales en la vanguardia.

Las investigaciones de seguridad han puesto de manifiesto algunos defectos en este proceso de transferencia y es más que probable que en 2020 seamos testigos de una vulnerabilidad de alta seguridad que permitirá a los atacantes acceder a la voz y/o datos de los teléfonos móviles 5G.

De hecho, gracias a las crecientes necesidades del público de ancho de banda en teléfonos inteligentes y tabletas, una gran parte del tráfico móvil se transfiere a las redes Wi-Fi cercanas para ayudar a igualar la carga. Cuando un dispositivo se encuentra dentro del alcance de un punto de acceso Wi-Fi configurado para él, la conexión cambia a Wi-Fi sin problemas y sin cambios visibles en el dispositivo.
Este proceso ya está ocurriendo hoy en día con el 59% del tráfico de 4G y Cisco predice que lo mismo ocurrirá con el 71% del tráfico de 5G. Esto significa que estas conexiones pueden estar expuestas a ataques Wi-Fi comunes, como el ataque *Evil Twin,* en el que un hacker crea un duplicado de un punto de acceso legítimo y espía los datos de cualquiera que se conecte a él[58].

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), publicó un extenso documento en el que se hace un profundo y exhaustivo diagnóstico de alrededor de 60 amenazas asociadas a las redes de quinta generación, entre los cuales se destacan:
la manipulación de la conexión para controlar los dispositivos ajenos y los accesos, la configuración ilegal de contenido y datos, fraudes múltiples y falsas alarmas, abuso de las interfaces de programación de aplicaciones abiertas, espionaje y robo de información. ENISA

La vulnerabilidad más importante y obvia será la proliferación de puntos finales conectados, comúnmente conocidos como dispositivos IoT (Internet de las cosas),

[58] AEC- ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE CONSULTORÍA. Op. cit.

habilitados por redes 5G. Los tipos de aplicaciones que sirven estos dispositivos van desde ayudarlo a encender o apagar las luces para mantener su hogar seguro. Los dispositivos conectados seguirán estando más interconectados que nunca:

Las cerraduras de puertas inteligentes, los termostatos inteligentes y los automóviles inteligentes representan amenazas para la seguridad física en caso de que sean pirateados por un actor con intenciones maliciosas. Los puntos finales conectados serán cruciales para asegurar, ya que los ciberdelincuentes pueden acceder a la red más amplia a través de puntos finales comprometidos para descubrir e infiltrarse en partes adicionales de la red, incluidos dispositivos IoT conectados adicionales[59].

5.2.10 Riesgos Para La Privacidad. 5G espera que sea el gran canal de comunicaciones de esta década. Todos los datos de redes públicas o privadas podrían acabar utilizando las infraestructuras de comunicaciones de 5G, y ligando esto al incremento de dispositivos conectados hace pensar que en la práctica todas las personas serán usuarios de esa red y todos los dispositivos estarán conectados de forma no exhaustiva y conforme a lo expuesto anteriormente, se pueden identificar al menos los siguientes riesgos para la privacidad de los datos. Muchos de estos riesgos están interrelacionados entre sí y nos son nuevos, sino que estaban presentes con las anteriores generaciones de telefonía móvil, pero pueden verse exponencialmente incrementados son la implantación de 5G alcanza las expectativas de éxito previstas

[59] CHYTRÝ, Filip. 5 vulnerabilidades provocadas por el cambio a redes 5G. [Sitio web]. Avast Blog. 2020. [Consulta: 13 febrero 2021]. Disponible en: https://blog.avast.com/es/5g-network-vulnerabilities-avast

- Geolocalización precisa del usuario: El hecho de que 5G emplee muchas más estaciones base y menos distancia entre ellas, hace que la localización geográfica basada en la red sea mucho más precisa.

- Perfilado y decisiones automatizadas: el incremento en cantidad y en categorías de datos circundando por la red, multiplicado por la cantidad de dispositivos que tendrá cada ciudadano mediante 5G (IoT), va a emitir llegar a una individualización precisa de las personas y el desarrollo de servicios que permitan la toma de decisiones automáticas sobre las personas (IA y servicios en tiempo real).

- Falta un modelo homogéneo de seguridad: al permitir el 5G la existencia de numerosos agentes en la cadena de comunicaciones, incluso dentro de la red Core de los operadores, a través de servicios desplegados por diversos operadores de servicio dentro de los MEC. Cada agente puede cumplir con distintos estándares de seguridad y podrá incluir segmentos que correspondan a protocolos de las primeras generaciones, por lo que la seguridad global será equivalente a la del elemento más débil.

- Aumento exponencial de la superficie de exposición a ciberataques: incremento de servicios, conectividad, interoperabilidad y puntos de entrada y gestión a la red incrementaran las oportunidades de que se materialicen amenazas a la privacidad[60].

[60] AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. Op. cit. p. 9-10.

5.3 ELABORACION DE UN DOCUMENTO SOPORTADO POR LA NORMATIVIDAD Y LOS ESTÁNDARES ESTABLECIDOS EN COLOMBIA, QUE PROPORCIONE RECOMENDACIONES PARA LA MEJORA DE UN ENTORNO DIGITAL SEGURO EN DISPOSITIVOS DE COMUNICACIÓN MOVIL

5.3.1 Documento soportado por la normatividad. Para abordar estas recomendaciones se hace énfasis en la normatividad y los estándares que se han establecido en Colombia para generar recomendaciones en la utilización de un entorno digital seguro en los dispositivos de comunicación móvil, ya que es una de la herramienta más indispensable en la actualidad en lo que a comunicaciones móviles se refiere, buscando proteger al sector público y privado, así como a usuarios de la exposición que se enfrentan en la cuarta revolución industrial 4.0.

5.3.2 Ley 1955 de 2019. En esta ley se busca que Colombia se encarrile a una sociedad digital además de la inclusión de la industria 4.0 por medio de la generación de confianza en la era digital incluyendo las estrategias relacionadas con la seguridad digital enfocadas a las redes de quinta generación 5G. Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 Pacto por Colombia, pacto por la equidad, las TIC se incluyen de manera transversal, dentro del Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento.

5.3.3 Artículo 310 de la Ley 1955 de 2019. Busca afianzar el marco normativo para el despliegue e implementación de las redes de quinta generación 5G articulando la política de trasformación digital a través del Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC). En este artículo 310 de la Ley 1955 del año 2019, se señala, que el Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), les dará prioridad a las iniciativas de acceso público a Internet, beneficiando a la población más pobre y vulnerable, o en lugares

apartados; de igual manera, se podrán adelantar iniciativas de implementación masiva del acceso a Internet con la incorporación del sector privado.

Asimismo, favorecerá a instituciones públicas y establecimientos educativos de carácter nacional y territorial para financiar sus necesidades de conectividad a Internet, y emprenderá iniciativas encaminadas a estimular la oferta y demanda de servicios de telecomunicaciones en beneficio de la ciudadanía. promover el despliegue de redes de acceso y ampliar la cobertura, así como donaciones o subsidios para la prestación de servicios o la provisión de equipos terminales, entre otras actividades.

Además, podrá establecer obligaciones de desempeño como forma económica de pago por el otorgamiento o renovación de licencias de uso del espectro radioeléctrico, a fin de ampliar la calidad, capacidad y cobertura del espectro radioeléctrico de los servicios, en beneficio de la pobre y vulnerable. áreas residenciales o remotas, en escuelas públicas rurales y otras instituciones formales como centros de salud, bibliotecas públicas e instituciones educativas, así como la provisión de subvenciones a redes de emergencia.

En cuanto a la transformación digital pública, se inicia con entidades nacionales en el PND 2018 - 2022, donde estas entidades deben integrar componentes relacionados con tecnologías emergentes, como de desintermediación, *DLT (Distributed Ledger Technology),* analítica de *(Big Data),* Internet de las cosas (IoT), inteligencia artificial (AI), robótica, etc., se definen como los de la cuarta revolución industrial 4.0, facilitando la entrega de servicios del estado por medio de nuevos modelos. En cuanto a las entidades territoriales, pueden determinar estrategias para ciudades y regiones inteligentes.

Asimismo, el gobierno nacional, por medio del Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC), orienta la política de gobierno digital, como política de implementación y gestión institucional, que considerará acciones prioritarias de acuerdo con las directrices y estándares de integración de procedimientos en el portal general del Estado de Colombia. . , la divulgación y uso de datos públicos, la adopción de modelos de ciudades y territorios inteligentes, la optimización de la contratación pública de tecnologías de la información, la provisión y uso de software público, el uso de tecnologías emergentes en el sector público, el aumento de la confianza digital y seguridad, y promoción de la participación y la democracia a través de medios digitales.

5.3.4 Ley 1341 de 2009 en materia del sector de TIC. Esta ley busca que el Estado vele por que cada ciudadano tenga acceso a las tecnologías de la información. La Ley 1341 de año 2009 en materia del sector de TIC, en su artículo 2, inciso 2° determinó que Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional Igualmente, en sus numerales 2 y 8 del artículo 4 de la presente Ley se determinó que, en desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr entre otros los siguientes fines: 1). Promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal. 2). Impulsar la ampliación de la cobertura del servicio.

5.3.5 Numeral 6 del artículo 2 de la Ley 1341 de 2009. En este artículo se sustenta la libre competencia incluyendo los equipos que los diferentes operadores pretendan utilizar para la implementación y despliegue de las tecnologías de quinta generación, siempre y cuando sean amigables con el medio ambiente.

El párrafo 6 del artículo 2 de la Ley 1341 de 2009 adoptó el principio de neutralidad tecnológica, según el cual el Estado asegura, tomando en cuenta las recomendaciones, conceptos y normativas de los organismos internacionales competentes, equitativos y adecuados al respecto, la libertad aplicación de tecnologías que promuevan la competencia libre y leal y la prestación eficiente de servicios, contenidos y aplicaciones utilizando las TIC, en armonía con el desarrollo ambientalmente sustentable.

5.3.6 Artículo 56 de la Ley 1450 de 2011. En esta ley se promueve el libre uso de los servicios de las redes de internet. Asimismo, el artículo 56 de la Ley 1450 de 2011 aplicó el principio de neutralidad de Internet, según el cual, entre otras medidas el derecho de cualquier internauta a no ser bloqueado, interferido, víctima de discriminación o prohibición de uso, envío, recibir o proporcionar cualquier contenido, aplicación o servicio legítimo en Internet, debe proporcionar a cada usuario una conexión o servicio de acceso El acceso a Internet no distingue arbitrariamente contenidos, aplicaciones o servicios, según su origen o su propiedad[61].

5.3.7 Seguridad y protección en las redes de quinta generación. Desde el punto de vista de la seguridad Informática, la especificación de la tecnología incorpora importantes mejoras en las medidas de seguridad respecto a las diversas generaciones anteriores. Tanto en la red de acceso como en la red Core.

Algunas de ellas son:

- Una nueva estructura de identificadores de usuario permanentes y, además

[61] MINTIC. Op.cit. p. 23-24

cifrados para evitar que pueda transmitirse en claro vía radio como ocurrían en determinadas circunstancias con las generaciones anteriores a 5G.

- Mejoras en los mecanismos de autenticación con la introducción de Authentication and Key Management 5G-AKA cuyas principales mejoras son que la red del operador con la que se contrata el servicio (Red Home) es quien autentica al terminal de usuario como a la red donde el móvil pretende conectarse (Red De Servicio), la red de servicio no tiene claves para descifrar las comunicaciones hasta que no ha sido autenticada por la Red *Home*, además cuenta con diferentes mecanismos de control de fraude.

- Datos de usuario protegidos en integridad en la interfaz de radio, adicional a la protección en confidencialidad que ya se proporciona en 4G.

- Posibilitar el acceso desde redes no 3GPP creando un túnel cifrado mediante una clave proporcionada por el operador.

- Cifrado TLS (*Transport Layer Security)* seguridad de la capa de transporte de las comunicaciones entre funciones de red dentro de la red Core.

- Incorporación de opciones de trazabilidad que facilitan el registro de las operaciones para auditar la seguridad de la red.

Estas mejoras a nivel de seguridad suponen un gran avance tanto en la confiabilidad de las comunicaciones aéreas de la red de acceso (Dispositivo de usuario-antena) como dentro de la red Core. Sin embargo, la especificación deja la implementación de alguno de estos mecanismos a criterio del operador, por lo que el incremento de seguridad de las redes 5G puede ser muy distinto entre operadores de telefonía en

función del despliegue de la tecnología afectando las decisiones de un solo actor a la seguridad global de las comunicaciones de redes 5G[62].

En Colombia desde hace algunos años se ha tomado importante el asunto de la Seguridad Informática enfocando en las tecnologías y en los sistemas de información más que en la infraestructura de redes de los proveedores de servicios. Y es allí donde se encuentra una oportunidad semejante a la que están aplicando en Europa y Estados Unidos con el advenimiento de 5G. Inicialmente en julio de 2011 se emitió el documento CONPES 3701 Lineamientos de Política para seguridad y Ciberdefensa, cuyo objeto fue generar lineamientos de política de Seguridad Informática orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.

Así mismo, en abril de 2016 fue aprobado el documento CONPES 3854 Política Nacional De Seguridad Digital el cual busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsara una mayor prosperidad económica y social en el país.

Bajo estos lineamientos el Ministerio de TIC, como ente rector de las industrias TIC en el país, promulgo el modelo de seguridad y Privacidad de la información, que contempla un ciclo de operación de cuatro fases (Planificación, Implementación, Evaluación de Desempeño y Mejoramiento Continuo), las cuales permiten que las entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad

[62] Ibid., p. 9.

de sus activos de información, permitiéndoles determinar las medidas y controles que se deben aplicar para realizar un aseguramiento apropiado de las plataformas así como de los diferentes medios donde se gestione la información, basado en un enfoque de gestión de riesgo. El Modelo de seguridad Y Privacidad de la información junto a las 21 guías de apoyo se encuentra disponible en el siguiente link: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue7275.htm[63].

5.4 REGLAMENTACIÓN PARA 5G Y SU DESPLIEGUE

Para conocer cuáles son las normas que regirán la implementación y despliegue de de las redes de quinta generación, se describirán a continuación cada criterio relacionando su descripción conociendo en que consiste cada uno.

5.4.1 Definir un nuevo modelo de administración de espectro para facilitar y agilizar el despliegue de la tecnología 5G.

El Ministerio de las TIC, con la asesoría técnica de la ANE, definirá y evaluará nuevos modelos de administración de espectro, para la asignación de este recurso, teniendo en cuenta que esta tecnología será demandada por diferentes actores Proveedor de Redes y Servicios de Telecomunicaciones (PRST), academia, empresas de diferentes sectores de la economía, etc. Lo anterior, con el fin de responder, a los avances técnicos y tecnológicos, y a la alta demanda que trae consigo las redes de quinta generación 5G. Esta acción deberá ser finalizada el segundo trimestre de 2021.

5.4.2 Establecer las especificaciones y la calidad que debe brindar el servicio de telecomunicaciones móviles.

Teniendo en cuenta los resultados del diagnóstico de redes móviles actuales elaborado por la Comisión Reguladora de

[63] MINTIC. Op. cit. p. 57-58.

Comunicaciones, esta unidad elaborará un estudio que constituirá la base y el aporte de futuras actualizaciones a los regímenes de calidad. calidad del servicio de telefonía móvil, protección de los usuarios y otros que estime oportunos. Esta actualización tendrá en cuenta que en el ecosistema de la red 5G, los usuarios no son solo humanos, sino también todos los dispositivos IoT, como vehículos, drones, máquinas en general, en cantidad de otros dispositivos. Se espera que este estudio esté terminado para el cuarto trimestre de 2020.

5.4.3 Actualizar y revisar periódicamente los estándares y regulaciones. El Ministerio de Información y Comunicaciones revisará periódicamente la normativa sobre gestión del espectro radioeléctrico para la tecnología 5G y su impacto en la difusión de las redes 5G. Asimismo, el Ministerio de las TIC o su respectiva entidad actualizará la normativa que pueda dificultar o retrasar el despliegue y masificación de la tecnología 5G.

5.4.4 Acelerar el desarrollo de aplicaciones o casos de uso en 5G. El Ministerio de las TIC, a través del programa Apps.co, promoverá el desarrollo de aplicaciones o casos de uso basados en 5G, así como explorará nuevos modelos de negocio que requieran especificaciones técnicas que brinde esta tecnología. Para ello, albergará llamadas a aplicaciones en startups permitiendo la validación de nuevas capacidades e incluyendo velocidades de descarga superiores a 100 Mbps y hasta 20 GBps, baja latencia y alta confiabilidad, favoreciendo áreas como salud, educación y defensa.

5.4.5 Identificar los impulsores de los modelos comerciales exigentes que requieren redes 5G. El Ministerio de las TIC realizará un análisis de esquemas de incentivos para promover el uso y uso de la tecnología 5G, teniendo en cuenta los casos de uso de cada sector industrial. Esta acción se completará para el primer

trimestre de 2021. Con base en lo anterior, el Ministerio de tecnologías de la informa ción y las Comunicaciones diseñará una estrategia para el uso de la tecnología 5G en los sectores manufactureros del país, tanto a nivel nacional como regional, para impulsar la demanda de aplicaciones y servicios que requieren la funcionalidad proporcionada por la tecnología 5G. Esta acción debería completarse en el segundo trimestre de 2021.

5.4.6 Definir lineamientos para el análisis y gestión de riesgos relacionados con la tecnología 5G. Se identificará una línea estratégica enfocada en la infraestructura 5G en el Plan de Zonas de Protección y Defensa para la Infraestructura de la Red de quinta generación 5G Crítica de Colombia - Sector TIC, que permitirá un plan que define lineamientos para la gestión y análisis de riesgos (físicos y lógicos amenazas), la gestión del modelo y los criterios utilizados para aplicar las medidas de seguridad adecuadas. Se tendrá en cuenta que dicha tecnología acelerará la conexión entre los recursos de infraestructura crítica. Esta línea de conducta estará liderada por el Ministerio de Información y Comunicación, con el apoyo del Ministerio de Defensa Nacional.

5.4.7 Acelerar la conexión entre los recursos de infraestructura crítica. Esta línea de conducta estará liderada por el Ministerio de Información y Comunicación, con el apoyo del Ministerio de Defensa Nacional. Promover modelos de gobernanza interna y vigilancia de la seguridad ante las nuevas tecnologías. El Ministerio de Información y las Comunicaciones promoverá modelos de gobernanza interna y vigilancia de la seguridad para el uso racional de las redes 5G. Asimismo, se promoverá la adopción de los marcos regulatorios y sistemas de evaluación que son existentes para la seguridad de los datos y la información. Para ello, tiene en cuenta análisis tecnológicamente neutrales, basados en el riesgo y basados en la evidencia.

5.4.8 Capacitar ciudadanos en el uso adecuado de las nuevas tecnologías. El Ministerio de Información y Comunicaciones organizará jornadas de difusión y formación a personas y entidades públicas sobre cómo utilizar adecuadamente las nuevas tecnologías, principalmente las redes 5G, para mantener la confianza y seguridad en el estado digital. Esta acción comenzará a implementarse en el primer trimestre de 2021[64].

5.4.9 CONPES 3701 (2011). En el año 2011 se elabora el documento CONPES 3701, el cual tiene como objetivo afianzar y fortalecer al estado en capacidad para mitigar las amenazas la parte cibernética, generando de esta manera las condiciones que se necesitan para suplir la protección en el ciberespacio, este documento contiene las estrategias para mitigar las amenazas que interfieren a la seguridad y la defensa del estado que están enfocadas a la ciberseguridad y Ciberdefensa, dando lugar a la creación de centros dedicados a este sector[65].

5.4.10 Ley 1581 del año 2012. Ley 1581 del año 2012. El objetivo de esta ley es impulsar el derecho constitucional que han adquirido todos los ciudadanos, ratificar y actualizar su información de carácter personal, en este mismo aspecto, se ha desarrollado un marco jurídico que contiene el reconocimiento de la información de los datos personales como bien jurídico tutelado[66].

5.4.11 CONPES 3854 (2016). En el año 2016 se elabora el documento CONPES 3854, donde se habla sobre la Política Nacional de Seguridad Digital, su principal objetivo era hacer un fortalecimiento de las capacidades de las diferentes partes de

---

[64] Ibid., p. 71-75.

[65] CONPES 3995. Op. cit. p. 9.

[66] Ibid., p. 11.

interés para gestionar, identificar mitigar y tratar los diferentes riesgos en cuanto a la seguridad digital. Sobre esto, el aporte significativo de esta política fue desarrollar las estrategias que definieron un marco en cuento a la seguridad digital enfocada a la gestión de riesgo de igual manera también dio lugar a la creación de condiciones que admitieran que las diferentes partes de interés hicieran gestión del riesgo en lo concerniente a la seguridad digital, con el fin de hacer más fuerte la seguridad de los usuarios y a su vez la del estado, también la soberanía y defensa nacional en el marco digital[67].

5.4.12 Decreto 1008 publicado en el año 2018. Decreto 1008 publicado en el año 2018, que trata sobre las directrices generales de lo que es la Política de Gobierno Digital. En este decreto se consigna sobre la seguridad de la información, es uno de los elementos principales que dan paso para desarrollar el Gobierno Digital. Adicional a esto, también busca esta política preservar la integridad, disponibilidad, confidencialidad y privacidad de todos los datos, asimismo se incluyó en el Manual de Gobierno Digital, elaborado por el Ministerio de tecnologías de la Información y la Comunicaciones, se estipulan las directrices que deben adoptar el sector público para implementar la Política de Gobierno Digita, además de aplicar el Modelo de Seguridad y Privacidad de la Información[68].

5.4.13 Ley 1955 del 2019. En el año 2019 se publicó la ley 1955 donde se expide el Plan Nacional de Desarrollo 2018-2022 Pacto por Colombia, Pacto por la Equidad. Puntualmente en el capítulo séptimo. Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento, se quiere que Colombia sea encaminado con dirección a que la sociedad sea más digital y en dirección de la Industria 4.0, por medio de las redes

[67] MINTIC. Op.cit. p. 57.

[68] CONPES 3995. Op. cit. p. 11-12.

de Quinta Generación en la parte digital y desarrollo en estrategias enfocada en la seguridad digital en el territorio nacional. Por otro lado, el capítulo referente al Pacto por la legalidad: seguridad efectiva y justicia transparente para que todos vivamos con libertad y en democracia, se define como una opción para suscitar el control integro terrestre, marítimo, fluvial, aéreo ciberespacial y espacial que fortalezca el gobierno nacional robustecer los alcances de Ciberdefensa y ciberseguridad para asegurar lo de interés nacional[69].

5.4.14 Plan TIC 2018-2022 El futuro digital es de todos. Plan TIC 2018-2022 El Futuro Digital es de Todos, con las propuestas del área TIC, diversos de estos están ligados a la seguridad digital, se pueden destacar entre ellos las generaciones con habilidades dirigidas a la igualdad de género, crear e impulsar los emprendimientos femenino, asimismo que fortalecer las capacidades de carácter nacional para promover la transición digital del estado[70]. Para preparase a la llegada de las redes de quinta generación 5G.

5.4.15 CONPES 3795 (2019). Para finalizar en el mes de noviembre del año 2019 se publicó CONPES 3795 Política Nacional para la Transformación Digital e Inteligencia Artificial. La cual tiene como objetivo aportar a la generación de un mayor valor en la economía y la sociedad por medio de la transformación digital en el área del sector privado y público, para que el país logre hacer provecho de las diversas oportunidades y asumir los retos que trae consigo la cuarta revolución industria 4.0, esta política, aparte de ser la que rige los temas sobre la digitalización en el país, también incluye en su accionar, los lineamientos de políticas públicas enfocadas en la ciberseguridad para elevar las capacidades de Colombia sobre el tema. Por medio de esta política es que se puede ver que en el año 2019 es que ha

[69] MINTIC. Op. cit. p. 23.

[70] CONPES 3995. Op. cit. p. 13.

surgido políticas que incluyan de forma más extensa la generación de la confianza digital además de las mejoras en el área de la seguridad digital con la mira a los ciudadanos y otras áreas del país[71].

5.4.16 Recomendaciones. De acuerdo a las normatividades vigentes los entes regulatorios que generan los lineamientos a seguir con el fin de mantener un entorno digital seguro frente a las redes de quinta generación y el desarrollo que esta promueve, es evidente que se tienen muchos aspectos en cuenta para garantizar el uso de esta nueva tecnología de una forma segura, ya que la implementación de la red 5G requiere de un aprendizaje de la utilización de nuevas herramientas tanto para las empresas en el sector público como privado y usuarios finales, es fundamental tener en cuenta algunos aspectos que no menos importante se deben atender según la revisión de los marcos regulatorios de países de primer mudo donde priorizan algunos detalles sobre los equipamientos que se deben revisar.

5.4.17 Implementación de equipos en la red 5G y los operadores. Teniendo en cuenta algunos aspectos los cuales se han divulgado por parte de países que se encuentran con la red 5G ya implementada como lo es Estados Unidos, es necesario tener en cuenta las recomendaciones sobre los microchips que contienen estos equipos que provee el gigante chino de algunas reconocidas marcas como lo son Huawei y ZT, los cuales posiblemente incluyan puertas traseras lo que afecta la seguridad nacional, ya que puede haber fuga de información sensible a estos proveedores, se debe analizar bien los equipos y proveedores que ofrezcan el equipamiento para la infraestructura critica de la red 5G que proveerá de servicio a todos los sectores del país, esto con el fin de mantener un entorno Digital Seguro.

[71] Ibid., p. 13.

5.4.18 Utilización de los dispositivos móviles en las redes de quinta generación. Sobre el uso de estos dispositivos móviles también llamados Smartphone, es importante que los usuarios conozcan el uso de la tecnología antes de comenzar a usar los aplicativos que llegan con la quinta generación de redes, ya que, así como su latencia será mucho más baja y ofrecerá diversos servicios, también aumenta la exposición en la red de cibercriminales que buscan vulnerar la seguridad con diferentes mecanismos y herramientas más efectivas a la hora de hacer un ataque a los teléfonos móviles, por eso se recomienda que por parte del estado colombiano se cree un departamento de soluciones móviles de quinta generación, donde los usuarios tengan acceso a una pronta respuesta cuando sean víctimas de un ciberataque por parte de ciberdelincuentes con el fin de mitigar los daños causados con base a un ataque cibernético.

5.4.19 Reglamentar la gobernanza en el sector privado en la implementación de la red 5G. Es primordial definir en el marco jurídico y regulatorio el modelo de funcionamiento sobre los operadores prestadores de servicio de telecomunicaciones donde se estipulen los acuerdos con el sector privado en el tema de inversión para incentivar a los operadores a invertir en la implementación de la red 5G, pues estas inversiones son muy costosas y sólo con una política clara se puede impulsar de una manera exponencial el despliegue en todo el territorio nacional; con el apoyo del estado en la parte de inversión, es posible incentivar su desarrollo masivo con el fin de abrirse a nuevos mercados en países desarrollados para promover los bienes y servicios basados en una economía digital.

5.4.20 Desarrollo de aplicaciones para el funcionamiento en la red de quinta generación. El programa del Ministerio de Tecnologías de la Información y las Comunicaciones va dirigido a las capacitaciones a muchos colombianos en desarrollo de aplicaciones para afrontar la cuarta revolución industrial, creado por medio del desarrollo de software soluciones a necesidades de los distintos sectores

lo que promete ser una buna política dentro del marco tecnológico, pero así mismo además de crear desarrollo en el área de las tecnologías para ser implementados en diferentes sectores como lo es la parte financiera, comercial, MiPymes, educación, industria entre otros, se debe estudiar detenidamente la solides en materia de seguridad dentro de un entorno digital seguro, ya que estas medidas pueden afectar significativamente estos sectores a los cuales pueden ser expuestos a los cibercriminales por una mala implementación o desarrollo por parte de los creadores de aplicativos y soluciones a estas entidades que se van a enfrentar a un mundo tecnológico con más alcance, más robusto en cuanto a al mercado digital, pero así mismo los atacantes evolucionan rápidamente y los ataques cibernéticos son más sofisticados lo que quiere decir que si un ataque es exitoso, las consecuencias pueden ser devastadoras para la entidad que se comprometida.

6. CONCLUSIONES

- La Seguridad Digital en las redes de quinta generación se debe enfocar en la inversión e implementación y despliegue de la tecnología de redes de quinta generación promoviendo el mercado digital y su desarrollo con base a la confianza de su utilización y la protección de datos de los diferentes usuarios, es necesario fortalecer la propiedad y privacidad de fabricantes en el sector industrial, evaluar con detenimiento los proveedores de los diferentes equipos de esta tecnología para evitar fallos de seguridad referentes a puertas traseras en sus componentes electrónicos que puedan afectar la seguridad nacional y el mercado digital el cual esta será la columna vertebral para su funcionamiento de sectores tales como; transporte, sector financiero, medios de comunicación, sector educativo, sector agro, telemedicina entre otros sectores dependientes de esta prometedor tecnología.

  Todas las medidas de seguridad que la Unión Europea ha evaluado a través de su informe de riesgo son indispensables que los demás países que se unen a este avance tecnológico lo implementen en la evaluación del riesgo que puede tener esta nueva tecnología, si bien es un aporte significativo el desarrollo de diferentes sectores, es importante que los factores de riesgo sean evaluados previamente para mitigar posibles afectaciones a futuro.

  La red 5G asociada a dispositivos de comunicación móvil se vinculan a la cuarta revolución industrial (4.0), debido a que cada vez más, aumenta el uso de dispositivos móviles unificando el comercio electrónico facilitando de esta manera promocionar o adquirir productos y servicios a través del comercio digital el cual es de fácil acceso para los usuarios finales a través de esta herramienta, esto ha masificado el consumo electrónico gracias a la tecnología móvil que avanza a pasos agigantados conectando los diversos mercados con

los consumidores diversificando y promoviendo el desarrollo comercial a través de la tecnología en especial los dispositivos de comunicación móviles.

- Las vulnerabilidades amenazas y riesgos informáticos en las redes 5G son predecibles a través de los diferentes avances tecnológicos de las redes 1G, 2G, 3G, 4G y la más reciente 5G la cual en cada etapa se heredan algunos fallos de seguridad que pueden afectar la nueva era tecnológica, los ataque comunes tradicionalmente conocidos en las redes, se estima que para esta nueva tecnología de la 5G, se identifiquen algunos de ellos como lo son los ataques de Man in The Middle (MiTM), debido a su alta latencia los ataques se pueden intensificar e incluso ejecutarse en menor tiempo que lo tradicional teniendo un mayor alcance por las tazas de velocidad que alcanza esta nueva tecnología.

  Las vulnerabilidades en la red de quinta generación son diversas, entre estas tenemos los ataques de DDoS que se cataloga hasta el momento como el más destacado para afectar eta nueva tecnología, debido al aumento de las conexiones Wireless se estima que se pueden ver afectadas por algunas vulnerabilidades conocidas como el ataque Evil Twin, que consiste en crear un duplicado de un punto de red real para vulnerar los datos que se envían por esta conexión. Asimismo, la red 5G impulsa el crecimiento del Internet de las cosas IoT, estos dispositivos contienen deficiencia de seguridad en sus códigos de configuración con el que interactúan con otros dispositivos inteligentes conectados a la red, lo que representa un peligro para la implementación en los hogares estos equipos como, por ejemplo; colocar las cerraduras basados en esta tecnología.

- Se busca realizar un documento soportado por las normatividades expedidas por los entes de control en el sector de las Telecomunicaciones con el fin de

garantizar el uso seguro de las tecnologías actuales y venideras en este caso las redes de quinta generación, se busca fortalecer bajo las normas gubernamentales los parámetros normativos que protejan al usuario de ciertas vulnerabilidades en el mundo digital, teniendo como base las leyes, normas y reglamentaciones orientadas a mantener un entorno digital seguro al momento de utilizar las tecnologías ya sea en un entorno corporativo o de usuarios finales.

En busca de una organización jurídica, se ha creado la Ley 1955 de 2019 quien se enfoca en la era digital con la llegada de la cuarta revolución industrial 4.0, buscando fortalecer la sociedad en un mundo digital encaminado a la seguridad con la nueva tecnología de las redes de quinta generación, involucrando a los sectores de; Gobierno, empresas y hogares conectados en el tiempo del conocimiento a través de las tecnologías. En la presente ley en el Artículo 310. Se pretende definir el marco de la norma para la implementación y despliegue de las redes de quinta generación afianzando la política de transformación digital por medio del Ministerio de Tecnologías de la Información y las Comunicaciones.

La seguridad y protección en las redes de quinta generación desde la una perspectiva de la seguridad informática la nueva tecnología de 5G incorpora importantes mejoras respecto a las generaciones anteriores. Algunas e ellas son: identificación de usuarios permanente, cifrado en la transferencia de mensajes, mecanismos de autenticación más robustos incorporando Authentication and Key Agreement 5G-AKA, protección de los datos en integridad, cifrado. *Transport Layer Security (TLS)* dentro de la red Core. Estas por mencionar algunas, pero existen muchas más, esto también puede variar de acuerdo al operador como proveedor del servicio ya que dependiendo de este pueden implementar diferentes medidas de seguridad para los diferentes usuarios de la red.

7. RECOMENDACIONES

Tener presente el impacto en todas las áreas que impactara las redes de quinta generación y la importancia de su desarrollo en todos los niveles, pero teniendo en cuenta un aspecto muy importante que es la seguridad informática como pilar fundamental de esta nueva tecnología que llega para cambiar el mundo, debido al aumento a la conectividad masificada de dispositivos móviles las vulnerabilidades a las que se enfrenta esta nueva era de la tecnología se hacen más extensos los riesgos para los usuarios finales como para grandes y medianas empresas que incorporan a sus nuevas funcionalidades tecnología de última generación.

Es por esto que se deben crear marcos regulatorios que delimiten y creen nuevas conductos de manipulación y uso de la información en los aplicativos en las comunicaciones móviles, ya que si bien la cuarta revolución industrial aporta grandes avances significativos en los diferentes sectores de la industria y sector tecnológico es fundamental contar con normas que marquen el camino sobre la seguridad que se debe adoptar en el uso de las telecomunicaciones las cuales permiten avanzar de una manera agigantada.

Es importante conocer y aprender de los países que son potencia los cuales ya están haciendo uso de la red de quinta generación mostrando diferentes aspectos en cuanto a la globalización e interconexión de las telecomunicaciones y los beneficios que trae ser líder de esta última tecnología, es fundamental que en los países latinoamericanos se tomen como ejemplo las diferentes medidas de seguridad tanto en los operadores de esta red como los usuarios que hacen uso de esta, asimismo en Colombia el ministerio de las telecomunicaciones ha publicado ciertas normas las cuales son de gran utilidad ya que marcan la pauta sobre los cuidados y usos de esta nueva tecnología que se debe adoptar pero con normas establecidas que protejan la interoperabilidad de las redes haciendo alianzas en

sector público con el privado bajo normas que favorezcan el crecimiento y avance de las nuevas oportunidades que se avecinan basadas en las redes de quinta generación (5G).

BIBLIOGRAFÍA

AEC- ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE CONSULTORÍA. Las vulnerabilidades 5G quedarán expuestas en 2020. [Sitio web]. Grupo Atico34. Madrid. 2019. [Consulta: 06 mayo 2021]. Disponible en: https://aecconsultoras.com/noticias-sectoriales/las-vulnerabilidades-5g-quedaran-expuestas-en-2020/

AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. Introducción a las tecnologías 5G y sus riesgos para la privacidad. [Sitio web]. AEPD. Madrid, 2020. 13p. [Consulta: 5 mayo 2021]. Disponible en: https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5g.pdf

ARAMILLO, Néstor, et al. Tecnología 5G. Vol. 4. Núm. 8. Bogotá: 2017. 43 p. Consultado en: DOI: http://dx.doi.org/10.21017/rimci.2017.v4.n8.a31

ARTEAGA, Félix. La UE ya tiene una evaluación de los riesgos 5G (ahora falta tomar medidas). Madrid: Ed. Real Instituto Elcano. 2019. 2 p.

BAIG, Edward C. Qué son las redes inalámbricas 5G y de gigabit. [En línea]. Hogar y Familia Tecnología Personal. Washington: AARP. 2020. [Consulta: 15 marzo 2021]. Disponible en: https://www.aarp.org/espanol/hogar-familia/tecnologia/info-2020/que-son-las-redes-inalambricas-5g.html

CHYTRÝ, Filip. 5 vulnerabilidades provocadas por el cambio a redes 5G. [Sitio web]. Avast Blog. 2020. [Consulta: 13 febrero 2021]. Disponible en: https://blog.avast.com/es/5g-network-vulnerabilities-avast

CIO MÉXICO. Ocho amenazas preocupantes para la seguridad móvil. [Sitio web]. México: CIO. [Consulta: 13 de septiembre 2021]. Disponible en: https://cio.com.mx/ocho-amenazas-preocupantes-para-la-seguridad-movil/

COMISIÓN EUROPEA. Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE. [Sitio web]. Bruselas, 2020. [Consulta: 15 marzo 2021]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?from=FR&uri=CELEX%3A52020DC0050

CONPES 3995. Política Nacional de Confianza y Seguridad Digital. Bogotá D.C.: Departamento Nacional de Planeación, Ministerio de Tecnologías de la Información y las Comunicaciones, Departamento Administrativo de la Presidencia de la República, 2020. 51p.

CORZO, German D. y ALVAREZ-AROS, Erick L. Estrategias de competitividad tecnológica en la conectividad móvil y las comunicaciones de la industria 4.0 en Latinoamérica. [Base de datos en línea]. Diciembre 2020. Revista Información Tecnológica, 3 (6), 183-192. [Fecha de consulta: 18 febrero 2021]. Disponible en: https://scielo.conicyt.cl/pdf/infotec/v31n6/0718-0764-infotec-31-06-183.pdf

El despliegue de las redes 5G, o la geopolítica digital [en Línea]. Madrid España: Real Instituto Elcano, 2019. [Fecha de consulta: 23 noviembre 2021]. Disponible en: https://www.realinstitutoelcano.org/analisis/el-despliegue-de-las-redes-5g-o-la-geopolitica-digital/

GONZÁLEZ, Yolanda. Tecnología 5G, Características, usos y posibles peligros. [Sitio web]. Grupo Atico34. Madrid. 2020. [Consulta: 10 mayo 2021]. Disponible en: https://protecciondatos-lopd.com/empresas/tecnologia-5g/

GONZÁLEZ CALLEJAS, Rafael. Implementación De Movilidad En Redes 5G. Granada: 2017 81 p.

GUEVARA CÓRDOBA, Fabián Andrés. Comparativo entre la tecnología de redes 4G y 5G y los beneficios de su implementación en Colombia. Santiago de Cali: 2018. 27 p.

JARAMILLO, Néstor, OCHOA, Páez, William y PEÑA, Alexander, Stephanie. Tecnología 5G. [Base de datos en línea]. Julio 05 de 2017. Revista Ingeniería, Matemáticas y Ciencias de la Información, 4 (8), 41-48. [Fecha de consulta: 05 febrero 2021]. Disponible en: http://ojs.urepublicana.edu.co/index.php/ingenieria/article/view/394/347

LÓPEZ MARTÍN, Tatiana y HERNÁNDEZ, Karol Violeta. El Contrato de Seguro Cibernético. Trabajo de grado de Abogado. Bogotá D.C.: Universidad Santo Tomás. Facultad de Derecho. 2020, 38p.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES MINTIC. Plan 5G Colombia El Futuro Digital es de Todos. Bogotá D.C.: 2019. 57 p.

MORET MILLÁS, Vicente. El despliegue de las redes 5G, o la geopolítica digital. [Base de datos en línea]. Marzo 12 de 2019. Revista Real Instituto Elcano, 1-6. [Fecha de consulta: en 08 de marzo 2021]. Disponible en http://www.realinstitutoelcano.org/wps/wcm/connect/1c87499a-f0df-4d11-bc4f-c40d30138fb3/ARI31-2019-Moret-despliegue-de-redes-5G-geopolitica-digital.pdf?MOD=AJPERES&CACHEID=1c87499a-f0df-4d11-bc4f-c40d30138fb3

MORET MILLÁS, Vicente. El despliegue de las redes 5G, o la geopolítica digital. Madrid: Ed. Real Instituto Elcano. 2019 3 p.

PIGHIN, Valentina. Nuevos desafíos de las redes 5G en Europa. Colombia. Ed. Universidad del Rosario: 2020 3 p.

PUERTO SUÁREZ, lorena lucía. Estudio De Prospectiva En El Uso De La Tecnología 5g En Colombia Al 2025. Colombia. Ed. Universidad Santo Tomas: 2017. 35 p.

RODRÍGUEZ RONCANCIO, Iván Orlando. Nuevos Desafíos En Seguridad Para 5G. Colombia: Ed. Universidad ECCI: 2019. 9 p.

SIERRA ROJAS, Juan Pablo. 5G, la gran apuesta de Colombia a la era digital. Bogotá: Ed. Universidad Militar Nueva Granada. 2020. 5 p.

SOTELO MONGE, Marco Antonio, et al. Marco para el Análisis e Inferencia de Conocimiento en Redes 5G. Valencia: Ed. Jitel: 2017 3 p.

TECHECETERA; 5G: historia y algunas verdades; [Sitio web]. [Consulta: 20 de octubre 2021]. Disponible en: https://techcetera.co/historia-y-verdades-acerca-del-5g/

ULLOA SALTOS, Andrea Carmen. Estudio De La Tecnología 5g Y El Impacto Que Tendrá En El País. Guayaquil – Ecuador: 2018. 41 p.

VEGA BENAVIDEZ, Adriana Marcela. Industria 4.0 en los países desarrollados y países de Latinoamérica. Trabajo de grado de Administrador de Empresas. Santiago de Cali: Universidad Cooperativa de Colombia. Facultad de Ciencias Administrativas, Económicas y Contables. 2021. 77 p.

Fecha de Realización:	22/Mayo/2022
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Infraestructura Tecnológica y Seguridad en Redes
Título:	REDES DE QUINTA GENERACIÓN: ESTÁNDARES Y NORMATIVAS QUE CONTRIBUYEN EN LA CONSOLIDACIÓN DE UN ENTORNO DIGITAL SEGURO EN EL USO DE DISPOSITIVOS DE COMUNICACIÓN MÓVIL EN COLOMBIA
Autor(es):	Tirado Romero Roberto Agustín, Romero Morera John Willmar
Palabras Claves:	Redes 5G, Comunicaciones Móviles, Seguridad Digital, Normatividad, Revolución Industrial 4.0
Descripción:	Este proyecto trata acerca de las redes de quinta generación 5G y las posibles vulnerabilidades, riesgos y amenazas que trae esta tecnología, además de conocer el estado de implementación a nivel global y los posibles riesgos que se enfrentan en la era digital y el comercio electrónico que genera esta innovación tecnológica, conocer los avances a nivel de América Latina y que tanto ha avanzado Colombia en esta transformación de tecnología que promete cambios significativos en diversos sectores industriales y económicos.
Fuentes bibliográficas destacadas:	

AEC- ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE CONSULTORÍA. Las vulnerabilidades 5G quedarán expuestas en 2020. [Sitio web]. Grupo Atico34. Madrid. 2019. [Consulta: 06 mayo 2021]. Disponible en: https://aecconsultoras.com/noticias-sectoriales/las-vulnerabilidades-5g-quedaran-expuestas-en-2020/

AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. Introducción a las tecnologías 5G y sus riesgos para la privacidad. [Sitio web]. AEPD. Madrid, 2020. 13p. [Consulta: 5 mayo 2021]. Disponible en: https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5g.pdf

BAIG, Edward C. Qué son las redes inalámbricas 5G y de gigabit. [En línea]. Hogar y Familia Tecnología Personal. Washington: AARP. 2020. [Consulta: 15 marzo 2021]. Disponible en: https://www.aarp.org/espanol/hogar-familia/tecnologia/info-2020/que-son-las-redes-inalambricas-5g.html

CHYTRÝ, Filip. 5 vulnerabilidades provocadas por el cambio a redes 5G. [Sitio web]. Avast Blog. 2020. [Consulta: 13 febrero 2021]. Disponible en: https://blog.avast.com/es/5g-network-vulnerabilities-avast

CIO MÉXICO. Ocho amenazas preocupantes para la seguridad móvil. [Sitio web]. México: CIO. [Consulta: 13 de septiembre 2021]. Disponible en: https://cio.com.mx/ocho-amenazas-preocupantes-para-la-seguridad-movil/

COMISIÓN EUROPEA. Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE. [Sitio web]. Bruselas, 2020. [Consulta: 15 marzo 2021].

Contenido del documento:	Este documento está estructurado de acuerdo a un planteamiento de problema, desarrollo de cada uno de los tres objetivos planteados que busca comprender de desde una perspectiva objetiva la seguridad en los entornos digitales y comunicaciones móviles, así como el comercio electronico, las medidas de seguridad que se deben tener en cuenta a la hora de utilizar la nueva tecnología de la red 5G, conclusiones y recomendaciones sobre los diferentes temas estudiados.
Conceptos adquiridos:	Entorno digital seguro, seguridad en las redes de quinta generación, Higiene de contraseñas, Alianzas del sector público privado para la implementación de la red 5G.
Conclusiones:	La Seguridad Digital en las redes de quinta generación se debe enfocar en la inversión e implementación y despliegue de la tecnología de redes de quinta generación promoviendo el mercado digital y su desarrollo con base a la confianza de su utilización y la protección de datos de los diferentes usuarios, es necesario fortalecer la propiedad y privacidad de fabricantes en el sector industrial, evaluar con detenimiento los proveedores de los diferentes equipos de esta tecnología para evitar fallos de seguridad referentes a puertas traseras en sus componentes electrónicos que puedan afectar la seguridad nacional y el mercado digital el

	cual esta será la columna vertebral para su funcionamiento de sectores. Las vulnerabilidades amenazas y riesgos informáticos en las redes 5G son predecibles a través de los diferentes avances tecnologicos de las redes 1G, 2G, 3G, 4G y la más reciente 5G la cual en cada etapa se heredan algunos fallos de seguridad que pueden afectar la nueva era tecnológica, los ataques comunes tradicionalmente conocidos en las redes, se estima que, para esta nueva tecnología de la 5G, se identifiquen algunos de ellos como lo son los ataques de Man in The Middle (MiTM). La seguridad y protección en las redes de quinta generación desde la una perspectiva de la seguridad informática la nueva tecnología de 5G incorpora importantes mejoras respecto a las generaciones anteriores. Algunas de ellas son: identificación de ususarios permanente, cifrado en la transferencia de mensajes, mecanismos de autenticación más robustos incorporando Authentication and Key Agreement 5G-AKA, protección de los datos en integridad, cifrado. Transport Layer Security (TLS).