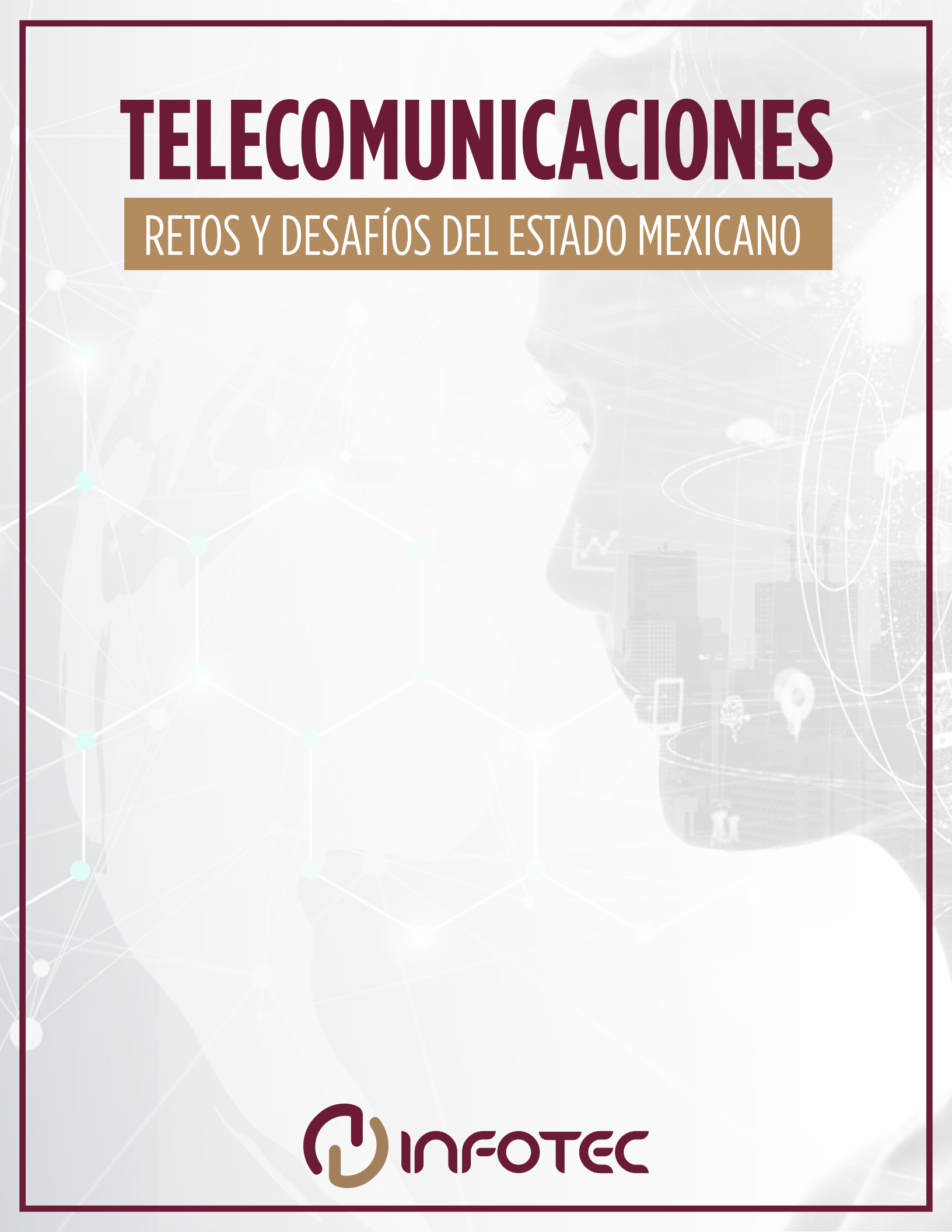
TELECOMUNICACIONES

RETOS Y DESAFÍOS DEL ESTADO MEXICANO



INFOTEC

TELECOMUNICACIONES: RETOS Y DESAFÍOS DEL ESTADO MEXICANO

Vanessa DÍAZ RODRÍGUEZ
Paulina Elisa LAGUNES NAVARRO
COORDINADORAS

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
MÉXICO, 2024

INFOTEC

Dirección Ejecutiva
Mtro. Federico C. González Waite

Dirección Adjunta de Administración
Lic. Karen Hortensia Gutiérrez Torres

Dirección Adjunta de Innovación y Conocimiento
Mtro. Carlos Josué Lavandeira Portillo

Dirección Adjunta de Administración de Proyectos
Lic. Claudio Morán Ponce

Dirección Adjunta de Competitividad
Mtro. Jesús Ríos Magos

Dirección Adjunta de Desarrollo Tecnológico
Ing. Eustasio Sánchez Montesinos

Dirección Adjunta de Asuntos Jurídicos
Mtro. Luis Mercurio Pérez Contreras

Asistencia editorial
Mtra. Julieta Alcibar Hermosillo

Diseño y maquetación
Lic. Luis David Olivares Lozano

Primera edición: Mayo, 2024
ISBN: 978-607-7763-31-4

Av. San Fernando No. 37 Colonia Toriello Guerra Delegación Tlalpan, C.P. 14050, México, CDMX.

México, 2024
www.infotec.mx

ÍNDICE

DRA. VANESSA DÍAZ RODRÍGUEZ

DOCTORA EN DERECHO POR LA UNIVERSIDAD DE TASMANIA (AUSTRALIA), MAESTRA EN DERECHO POR LA UNIVERSIDAD ANÁHUAC DEL SUR.

Estudió la Licenciatura en Derecho en la Universidad del Pedregal. Realizó un Diplomado en Derecho Comparado de la Información por la Universidad de Oxford (Inglaterra). Estuvo adscrita al Instituto de Investigaciones Jurídicas de la UNAM de 2000 a 2018. Se desempeñó como titular en la Jefatura de Departamento de Asesoría y Registro de Organizaciones Ciudadanas en el Instituto Electoral de la Ciudad de México de 2019 a mediados de 2020. Fue investigadora en el INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. Actualmente, se desempeña como profesional operativo en la Suprema Corte de Justicia de la Nación.

Se especializa en temas de biometría digital, neuroderechos, ciberseguridad, telecomunicaciones, drones, trans-post-anti-metahumanismo, mecanismos de participación ciudadana, acceso a la información y protección de datos personales con Nuevas Tecnologías de Información y Comunicación. Fue integrante del Comité Académico de Diseño (CAD) del Examen para la Certificación como Oficial de Protección de Datos Personales de los Sujetos Obligados en el Ámbito Federal, por parte del INAI y del CENEVAL, en julio de 2023. Ha participado como miembro de Jurado del Premio de Innovación y Buenas Prácticas en la Protección de Datos Personales 2020, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales 2020, así como Jurado en el Concurso de Ensayo 2019, Instituto Electoral de la Ciudad de México, agosto 2019.

Ha obtenido los siguientes premios y distinciones: Premio "Writing Up Fellowship" del Institute for the Study of Social Change", de la Facultad de Artes, agosto 2014; Distinción "Neasey"; Distinción "Andrew Inglis Clark in Law and History"; Premio "McDougall Postgraduate Scholarship" todos de la Facultad de Derecho, de la Universidad de Tasmania, marzo 2011.
Es miembro fundador de DH Painal Media; asociada del Instituto Nacional de Administración Pública (INAP), miembro de International Media Law Advocates y Media Law Advocates Programme, ambos del Centro de Estudios Socio-Jurídicos de la Universidad de Oxford, Inglaterra.

Se destaca su participación en el "Primer Seminario Regional sobre el Papel de la Industria Química e Industrias Afines en la Aplicación de la Convención sobre las Armas Químicas en América Latina y el Caribe", organizado por la Secretaría de Relaciones Exteriores (SRE) y la Organización para la Prohibición de las Armas Químicas (OPCW) en 2003. Colaboró dentro del marco del proyecto "Implementación de las Recomendaciones Derivadas del Diagnóstico sobre la Situación de los Derechos Humanos en México" organizado por la Oficina en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH) con el apoyo de la Comisión Europea en el 2007.

Así como su participación en la Reunión de Expertos de América Latina en Acceso a la Información y Derecho a la Verdad organizado por la Relatoría Especial de la Organización de Naciones Unidas para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, bajo los auspicios de la Oficina en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH) con apoyo de la Open Society Foundation, 2013.

Por lo que respecta a productividad académica ha dictado numerosas conferencias como ponente –tanto a nivel nacional como internacional-; ha moderado y coordinado varias mesas de trabajo y paneles; ha publicado 5 libros en coautoría, 44 capítulos en libros, 10 artículos en revistas científicas, 7 reseñas y 4 traducciones. También ha publicado 20 artículos de difusión.

DRA. PAULINA ELISA LAGUNES NAVARRO

DOCTORA EN DERECHO POR EL PROGRAMA DE DOCTORADO EN DERECHO POR LA UNIVERSIDAD CRISTÓBAL COLÓN Y EL INSTITUTO DE INVESTIGACIONES JURÍDICAS DE LA UNAM.

Actualmente se desempeña como investigadora del programa de Derecho de las Tecnologías de la Información y Comunicación en INFOTEC.

En su experiencia docente, ha impartido clases en licenciatura y maestría en los estados de Veracruz y Ciudad de México. De igual forma, ha estado participando en cursos sobre temas de educación y TIC; niños, niñas y adolescentes en entornos digitales, entre otros.

En el 2019, se certificó en el "Estándar de Competencia Diseño de cursos de capacitación para ser impartidos mediante Internet", por el Consejo Nacional de Normalización y Certificación de Competencias Laborales.

En el 2018, fue revisora de programas académicos de nivel superior. Así mismo, asesoró en la iniciativa relativa a datos genéticos.

Ha participado en 9 congresos como ponente (tanto a nivel nacional como internacional); así como, moderando y organizando diversos eventos académicos.

Su línea de investigación es: Bioderecho y derecho ambiental. Sus temas de interés son: Regulación de OGMs, Biotecnología, seguridad alimentaria, agricultura y TIC; datos genéticos, derecho y nuevas tecnologías; educación y TIC.

INTRODUCCIÓN

Esta obra es resultado del 1er Congreso Nacional de Telecomunicaciones: Retos y Desaf²os del Estado mexicano, celebrado los d²as 19 al 21 de abril de 2022, por INFOTEC Centro de Investigaci· n e Innovaci· n en Tecnolog²as de la Informaci· n y Comunicaci· n. Por lo que, es una colaboraci· n entre diversas personas expertas en Tecnolog²as de la Informaci· n y Comunicaci· n relacionadas al §rea de las telecomunicaciones.

En este sentido, se recopilan diversas contribuciones acad®micas las cuales se clasifican en tres secciones: I) Sustentabilidad, innovaci· n y conectividad; II) Regulaci· n e innovaci· n, y III) Infraestructura y ciberseguridad.

En el cap²tulo *La sostenibilidad como estrategia tecnológica*, redactado por Nora del Carmen Osuna Mill§n, Hilda Beatriz Ram²rez Moreno y Virginia Berenice Niebla Zatarain, se visibiliza c· mo el uso ineficaz de las Tecnolog²as de la Informaci· n y Comunicaci· n (TIC) tiene un impacto ambiental; por lo que proponen, a trav®s de la responsabilidad social, acciones sobre el uso sostenible de estas, pero para ello, las empresas deben considerar diversos factores, tales como: bienestar de las personas empleadas, calidad del producto, el origen de sus insumos, el alcance de sus actividades y deshechos en el §mbito ambiental.

En el cap²tulo referente a *Derechos humanos, inteligencia artificial y gobernanza: retos de la era digital*, elaborado por Jes¼s Manuel Niebla Zatarain, se se¶ala que el avance tecnol· gico ha generado la necesidad de contar con herramientas que sean capaces de procesar grandes vol¼menes de datos y de ah² la importancia de la Inteligencia Artificial (IA), la cual tiene varios retos en materia jur²dica y ®tica.

En el cap²tulo *Regulación de redes sociales con perspectiva de género y de derechos humanos*, la propuesta de Maricela Hazel Pacheco Pazos y Alejandro Francisco Herr§n Aguirre, se centra en la importancia de regular las redes sociales desde la perspectiva de g®nero y derechos humanos, toda vez que en ellas se lleva a cabo la interacci· n entre personas de diversos or²genes, sin embargo, se hace especial ®nfasis en las personas integrantes de los

grupos vulnerables, las cuales pueden ser susceptibles de alguna transgresión a sus derechos en el entorno digital.

Por lo que respecta al capítulo sobre *Aspectos regulatorios de 5G. Derecho a la salud, medio ambiente, protección de datos personales y ciberseguridad*, Marco Antonio Vega Servín hace manifiesta el área de oportunidad para regular la tecnología 5G, la cual puede ser empleada en diversos sectores pero que sin una estrategia óptima podría traer impactos negativos a los derechos de las personas en materia de salud, medio ambiente y protección de datos personales. En consecuencia, la persona autora realiza un análisis de los instrumentos jurídicos nacionales e internacionales en materia de esta tecnología.

Por su parte, Aida Huerta Barrientos y César Martín Rodríguez argumentan en el capítulo *Compartición de infraestructura para la conectividad universal*, que un área de oportunidad radica en la adecuación de los modelos de negocios de los servicios de telecomunicaciones dado que se recomienda la inclusión de la compartición de infraestructura con el propósito de optimizar los costos de sus redes. Así, las personas autoras presentan una propuesta encaminada a la infraestructura asociada a la red carretera y a la red ferroviaria bajo el fin de lograr las metas trazadas en el Programa de Cobertura Social del Gobierno Federal Mexicano.

En el capítulo *Experiencias en la gestión de activos físicos. Caso: redes de cómputo corporativo en una firma de manufactura* de Adrián López Martínez, realiza una breve exposición sobre la gestión estratégica de los activos tecnológicos en una empresa, por lo que, a lo largo del documento la persona autora analiza los principios y desarrolla una propuesta sobre la misma.

En el capítulo de *Ciberseguridad en las instituciones de educación superior*, Juan José López Ávila e Irma Pérez Hernández reflexionan sobre la importancia de la introducción a la cultura de la ciberseguridad en las instituciones de educación superior; por lo que, discuten sobre diversos casos en la materia; así como, instrumentos jurídicos y estándares internacionales.

En el capítulo Retos *de ciberseguridad para México*, elaborado por Salim Daniel Sigales Montes, se realiza una reflexión sobre los retos que tiene el Estado mexicano en materia de ciberseguridad; por lo que, se observa la necesidad de capacitar a los sectores en este tenor para prevenir alguna vulneración cibernética.

Con base en lo anterior, se desprende que esta obra representa la culminación de un gran esfuerzo por parte del Maestro Federico C. González Waite, Director Ejecutivo del INFOTEC, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, por su cuidadosa organización que redunda en su impecable realización.

Vanessa DÍAZ RODRÍGUEZ
Paulina Elisa LAGUNES NAVARRO
COORDINADORAS

PARTE I:
SUSTENTABILIDAD, INNOVACIÓN Y CONECTIVIDAD

DERECHOS HUMANOS, INTELIGENCIA ARTIFICIAL Y GOBERNANZA: RETOS DE LA ERA DIGITAL

Jesús Manuel NIEBLA ZATARAIN[4]
Paola Jackeline ONTIVEROS VÁZQUEZ[5]

[4]Profesor investigador de tiempo completo de la Facultad de Derecho Mazatlán perteneciente a la Universidad Autónoma de Sinaloa. Doctor en Derecho por la Universidad de Edimburgo, Escocia, Reino Unido, en el área de Inteligencia Artificial aplicada al Derecho. Esta colaboración forma parte del proyecto Inteligencia artificial legal para la regulación de entornos digitales" con clave PRO_A6_015 del programa PROFAPI de la Universidad Autónoma de Sinaloa. j.niebla@uas.edu.mx.
[5]Profesora adscrita al Posgrado de Derecho en la Universidad Nacional Autónoma de México, correo electrónico: paolaontiveros@hotmail.com ORCID ID: 0000-0003-1460-7914.

DERECHOS HUMANOS, INTELIGENCIA ARTIFICIAL Y GOBERNANZA: RETOS DE LA ERA DIGITAL

Resumen

La tecnología digital se ha convertido en un elemento relevante para el sector jurídico particularmente, desde el advenimiento del Internet. Ante esto, el modelo tradicional de aplicación de la ley resulta ineficaz para brindar un nivel adecuado de protección tanto a usuarios como proveedores de servicios específicamente, desde los derechos humanos. Como parte de esto, la presente colaboración señala la factibilidad de dotar a la Inteligencia Artificial como componente tecnológico presente en este entorno con la capacidad de adecuar su operación acorde al marco jurídico aplicable. Paralelamente, esto dará pie al fortalecimiento de la gobernanza a través de medios digitales.

Palabras clave: inteligencia artificial, derechos humanos, gobernanza.

Abstract

Digital technology has become a relevant element for the legal sector, particularly since the advent of the internet. Given this, the traditional model of law enforcement is ineffective to provide an adequate level of protection to both users and service providers specifically, from the perspective Human Rights. As part of this, this collaboration points out the feasibility of providing artificial intelligence as a technological component present in this environment with the ability to adapt its operation according to the applicable legal framework. In parallel, this will lead to the strengthening of governance through digital media.

Keywords: *artificial intelligence, human rights, governance.*

I. Introducción

La tecnología digital desarrollada a partir de la segunda mitad de la década de 1990 ha tenido un efecto particular en el derecho. En este sentido, es posible señalar la migración de diversos actos jurídicamente hacia este tipo de entornos, siendo la principal, el Internet. Esto ha generado la necesidad de contar con herramientas que permitan procesar grandes volúmenes de información generados por dicho

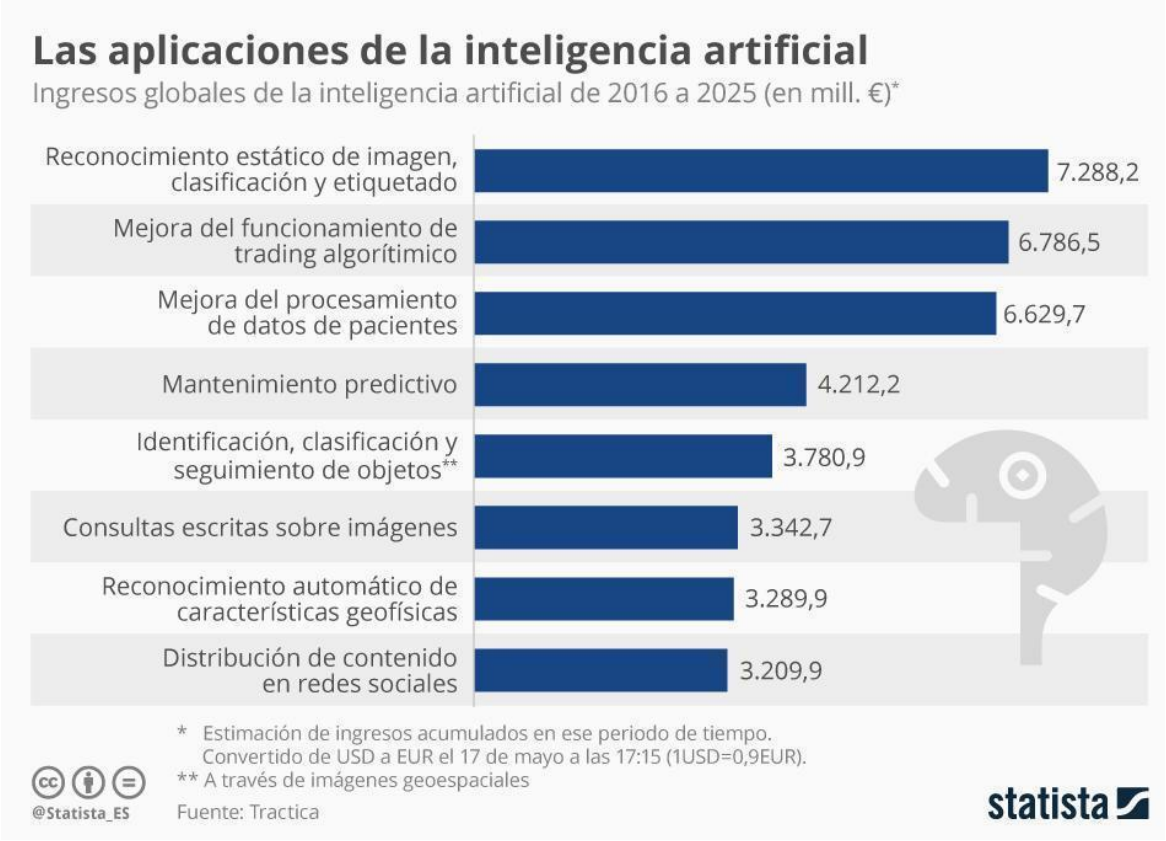
fenómeno, es aquí donde surge la Inteligencia Artificial como herramienta no solamente de procesamiento, sino capaz de brindar compatibilidad jurídica a este entorno. Esta colaboración abordará este escenario desde la perspectiva del sector público como usuario de tecnología inteligente, abordando los potenciales riesgos que su implementación puede ocasionar a la esfera jurídica de los gobernados desde la perspectiva de los derechos humanos.

II. La Inteligencia Artificial y el derecho: las primeras interacciones

La Inteligencia Artificial (IA) es el estudio de los procesos cognitivos utilizando marcos conceptuales y herramientas computacionales (Kok et al., 2009). Este sector emergió como un área independiente de la ciencia computacional tradicional, hacia la segunda mitad del siglo XX. Hacia 1968 Marvin Minsky, uno de los fundadores de la IA, propuso una de las definiciones más importantes, abordándola como "la ciencia de hacer que las máquinas realicen cosas que requerirían de inteligencia si las hiciera el hombre ". Eventualmente, la IA comenzó a diseminarse en diversas áreas, como es el caso particular de las matemáticas, particularmente la resolución de problemas de cálculo, ajedrez, comprender cuentos cortos, desarrollo de obras literarias, aprender nuevos conceptos, interpretar escenas visuales, razonamiento por casos y razonar por analogía, todos ellos, con la característica de requerir aspectos cognitivos como parte de su operación.

De manera general, es posible señalar que la investigación relativa a la IA presenta como objetivos, la comprensión de los procesos que conforman las diversas arquitecturas de razonamiento que influyen en el desarrollo y la implementación de dichos dispositivos a escenarios concretos de la misma manera que lo haría la inteligencia humana.

Hacia 2017, las principales tendencias de Inteligencia Artificial eran las siguientes (Statista, 2017):



Dicha tendencia, la cual ha variado según la participación de nuevos sectores industriales y la cada vez mayor adopción de esta tecnología por sectores tradicionales, permite ilustrar la relevancia que el desarrollo de dispositivos inteligentes tiene tanto para el mercado digital como para el ámbito social. Esto ha generado la tendencia de abordar la Inteligencia Artificial como plataforma para representar intereses convergentes que van más allá de los aspectos técnicos tradicionales.

En el contexto jurídico, estos dos objetivos tienen como finalidad comprender aspectos clave del razonamiento legal y el desarrollo de herramientas computacionales útiles para el ejercicio profesional, la enseñanza o la investigación del derecho. Lo anterior puede abordarse a través del desarrollo de un modelo de IA para el razonamiento jurídico basado en doctrinas precedentes. Aquí, el desarrollo de un módulo jurídico cognitivo resulta el componente central para la operación de estos dispositivos la cual opera procesando decisiones jurídicas existentes aplicables a un caso en particular. De no encontrar precedentes aplicables, el sistema es capaz de realizar construcciones propias y generar respuestas basados en procesos cognitivos independientes, cuyos resultados serán integrados a la base de datos para accederlos de ser necesarios en el futuro.

Como parte del sector computacional, la IA se encuentra en constante innovación particularmente en lo relativo al manejo y procesamiento de datos y estadística. La llegada y diseminación del Internet (Vivant, 2017) ha generado un nuevo interés en el aspecto jurídico de la IA, toda vez que el procesamiento de datos personales supone la necesidad de operar bajo las especificaciones señaladas por la ley. Esto significa el alejamiento de la doctrina tradicional *ex-post* la cual señala la ejecución de las consecuencias jurídicas una vez cometido un acto contrario al marco normativo, en favor de una *ex-ante*, la cual busca prevenir la generación de consecuencias jurídicas a través de la operación ética-jurídica de esta tecnología.

III. La expresión lógica jurídica y su expresión a través de Inteligencia Artificial

Sudden (2018) señala como formas de interacción entre el derecho y la IA las siguientes: el objetivo detrás la lógica, la representación de reglas y la expresión de conocimiento como área de la IA (Shoham, 2015) es el modelado de fenómenos o procesos del mundo real en una forma en que las computadoras los puedan utilizar, normalmente con fines de automatización (Surden, 2011). La mayoría de las ocasiones, esto significa que los desarrolladores crean una serie de reglas para representar la lógica relativa a la expresión cognitiva del área del conocimiento a modelar para fines de automatización. De manera relevante, la practicidad de estos dispositivos es proporcional a la complejidad de las reglas del conocimiento sobre las cuales operan, lo cual se traduce en la aplicación de un modelo de razonamiento deductivo. Esto conlleva al principio generalmente aceptado que indica que mientras mejor esté delimitada el área de operación, mayor será la efectividad operativa de dichos dispositivos.

Consecuentemente, la representación de conocimiento es uno de los campos de investigación más relevantes en la Inteligencia Artificial, habiendo generado un vasto volumen de implementaciones exitosas, las cuales no solamente reflejan su plausibilidad operativa, sino su capacidad para mejorar el desempeño de un sector en particular. En este sentido, una de las primeras contribuciones exitosas son los denominados sistemas expertos (Susskind, 1986). Aquí, los programadores interactúan con expertos en un campo de conocimiento en particular, traduciendo expresiones lógicas inherentes a un área del conocimiento para después analizar la factibilidad de traducirlos a lenguaje computacional. Regularmente, los diseñadores intentan traducir el conocimiento de los expertos en una serie de reglas y estructuras formales las cuales representan un fenómeno particular y escenarios derivados de éste. Una vez concluidos dichos procesos, un sistema experto puede operar con una precisión equiparable a un experto humano.

En términos generales, los métodos de inteligencia artificial basados en el conocimiento, la lógica y las reglas de representación deben verse complementadas con la delimitación del escenario donde habrán de operar. Esto da lugar al desarrollo

de un modelo computacional más eficiente en términos jurídicos y computacionales y con menor tendencia a producir errores. Lo anterior significa que los programadores deben proporcionar al dispositivo todas sus reglas de funcionamiento y decisión. No obstante, la eficiencia de esta propuesta, esta contrasta con enfoques de última generación basados en métodos estadísticos, particularmente el aprendizaje automático (*machine learning*) el cual opera a través de una metodología de abajo hacia arriba (*top-down*). Aquí, el algoritmo determina orgánicamente sus reglas de funcionamiento bajo criterios propios (Surden, 2011), lo que lo convierte en una propuesta sumamente eficiente en términos de manejo de recursos operativos y aproximaciones de certeza.

Existen algunas consideraciones de los sistemas basados en representación del conocimiento que vale la pena mencionar, una vez que las reglas del área donde habrá de operar el dispositivo son representadas en lenguaje computacional, este puede manipularlas por medio de cadenas deductivas para construir conclusiones sobre dicho entorno. Lo anterior permite que estos sistemas puedan combinar hechos sobre el mundo, utilizando reglas lógicas, para informar a los usuarios sobre fenómenos poco frecuentes o difíciles de detectar como lo son contradicciones discernir (De Marneffe et al, 2008).

Consecuentemente, los sistemas de IA basados en reglas requieren de un desarrollo basado en las particularidades inherentes del escenario donde habrán de operar. No obstante, su capacidad por emular los métodos de razonamiento implementado por operadores humanos, este enfoque es considerado innecesariamente lento debido al volumen de recursos que requiere para operar, lo que a su vez limita de manera considerable su implementación en entornos operativos reales, particularmente en entornos digitales. En lo relativo a la implementación de estos desarrollos en el derecho, fueron pioneros en la colaboración entre la ciencia jurídica y la IA, atendiendo las primeras interacciones entre ambas áreas. De igual forma, brindaron aprendizajes que impactaron de manera positiva esta relación al hacer evidente que la adopción de esta tecnología no dependía del grado de precisión en la representación del conocimiento (Sajja y Akerkar, 2010), sino del grado de asertividad con la que estos dispositivos generarán respuestas a problemas jurídicos concretos. En la siguiente sección se abordará esta postura, a través del método estadístico denominado aprendizaje automático.

III.I. Aprendizaje automático

Este término refiere a un conjunto de técnicas de IA las cuales comparten características en común, principalmente de corte estadístico (Fumo, 2017). En esencia, estos métodos operan detectando patrones preestablecidos considerados relevantes en grandes cúmulos de datos (Mitchell, 1999). El área de implementación de esta técnica abarca prácticamente la totalidad de los sectores donde puede ser

implementada la IA, desde dispositivos inteligentes desarrollados para escenarios jurídicos, como conducir un automóvil inteligente (Marr, 2016).

El aprendizaje automático no es un enfoque basado solamente en lenguaje computacional, refiere a una amplia categoría de técnicas que abarcan diversos enfoques computacionales. Como parte de estas destacan las redes neuronales de aprendizaje profundo, clasificador bayesiano ingenuo, regresión logística y bosques aleatorios, entre otras (Sidana, 2017). Este es el enfoque predominante en la IA en la actualidad, el cual prevé estrategias de aprendizaje que distan de los métodos tradicionales contenidos en el aprendizaje basado en reglas. El aprendizaje automático cuenta con la capacidad de "aprender" en el sentido de que también pueden mejorar su desempeño a lo largo del tiempo, examinando volúmenes de datos cada vez mayores y detectando patrones, los cuales mejoran el proceso de creación de decisiones automatizadas. En este sentido, Surden (2014) establece una serie de escenarios donde la implementación de este enfoque estadístico (Surden, 2014) brinda resultados jurídicamente relevantes a escenarios dinámicos, los cuales presentan las mismas características operativas de los enfoques de IA tradicional. En este sentido, el derecho por ser un sistema de reglas las cuales activan consecuencias jurídicas según determinados supuestos, resulta ser un área natural para el desarrollo de modelos analíticos computacionales (Hoeschl y Barcellos, 2004). Entre las características que el campo jurídico ofrece a la IA destacan los siguientes (Hoeschl y Barcellos, 2004):

1. Razonamiento jurídico basado en reglas, casos, jurisprudencias y principios (Surden, 2014).
2. La jurisprudencia está basada bajo un principio de razonamiento estandarizado.
3. Conocimiento jurídico especializado, como casos y reglas procedimentales, las cuales se encuentra debidamente documentadas y en gran volumen.
4. El derecho es introspectivo y autocrítico, cuenta con sus propios métodos para examinar sus procesos y suposiciones.
5. La naturaleza de las respuestas jurídicas en la ley difiere de otras disciplinas: estas dependerán en gran medida del escenario y pueden variar conforme el paso del tiempo.
6. El conocimiento implementado en el razonamiento jurídico es diverso, yendo desde el sentido común hasta el conocimiento especializado, variando su estructura, carácter y uso.

La aplicación de este enfoque permite la inserción de dispositivos inteligentes en entornos dinámicos socialmente relevantes. De igual forma, cuenta con la capacidad de operar en grupos, bajo objetivos particulares y a través de esquemas que permiten compartir los resultados jurídicos construidos a la colectividad a la cual pertenece.

Una de las áreas de aplicación más importante de esta tecnología es el sector público. Presentado como una respuesta derivada del problema de la sobre burocratización de procesos administrativos, la Inteligencia Artificial ha colaborado en el rediseño operativo de este sector. Esto ha traído efectos positivos paralelos derivados de la mejora en la calidad del servicio público, dando lugar al acercamiento entre la ciudadanía y el sector público para la discusión e implementación de políticas públicas. No obstante, existen prejuicios sobre la Inteligencia Artificial derivados de su operación, los cuales pueden llegar a producir afectaciones a la esfera jurídica de sus usuarios. Esto habrá de ser abordado a profundidad en la sección posterior.

IV. Riesgos de la Inteligencia Artificial

Al hablar de la aplicación de la Inteligencia Artificial en el sector público, surge diversas dudas relativas al nivel de fiabilidad inherente a esta tecnología, como es el caso puntual de la parcialidad sobre la cual opera (Pasquale, 2015). En este sentido, diversos estudios han demostrado que, elementos tales como raza, antecedentes e incluso sector social han resultado factores que terminan por influir la operación de determinados sistemas inteligentes. Esto ha generado preocupación e incluso, ha ocasionado que el diseño operativo de algoritmos implementados en sectores clave como es la aplicación de justicia, sean revisados y su operación sea puesta en duda. Como parte de esto, el rol al que esta tecnología aspiraba fue, en el mejor de los casos limitada, toda vez que resultó evidente que la construcción de sus resultados distaba de reflejar la realidad del entorno social en el cual operaba.

En este sentido, Virginia Eubanks (2018) señala que diversos sectores públicos alrededor del mundo implementan tecnología inteligente para vigilar e incluso infligir efectos negativos en contra de grupos marginados. Dicha autora señala que en los Estados Unidos esta tecnología está encaminada principalmente a los sectores económicos más bajos y que, por ende, requieren apoyo gubernamental. De igual forma, Eubanks señala que la *Allegheny Family Screening Tool* (Herramienta de Estudio de Familias de Allegheny, en español) un sistema operado por la Oficina para la Niñez, Juventud y Familias de dicho condado, para prever y evaluar potenciales situaciones de abuso ha tenido efectos que podrían considerarse no del todo positivos, llegando a ocasionar que los operadores humanos cuestionen sus propias decisiones. Este escenario ilustra como la sobre dependencia de una plataforma, puede ocasionar una tendencia negativa en la forma en cómo se atienden determinadas situaciones. Aunado a lo anterior, este sistema tiene la capacidad de anular las decisiones emitidas por los trabajadores de dicha dependencia, imponer las propias y solicitar una investigación que aclare la operación del funcionario. Las fallas de este dispositivo resultan evidentes: su base

operativa consiste particularmente, de información de familias en estado de pobreza lo que hace que sean su principal sector operativo (Eubanks, 2018).

En lo que refiere a otros países, la misma problemática es perceptible. En el caso particular de China, existen diversos algoritmos encaminados a clasificar a la población según características particulares que puedan convertirlos en "problemáticos". Esta clasificación es diversa y no sigue necesariamente patrones establecidos en occidente, tal es el caso del Sistema de Crédito Chino, el cual recopila información de los ciudadanos de dicho país asiático y los evalúa según su nivel de confianza social la cual es definida por el mismo gobierno de este país. Esta plataforma incluye elementos punitivos, como es el desplegar la imagen de los deudores en pantallas gigantes en las principales ciudades, así como, en el transporte público y eventos multitudinarios, bajo el término "deudor" (Hong, 2015).

Otro escenario relevante, donde la tecnología inteligente es utilizada en perjuicio de la ciudadanía es Sudáfrica. Este escenario resulta particular, ya que, dichos algoritmos son previstos de información generada por medio de procesos pseudocientíficos basados en elementos racionales, los cuales generan estrategias de control y limitan el desarrollo de los sectores impactados. De manera paralela, es posible señalar cómo incluso en áreas de bajo impacto como simples procesos burocráticos, estos desarrollos han limitado la capacidad de realizarlos y en algunos casos, impedirlos.

Una primera postura con respecto a Sudáfrica, es que dichos desarrollos no son generados por el sector público, sino que, son adquisiciones obtenidas del sector privado. Esto ha permitido que en una primera instancia estas no contaran con la interpretación de elementos jurídicos que evitaran dicha forma de operación (Naciones Unidas, 1989).

Lo anterior abre la discusión a un punto fundamental en la adopción de tecnología inteligente por el sector público la debida discriminación de información.

IV.I. La ética, la IA y la convergencia con el derecho en el sector público

La convergencia entre la tecnología inteligente y el derecho resulta particularmente relevante no solamente por su complejidad, sino por el alto volumen de escenarios donde estas pueden gestarse. De manera particular, la implementación de estos desarrollos por parte del sector público genera la preocupación por la eventual vulnerabilidad que puede presentar la esfera jurídica de los gobernados especialmente los derechos humanos. En este sentido, existe el debate constante sobre cómo deben implementarse de manera efectiva en aquellos escenarios relativos a entornos digitales. Entre estos ordenamientos, destaca la Declaración Universal de Derechos Humanos (DUDH) y el Pacto Internacional de Derechos Civiles y Políticos, así como, los numerosos instrumentos jurídicos internacionales y regionales, en los cuales el principal objeto de discusión es la adecuación del derecho hacia el entorno digital.

Sin embargo, es cada vez más frecuente el uso de IA por parte de las fuerzas del orden público y otros sectores gubernamentales, como un enfoque que permite atender escenarios digitales idealmente, por medio de un enfoque ético (Waller y Waller, 2020). Le ética es un tema complejo y depende en gran medida posturas filosóficas o variaciones sociales contextuales (Asaro, 2019). Esto hace que su inclusión como componente activo en esta tecnología sea complejo, atendiendo a posturas particulares que, si bien permitan su funcionamiento legítimo, no deben sacrificar su capacidad operativa.

En contraposición a la postura relativa a la aplicación de justicia, el sector administrativo ha visto dicha operación con un área factible de incrementar la calidad de su operación a través de la IA.

IV.II. Hacia un procesamiento ético de la información en autómatas para el sector público

Para el 2018, en el Foro Económico Internacional se discutía la importancia de establecer parámetros operativos que garantizaran el legítima procesamiento de información por medio de autómatas (World Economic Forum, 2018). Este reporte señaló la importancia de mantener los derechos humanos como núcleo operativo de esta tecnología (World Economic Forum, 2018):

> Incluso cuando no hay intención de discriminar, los sistemas de AA [aprendizaje automático] cuyo éxito se mide estrictamente en términos de eficiencia y beneficios pueden terminar consiguiéndolos a expensas de la responsabilidad de la empresa de respetar los derechos humanos.

Este reporte reconoce la ya mencionada necesidad de establecer parámetros de desarrollo de Inteligencia Artificial cuyo núcleo sean los derechos humanos. No obstante, cuenta con una particularidad, llama al establecimiento de normatividad y figuras de responsabilidad que acrediten la indebida participación del desarrollador en esta tecnología y resulte jurídicamente responsable.

Hacia el mismo año, surge la propuesta denominada como *The Toronto Declaration: Protecting the Rights to Equality and Non-Discrimination in Machine Learning Systems* (La Declaración de Toronto: Protección de los Derechos de Igualdad y No Discriminación en Sistemas de Aprendizaje Automático, en español). Este documento, generado por un sector de la comunidad de desarrollo de inteligencia artificial, se descarta por el reconocimiento de los potenciales riesgos que esta tecnología puede llegar a suponer a la sociedad, llama al uso ético de esta tecnología y al acercamiento del sector jurídico con el tecnológico para crear estrategias preventivas y en su caso punitivas para los efectos perjudiciales de esta tecnología.

Otro escenario relevante, es aquel enfocado a la participación política. Como parte de esto, el Instituto Brookings ha señalado (Polyakova y Boyer, 2018): “los avances en Inteligencia Artificial y capacidades cibernéticas abrirán oportunidades para que los actores maliciosos socaven las democracias de manera más encubierta y efectiva que lo que hemos visto hasta ahora”. Este escenario ha quedado demostrado en diversas campañas políticas alrededor del mundo. De manera particular, la participación de esta tecnología en los comicios del Reino Unido, donde fue implementada para cambiar la postura de sectores tradicionales de votantes por medio del uso de *bots.* La arquitectura operativa de estos desarrollos está basada en el comportamiento e interacciones humanas tradicionales, lo cual incrementa la dificultad de detectarlos a la par de que facilita el esparcimiento de información falsa sobre temas sensibles, las denominadas *fake news.* De manera relevante, el impacto de esta tecnología se ve incrementada por la factibilidad de operar a través de servicios digitales como es el caso de redes sociales, tales como *Facebook o Twitter* (Swaine, 2018). Esto ha generado un nuevo enfoque a la controversia derivada de la responsabilidad que guardan los administradores de estos servicios ya que, en situaciones como en las abordadas ante el Senado de los Estados Unidos por Zuckerberg, se hace evidente el impacto que estos sistemas han tenido en diversos procesos electorales (Transcript of Mark Zuckerberg’s Senate hearing, 2018).

Lo anterior terminó por ilustrar el peligro potencial que esta tecnología supone para la participación y autodeterminación política, así como, la equidad de participación en materia pública por parte de un sector de la ciudadanía. Desde la sola perspectiva de los derechos humanos, la utilización no ética de la inteligencia artificial supone un riesgo que debe ser atendido tanto desde la perspectiva jurídico-tecnológica como la cultural. Esta última hace necesario el desarrollar estrategias de conciencia y entendimiento de los riesgos inherentes que el uso de la tecnología inteligente supone para los ciudadanos. Esto permitirá que el nivel de éxito de este tipo de estrategias se vea reducido considerablemente.

La privacidad y el uso legítimo de datos personales es un elemento de suma importancia al señalar la relación entre derechos humanos y tecnología inteligente. Un escenario particularmente relevante, es el derivado de un proyecto llevado a cabo por la Universidad de Stanford con la finalidad de predecir la orientación sexual de individuos a través de la recolección de imágenes obtenidas de sitios de citas web (Wang y Kosinski, 2018). Aunado a la complejidad y del sentido amoral que este proyecto supone, el principal riesgo resulta evidente al poder abordar elementos de la vida íntima de los ciudadanos a través del procesamiento de información. Esto resulta particularmente relevante para aquellos sectores quienes habitan bajo regímenes que puede utilizar dicha información para campañas de opresión y segregación (Penagos, 2018). Otro proyecto relevante es el de reconocimiento facial basado en una Inteligencia Artificial desarrollada por Amazon.

Los resultados obtenidos por este desarrollo fueron controversiales desde inicio. Desde la perspectiva computacional, mostró un considerable nivel de certeza. No obstante, mostró indicios controversiales al proveer disposiciones raciales y hacia sectores considerados en estado de vulnerabilidad económica y social. La preocupación ante las implicaciones de este desarrollo se incrementó tras ser adquirido por diversos departamentos de policía en Estados Unidos (Snow, 2018).

Una de las propuestas de mayor relevancia es el incluir al elemento ético como componente de diseño en un dispositivo inteligente. Esta propuesta ha sido desarrollada por la Unión Europea y para noviembre de 2021 se presentó un documento en el cual se abordan seis principios éticos que cualquier sistema de Inteligencia Artificial debe contener para preservar y proteger los derechos contenidos en la Carta de Derechos Fundamentales de la Unión Europea, estos son (Comisión Europea, 2021):

1. Respeto a la autonomía humana: cada humano debe contar con la libertad de tomar sus propias decisiones y llevar a cabo sus propias acciones.
2. Privacidad y gobernanza de datos: los individuos deben de contar con privacidad y protección de datos y estos deben ser respetados en todo momento.
3. Justicia: las personas deben recibir las mismas oportunidades y no deben recibir ninguna ventaja o desventaja inmerecidamente.
4. Bienestar ambiental, individual y social: los sistemas de Inteligencia Artificial deben ser capaces de contribuir y no dañar el bienestar del individuo, la sociedad y del entorno.
5. Transparencia: el propósito, aporte y operación de los sistemas de Inteligencia Artificial deben ser del conocimiento de los individuos, así como, deben ser entendibles para las partes interesadas.
6. Rendición de cuentas y supervisión: los humanos deben ser capaces de entender, supervisar y controlar el diseño y operación de los sistemas basados en Inteligencia Artificial; y los actores que participan en su desarrollo y operación deben ser responsables de la forma en que estas aplicaciones funcionan y por las consecuencias resultantes.

Estos principios tienen el objetivo principal de garantizar el derecho a vivir una vida plena en la cual puedan aspirar a satisfacer sus propias necesidades y deseos a través del respeto mutuo. Como reconocimiento a dicho derecho y a manera de contribución, se reconoce la necesidad de desarrollar instituciones que permiten la consecución de dichos objetivos, como es el caso de salud, educación y cultura, las cuales se verían particularmente beneficiadas de la adopción de dichos principios por parte del sector de desarrollo.

La libertad de expresión es otro derecho humano que se ve afectado por el uso de tecnología inteligente. Al igual que la participación política, la libertad de expresión puede verse influida gracias al uso de tecnología inteligente. En 2014, un

estudio demostró la plausibilidad de un fenómeno de contagio a través de redes sociales. Los investigadores manipularon la experiencia de uso de casi 700 000 usuarios de Facebook (hoy *Meta*) a través del uso de herramientas para detectar comentarios negativos o positivos de diversas personas o incluso de contactos dentro de la red. Una vez analizado el contenido de dichos mensajes, se removieron aquellos de carácter negativo. Esto produjo que el tiempo dedicado a este servicio se incrementara e incluso, participaran de manera más frecuente en dicha plataforma (Kramer et al, 2014).

De igual manera, al convertirse las redes sociales en el principal centro de discusión política en los últimos años, ha surgido el debate relativo a la necesidad de establecer pautas de moderación de contenido (Napoli y Caplan, 2017).

Con la proliferación de discursos de odio, noticias falsas y el ya reconocido fenómeno de manipulación mediática en redes sociales establecidas como *Facebook* y *Twitter*, el sector legislativo y el público en general demandan acciones inmediatas de control y moderación efectivas. Esto tiene la finalidad de establecer barreras claras, concisas y operantes para la libertad de expresión en redes sociales y que su ejercicio se vuelva parte del debido desarrollo del individuo y no una herramienta para la diseminación de ideas en este entorno.

Consecuentemente, el desarrollo de esta tecnología debe dejar de ser percibida como un proceso exclusivo del ámbito computacional, para dar paso a la incorporación de elementos de carácter social y jurídico. Esto, con la finalidad de crear implementaciones compatibles con los principios éticos mencionados, la dinámica social del entorno y que operen con un rango mínimo de perjuicios para sus usuarios.

IV.III Convergencia entre la gobernanza y los derechos humanos: el caso particular de México

El ejercicio de la administración pública depende de la interacción entre el sector gubernamental con la ciudadanía, lo cual conlleva la relación con los derechos humanos. En el caso particular de México, dichas prerrogativas se encuentran contenidas en la Constitución Política y se extienden a cualquier individuo por el simple hecho de encontrarse dentro de la jurisdicción mexicana.

En lo que respecta a las relaciones surgidas a través de medios digitales, estas también se ven reguladas por los derechos humanos reconocidos por el Estado Mexicano, convirtiéndose entonces en una extensión del mismo. De manera particular, al abordar elementos tales como la libertad de expresión y de acceso a la información, la Constitución Política de México en su artículo 6to párrafo I, II y III señala:

> “La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.
> Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.
> El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios”.

Este artículo resulta relevante para el entorno digital, ya que, dichas plataformas se han convertido en un punto de encuentro para la presentación, debate e intercambio de ideas entre usuarios sobre diversos tópicos. En este sentido, el marco normativo mexicano establece las facilidades que el Estado debe brindar para que este se lleve de manera adecuada, sin lesionar intereses de terceros y sin influir en la gestación de ideas ni opiniones propias de sus ciudadanos en cualquier ámbito. De igual forma, resulta el pilar para la colaboración entre el sector público y el privado la cual se ha visto incrementada desde el advenimiento de la revolución digital resultando particularmente perceptible desde la óptica de las políticas públicas.

Como tal, es importante señalar la necesidad establecer medidas de contenido, las cuales son herramientas necesarias para garantizar el debido ejercicio de estos derechos. No obstante, su gestión e implementación es objeto de debate, ya que, no existe una postura general pues dependen de la arquitectura particular de cada plataforma de servicio.

Lo anterior, se ve complementado con el contenido del artículo 7° del máximo ordenamiento jurídico mexicano, el cual señala en su primer párrafo:

> “Es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio. No se puede restringir este derecho por vías o medios indirectos, tales como el abuso de controles oficiales o particulares, de papel para periódicos, de frecuencias radioeléctricas o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios y

> tecnologías de la información y comunicación encaminados a impedir la transmisión y circulación de ideas y opiniones".

En lo relativo a la privacidad, la Constitución Política de México la prevé en el artículo 16 párrafos I y II, al señalar:

> "Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo. Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".

Dichos preceptos establecen el reconocimiento y protección de la intimidad de los ciudadanos, los cuales tienen como objetivo fundamental el libre desarrollo del individuo y permiten la debida interacción con los órganos públicos, y este no podrá intervenir sin que exista causa que justifique dicha acción.

V. Conclusiones

El derecho se encuentra en un estado de franca evolución como resultado directo de la revolución digital y la consecuente diseminación de las Tecnologías de la Comunicación y de la Información (TIC). En este escenario, las plataformas digitales se han convertido en el nuevo entorno de convergencia donde tanto usuarios particulares como entes gubernamentales celebran actos que deben ser regulados jurídicamente. No obstante, el avance computacional implica la inclusión de nuevos medios técnicos para un manejo más eficiente de la información los cuales llegan a ser incompatibles con la ley. En este sentido, la adopción de tecnología inteligente representa esta dicotomía: por una parte, permite el debido manejo de grandes volúmenes de datos de manera eficiente y a través de esquemas que implementen la ley aplicable, mientras que, por otra, presenta riesgos tanto jurídicos como éticos tanto para usuarios como para operadores.

Consecuentemente, este escenario requiere la adopción de medidas particulares de naturaleza convergente: incluir elementos éticos-jurídicos como componentes propios de la arquitectura computacional. No obstante, dicha propuesta contrasta con la postura del sector de desarrollo, ya que, su adopción implica la reducción de la eficiencia operativa de estos dispositivos en pro de procesos que garanticen su debido funcionamiento. Como parte de lo anterior, el desarrollo de diversos marcos normativos se ha visto complementado con diversas estrategias complementarias que incentivan la inclusión de dichos componentes a la estructura computacional. Esto ha dado lugar a que sectores tradicionales poco tendientes a la adopción de tecnología inteligente, comiencen a considerar estas plataformas para la gestión de información, siendo uno de los casos más importantes el del sector público.

Los procesos administrativos gubernamentales representan una de las áreas de aplicación más importantes para la Inteligencia Artificial. Esta tecnología brinda la capacidad de eliminar diversos vicios burocráticos y elevar la calidad de la prestación de servicios públicos, lo impacta de manera directa en la percepción y colaboración de la ciudadanía. Sin embargo, resulta fundamental que los principios éticos-jurídicos ya mencionados se vuelvan un elemento obligatorio en los desarrollos inteligentes orientados a este sector. Si bien esto no es una solución definitiva, disminuiría de manera considerable el riesgo de ser afectado por perjuicios ocasionados por esta tecnología y al mismo tiempo, elevaría la confianza al operar bajo esquemas que repliquen marcos jurídicos fundamentales, como son los derechos humanos.

VI. Bibliografía

Hong, Kevin. (21 de octubre de 2017). *“Big Brother Is Watching: How China Is Compiling Computer Ratings on All Its Citizens”.* https://www.scmp.com/news/china/policies-politics/article/1882533/big-brother-watching-how-china-compiling-computer.

“CCPR General Comment No. 18: Non-Discrimination”. (10 de noviembre de 1989). UN Human Rights Committee (HRC). Disponible en: http://www.refworld.org/docid/453883fa8.html.

“The Toronto Declaration: Protecting the Rights to Equality and Non-Discrimination in Machine Learning systems”. (mayo de 2018). https://www.accessnow.org/cms/assets/uploads/2018/05/Toron-to-Declaration-D0V2.pdf.

Allegheny County. https://www.alleghenycounty.us/Human-Services/News-Events/Accomplishments/Allegheny-Family-Screening-Tool.aspx.

Asaro, Peter M. (2019). *AI ethics in predictive policing: From models of threat to an ethics of care*. IEEE Technology and Society Magazine 38, no. 2, p. 40-53.

Comisión Europea. (2021). *Ethics By Design and Ethics of Use Approaches for Artificial Intelligence.* Research Ethics and Integrity Sector, (pág. 5).

De Marneffe, M. C., Rafferty, A. N., & Manning, C. D. (2008). Finding contradictions in text. *In Proceedings of ACL-08: HLT*, p. 1039-1047.

Eubanks, Virginia (2018). *Automating Inequality.* St. Martin's Press.

Fumo, D. (2017). Types of machine learning algorithms you should know. *Towards Data Science, Towards Data Science*, *15*.

Hoeschl, H. C., & Barcellos, V. (2004). Artificial intelligence and law. In *IFIP International Conference on Artificial Intelligence Applications and Innovations.* (pp. 25-34). Springer, Boston, MA.

How to Prevent Discriminatory Outcomes in Machine Learning. World Economic Forum, March 12, 2018, http://www3.weforum.org/docs/WEF_40065_White_Paper_How_to_Prevent_Discrimina-tory_Outcomes_in_Machine_Learning.pdf.

Kok, Joost N., E. J. Boers, Walter A. Kosters, Peter Van der Putten y Mannes Poel. (2009). *Artificial intelligence: definition, trends, techniques, and cases*. Artificial intelligence*,* 1, 1-20.

Kramer, A. D., Guillory, J. E., & Hancock, J. T., (2014). *Experimental Evidence of Massive-Scale Emotional Conta-gion Through Social Networks*. PNAS vol. 111 no. 24.

Marr, Bernard. (2016). *The Top 10 AI and machine learning use cases everyone should know about*." *Forbes*. Disponible en: https://www.forbes.com/sites/bernardmarr/2016/09/30/what-are-the-top-10-use-cases-for-machine-learning-and-ai/.

Mitchell, T. M. (1999). Machine learning and data mining. *Communications of the ACM*, *42*(11) (pp. 30-36).

Naciones Unidas *CCPR General Comment No. 18: Non-Discrimination*". UN Human Rights Committee (HRC), 10 de noviembre de 1989. Disponible en: http://www.refworld.org/docid/453883fa8.html. Accesado por última vez el 18 de abril de 2023.

Napoli, Philip M. y Caplan, Robyn. (2017). "*Why Media Companies Insist They're Not Media Companies. Why They're Wrong, and Why It Matters. First Monday* vol. 22, no. 5.

Pasquale, Frank. (2015). *Black Box Society.* Cambridge, Harvard University Press.

Penagos, Melanie. (2018). "AI Systems and Research Revealing Sexual Orientation Case Study," *AI and Human Rights Workshop, Data & Society Research Institute*, April 26-27, Disponible en: https://datasociety.net/wp-content/uploads/2018/05/AI-Sys-tems-and-Research-Revealing-Sexual-Orientation_Case-Study_Final_CC.pdf.

Polyakova, Alina y Boyer, Spencer P. (2018). *The Future of Political Warefare: Russia, the West, and the Coming Age of Global Digital Competition*.5,

Brookings. Disponible en: https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf. Accesado por última vez el 18 de abril de 2023.

Sajja, P. S., & Akerkar, R. (2010). Knowledge-based systems for development. *Advanced Knowledge Based Systems: Model, Applications & Research*, *1*, 1-11.

Shoham, Y. (2015). Why knowledge representation matters. *Communications of the ACM*. 59 (1), 47-49.

Sidana, Mandy. (2017). *Types of classification algorithms in Machine Learning.* https://medium. com/@ Mandysidana/machine-learning-types-ofclassification-9497bd4f2e14.

Snow, Jacob. (2018). *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*. *ACLU*, https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28.

Statista (2017). *Las aplicaciones más rentables de la inteligencia artificial.* https://es.statista.com/grafico/9437/las-aplicaciones-mas-rentables-de-la-inteligencia-artificial/.

Surden, H. (2011). *The Variable Determinacy Thesis. The Columbia Science & Technology Law Review*. 12, 1. 1.

Surden, Harry. (2014). *Machine learning and law. Washington Law Review*. *89* (2). (pp. 96-97).

Surden, Harry. (2018). *Artificial intelligence and law: An overview*. *Georgia State University Law Review*. 35-(pp. 1305).

Susskind, R. E. (1986). *Expert systems in law: A jurisprudential approach to artificial intelligence and legal reasoning*. *The modern law review*, *49*(2), 168-194.

Swaine, Jon. (2018). *Twitter Admits Far More Russian Bots Posted on Election Than It Had Disclosed*. *The Guardian.* https://www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed. Accesado por última vez el 18 de abril de 2023.

Transcript of Mark Zuckerberg's Senate Hearing". The Washington Post. April 10, 2018, Disponible en: https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.b0a2f734d2dc. Accesado por última vez el 18 de abril de 2023.

Vivant, Michel. (1997). "Internet et modes de régulation, dans: Internet face au droit", *Cahiers du Centre de Recherches Informatique et Droit*, Namur, Bélgica, núm. 12,p. 66.

Waller, M., y P. Waller. (2020). "Why Predictive Algorithms are So Risky for Public Sector Bodies." *Disponible en SSRN 3716166.*

Wang, Yilun & Kosinski, Michal. (2018). “Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images,” *Journal of Personality and Social Psychology*. Disponible en: https://osf.io/zn79k/. Accesado por última vez el 18 de abril de 2023.

PARTE II:
REGULACIÓN E INNOVACIÓN

REGULACIÓN DE REDES SOCIALES CON PERSPECTIVA DE GÉNERO Y DE DERECHOS HUMANOS

Maricela Hazel PACHECO PAZOS[6]
Alejandro Francisco HERRÁN AGUIRRE[7]

[6]Doctora y Maestra en Derecho por el Instituto de Investigaciones Jurídicas de la Universidad Autónoma de Chiapas. Sus líneas de investigación son: género y derechos de las mujeres, en las cuales ha publicado diversas obras. Es candidata a investigadora del Sistema Nacional de Investigadores e integrante del Sistema Estatal de Investigadores de Chiapas. Actualmente es Directora de la Defensoría de Derechos Humanos y Universitarios de la Universidad Autónoma de Chiapas. Puede ser contactada en hazel.pazos@unach.mx; ORCID: https://orcid.org/0000-0002-9045-844X.
[7]Profesor investigador del Instituto de Investigaciones Jurídicas de la Universidad Autónoma de Chiapas, su trabajo de investigación se ha dedicado a estudiar la libertad de expresión y su ejercicio y regulación a través del Internet, es becario Fullbright e integrante del Sistema Nacional de Investigadores. Es Doctor en Derecho por el IIJ-UNACH, puede ser contactado en alejandro.herran@unach.mx; ORCID: https://orcid.org/0000-0003-1661-0818.

REGULACIÓN DE REDES SOCIALES CON PERSPECTIVA DE GÉNERO Y DE DERECHOS HUMANOS

Social Media Regulation Through Human Rights and Gender Perspectives

RESUMEN

La forma en que las personas nos relacionamos con las tecnologías, y en la que accedemos a Internet, así como las redes sociales que utilizamos y cómo las utilizamos puede ser muy diversa, atendiendo a factores tales como el género, la edad, las condiciones sociales, e incluso, la región geográfica en la que vivimos, por ello, ante la necesidad de regular las redes sociales, es indispensable pensar en una regulación con enfoque de género y de derechos humanos, que busque respetar todos los derechos de todas las personas, especialmente de aquellas que pertenecen a grupos que históricamente han sido vulnerados.

Palabras clave:

redes sociales, moderación de contenidos, género y libertad de expresión.

ABSTRACT

The way in which people relate to technologies, and in which we access the internet, as well as the social media we use and how we use them can be very diverse, taking into account factors such as gender, age, social conditions and even the geographical region in which we live, therefore, given the need to regulate social media it is essential to think about a regulation with a gender and human rights approach, which seeks to respect all the rights of all people, especially those who belong to groups that have been violated.

Keywords

Social media, content moderation, gender and freedom of speech.

I. Introducción

Las redes sociales son espacios en donde pasamos gran parte de nuestra vida. Las usamos prácticamente para todo, no solo para los usos tradicionales como relacionarnos con otras personas o para obtener información, también nos sirven para comprar, vender e incluso para trabajar. A pesar de su utilidad innegable se han convertido en espacios en donde se pueden afectar derechos, especialmente para personas en situación de vulnerabilidad. La importancia de esta realidad demanda regularlas, lo cual no es nuevo, pero que ha cobrado especial relevancia con el aumento de personas usuarias y con el incremento del tiempo que pasamos en ellas.

Si bien hay consenso en cuanto a la necesidad de regular las redes sociales, la forma de hacerlo y la dificultad sobre cómo lograrlo generan importantes debates. La regulación necesariamente afecta las características que hacen que las redes sean poderosas herramientas de comunicación. Imponer obligaciones a las plataformas para moderar contenido con el objetivo de evitar expresiones lesivas afecta la libertad de expresión, de manera opuesta, una política permisiva en exceso en la moderación puede resultar en afectaciones personales o incluso en expresiones que sean ilegales. La búsqueda de soluciones efectivas se complica gracias a la politización de las conversaciones sobre la regulación y la ignorancia técnica de las personas encargadas de legislar al respecto. Sin embargo, sin importar la estrategia que se utilice para la regulación, se requiere que se haga con enfoque de derechos humanos y con perspectiva de género, pues las investigaciones demuestran que el espacio virtual no es neutro, es decir, no afecta a todas las personas de la misma manera.

En este capítulo se abordan las formas de regulación implementadas internacionalmente, enfatizando la necesidad de que estas protejan los derechos humanos de las mujeres y grupos en situación de vulnerabilidad.

Sin duda, las formas de comunicación entre las personas han evolucionado y van trasladándose cada vez más a los entornos virtuales. Dichas interacciones impactan de manera importante en la realidad, pues en las redes sociales no solo reproducimos las conductas consideradas lícitas o aceptables, sino que también reproducimos el machismo y la discriminación, afectando la integridad mental o física de las personas. Surgen nuevas formas de violencia a catalogar, que abarcan desde aspectos de seguridad hasta las que tienen que ver con el contenido de los mensajes, como el discurso de odio.

Elementos como el desarrollo tecnológico, que impacta desigualmente a diferentes países, la globalización tecnológica, o hechos históricos como la pandemia de SARS-CoV2, o Covid-19, dieron lugar a un avance desproporcionado en el uso de las diversas plataformas de comunicación y dejaron ver también las deficiencias de capacitación en cuanto a temas educativos. Pero también detonaron

el incremento de violencias de diferentes clases, tanto en el espacio tradicional u *offline*, como las que se presentan en las redes sociales, o en el entorno *online*.

En ese sentido, se ha observado que muchas de las violencias que se han presentado dentro de las redes sociales afectan en mayor forma a las mujeres que a los hombres, y que dañan también, en mayor medida, a las personas provenientes de una etnia dado que hablan una lengua indígena, generando con ello desigualdades.

II. Brecha digital y discriminación

A estas barreras o desigualdades en el acceso a las tecnologías en general, y a Internet en particular, se les conoce como brecha digital, y pueden deberse a muchos motivos, por ejemplo, género, raza, situación social o edad, aunque no en términos absolutos.

Este concepto puede tener muchas definiciones, una de ellas es la que presenta la Organización para la Cooperación y el Desarrollo Económicos, quien menciona que es "la brecha entre individuos, hogares, regiones económicas y geográficas con diferentes niveles socioeconómicos en relación tanto a sus oportunidades de acceso a las TIC como al uso de internet para una amplia variedad de actividades" (OECD, 2001).

Esta brecha puede ser de diversas clases. Delia Crovi menciona al menos cinco escenarios relacionados con la brecha digital:

1. Tecnológico: tiene que ver con la infraestructura material;
2. Económico: se refiere a la carencia o disponibilidad de recursos para acceder a las redes;
3. Habilidades informáticas: son las capacidades cognitivas que las personas usuarias deber poseer;
4. Capital cultural: entendido como la acumulación propia de una clase, que heredada o adquirida mediante la socialización, tiene mayor peso en el mercado simbólico cultural entre más alta es la clase social de su portador, y,
5. Político: relacionado a las políticas públicas sobre el acceso a las redes y la voluntad de generar participación en torno a ellas (Crovi, 2008, p. 70).

Parafraseando a Claudia Ivette Pedraza, se puede hablar de tres aspectos de la brecha digital: brecha de acceso, que se relaciona con la diferencia de conectividad y disponibilidad de redes, dispositivos y servicios; la brecha de uso son los conocimientos y habilidades para ser utilizados los dispositivos, y; la brecha de apropiación, que tiene que ver con las posibilidades de elegir y orientar su uso para beneficio de las personas usuarias (Pedraza, 2021).

Los datos acerca del uso de las Tecnologías de la Información y la Comunicación reflejan estas desigualdades, pues, de acuerdo con la Unión Internacional de Telecomunicaciones (UIT), a finales de 2018, el 51,2% de las personas; es decir, 3 900 millones, utilizaban Internet, sin embargo, son los países más desarrollados los que presentan niveles de conexión más elevados, 4 de cada 5 personas están conectadas. Además, ese mismo informe refleja una brecha en cuanto a uso, pues señala que cuanto más compleja es una actividad, menos personas la realizan, y que los usuarios de computadoras en los países desarrollados parecen poseer más conocimientos sobre las TIC que los usuarios de los países en desarrollo (Unión Internacional de Telecomunicaciones, 2018).

Entender que las personas no acceden de la misma manera y que no utilizan las redes sociales de la misma forma es indispensable cuando se habla de regulación, pues los sistemas automatizados de moderación de contenido pueden afectar desproporcionadamente a algunas personas o grupos de personas, por ejemplo, a quienes hablan alguna lengua indígena, pues dichos sistemas han sido desarrollados para servir a los grupos mayoritarios, a las lenguas dominantes.

III. Violencia en línea contra mujeres y grupos en situación de vulnerabilidad

Los datos antes mencionados, ponen en evidencia que son las mujeres y las personas integrantes de grupos en situación de vulnerabilidad quienes se encuentran en desventaja respecto del acceso y uso de las redes sociales. Esta desventaja, además, produce discriminación y violencia contra estas personas.

De acuerdo con datos del grupo de trabajo de la Comisión de la Banda Ancha para el Desarrollo Digital de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, una de cada 5 mujeres considera que Internet es inapropiado para ellas, también es una realidad que usuarios con nombres femeninos sufren más amenazas que los que tienen nombres masculinos, y quienes están más propensas a sufrir esta violencia son las mujeres entre 18 y 24 años (Comisión de la Banda Ancha para el Desarrollo Digital de la UNESCO, 2015).

En este sentido, el estudio de las violencias digitales que afectan específicamente por razón de género, también puede analizarse junto con otros factores que se conectan con él, tales como la edad, el origen étnico o nacional, la orientación sexual, entre otras, pues estas características pueden tener tanto peso como el género a la hora de definir el trato que se recibe en el mundo físico y en el digital.

Para el análisis de estas relaciones se puede tomar en cuenta la interseccionalidad, entendida como “una lente a través de la cual se puede ver dónde aparecen las relaciones de poder y dónde chocan, dónde se conectan y dónde se intersectan. No estamos hablando simplemente de un problema de raza, o de género, o de clase, o de LGBTQ[+]. Muchas veces, si encasillamos la

discriminación en este marco, dejamos de lado a los que son discriminados por todas estas cosas" (Crenshaw, 2017).

El informe #ToxicTwitter violencia y abuso contra las mujeres en Internet, de Amnistía Internacional, menciona algunos ejemplos de esta violencia interseccional, uno de ellos es el de la parlamentaria escocesa y líder de la oposición, Ruth Davidson, quien señala:

> "... Porque soy abiertamente gay —fui la primera líder gay de uno de los principales partidos políticos en el Reino Unido— y cuando empecé, el abuso homofóbico era muy habitual. Tengo muchos seguidores en Twitter que son jóvenes homosexuales y para mí siempre ha sido muy importante mencionarlo. De vez en cuando, una vez al mes, retuiteo o rechazo algunos comentarios homofóbicos porque creo que es importante que las personas vean que ese tipo de lenguaje no es aceptable, no tienes por qué soportarlo" (Amnistía Internacional, 2018, p. 22).

Como ha sido señalado, la violencia *online* puede considerarse como un reflejo de la violencia sistemática que viven las mujeres en los medios "tradicionales", ahora trasladada al entorno virtual, lo cual presenta desafíos propios, especialmente a nivel jurídico, pues, por las características que posee, el entorno virtual tiene la capacidad de maximizar los efectos de los ataques, por ejemplo, "una agresión filmada y subida a Internet, al poder ser vista por otras personas perpetua el ciclo de violencia revictimizando a la persona sujeto del ataque y exponiéndola a nuevas formas de violencia" (Vergés, 2017, p. 36).

La Comisión de la Banda Ancha para el Desarrollo Digital, la cual fue creada por las Naciones Unidas, señala que el 73% de las mujeres en el mundo han estado expuestas o han experimentado algún tipo de violencia en línea (UNESCO, 2015, p. 15).

La condición de género y la identidad sexual no son las únicas características por las cuales las personas pueden ser violentadas en redes sociales, las investigaciones muestran que otros factores como la pertenencia a un grupo étnico o minoría racial son utilizados para discriminar a las personas usuarias, a esta forma de violencia se le ha denominado *ciberodio*.

Este fenómeno se ha vuelto tan relevante, que hay organizaciones que se dedican a combatirlo, como INACH *(International Network Against CiberHate),* una de las redes con mayor actividad en Europa respecto a la denuncia del ciberodio, y que agrupa a numerosas ONG en Internet, entre ellas, a Movimiento contra la Intolerancia. La actividad principal de esta red es recabar aquellas situaciones complejas, y en muchas ocasiones dolorosas, que se generan en torno al odio a las minorías. Por citar un ejemplo, en sus informes más recientes señala que en el norte de Inglaterra los delitos de odio que se han cometido a través de las redes sociales se han multiplicado por 30 en relación a la realidad no virtual (Universidad Internacional de Valencia, s/f).

Las características propias de las redes sociales las hacen un espacio en el que se pueden reproducir de manera importante los comentarios racistas.

Para el año 2010, INACH había descubierto más de 11 500 sitios de odio diferentes. Y en 2014, hasta 30 000 sitios webs, foros y usos de redes sociales racistas y antiminorías, subiendo un 30% desde el año 2013 (Universidad Internacional de Valencia, s.f.).

Estos datos alarmantes nos señalan que el Internet y las redes sociales de manera específica se ha utilizado como medio para difundir y organizar grupos racistas y xenófobos, en donde se encuentran en aumento las agresiones motivadas por la intolerancia, entre otras conductas violentas.

El ciberodio crea un clima que normaliza la discriminación, la intolerancia, la violencia y el crimen hacia personas migrantes, personas refugiadas, personas con identidades sexo-genéricas no normativas, minorías religiosas, y de todo ser humano que pertenezca a grupos que históricamente han sufrido discriminación.

Algunas herramientas que pueden servir como medida para contrarrestar el desarrollo digital del odio que se está evidenciando mediante el uso de Internet, pueden ser la alfabetización realizada a través de un uso correcto, formativo y proactivo de la educación *online,* a la par del control legal y la aplicación de sanciones penales cuando se comente alguna conducta que puede ser tipificada como delito, y por supuesto, la regulación de las redes sociales.

IV. Regulación de las redes sociales

Conviene hacer una precisión en cuanto al uso del término “regulación” pues este término suele relacionarse exclusivamente con la legislación, sin embargo, en este documento es utilizado de forma más amplia y se refiere a todos los mecanismos que se utilizan para moderar, controlar o vigilar lo que se publica en las redes sociales. Estos mecanismos pueden incluir, por supuesto, legislación, –nacional e internacional– pero también incluye aspectos técnicos o mecanismos automatizados, entre otros.

La regulación del Internet y de las redes sociales no es un tema reciente, desde que estas surgieron se ha buscado tomar medidas para controlar los contenidos que se publican en estos espacios, así como. el uso que le dan las personas usuarias, sin embargo, con hechos como el bloqueo de la cuenta del expresidente de los Estados Unidos, Donald Trump, además de temas relacionados con daño al patrimonio de las y los usuarios y el *bullying* en redes –*ciberbullying–,* han hecho que el tema cobre relevancia.

La regulación de las redes sociales no abarca únicamente la legislación nacional, sino también la legislación internacional, así como, todos los mecanismos que se utilizan para moderar, controlar o vigilar lo que se publica en las redes sociales, los cuales, pueden incluir, aspectos técnicos o mecanismos automatizados, entre otros.

Esta regulación puede hacerse de distintas formas, se pueden mencionar tres principales, la moderación o también llamada autorregulación, que se refiere a la manera en la que las propias plataformas de redes sociales controlan el contenido que se publica en ellas; la regulación externa, que, como el nombre lo indica, es la que hacen agentes externos –generalmente los Estados–, y la co-regulación que busca que los principales agentes involucrados –empresas de redes sociales y Estados– puedan participar de manera coordinada en la regulación.

En relación con la primera de estas, la moderación, vale la pena señalar que no es una actividad nueva, pues, desde su inicio, las empresas de redes sociales han implementado acciones para restringir las publicaciones o las personas usuarias que incumplen con sus normas, las cuales, pueden imponer una gran cantidad de restricciones.

Es así, que son las propias redes sociales quienes establecen los requisitos que las personas deben cumplir para poder ser parte de su comunidad, es decir, para ser usuarias de determinadas plataformas se debe cumplir con las restricciones que se imponen a sus publicaciones, restricciones que a veces, van más allá incluso que la legislación nacional. El caso que mejor ejemplifica esto es en relación con los desnudos y el contenido erótico, que si bien, no es ilegal y la legislación no lo prohíbe, en las redes sociales este contenido está restringido por las normas comunitarias.

Un ejemplo de las acciones de regulación implementadas por las propias redes sociales en cuanto al tema de las violencias en contra de las mujeres, son las políticas implementadas para contrarrestarlas –específicamente pornografía no consensuada– siendo una de estas el “Programa piloto sobre imágenes íntimas no consensuadas” de Facebook, a través del cual, se busca evitar la difusión de estas imágenes.[12]

Otra modificación que implementó Meta[13] es la relativa a la creación del Consejo Asesor de Contenido, que es un órgano autónomo integrado por expertos en libertad de expresión que recibe apelaciones sobre las decisiones tomadas por la plataforma respecto a la eliminación o mantenimiento de publicaciones problemáticas. “Las decisiones del Consejo de ratificar o revertir las decisiones de contenido de Facebook serán vinculantes, lo que significa que Facebook deberá implementarlas, a menos que hacerlo suponga infringir la ley”. Al momento de la redacción, se han emitido 23 decisiones, que vinculan a diversos países y sobre

[12] Para mayor información sobre este programa se puede consultar el siguiente enlace https://www.facebook.com/safety/notwithoutmyconsent/pilot.

[13] Meta es una empresa de tecnología y redes sociales a la que pertenecen, entre otras redes sociales, Facebook e Instagram.

una variedad de temas, entre los más comunes: incitación al odio, personas peligrosas y libertad de expresión.[14]

Otro aspecto interesante para resaltar de Facebook es lo concerniente a hacer mucho más transparentes sus procesos, parte de ello es la publicación semestral de información relacionada con diversos temas, entre los que están las solicitudes de restricciones de contenido, y un dato interesante es que en los últimos tres semestres publicados (enero-junio 2020, julio-diciembre 2020, enero-junio 2021). México se encuentra entre los tres primeros lugares.[15]

Twitter también ha hecho modificaciones en sus políticas de moderación de contenido, inicialmente poniendo mensajes de advertencia en las publicaciones con contenido sospechoso, y bloqueando cuentas de usuarios, siendo el bloqueo más famoso, sin duda, el de la cuenta del entonces Presidente de los Estados Unidos, Donald Trump -@realDonaldTrump- (Alizadeh et al., 2021).

Un problema al que se enfrenta la moderación de contenido es que la cantidad de contenido que se publica en las redes sociales supera la capacidad de monitoreo humano, por ello, se han implementado soluciones automatizadas –algoritmos–, los cuales, con frecuencia se presentan como la mejor solución al problema, sin embargo, estos mecanismos, no pueden resolver el problema de manera satisfactoria cumpliendo con los estándares de derechos humanos.

En cuanto a la regulación externa, se han propuesto disposiciones en diversos países del mundo. Una de las primeras disposiciones es la Sección 230 de la Ley sobre Decencia en las Comunicaciones, mejor conocida simplemente como Sección 230, en Estados Unidos, la cual, de manera muy sintetizada, establece que los proveedores de servicios de internet no son responsables por el contenido que se publica en sus plataformas siempre que sea otra persona quien ha generado ese contenido.

Esta disposición ha permitido el desarrollo de las redes sociales como las conocemos, pues estas plataformas han logrado tener el auge que tienen actualmente gracias a que las personas usuarias pueden publicar el contenido que deseen –siempre y cuando no infrinja las propias normas comunitarias de la red– sin que las plataformas sean sancionadas por ello.

En Europa, se puede mencionar los artículos 12, 13 y 14 de la Directiva Europea de Comercio Electrónico, que, en términos generales, se puede decir que sigue las bases señaladas por la sección 230, estableciendo un régimen de responsabilidad intermedia que da cierta inmunidad a los intermediarios (Julià-Barceló & Koelman, 2000).

[14] Las decisiones de este consejo pueden consultarse en el siguiente enlace https://oversightboard.com/?page=decision.

[15] En enero-junio 2020 se situó en la posición número uno, en julio-diciembre 2020 en la posición dos, solo después de Brasil y enero-junio 2021 también ocupó la posición número dos, después de Alemania.

Otra disposición legal importante en relación con la protección de datos personales es el Reglamento General para la Protección de Datos (GDPR por sus siglas en inglés) de la Unión Europea. El propósito del GDPR es proteger la privacidad y la seguridad de la ciudadanía europea mediante la regulación del tratamiento de la información. En esta norma, se establecen obligaciones a las personas —públicas y privadas— que manejan datos relacionados con personas europeas. Su aplicación ahora es generalizada y contiene importantes disposiciones respecto de la forma y los datos que las empresas deben respetar para la guarda y protección de la privacidad de las personas.

Otra disposición que se puede mencionar es la *Netzwerkdurchsetzungsgesetz*—Ley para Control de la *Red o Net Enforcement Act o NetzDG*— que tiene como propósito combatir el discurso de odio y la desinformación en Alemania, la cual impone varias obligaciones a las plataformas de redes sociales con importantes multas en caso de incumplimiento.

Uno aspecto que se debe considerar cuando se trata de regular las redes sociales es que es necesario legislar con conceptos claros y bien definidos, pues de lo contrarios pueden resultar efectos contrarios al derecho a la libertad de expresión, a la privacidad y a la información.

En la región de América Latina se pueden mencionar los *Estándares para una regulación democrática de las grandes plataformas que garantice la libertad de expresión en línea y una Internet libre y abierta*, documento publicado en 2020 en el cual se establecen una serie de principios que, de acuerdo con las organizaciones involucradas, deben ser aplicados en la región para lograr procesos de moderación privada de contenidos compatibles con los estándares internacionales de derechos humanos.

De manera específica, señala siete ejes sobre los cuales se deben enfocar los esfuerzos de regulación, estos son: alcance y carácter de la regulación, términos y condiciones de servicio, transparencia, debido proceso, derecho a defensa y apelación, rendición de cuentas y co-regulación, y regulación.

Una de las intersecciones más importantes entre la moderación y la regulación de las redes sociales es que, ante la obligación de la segunda, el algoritmo que se ponga en marcha para moderar el contenido cometerá errores, si los incentivos son inadecuados esto produce remoción excesiva de contenido que no debería ser removido (Keller, 2015). Cuando la moderación se deja en manos de aplicaciones automatizadas estas privilegiarán los incentivos de las plataformas, y estas, por lo general en el clima político actual, buscarán evitar la imposición de responsabilidades, lo que resultará en acallamiento de expresiones que no solo son legales, sino que no van en contra de los términos de uso de las plataformas mismas.

V. Impacto de las violencias contra las mujeres en las políticas y regulación de las redes sociales

La legislación destinada a proteger a las mujeres contra la violencia en línea, pero que no se concibe cuidadosamente de conformidad con el marco internacional de derechos humanos puede tener efectos colaterales negativos sobre otros derechos humanos, por ejemplo, el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión ya señaló que toda restricción de contenido impuesta por el Estado debe estar prevista por la ley, obedecer a uno de los fines establecidos en el artículo 19, párrafo 3, del Pacto, y respetar los principios de necesidad y proporcionalidad (véase A/HRC/17/27, párr. 24 y A/66/290, párr. 15).

En una declaración conjunta con el titular del mandato, la Relatora Especial había subrayado anteriormente que el abuso y la violencia en línea por razón de género atentaban contra los principios básicos de la igualdad en virtud del derecho internacional y la libertad de expresión, y subrayó que velar por que Internet estuviera libre de violencia por razón de género aumentaba el empoderamiento de la mujer.

También pusieron de relieve el hecho de que las mujeres víctimas y supervivientes necesitaban respuestas rápidas y transparentes y recursos efectivos, que solo podían obtenerse si tanto los Estados como los agentes privados trabajaban juntos y actuaban con la diligencia debida para eliminar la violencia en línea contra la mujer (Organización de las Naciones Unidas, 2020, párr. 76).

En el marco de su recomendación general núm. 35 (2017), el Comité para la Eliminación de la Discriminación contra la Mujer recomendó a los Estados que fomentaran la participación del sector privado, en particular de las empresas y las sociedades transnacionales, en los esfuerzos por erradicar todas las formas de violencia por razón de género contra la mujer y que asumieran la responsabilidad por todas las formas de violencia. De ello se desprende que debe alentarse a los medios sociales y los medios en línea a crear o fortalecer los mecanismos centrados en la erradicación de los estereotipos de género, y a poner fin a toda violencia por razón de género cometida en sus plataformas.

VI. Enfoque de género y de derechos humanos en la regulación de las redes sociales

Existen diversos aspectos que deben considerarse al momento de regular las redes sociales, tanto económicos como sociales y tecnológicos, por ello, se requiere de una regulación inteligente y, “es aquella que no pone cargas excesivas a actores que, por su desarrollo y características no pueden cumplirlas, considerando de manera adecuada y diferenciada a las grandes plataformas de contenidos, respecto

de aquellas que sean de menor porte o estén direccionadas a finalidades específica" (Observacom, *et al.,* 2020).

En dicha regulación, deben de tomarse en cuenta, por supuesto, los derechos de todas las personas, sin embargo, ante una situación en la que estén en conflicto uno o más derechos, es necesario que se considere aquel que beneficie más a las personas integrantes de grupos en situación de vulnerabilidad, como niñas, niños y adolescentes, mujeres, poblaciones indígenas, afrodescendientes, entre otros.

Cabe señalar la importancia de comprender la forma de aplicar de manera eficaz un enfoque basado en los derechos humanos con el objetivo de prevenir y combatir la violencia en línea y facilitada por las TIC contra la mujer como violaciones de los derechos humanos, que comparte sus causas profundas con otras formas de violencia contra las mujeres y que debe tratarse en el contexto más amplio de la eliminación de todas las formas de discriminación contra la mujer.

Debemos mencionar que el reconocimiento de los derechos humanos ha avanzado históricamente, y el acceso a Internet se ha considerado como un derecho fundamental para que las personas puedan ejercer otros derechos, sin embargo, su efectividad depende del contexto que cada región presenta, lo cual nos lleva a pensar en la complejidad de su regulación.

Se han implementado diversas estrategias con el propósito de regular el uso de las redes sociales, sin embargo, no hay una respuesta única y definitiva, pues los desafíos que presenta esta regulación dependen de muchos factores, tales como la región geográfica, que presenta dificultades como atender al sistema jurídico de cada lugar, así como, las propias características de las redes, la intervención de múltiples actores, entre otros, los diversos intereses tanto públicos, como privados.

En ese sentido, en su informe sobre los medios de cerrar la brecha digital entre los géneros desde una perspectiva de derechos humanos (A/HRC/35/9), el Alto Comisionado de las Naciones Unidas para los Derechos Humanos destacó que la violencia *online* contra la mujer debía abordarse en el contexto más amplio de la discriminación y la violencia por razón de género fuera de línea, y que los Estados debían promulgar medidas legislativas adecuadas y asegurar las debidas respuestas para hacer frente al fenómeno de la violencia en línea contra la mujer (Organización de las Naciones Unidas, 2017).

Sobre el tema de la regulación de redes, específicamente, señaló que si bien, el fin puede ser apropiado (v.gr., limitar un discurso de odio, actividades terroristas y la distribución de material ilegal), la regulación debe ser muy cuidadosa para no tener efectos contrarios al ejercicio de derechos humanos. No se puede ignorar que algunos Estados han utilizado como excusa estos fines legítimos y han implementado sus capacidades de control con el objetivo de silenciar a quienes

tienen una voz, lo que ha provocado que personas activistas se sientan excluidas, perseguidas o violentadas.

Cuando se consideren mecanismos para regular las redes sociales, es muy importante reconocer que los instrumentos de derechos humanos son el único conjunto de normas internacionales que ofrecen una base sólida para pensar en las posibles restricciones a la libertad de expresión o a la privacidad.

VII. Prevención, protección, enjuiciamiento, castigo, recurso reparación y compensación alrededor de la violencia contra las mujeres y los derechos humanos en las redes sociales

En primer lugar, hay que ahondar un poco en algunos de los conceptos relacionados a este apartado, por ello, podemos decir que el enjuiciamiento consiste en la investigación y la interposición de actuaciones penales contra los autores. Con frecuencia, los órganos encargados de hacer cumplir la ley trivializan la violencia en línea contra la mujer, y sus acciones lamentablemente a menudo se caracterizan por la culpabilización de las víctimas en relación con estos casos. Esta actitud se traduce en una cultura de silencio y en la denuncia insuficiente de casos pues las mujeres víctimas se resisten a hablar por temor a ser culpadas.

Aun en los casos en que las mujeres presentan denuncias y se inician investigaciones, tropiezan con nuevos obstáculos debido a la falta de conocimientos técnicos y de capacidad en el poder judicial (incluidos los sistemas judiciales, los magistrados y los jueces). Además, las costas de los litigios impiden que muchos supervivientes, en particular las mujeres más pobres, presenten sus causas ante los tribunales.

Por lo tanto, es fundamental evaluar la labor de los equipos de respuesta inicial —incluidos los intermediarios de Internet, la policía y las líneas telefónicas de asistencia (ONU, 2018, A/HRC/38/47, párr. 67) — y del poder judicial y los organismos reguladores a fin de obtener una descripción fiel de la realidad de las experiencias de las mujeres y facilitar su acceso a la justicia y los recursos.

Las medidas de reparación también incluyen la eliminación inmediata de los contenidos nocivos, así como, formas de restitución, rehabilitación, satisfacción y garantías de no repetición, que combinen medidas simbólicas, materiales, individuales y colectivas, en función de las circunstancias y de las reclamaciones de la víctima. También deberían incluir un requerimiento inmediato a fin de impedir la publicación de contenidos nocivos.

> “Los intermediarios de Internet, todas las empresas de almacenamiento de datos de clientes y las que proporcionan almacenamiento en la nube también tienen el deber de cumplir con las normas de derechos humanos manteniendo los datos seguros, y deben rendir cuentas de la piratería de los

> datos si no cuentan con las salvaguardias suficientes" (ONU, 2018, A/HRC/38/47, párr. 72).

Otro aspecto que se debe considerar es que, desde una perspectiva de género, las mujeres deberían estar en condiciones de utilizar seudónimos, que podrían ayudarlas a huir de una pareja que las maltrata, de acosadores o de acosadores reincidentes, y a desvincularse de cuentas relacionadas con la publicación de pornografía no consentida (ONU, 2018, A/HRC/38/47, párr. 75).

Como resultado de ello, las mujeres, especialmente las defensoras de los derechos humanos, que prefieren permanecer en el anonimato en sitios web como Facebook, suelen ser denunciadas por los acosadores por poseer un perfil "falso". En lugar de entablar acciones contra los acosadores, algunas veces los intermediarios exigen a las mujeres afectadas que revelen su identidad, lo que puede ponerlas en riesgo de sufrir daños. Por esta razón, la política ha sido objeto de fuertes críticas por parte de algunos grupos de la sociedad civil. En respuesta a estas críticas, Facebook ha modificado ligeramente su política y ahora exige que los denunciantes proporcionen cierta medida de prueba. En este contexto, las salvaguardias de los derechos humanos contra la censura arbitraria por los intermediarios son fundamentales (ONU, 2018, A/HRC/38/47, párr. 75).

La regulación implica tener conocimientos y claridad en los planteamientos, de manera que se pueda mantener un equilibrio con la libertad y apertura que históricamente ha representado Internet.

VIII. Conclusiones

Con todo lo anteriormente expuesto, la co-regulación se presenta como el camino más adecuado, pues es importante alcanzar un equilibrio en la regulación de contenidos en línea, de manera que coexistan la autorregulación que puedan hacer las propias plataformas y las acciones del Estado, las cuales deben estar dirigidas a la protección de los derechos humanos de las personas usuarias frente a decisiones y políticas de actores que amenacen con coartar la libertad de expresión.

Aplicar el enfoque de género en la regulación de las redes sociales, implica reconocer las desventajas a las que las mujeres se enfrentan en el uso de estas plataformas, desarrollando acciones que busquen cerrar esta brecha y que puedan prevenir las violencias que ellas sufren en estos espacios.

El enfoque de derechos humanos debe considerar todas las disposiciones nacionales e internacionales en esta materia, reconociendo las desigualdades que las personas viven por su condición de género, edad, origen étnico, creencia, situación migratoria, entre otras y procurando la aplicación menos restrictiva, que proteja los derechos humanos de manera integral.

Sin importar qué tipo de regulación se decida implementar, es esencial que las medidas que se establezcan tomen en cuenta las diferentes formas de violencia

online contra las mujeres y las niñas, y las violencias que sufren las personas pertenecientes a grupos en situación de vulnerabilidad, al tiempo que se respeta el derecho a la libertad de expresión, incluido el acceso a la información, el derecho a la privacidad y la protección de los datos, así como los derechos de las mujeres que están protegidos por el marco internacional de derechos humanos.

IX. Bibliografía

ALIZADEH, M., GILARDI, F., HOES, E., KLÜSER, K.J. y otros, (2021). *Content moderation as a political issue: The twitter discourse around Trump's ban.* University of Zurich.

Amnistía Internacional. (2018). *#ToxicTwitter violencia y abuso contra las mujeres en Internet.*

CRENSHAW, K. (2017). *The African American Policy Forum, Kimberlé Crenshaw on Intersectionality. More than Two Decades Later*. https://www.law.columbia.edu/news/archive/kimberle-crenshaw-intersectionality-more-two-decades-later.

CROVI, D. (2008). *Dimensión social del acceso, uso y apropiación de las TIC*, *Contratexto* N° 16, ISSN 1025-9945, pp.

Julià-Barceló, R., & Koelman, K. J. (2000). *Intermediary liability: intermediary liability in the e-commerce directive: so far so good, but it's not enough*. Computer Law & Security Review, 16(4). 231-239.

OBSERVACOM et al., (2020). *Estándares para una Regulación Democrática de las Grandes Plataformas que Garantice la Libertad de Expresión en Línea y una Internet Libre y Abierta* https://www.observacom.org/estandares-para-una-regulacion-democratica-de-las-grandes-plataformas-que- garantice-la-libertad-de-expresion-en-linea-y-una-Internet-libre-y-abierta/.

OECD, Understanding the Digital Divide, OECD Digital Economy Papers, No. 49, OECD Publishing, Paris. 2001, disponible en: http://dx.doi.org/10.1787/236405667766

ORGANIZACIÓN DE LAS NACIONES UNIDAS. (2017). A/HRC/35/9. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/111/86/PDF/G1711186.pdf?OpenElement.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. (2018). A/HRC/38/47. Disponible en: https://acoso.online/wp-content/uploads/2018/10/G1818461.pdf.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. (2018). Informe ONU.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. (2020). A/HRC/44/952 Disponinible en: https://digitallibrary.un.org/record/3870659/files/A_HRC_44_52-ES.pdf.

PEDRAZA BUCIO, C. “La brecha digital de género como vértice de las desigualdades de las mujeres en el contexto de la pandemia por Covid-19”, *Logos* / Año XLIX / Número 136 / ene-jun 2021 / p. 11.

UNESCO. (2015). *Broadband commission for digital development working group on broadband and gender, Cyber violence against women and girls: A world-wide wake-up call.*

UNESCO. *Informe final del Grupo de Trabajo sobre Género de la Comisión de Banda Ancha*. (2015). Combatir la violencia en línea contra las mujeres y las niñas: Una llamada de atención al mundo. Disponible en: https://en.unesco.org/sites/default/files/highlightdocumentspanish.pdf.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2018). *Informe sobre Medición de la Sociedad de la Información*. ITU Publicaciones, Suiza.

VERGÉS, N., (coord.). (2017). *Redes sociales en perspectiva de género: guía para conocer y contrarrestar las violencias de género online.* Instituto Andaluz de Administración Pública, España.

ASPECTOS REGULATORIOS DE 5G. DERECHO A LA SALUD, MEDIO AMBIENTE, PROTECCIÓN DE DATOS PERSONALES Y CIBERSEGURIDAD

Marco Antonio VEGA SERVÍN[8]

[8]Es Licenciado en Derecho por la Facultad de Derecho de la Universidad Nacional Autónoma de México (UNAM). Cuenta con una Maestría en Derecho de las Tecnologías de Información y Comunicación, por el INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, México. Correo electrónico marco.vega1012@gmail.com. Número ORCID: 0000-0003-1900-5154.

ASPECTOS REGULATORIOS DE 5G. DERECHO A LA SALUD, MEDIOAMBIENTE, PROTECCIÓN DE DATOS PERSONALES Y CIBERSEGURIDAD

5G Regulatory aspects. Right to health, environment, privacy and cybersecurity

Resumen

El objetivo de este artículo es identificar algunos de los principales desafíos globales en materia de derechos humanos como la salud, el medio ambiente y la protección de datos personales que presenta la tecnología 5G. Para ello, se analizaron algunos casos prácticos, normas internacionales y buenas prácticas adoptadas por países líderes en el despliegue de 5G. Con lo anterior, se busca proponer algunos posibles cambios regulatorios en México, así como, el fomento de políticas públicas coordinadas con instituciones de los sectores público, privado, social y académico que incentiven la innovación y respeto de los derechos humanos en materia de salud, medio ambiente y protección de datos personales en la adopción de la quinta generación de redes móviles de telecomunicaciones en México.

Palabras clave: 5G, infraestructura, telecomunicaciones, medio ambiente, datos personales, salud, hipersensibilidad electromagnética, ciberseguridad, ondas electromagnéticas, IoT, contaminación electromagnética, desechos electrónicos, régimen de certificación.

Abstract

The objective of this article is to identify some of the main global challenges in terms of human rights such as health, the environment and the protection of personal data presented by 5G technology. To this end, some practical cases, international standards and good practices adopted by leading countries in the deployment of 5G were analyzed. With the above, we seek to propose some possible regulatory changes in Mexico, as well as the promotion of public policies coordinated with institutions from the public, private, social and academic sectors that encourage innovation and respect for human rights in matters of health, environment. environment and protection of personal data in the adoption of the fifth generation of mobile telecommunications networks in Mexico.

Keywords: *5G, infrastructure, telecommunications, environment, personal data, health, electromagnetic hypersensitivity, cybersecurity, electromagnetic waves, IoT, electromagnetic pollution, electronic waste, certification regime.*

I. Introducción

La innovación y las tecnologías presentan retos sociales, económicos y también jurídicos. La tecnología se caracteriza por ser una herramienta que mejora modelos productivos y económicos, pero, al mismo tiempo, transforma la manera en que la sociedad interactúa. No obstante, a medida que la tecnología ofrece mayores capacidades para el desarrollo económico y social también presenta desafíos para garantizar los derechos humanos en entornos cada vez más digitales.

Un ejemplo de ello es lo que sucede con la tecnología 5G la cual, al demandar mayor despliegue de infraestructura y puntos de conexión para el intercambio masivo de datos, representa diversos desafíos no solo para el sector de las telecomunicaciones, sino también para la protección de datos personales, la protección a la salud, el medio ambiente, y la seguridad de la información. Lo anterior representa retos multidisciplinarios que deben ser considerados en el despliegue de 5G en cualquier país y que involucra la colaboración de distintas partes relacionadas más allá del sector de las telecomunicaciones.

Así, el objetivo del presente ensayo es identificar los desafíos regulatorios y necesidades de coordinación con diferentes sectores que el Estado mexicano debería considerar en el despliegue de la tecnología 5G, cuya carencia puede significar un impacto negativo en la protección de los derechos humanos como la salud, el medio ambiente y la protección de datos personales. Para ello, se utilizó un tipo de método de investigación sistémico y de derecho comparado a través del análisis documental de normas jurídicas, políticas públicas y casos de uso a nivel internacional relacionados con la tecnología 5G.

II. ¿Qué es 5G?

Para identificar los desafíos de esta nueva tecnología debemos partir por definir qué entendemos por 5G, la cual se refiere a la "*quinta generación de tecnologías de redes inalámbricas móviles*" que facilita la comunicación entre personas y, ahora, también entre objetos. Uno de los grandes retos de la humanidad ha sido siempre la comunicación a distancia a través de distintos medios. Desde las señales de humo, señales luminosas, el telégrafo y ahora las telecomunicaciones, las personas nos hemos podido comunicar a distancia a través de diferentes medios.

Las *telecomunicaciones* son una forma de comunicación a distancia que ha cobrado relevancia en un mundo cada vez más globalizado y digitalizado, las cuales se definen como "*un sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos"* (Real Academia Española, 2021). En el artículo 2.2 del "Reglamento de las Telecomunicaciones Internacionales" encontramos un concepto más detallado de las telecomunicaciones como "*toda*

transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medio ópticos u otros sistemas electromagnéticos (UIT, 2012).

Es decir, a través de las telecomunicaciones podemos transmitir datos, sonidos, imágenes o cualquier información utilizando diversos medios que en su conjunto se denominan "redes de telecomunicaciones", la cuales constituyen los medios de transmisión, equipos y sistemas (Álvarez, 2012) que facilitan la comunicación a distancia y que pueden clasificarse en dos tipos: (I) cables -por ejemplo, cobre, cable coaxial, fibra óptica, cable submarino- y (II) frecuencias del espectro radioeléctrico -ondas electromagnéticas por debajo de los 3 000GHz- (Luque, 2017). La primera es una comunicación alámbrica; la segunda una comunicación inalámbrica.

Por lo que hace a la tecnología 5G podemos señalar que se trata de la "quinta generación" de tecnologías de "*redes inalámbricas móviles*" que utilizan las frecuencias del espectro radioeléctrico para facilitar la comunicación a distancia entre personas y también entre máquinas. La letra "G" en 1G, 2G, 3G, 4G y 5G significa "generación" y el número es solo una representación de la evolución de las redes móviles, actualmente utilizamos principalmente el 4G y el mundo está transitando al 5G (Singh, 2017).

Las redes móviles surgieron en 1980 (H. Lehne, 2005) y aproximadamente cada 10 años surge una nueva generación. Cada generación de red móvil se caracteriza por habilitar "nuevos servicios" de telecomunicaciones. En el 1G, encontramos los grandes teléfonos móviles en donde solo era posible realizar llamadas telefónicas. Con el 2G se introdujo la mensajería de texto. El 3G viene acompañado del acceso a Internet. Mientras que el 4G dio un salto con mejores velocidades de descarga de datos para permitir a los usuarios transmitir películas en dispositivos móviles o comunicarnos a través de una videollamada (Singh, 2017).

Podemos destacar que con el 4G se han detonado nuevos modelos de negocios en el intercambio de datos que facilitan la creación de nuevos bienes y servicios digitales a través de aplicaciones móviles, y dando paso a un comercio digital a nivel mundial, como por ejemplo, el servicio de taxi (Uber); hospedaje (*Airbnb)*; distribución de productos (Rappi); música (Spotify), o el comercio electrónico (Amazon). Con ello, podemos observar que los nuevos modelos de economía digital aumentaron considerablemente gracias a las nuevas generaciones de redes móviles de telecomunicaciones que ofrecen mayores capacidades de velocidad y volumen en la transmisión de información.

Cada nueva generación de redes móviles de telecomunicaciones incorpora nuevas capacidades a la comunicación a distancia. Ahora, con 5G, uno de los principales valores agregados es habilitar servicios a distancia entre personas y máquinas con grandes volúmenes de datos y a mayores velocidades que sus antecesoras, detonando una economía basada en el Internet de las cosas al reducir

el tiempo entre la emisión y recepción del mensaje entre dos dispositivos. Lo anterior, está fomentando la innovación tecnológica a través de casos de uso en diversas áreas tales como: cirugías remotas, vehículos autónomos, ciudades inteligentes, agricultura inteligente, minería a distancia, robótica industrial, realidad virtual y aumentada, entre otros (Department for Digital, Culture, Media & Sport, 2020), lo que sin duda representa nuevos retos para la ciencia jurídica y la protección de los derechos humanos.

Hasta aquí, podemos observar que 5G se ubica dentro de las redes móviles de telecomunicaciones y, en este contexto, se puede definir como "*la quinta generación de redes móviles de telecomunicaciones que facilita la comunicación a distancia con altas velocidades y baja latencia de transmisión de información entre personas y/o dispositivos tecnológicos"* (Brown, 2020). Sin embargo, las nuevas capacidades de 5G presentan nuevos desafíos debidos a las posibles aplicaciones de esta tecnología en diversos sectores. Para facilitar el estudio de estos desafíos, en el contexto internacional, la Unión Internacional de Telecomunicaciones (UIT) ha desarrollado una clasificación en tres categorías del 5G basado en el nivel de frecuencias electromagnéticas para el desarrollo de casos de uso que consideramos relevante tanto para la gestión del espectro radioeléctrico como para alcance económico, social y jurídico que puede tener el despliegue de 5G en cada país.

II.1. Tres categorías de 5G para el desarrollo de casos de uso

La UIT estructura en tres categorías el posible desarrollo de casos de uso en 5G: a) banda ancha móvil; b) banda ancha mejorada en entornos interiores y exteriores, y c) comunicaciones ultra fiables y de baja latencia (Oficina de Desarrollo de las Telecomunicaciones de la UIT, 2018, pp. 7-8).

La primera es la *Banda ancha móvil mejorada (Enhanced Mobile Broadband -eMBB)*, que es una banda ancha mejorada en entornos interiores y exteriores a la ya existente, y que puede considerarse una extensión directa del servicio de la banda ancha 4G. Esta banda facilita la colaboración empresarial y la realidad virtual. Se caracteriza por mejorar la capacidad de carga y de activación del dispositivo que permanece estable durante un intervalo de tiempo prolongado. Su objetivo es maximizar la tasa de datos y garantizar al mismo tiempo una confiabilidad moderada (IEEE, 2018).

La segunda es la *Banda ancha mejorada en entornos interiores y exteriores (Mass Type Communication -mMTC-)*. Al igual que la eMBB facilita la colaboración empresarial y la realidad virtual, pero, además, facilita las comunicaciones masivas entre máquinas dando paso a innovaciones relacionadas con el IoT, la agricultura inteligente, ciudades inteligentes, control energético, hogares inteligentes, o el seguimiento a distancia. Un dispositivo mMTC demanda mayor capacidad y está

activo de manera “intermitente”. Habilita la conexión de varios dispositivos mMTC a una estación base determinada en un momento determinado (IEEE, 2018).

La tercera categoría es la *Comunicación ultra fiable y de baja latencia (Ultra Reliability y Low Latency Communication -URLLC-)*. Esta categoría habilita un nivel mayor de interacción entre personas y máquinas. Se encuentran casos como los vehículos autónomos, las redes eléctricas inteligentes, la vigilancia de pacientes a distancia, servicios de telesalud y la automatización industrial.

Lo anterior es relevante ya que a simple vista podemos observar que no serán los mismos riesgos que estudiar para casos de uso 5G desarrollado en la banda EMBB en casos de uso como realidad virtual, que en casos de uso desarrollados en la banda ultra latencia URLLC en casos como automatización industrial o vehículos autónomos a través de redes móviles de telecomunicaciones. En el cuadro 01 pueden observarse con mayor claridad las categorías de 5G y su aplicación en diferentes casos de uso:

Cuadro 01: Casos de uso 5G por tipo de categoría de banda ancha.
Fuente: ITU.

Lo anterior ayuda a identificar qué casos de uso se pueden desarrollar de acuerdo con las diferentes capacidades de 5G, así como, prevenir sus riesgos identificando las normas jurídicas y partes relacionadas que deberán participar en el modelo de gobernanza de nuevos casos de usos desarrollados con 5G. Así, por ejemplo, en la primera categoría podemos asociar riesgos de privacidad y seguridad relacionados con 4G. Mientras que en las categorías dos y tres advertimos posibles riesgos sectoriales como en la salud de las personas, infraestructuras críticas, las cadenas de suministro o determinar la responsabilidad civil objetiva en la conducción de vehículos autónomos y manejo de uso de maquinaria a distancia.

II.2. Beneficios de 5G

El alcance de 5G impacta y se correlacionan también con el desarrollo y adopción de tecnologías como la Inteligencia Artificial, la robótica, la nube y *blockchain*, lo que dificulta medir los beneficios específicos de 5G. Lo anterior, ya que incluso sus beneficios se analizan a través de la lente de mejoras incrementales en los negocios de hoy, en lugar de imaginar cómo podrían usarse para remodelar industrias y, aún más ampliamente, atender soluciones contemplando problemas como el medio ambiente, la pobreza y la atención de la salud (Abbosh, O., & Downes, L, 2019). No obstante, se espera que 5G genere importantes beneficios económicos y sociales en nivel global.

Los estudios sobre el impacto económico de 5G cuentan con diversos resultados. No obstante, entre los principales hallazgos se estima una contribución del 5G al PIB mundial entre 1,4 billones de dólares y 3,5 billones de dólares durante los próximos 10 a 15 años (*Oxfords Economics*, 2019). Igualmente, algunos datos alrededor del mundo son los siguientes:

- KISDI, grupo de expertos en TIC estatal líder en Corea del Sur, predijo que 5G agregará 967.5 mil millones de dólares a la economía mundial para 2026, creciendo a una tasa promedio anual del 43.3 por ciento entre 2022-2026. (*Inter-American Development Bank*, 2020).
- El Banco Mundial estima que el aporte de 5G será de 13,2 billones de dólares en valor económico global para 2035, generando 22,3 millones de puestos de trabajo solo en la cadena de valor global 5G (*World Economic Forum*, 2020).
- En la Unión Europea se estima que en 2025 los beneficios de 5G podrían alcanzar los 113.100 millones de euros al año en cuatro sectores clave que serán los primeros usuarios de la conectividad 5G: automoción, salud, transporte y energía. Y es probable que las inversiones de 56 600 millones de euros creen 2,3 millones de puestos de trabajo en Europa (*European Commission*, 2016).
- En Estados Unidos, para 2025 se espera que 5G otorgue 16 millones de puestos de trabajo en todos los sectores de la economía; 2,7 billones de dólares en crecimiento adicional de la producción bruta (ventas); y 1.5 billones al PIB de los Estados Unidos, más que el PIB anual (*Accenture*, 2021).
- En China se espera que 5G genere 6.3 billones de yuanes (930 mil millones de dólares) de producción económica para 2030 y 8 millones de nuevos puestos de trabajo (*Xinhua*, 2017).
- Para América Latina también se espera un crecimiento económico derivado del 5G. Se espera un aumento considerable del PIB durante diez años (2019-2029) si la tecnología 5G se despliega en América Latina con un total de 292,637 millones de dólares (*Statista, 2021)*.

Sin duda, 5G puede traer grandes beneficios a distintos sectores. Sin embargo, para ello tendrán que abordarse sus desafíos de manera sistémica. Uno de ellos es la estandarización nacional e internacional, ya que, las redes de telecomunicaciones móviles facilitan una comunicación a distancia a nivel internacional que trasciende fronteras. Estos desafíos se han abordado en diferentes foros internacionales entre los que destacan la UIT y el grupo de trabajo 3GPP que ha generado estándares internacionales para las telecomunicaciones móviles, tales como las IMT-2020 (*International Mobile Telecommunication*) en donde se advierten tres categorías de 5G: (I) banda ancha móvil mejorada (eMBB), las comunicaciones masivas tipo máquina (mMTC), y las comunicaciones ultra confiables y de baja latencia (URLLC) (3GPP, 2020). La categorización de 5G se basa en sus capacidades técnicas y uso de frecuencias de espectro radioeléctrico lo cual es relevante a la hora de conocer sus posibles riesgos a la salud o incluso a riesgos de seguridad en las infraestructuras críticas.

II.3. Desafíos en 5G

Son varios los desafíos de 5G, algunos incluso se relacionan con el sector de aviación. Por ejemplo, en Estados Unidos la Administración Federal de Aviación (FAA) se pronunció sobre los posibles riesgos de la "banda C" de 5G -*ultra confiables y de baja latencia URLLC*- en los radares de aviación para los aterrizajes de vuelos comerciales, por lo que solicitó a Verizon y AT&T prolongar el despliegue 5G en ciertas zonas del aeropuerto (FAA Aviation Safety, 2021). En el mismo sentido, durante el despliegue de 5G en Chile se analizaron los posibles inconvenientes de esta tecnología para el sector de aviación y la Subsecretaría de Telecomunicaciones generó un plan de fiscalización en los 17 aeropuertos del país que contarán con 5G (Espinosa, 2022).

De esta forma podemos advertir que 5G implica grandes retos que van más allá del tema económico y despliegue de infraestructura de telecomunicaciones. Algunos que consideramos relevantes en materia de derechos humanos que los países deben considerar en torno a 5G son aquellos relacionados con la salud, el medio ambiente y la protección de datos personales que analizaremos en seguida.

II.3.1. Salud

En materia de 5G y salud se discuten principalmente dos temas. El primero su relación con algunos tipos de cáncer en las personas por la exposición a campos electromagnéticos (OMS, 2014). El segundo, por la hipersensibilidad electromagnética que las ondas electromagnéticas de altos rangos niveles pueden causar en ciertas personas (*International Agency for Research on Cancer*, 2011). Incluso, éstos temas han generado diversas protestas sociales y ataques a infraestructura 5G tales como antenas en ciudades como Barcelona, Reino Unido o Suiza (Pretz, 2019).

Actualmente, entre los primeros estudios científicos sobre a exposición de ondas electromagnéticas y su relación con cáncer en las personas, afirman que las exposiciones menores a 6 GHz se consideran fuera de peligro; mientras que las mayores a 6 GHz aún están en estudio y no existe evidencia científica de su afectación a la salud por lo que se sugiere recabar mayor información, (*Australian Radiation Protection and Nuclear Safety Agency*, 2019). En el segundo punto, sobre la hipersensibilidad electromagnética, la OMS recomienda a los gobiernos proporcionar información a la población sobre los posibles peligros para la salud de los Campos Electromagnéticos (CEM), y sugiere incluir una declaración clara en el sentido que actualmente no existe una base científica para determinar una conexión entre la hipersensibilidad electromagnética y la exposición a los CEM (OMS, 2020).

De igual manera debemos destacar que recientemente la OMS, la Comisión Internacional de Protección de Radiación, la UIT, y el Centro Internacional de Investigaciones sobre el Cáncer, son algunas de las instituciones más importantes que estudian a nivel internacional los efectos negativos de las ondas electromagnéticas en la salud de las personas. No obstante, algunos países que lideran la regulación sobre los límites de exposición a CEM son Corea del Sur, Alemania, Nueva Zelanda, Finlandia, Suecia, Reino Unido, Australia, Estados Unidos y Colombia en Latinoamérica (*Existence of Standards*, 2022).

Por otro lado, destacamos los estudios realizados por países como Australia y Estados Unidos respecto al impacto en la salud de 5G de manera específica. En Australia, la Agencia Australiana de Protección Radiológica y Seguridad Nuclear estableció límites para la exposición a energía electromagnética y radiofrecuencia vinculada a 5G (ARPANSA, 2019), argumentando que, si bien no existe evidencia científica que concluya que la exposición por debajo de 6 GHz afecte la salud de las personas, recomienda continuar con la investigación de frecuencias superiores a 6 GHz (ARPANSA, 2019).

Por otro lado, actualmente la OMS lleva a cabo una evaluación específica sobre los riesgos para la salud derivados de la exposición a las radiofrecuencias que cubre todo el rango de radiofrecuencias incluido el 5G el cual, a la fecha de publicación de este artículo está pendiente de publicación (OMS, 2020). No obstante, en tanto, la OMS reconoce como pautas de exposición internacional las emitidas por la Comisión Internacional de Protección contra las Radiaciones No Ionizantes, (*International Commission on Non-Ionizing Radiation Protection*, 2020), y el *Instituto de Ingenieros Eléctricos y Electrónicos, a través del Comité Internacional de Seguridad Electromagnética*, quienes, si bien no emiten pautas específicas sobre 5G cubren radiofrecuencias de hasta 300 GHz, incluidas las frecuencias en discusión para 5G, por lo que muchos países se adhieren actualmente a dichas pautas.

En el caso de México debemos destacar que estas recomendaciones son consideradas en el numeral 6.1.1 del *Acuerdo mediante el cual el Pleno del Instituto*

*Federal de Telecomunicaciones expide la Disposición Técnica IFT-007-2019: Límites de exposición máxima para seres humanos a radiaciones electromagnéticas de radiofrecuencia no ionizantes en el intervalo de 100 kHz a 300 GHz en el entorno de estaciones de radiocomunicación o fuentes emisoras (*DOF, 25/02/2020). No obstante, para garantizar el derecho a la salud en relación con el despliegue de nuevas redes de telecomunicaciones, consideramos necesario fortalecer los procesos de verificación en el despliegue de nuevas redes de telecomunicaciones móviles 5G. Esto requerirá un esfuerzo de coordinación entre autoridades a nivel federal, local y municipal por la instalación de antenas 5G.

II.3.2. Medio ambiente

En medioambiente y 5G se destacan aspectos positivos y negativos. Por una parte, se discuten los inconvenientes de los desechos electrónicos y la contaminación electromagnética. Por el otro, se destacan los beneficios que podría arrojar la tecnología 5G para combatir el cambio climático a través de sus diversas aplicaciones tecnológicas.

Como un primer punto de partida en medio ambiente y 5G es importante considerar las recomendaciones de la Comisión de Estudio CE5 de la UIT (UIT, 2022), sobre los efectos de las TIC en el cambio climático, en donde podemos destacar los siguientes temas: (I) la economía circular, incluida la basura electrónica (UIT, 2021), (II) el cambio climático y la evaluación de las TIC en el marco de los Objetivos de Desarrollo Sostenible de la ONU (UIT, 2021), (III) la adaptación de la tecnología de bajo costo y sostenible (UIT, 2021), y (IV) un mayor número de dispositivos IoT y antenas (Curran, 2020). Estas acciones son acordes con el Acuerdo de París (United Nations, 2015) sobre el cambio climático, en donde se destaca en el numeral 10 la importancia de la tecnología para poner en práctica medidas de mitigación al cambio climático (El Acuerdo de París, 2020).

Por otra parte, algunos de los efectos positivos que 5G podría ofrecer al medio ambiente derivan de sus propias capacidades en la innovación de soluciones tecnológicas que permiten medir y mejorar el consumo energético en distintos sectores industriales. Por ejemplo, mejorar de la eficiencia energética; reducir las emisiones de gases de efecto invernadero; incrementar el uso de energías renovables; reducir la contaminación del aire y el agua; minimizar el desperdicio de agua y alimentos; proteger la vida silvestre; mejorar la toma de decisiones sobre el clima, la agricultura y las plagas, o la reducción de desechos electrónico, entre otros (Cho, 2020).

Igualmente, a nivel internacional existe una serie de recomendaciones por parte de la UIT en relación con el uso de tecnologías móviles y eficiencia energética que pueden ayudar a instituciones públicas y privadas a llevar a cabo un despliegue y adopción sustentable de la tecnología (ITU, 2021), entre las que podemos destacar: (I) Recomendación UIT-T L.1210 sobre soluciones sostenibles de

alimentación de energía para redes 5G, (II) Recomendación UIT-L L 1331 sobre Evaluación de la eficiencia energética de las redes móviles, (III) UIT-T L Suppl.36 a UIT-T L. 1310 sobre Estudios de métodos y métodos para avaluar la eficiencia energética para futuros sistemas 5G.

En el caso mexicano, el derecho al medio ambiente se garantiza conforme a los artículos 4, quinto párrafo y 25 párrafo noveno de la CPEUM, al señalar respectivamente que: "*Toda persona tiene derecho a un medio ambiente sano para su desarrollo y bienestar. El Estado garantizará el respeto a este derecho. El daño y deterioro ambiental generará responsabilidad para quien lo provoque en términos de lo dispuesto por la ley",* y "*bajo criterios de equidad social, productividad y sustentabilidad se apoyará e impulsará a las empresas de los sectores social y privado de la economía, sujetándolos a las modalidades que dicte el interés público y al uso, en beneficio general, de los recursos productivos, cuidando su conservación y el medio ambiente*".

En relación con lo anterior, en el artículo 147 de la LFTR se prevé que es obligación del Ejecutivo Federal, a través de la Secretaría de Comunicaciones y Transportes (SCT), coordinar *con las dependencias o entidades administradoras de inmuebles, el INDAABIN, la Secretaría de Hacienda y Crédito Público, la Secretaría de Energía, la Secretaría de Medio Ambiente y Recursos Naturales, la Secretaría de Desarrollo Agrario, Territorial y Urbano, a fin de establecer las bases y lineamientos para instrumentar la política inmobiliaria que permita el despliegue de infraestructura de telecomunicaciones*.

No obstante, lo anterior, no observamos una atribución específica del IFT en materia de medio ambiente y telecomunicaciones en cuanto al despliegue de infraestructura como lo son las redes móviles de telecomunicaciones. Es aquí en donde observamos necesario fortalecer las atribuciones del IFT en relación con la SCT, y la Secretaría de Medio Ambiente y Recursos Naturales para:

- Dotar al IFT de atribuciones legales para la protección del medio ambiente en colaboración con las instituciones públicas competentes en la materia;
- Emitir lineamientos mínimos que deberán observar los concesionarios de telecomunicaciones en el despliegue de infraestructura incluyendo las redes móviles, en colaboración con la Secretaría de Medio Ambiente y Recursos Naturales;
- Establecer los requisitos de protección de medio ambiente en los procesos de licitación de despliegue de infraestructura a cargo de los concesionarios, considerando como punto de partida las recomendaciones de la UIT;
- Obtener opinión vinculante de la Secretaría del Medio Ambiente y Recursos Naturales previo al despliegue de la infraestructura de telecomunicaciones por parte de los concesionarios de telecomunicaciones;

- Promover casos de uso basados en tecnologías como 5G para combatir el cambio climático en colaboración con el sector público, privado, social y académico;
- Establecer centros de innovación en colaboración con la Secretaría de Economía, la Secretaría de Salud, el INFOTEC, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación; así como, las universidades públicas y privadas, con el objeto de identificar y promover el uso de 5G en sectores productivos del país.

Con lo antes descrito, consideramos que en México puede fortalecerse el despliegue de infraestructura de telecomunicaciones con respeto al derecho al medio ambiente previsto en la CPEUM, para lo cual la coordinación entre instituciones públicas, y la actualización del marco normativo de telecomunicaciones será indispensable.

II.3.3. Protección de datos

Las mayores capacidades de 5G en velocidad y volumen de transmisión de información a través de redes de telecomunicaciones requiere de mayor capacidad de infraestructura, tales como puntos de acceso y equipos terminales para los usuarios. Un ejemplo de ello son la necesidad de antenas que se requieren para el funcionamiento 5G. Por ejemplo, para cubrir con 4G la ciudad de Manhattan se requieren aproximadamente 100 antenas, mientras que para llevar 5G a la misma ciudad se requiere de 5 000 a 20 000 antenas las cuáles además estarán más cerca de las personas (Cooley, 2020), lo que, a su vez, podría incrementar riesgos en privacidad y seguridad de información al conocer su ubicación de manera más precisa.

Igualmente, la gran cantidad de dispositivos conectados a Internet y los diferentes proveedores de *hardware* y *software* dificultan la determinación de responsabilidades y armonización de estándares en materia de privacidad y seguridad de la información, lo que podría incluso afectar la neutralidad de la red. Ante estas preocupaciones, instituciones como la Agencia Española de Protección de Datos, la *Commission Nationale de l'Informatique et des Libertés* (CNIL, por sus siglas en francés), ENISA, NIST, la Unión Europea (UE), y países como Australia, Japón, Chile, España, han desarrollado recomendaciones y/o marcos regulatorios en materia de privacidad y ciberseguridad vinculados con 5G, de los cuales identificaremos las principales coincidencias en los siguientes apartados.

Un primer aspecto para destacar con 5G es el incremento de dispositivos IoT a través de redes móviles de telecomunicaciones. El desarrollo y uso de dispositivos IoT implicará la convergencia de fabricantes de dispositivos, proveedores de servicios de telecomunicaciones, plataformas de servicios y desarrolladores de aplicaciones. Esto sin duda dificultará determinar las obligaciones de cada uno de ellos en relación con el actual marco normativo en protección de datos personales

a nivel mundial. Por ejemplo, identificar quien tiene el deber informar y de obtener el consentimiento del titular de los datos con base en el flujo de datos en dispositivos IoT será uno de los principales desafíos de las autoridades de protección de datos en relación con el 5G.

En este contexto, la AEPD identifica que los principales riesgos de 5G en la protección de datos personales son aquellos relacionados con: (I) el perfilado y decisiones automatizadas, ante un aumento en la cantidad y categorías de datos que circulan en Internet por el uso de dispositivos IoT, (II) distinguir las responsabilidad entre fabricantes, operadores de red y proveedores de servicios, (III) la falta de un modelo homogéneo de seguridad ya que 5G permite la existencia de múltiples agentes en la cadena de comunicación y cada agente puede cumplir con diferentes estándares de seguridad, (IV) las vulnerabilidades derivadas de los entornos virtuales y funciones compartidas, (V) la geolocalización de la persona ya que 5G utiliza más estaciones base a una menor distancia entre sí, que hace que la localización geográfica basada en la red sea más precisa, y (VI) la posible pérdida de control del usuario sobre sus datos personales, toda vez que el flujo de datos y la diversidad de responsables puede implicar transferencias internacionales complicando además el ejercicio de sus derechos (AEPD, 2020).

Antes estos desafíos es importante traer a colación lo que establece el considerando 30 del Reglamento General de Protección de Datos (RGPD) de la UE, al señalar que las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus "*dispositivos*", aplicaciones, herramientas y protocolos, con lo que podemos observar que independientemente de 5G y la ubicación de las antenas de telecomunicaciones más cercana a las personas, los riesgos a través de dispositivos tecnológicos ya son considerandos en legislaciones de protección de datos personales, en donde podemos observar cada vez más común el uso de dispositivos como teléfonos móviles, tabletas, televisiones inteligentes, robots aspiradores, pulseras de actividad física, o asistentes virtuales con altavoces inteligentes, que en muchas ocasiones no cumplen con principios de protección de datos desde su diseño.

Un ejemplo de lo anterior son las aspiradoras de la empresa "*Roomba*" (Wolfe, 2017), quien hace algunos años anunció, junto con *Google*, su intención de vender los mapas de los hogares que el robot aspirador realizaba al moverse por las casas de sus usuarios. Igualmente, en el año 2020, la empresa Izan anunció la venta de televisiones inteligentes, las cuales pueden incorporan un micrófono y/o cámara con las que se puede recoger sonidos e imágenes sin el consentimiento del titular (Izan, 2020).

El tema se agrava aún más cuando los dispositivos móviles tratan datos personales sensibles. Un caso es el de Alexa, un asistente de hogar que puede dar consejos "médicos" a los pacientes desde sus casas y, a cambio de ello, Amazon podía monetizar dicha información con *marketing* personalizado (*Department of*

Health and Social Care, 2019). Otro ejemplo más fue la intención de *Google* de comprar la empresa americana *Fitbit*, dedicada a ofrecer dispositivos para monitorear la actividad física de las personas a través de relojes inteligentes incluyendo su frecuencia cardiaca (*European Commission*, 2020), en donde en el marco del RGPD, la UE le prohibió a Google utilizar los datos de *Fitbit* para mostrar publicidad a sus usuarios (AEPD, 2021).

Incluso en el desarrollo de dispositivos IoT encontramos algunas innovaciones en biotecnología que pueden incorporarse al cuerpo humano, lo que se ha denominado *Internet de los Cuerpos (IoB, por sus siglas en inglés)*. Estos dispositivos conectados a Internet pueden medir datos sobre la salud de las personas desde el interior de sus cuerpos, por ejemplo, los marcapasos, las "píldoras digitales" que permiten transmitir datos desde el interior del sistema digestivo de una persona a través de sensores una vez ingeridas, o los estudios sobre el desarrollo de órgano en impresión 3D, como la bioimpresión de un páncreas que permitirá el uso regular de insulina para individuos con algunos tipos de diabetes (AEPD, 2021).

Sin duda estas innovaciones pueden ser de gran ayuda para las personas es áreas como la salud, sin embargo, presentan aún grandes desafíos en materia de protección de datos personales ya que sus fabricantes aún no consideran los principios de privacidad desde su diseño, por lo que temas como el principio de privacidad desde el diseño o la evaluación de impacto en dispositivos IoT, son nuevos retos a la legislación de datos personales. Igualmente, temas como la determinación de responsable, la obtención del consentimiento, la elaboración de perfiles, geolocalización o el procedimiento para el ejercicio de derechos son temas que pondrán a prueba a aplicación de la legislación de privacidad alrededor del mundo, ante el uso cada vez más común de dispositivos IoT impulsados por las redes móviles de telecomunicaciones de quinta generación.

Al día de hoy ya comienzan a verse algunos conflictos relacionados con IoT y datos personales. Por ejemplo, la autoridad de control de Noruega impuso una multa a la empresa americana "*Zeta Global*" por 2.5 millones de euros, al concluir que realizaba un seguimiento a ciudadanos noruegos en sitios web, servicios y "dispositivos", con lo cual creaban perfiles de usuarios y divulgaban sus datos para fines de *marketing* sin su consentimiento (*European Data Protection Board*, 2021).

Ante este tipo de nuevos conflictos para la protección de datos, consideramos relevante adoptar buenas prácticas en la evaluación de impacto da datos personales que consideran diversas legislaciones alrededor del mundo, como la emitida por la autoridad de control francesa para dispositivos IoT: *Guía de Evaluación de Impacto en Privacidad en dispositivos IoT*. En dicha guía se destacan controles relacionados con la minimización, la duración del almacenamiento de datos, el flujo sobre tratamiento de datos en dispositivos, controles de derechos de los usuarios; así como, la obtención del consentimiento en diversos dispositivos y aplicaciones que

interactúan entre sí para prestar un servicio al usuario final (CNIL, 2018). Sin duda, estos temas serán una tarea pendiente para las autoridades de control de datos personales de cualquier país con la adopción de tecnologías como 5G y el creciente uso de dispositivos móviles.

II.3.4. Ciberseguridad

Actualmente existen aproximadamente 9 mil millones de dispositivos IoT activos en el mundo, y se espera que este número se triplique para 2030 a casi 25,5 mil millones (Khantimirov, 2021). Sin duda, con más dispositivos y velocidades más rápidas aumenta el riesgo de ciberataques. Ahora bien, entre los riesgos identificados en relación con 5G y seguridad de la información son diversos, los cuales pueden clasificarse en nueve grupos para facilitar su análisis, tales como: 1) abuso de activos; 2) intercepción de información; 3) ataques físicos a redes de telecomunicaciones y dispositivos móviles; 4) daños no intencionales; 5) fallas de redes y equipos de telecomunicaciones; 6) daños no intencionales; 7) averías o mal funcionamiento a redes y dispositivos de telecomunicaciones de energía; 8) desastres naturales, y 9) aspectos legales (ENISA, 2020).

De las amenazas antes listadas podemos observar que algunas son comunes a las que observamos con las actuales redes de telecomunicaciones. Sin embargo, destacamos que con 5G se prevé un incremento de amenazas a las redes móviles de telecomunicaciones, a la intercepción de información y la falta de mecanismos de seguridad y autenticación en dispositivos móviles. Algunos ejemplos de lo anterior son los ataques a las antenas 5G en Europa durante 2020 (EL PAÍS, 19 de mayo 2020), algunos ataques provocados por noticias falsas que el 5G propagaba el virus Covid-19 y la falta de una comunicación oficial de las autoridades a la población sobre el despliegue de 5G y sus implicaciones.

Otro riesgo que puede repetirse con 5G es el ocurrido en 2016 conocido como "*ciberataque Dyn de 2016*", en donde a través de dispositivos móviles conectados a Internet sin requisitos mínimos de seguridad tales cámaras de seguridad, impresoras y monitores para bebés que dejó inaccesible grandes plataformas y servicios de Internet afectando a una gran cantidad de usuarios en Europa y Norteamérica (Mucientes, 2016).

Además, entre las principales preocupaciones a nivel internacional por ciertos países es que 5G requiere de la instalación de más torres y antenas, lo que también aumenta los riesgos de la instalación de torres falsas; así como, diversas formas de vigilancia. Un ejemplo de lo anterior es el caso de Huawei contra el gobierno de los Estados Unidos de América, en donde a los funcionarios estadounidenses les preocupa que la tecnología de dicha empresa pueda usarse contra la nación estadounidense como una herramienta de espionaje a favor del gobierno chino (Madnick, 2020).

La buena noticia es que otros países como Japón, España, Australia y en general la UE se han preocupado por mejorar sus leyes políticas públicas en materia de 5G y seguridad de la información. Por ejemplo, la Unión Europea desarrolló una "caja de herramientas de ciberseguridad y 5G", en donde se promueve contar con un perfil de riesgo de proveedores de telecomunicaciones y un régimen de certificación de fabricantes de dispositivos IoT, aunado al fortalecimiento de infraestructuras críticas (*Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, EC*, 2021).

En Japón podemos destacar incluso aspectos de ciberseguridad relacionados con la autenticación de usuarios a través de *blockchain,* la firma electrónica y el sello del tiempo; así como, la ciberseguridad en ciudades inteligentes y el desarrollo de medidas de seguridad desde el diseño en IoT, como respuesta a las vulnerabilidades tanto del software como del hardware (Medidas integrales de seguridad IOT/5G 2020, Grupo de Trabajo de Seguridad Cibernética, 2020). En el caso de España podemos destacar la creación de un análisis de riesgo de operadores de telecomunicaciones; la certificación de redes 5G; el análisis de vulnerabilidad en la cadena de suministro, y los requisitos de seguridad en equipos terminales de telecomunicaciones y dispositivos móviles (Proyecto de Ley de Ciberseguridad en 5G, Ministerio de Asuntos Económicos y Transformación Digital, 2021).

Por último, tenemos el caso de Australia y Chile. El primero establece la obligación de seguridad incluso a proveedores de transportes para cuidar la cadena de suministro al igual que España y que Chile (Norma de ciberseguridad, Diario Oficial Chile, 2020), prevé un procedimiento de notificación de brechas de seguridad a operadores de telecomunicaciones Parlamento Australiano (Minister for Communications and the Arts, 2018).

Como observamos, la regulación en ciberseguridad y 5G se enfoca en diversas áreas. Algunas están destinadas a fabricantes de productos. Otras a operadores de redes de telecomunicaciones y otras más a proteger la infraestructura crítica y la cadena de suministro. Entre las principales coincidencias de regulación en ciberseguridad y 5G encontramos las siguientes: (I) reforzar requisitos de seguridad a operadores de telecomunicaciones, (II) establecer un perfil de riesgo de proveedores de productos IoT, (III) contar con un régimen de certificación para la seguridad de equipos terminales y dispositivos, (IV) desarrollar medidas de seguridad en ciudades inteligentes, (V) reforzar servicios de confianza para reducir riesgos de suplantación de identidad a través de la autenticación de usuarios como la firma electrónica y el sello de tiempo, (VI) la seguridad de infraestructuras críticas, (VII) implementar criterios para analizar vulnerabilidades a la cadena de suministro, (VIII) apoyar la investigación en ciberseguridad, y (IX) establecer procedimientos de notificación a las autoridades gubernamentales sobre brechas de seguridad relacionada con infraestructura de telecomunicaciones.

Por otra parte, Estados Unidos, a través de NIST generó un primer borrador de prácticas que permitan a operadores y usuarios de redes 5G mitigar los riesgos de ciberseguridad, la cual se estructura en dos áreas. La primera en seguridad de la infraestructura en la nube confiable y segura. La Segunda, relacionada con las configuraciones de seguridad en 5G como el despliegue de estaciones base 5G *New Radio* y un 5G de siguiente generación, y propone un monitoreo continuo del tráfico 5G en las capas de señalización y datos para detectar y prevenir ataques y amenazas de seguridad cibernética (*National Cybersecurity Center of Excellence*, 2021).

Por último, algunos fabricantes de dispositivos como Ericsson y Nokia (Nokia, 2021) también consideran elementos de seguridad vinculados con 5G, entre los que destacamos: 1) contar con esquemas de gestión de identidad superior en IoT; b) desarrollar soluciones de seguridad de extremo a extremo (entre el dispositivo y el servidor en Internet); 3) fortalecer la seguridad en la nube de telecomunicaciones; 4) fomentar el uso de estándares internacionales como 3GPP; 5) priorizar la seguridad en infraestructuras críticas; y 6) explorar el uso de *blockchain* para garantizar la seguridad y privacidad en redes 5G (Ericsson, 2021).

Como observamos, los aspectos de seguridad y 5G van más allá de las redes de telecomunicaciones, se requiere la creación de otras políticas públicas o marcos regulatorias en materia de ciberseguridad. Igualmente, se requerirá fortalecer la coordinación de autoridades competentes en materias como las telecomunicaciones, ciberseguridad, economía, protección de datos; así como, con los sectores privados como los fabricantes de dispositivos móviles.

Entre las medidas de seguridad 5G que destacamos, y consideramos que para el caso de México sería esencial que el IFT, en coordinación con el sector público y privado, considere armonizar con la política de telecomunicaciones son aquellas relacionadas con la autenticación e identidad de los usuarios, contar con mecanismos de certificación de fabricantes de dispositivos IoT, mejorar la seguridad de la nube, y fortalecer la seguridad de infraestructuras críticas. Todas ellas son comunes a las normas y proyectos de ciberseguridad a nivel internacional e implican un gran reto que requiere la coordinación de diferentes partes relacionadas para su puesta en marcha.

III. Conclusiones

El despliegue de 5G debe considerar diferentes áreas de manera sistémica además del sector de las telecomunicaciones. Si bien, se prevé que esta tecnología traiga beneficios económicos al desarrollo de los países, también representan riesgos a los derechos humanos como la salud, el medio ambiente y la protección de datos personales. Por ejemplo, las mayores capacidades en volumen y velocidad de información que ofrece la quinta generación de redes móviles de

telecomunicaciones requiere el despliegue de infraestructura como las antenas 5G que procesarán frecuencias radioeléctricas por encima de los 6GHZ, lo cual ha representado ya a nivel internacional nuevos retos como la hipersensibilidad electromagnética, la vigilancia, la geolocalización más precisa o la contaminación electromagnética y el incremento de desperdicios de dispositivos IoT.

Para reducir los riesgos a los derechos humanos como la salud, el medio ambiente y la protección de datos personales, la coordinación de sectores públicos, privados y académicos será indispensable para maximizar los beneficios de 5G y mitigar sus riesgos. Es decir, las políticas de telecomunicaciones 5G deben conectarse de manera sistémica con otras políticas públicas y marcos regulatorios, que incluya los tres niveles de gobierno y los sectores público, privado, social y académico de manera coordinada en un contexto nacional e internacional conectividad digital en México y en el mundo.

En el caso de México, consideramos que la regulación internacional y buenas prácticas internacionales pueden considerarse como un punto de referencia para el despliegue de 5G en el país. Será necesario incorporar algunos elementos a la LFTyT para afrontar los desafíos vinculados de las nuevas redes móviles de telecomunicaciones con la protección de datos personales, la salud y el medio ambiente. No obstante, debemos destacar que, en el marco de políticas públicas, el IFT ha impulsado en México un mecanismo de coordinación a nivel nacional a través del “Comité 5G” en donde se observa la participación de instituciones públicas, privadas y académicas. Sin duda, uno de los retos será mantener vigente y operante esta iniciativa en donde se permita identificar las necesidades técnicas, económicas y de despliegue de infraestructura que atienda las necesidades de desarrollo económico, industrial y social del país.

De esta forma, entre las principales conclusiones y recomendaciones que consideramos pueden aportar valor en el despliegue de 5G en México, acorde al alcance de esta investigación en áreas de salud, medio ambiente, protección de datos personales y seguridad de la información, destacamos las siguientes:

Primero, en *materia de salud y 5G* debemos destacar que la instalación de un mayor número de antenas más cerca de la población genera incertidumbre sobre sus posibles riesgos en la salud como la causa de cáncer, y la hipersensibilidad electromagnética. Al respecto, si bien existen estudios científicos que refieren que ondas de frecuencia baja de 5G –por debajo de los 6Ghz- no representan un riesgo a la salud de las personas, autoridades de Estados Unidos y Australia han sugerido continuar realizando mayores estudios sobre ondas electromagnéticas superior a los 6GHZ, con la finalidad de obtener mayor evidencia científica.

Lo anterior es interesante, ya que, incluso al día de hoy la OMS considera a los campos electromagnéticos de radiofrecuencia en el grupo 2B de agentes clasificados como cancerígenos, independientemente del nivel de frecuencia de que se trate (OMS, *Agents Classified by the IARC*). En este sentido, para reducir los

riesgos a la salud del 5G, la propia OMS ha sugerido a los países observar las disposiciones emitidas por la *Comisión Internacional de Protección contra las Radiaciones No Ionizantes,* en donde se prevén los límites máximos de exposición y la distancia de instalación de redes de telecomunicaciones a cargo de operadores de redes móviles de telecomunicaciones para minimizar el impacto negativo a la salud de las personas.

En el caso de México observamos que el IFT publicó en 2020 el *Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide la Disposición Técnica IFT-007-2019: Límites de exposición máxima para seres humanos a radiaciones electromagnéticas de radiofrecuencia no ionizantes en el intervalo de 100 kHz a 300 GHz en el entorno de estaciones de radiocomunicación o fuentes emisoras.* En el numeral 6.1.1. de dicho acuerdo se contemplan las normas internacionales sobre límites máximos de exposición de radiaciones electromagnéticas para seres humanos de la *Comisión Internacional de Protección contra las Radiaciones No Ionizantes,* lo cual nos parece muy acertado por parte del IFT. No obstante, lo anterior, consideramos que las siguientes cuatro acciones pueden fortalecer el derecho a la salud en México en relación con el despliegue de 5G:

- Dotar de facultades de verificación al IFT en la instalación de infraestructura 5G en colaboración con autoridades federales y locales; así como, con la Secretaría de Salud, con el objeto de supervisar el debido cumplimiento de esta normas nacionales e internacionales.
- Incluir en los procesos de licitación que realice el IFT una descripción específica sobre el cumplimiento de normas nacionales e internacionales de protección a la salud en relación con el despliegue de infraestructura móvil de telecomunicaciones, con el objeto de orientar a los operadores de redes de telecomunicaciones sobre la importancia de cumplir con estándares internacionales de protección de a la salud y campos electromagnéticos.
- También, consideramos importante que el IFT, a través de su departamento de comunicación genere campañas de información a la población sobre 5G y sus riesgos a la salud, con la finalidad evitar la desinformación en la población como lo ocurrido en la Unión Europea en donde personas atacaron antenas 5G por considerar que propagaba el virus SARS-CoV-2.
- Por último, consideramos relevante impulsar casos de uso basados en 5G en el sector de salud como la medicina a distancia, en colaboración con el sector privado, la Secretaría de Salud; así como, con universidades y centros de innovación en el país.

En segundo lugar, en *materia 5G el derecho al medio ambiente* observamos que existen aspectos positivos y negativos de esta tecnología. Por una parte, existen preocupaciones a nivel internacional sobre la contaminación electromagnética en lo que hace a uso de nuevas frecuencias radioeléctricas y a los desperdicios

tecnológicos debido al incremento del uso de dispositivos IoT. Sin embargo, se destaca que gracias a las mayores capacidades de 5G la innovación tecnológica puede traer nuevas soluciones al combate del cambio climático alrededor el mundo.

Ahora bien, algunas de las posibles soluciones que la UIT recomienda para reducir los riesgos de 5G al medio ambiente son: fomentar la "*economía circular*", es decir, aprender a compartir, alquilar, reutilizar, reparar, renovar y reciclar materiales para la producción y consumo de tecnología que reduzca su impacto negativo al medio ambiente. Para ello, contar con mecanismos de coordinación que faciliten información a todas las partes relacionadas será una pieza clave para promover nuevos modelos económicos más sustentables al medio ambiente.

En el caso de México consideramos que deben fortalecerse las facultades del IFT en materia ambiental e infraestructura de telecomunicaciones. Por ejemplo, en el actual artículo 15 de la LFTyR sería idóneo establecer la competencia del IFT para promover, en coordinación con autoridades medioambientales, empresas del sector privado y social, la protección del medio ambiente en el despliegue de infraestructura móvil de las telecomunicaciones y el uso de dispositivos IoT.

Otra posible alternativa es incluir en el plan de trabajo del Comité 5G de México temas relacionados con la protección del medio ambiente y telecomunicaciones; así como, la promoción y difusión de modelos económicos de economía circular que promuevan la protección al medio ambiente e incluso incentiven la innovación tecnológica en ésta materia.

Además, como punto de partida para llevar a cabo un despliegue de nueva infraestructura de telecomunicaciones con respeto al medio ambiente, pueden adoptarse en los proceso de licitación las recomendaciones de la UIT tales como: (I) la Recomendación UIT-T L.1210 sobre soluciones sostenibles de alimentación de energía para redes 5G; (II) Recomendación UIT-L L 1331 sobre evaluación de la eficiencia energética de las redes móviles; (III) UIT-T L Suppl.36 a UIT-T L. 1310 sobre estudios de métodos y métodos para avaluar la eficiencia energética para futuros sistemas 5G.

Igualmente, el IFT puede establecer requisitos de protección al medio ambiente en los procesos de licitación de despliegue de infraestructura a cargo de los concesionarios; así como, promover casos de uso basados en tecnologías como 5G para combatir el cambio climático en colaboración con el sector público, privado, social y académico. Para ello, en el Comité 5G, puede establecerse una línea de trabajo junto con la Secretaría de Economía, la Secretaría de Medio Ambiente y Recursos Naturales, y INFOTEC, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación; así como, con las universidades públicas y privadas, con el objeto de desarrollar y promover políticas de "economía circular" en el sector de las telecomunicaciones y dispositivos IoT e identificar y desarrollar casos de uso 5G en sectores productivos del país para la protección de medio ambiente.

En tercer lugar, *en materia de privacidad y seguridad de la información*, observamos que el incremento en el uso de dispositivos IoT representa nuevos desafíos para la legislación de protección de datos personales, tales como, la obtención del consentimiento, la determinación del responsable o el ejercicio de derechos en razón de todos los proveedores de productos y servicios a través de dispositivos IoT. En otras palabras, la interacción entre fabricantes, operadores de redes de telecomunicaciones y proveedores de servicios sin duda complica el cumplimiento de las obligaciones y principios en protección de datos personales como el deber de informar, los procedimientos para el ejercicio de datos personales, o la determinación de corresponsables de tratamiento.

Un ejemplo de lo anterior es que con el uso de dispositivos IoT a través de redes móviles de telecomunicaciones, puede obtenerse una geolocalización y perfilado de los usuarios, más preciso, una vigilancia por parte de gobiernos que argumentan seguridad pública o nacional, o el incremento a ataques a infraestructuras críticas a través del despliegue de más antenas instaladas con mayor proximidad a la población.

Para atender algunos desafíos en protección de datos personales, la Agencia Española de Protección de Datos en relación con 5G resaltan la importancia de: reforzar los principios y obligaciones en la materia como el deber de informar en donde se describa claramente las finalidades de tratamiento, y se delimiten las obligaciones de los responsables del tratamiento de datos; así como, aplicar criterios de seguridad homogéneos para los diferentes agentes y segmentos de la red.

Otras medidas de protección de datos y seguridad de la información relacionadas con 5G y dispositivos IoT es aquella relacionada con el uso de firma electrónica y el fomento de comunicaciones cifradas de extremo a extremo en dispositivos móviles, incluso utilizando tecnologías *blockchain* en dispositivos móviles que facilite los procesos de autenticación de los usuarios.

En el caso de México, consideramos necesario impulsar la colaboración entre el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), la Secretaría de Economía, y el IFT con el objeto de garantizar el derecho de protección de datos personales en materia de 5G y dispositivos IoT.

Por ejemplo, en términos de los artículos 39, fracción VII y 43, fracciones III y IV de la Ley Federal de Protección de Datos Personales y Posesión de los Particulares (LFPDPPP), y las disposiciones previstas en la Ley Federal sobre Metrología y Normalización, se pueden regular los requisitos mínimos que deben cumplir los dispositivos IoT en materia de protección de datos. Lo anterior ha sido una recomendación a nivel internacional sobre la creación de esquemas de certificación de dispositivos IoT en países de la Unión Europea y Japón.

Igualmente, consideramos que el INAI debe fortalecer sus funciones de vigilancia y verificación del cumplimiento de las disposiciones contenidas en esta

LFPDPPP respecto al tratamiento de datos personales en dispositivos IoT, algunas pautas para ello son la guía de evaluación de impacto desarrolladas por la autoridad francesa.

En lo que hace a temas de ciberseguridad y 5G debemos resaltar que dicha tecnología tendrá un impacto significativo en industrias como la minería, el transporte o el energético, en donde las infraestructuras críticas de convierten en un factor prioritario. Algunas de las principales amenazas previstas para 5G son, por ejemplo, la intercepción de información, los ataques físicos a redes de telecomunicaciones y dispositivos móviles, averías o mal funcionamiento a redes y dispositivos de telecomunicaciones de energía, desastres naturales, y aspectos regulatorios.

Por ello, en el contexto internacional países de la Unión Europea, Japón, en específico España y Chile, en Latinoamérica, han desarrollado marcos regulatorios y de política pública para reducir los riesgos seguridad de la información y 5G a través de procedimientos para que los operadores de telecomunicaciones, sin distinción alguna, informen a las autoridades de telecomunicaciones sobre posibles riesgos de seguridad de información relacionada con la infraestructura de redes de telecomunicaciones, la cadena de suministro y contar con régimen de certificación para fabricantes de dispositivos IoT. Estas medidas en particular coinciden con la regulación y políticas públicas de los países que han tomado el liderazgo para prevenir riesgos en relación con 5G y el uso exponencial de dispositivos móviles.

Aunado a estas dos medias el caso de Japón es de llamar la atención. En dicho país se va un paso más allá para establecer medidas de seguridad en ciudades inteligentes, tales como, la autenticación de usuarios, la interoperabilidad de servicios móviles; así como, generar servicios de confianza como el sello de tiempo aplicable a dispositivos IoT. Otro ejemplo que podemos desatacar al respecto es Australia quien se ha enfocado en promover buenas prácticas para salvaguardar la infraestructura de telecomunicaciones, por ejemplo, el deber de informar de los operadores de redes de telecomunicaciones al gobierno australiano sobre cualquier cambio en sus redes, sistemas o servicios que puedan tener un efecto adverso en su capacidad para cumplir con su obligación de seguridad de información.

Para el caso de México sin duda consideramos que las buenas prácticas a nivel internacional en materia de protección de datos y ciberseguridad vinculados con 5G son acciones de pueden adoptarse como punto partida en el despliegue de nuevas redes móviles de telecomunicaciones y la certificación de productos IoT con base en principios de privacidad y seguridad desde el diseño.

Sin embargo, consideramos que el marco normativo, las políticas públicas y la coordinación de entidades públicas y privadas es esencial para salvaguardar, por un lado, el derecho de protección de datos personales y el uso de nuevas tecnologías móviles y, por el otro, para fortalecer aspectos de seguridad de la

información que impactan incluso en temas como la seguridad pública y seguridad nacional en cuanto a las amenazas que pueden sufrir las infraestructuras críticas del país.

En México debemos destacar que, hoy en día, se cuenta con regulación relacionada con protección de datos y seguridad de la red. En el numeral 145, fracción III de dicha LFTyR se establece la facultad del IFT para emitir lineamientos dirigidos a los concesionarios y autorizados que presten servicios de acceso a Internet para proteger, entre otros aspectos, la privacidad de los usuarios y la seguridad de la red. Estos lineamientos son los "*Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet*", publicados en el DOF el 05 de julio de 2021. No obstante, dichos lineamientos solo están dirigidos a los prestadores de servicios de Internet y dejan fuera a los concesionarios únicos de telecomunicaciones (artículo 4.1. *lineamientos).* Lo anterior resulta relevante ya que en el contexto internacional la pauta general en materia de ciberseguridad y protección de datos aplica a todos los prestadores de servicios de telecomunicaciones sin ninguna distinción.

Así, por una parte, para salvaguardar el derecho de protección de datos personales en México, en relación con 5G, consideramos necesario modificar el artículo 145 de la LFTyR para incluir a todos los operadores de telecomunicaciones; así como, incluir a nivel legal como parte de dichos lineamientos, temas como la elaboración de perfiles de riesgo de operadores telecomunicaciones, o establecer un esquema de certificación de fabricantes de dispositivos IoT en colaboración con la Secretaría de Economía.

De la misma forma, consideramos que el IFT debe colaborar con el INAI y la Secretaría de Economía en la generación de esquemas de certificación en privacidad de dispositivos y aplicaciones IoT basados en la tecnología 5G con la finalidad de fomentar la aplicación de principios de privacidad y seguridad desde la fabricación de dichos dispositivos.

Por último, nos parece indispensable que en el marco del Comité 5G en México se impulsen nuevas políticas públicas en materia de *protección de datos personales* y *ciberseguridad* en colaboración con autoridades públicas y privadas, a efecto de identificar los retos de las tecnologías 5G y promover buenas prácticas internacionales y nacionales en estas dos materias que hoy en día resultan relevantes en el despliegue de infraestructura de telecomunicaciones y en la fabricación de dispositivos IoT.

IV. Bibliografía

3GPP. (2020). 3GPP meets IMT-2020. Recuperado 21 de marzo de 2022, de https://www.3gpp.org/news-events/2143-3gpp-meets-imt-2020.

Abbosh, O., & Downes, L. (2019). 5G's Potential, and Why Businesses Should Start Preparing for It. Harvard Business Review. Recuperado 18 de marzo de 2022, de https://hbr.org/2019/03/5gs-potential-and-why-businesses-should-start-preparing-for-it.

Accenture. (2021). 5G accelerates economic growth. Recuperado 20 de marzo de 2022, de https://www.accenture.com/cz-en/insights/high-tech/5g-economic-impact.

Agencia Española de Protección de Datos. (2021). IoT (II): from the internet of things to the internet of bodies. AEDP. Recuperado 27 de marzo de 2022, de https://www.aepd.es/en/prensa-y-comunicacion/blog/iot-ii-from-iot-to-iob.

Agencia Española en Protección de Datos. (2020). INTRODUCTION TO 5G TECHNOLOGIES AND THEIR RISKS IN TERMS OF PRIVACY. AEPD. Recuperado 27 de marzo de 2022, de https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.

Agencia Española en Protección de Datos. (2021). IoT (II): Del Internet de las Cosas al Internet de los Cuerpos. AEPD. Recuperado 10 de abril de 2022, de https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-ii-del-iot-al-iob.

AGENCIA NACIONAL DEL ESPECTRO COLOMBIA. (2018). RESOLUCIÓN 774 DE 2018. normograma.mintic.gov.co. Recuperado 25 de marzo de 2022, de https://normograma.mintic.gov.co/mintic/docs/resolucion_ane_0774_2018.htm.

Álvarez, C. L. (2012). Derecho de las Telecomunicaciones (2.a ed.). Fundalex. http://claraluzalvarez.org/wp-content/uploads/2014/10/Clara-Luz-Alvarez-Dcho-Telecom-2013-final.pdf.

Australian Radiation Protection and Nuclear Safety Agency. (2019). 5G: the new generation of the mobile phone network and health. arpansa.gov.au. Recuperado 13 de marzo de 2022, de https://www.arpansa.gov.au/news/5g-new-generation-mobile-phone-network-and-health.

Banco Mundial. (2022). Personas que usan Internet % de la población [Gráfico]. Banco Mundial. https://datos.bancomundial.org/indicator/IT.NET.USER.ZS.

Bartley, K. (2021). Estadísticas de Big Data: ¿Cuántos datos hay en el mundo? Rivery. Recuperado 16 de marzo de 2022, de https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/.

Brown, S. (2020). 5G, explained. mitsloan.mit.edu. Recuperado 19 de marzo de 2022, de https://mitsloan.mit.edu/ideas-made-to-matter/5g-explained.

C. Gallagher, J., & E. DeVine, M. (2019). Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress (R45485). crsreports.congress.gov.

Recuperado 20 de marzo de 2022, de https://crsreports.congress.gov/product/details?prodcode=R45485.

Cho, R. (2020, 13 agosto). The Coming 5G Revolution: How Will It Affect the Environment? Columbia Climate School. Recuperado 26 de marzo de 2022, de https://news.climate.columbia.edu/2020/08/13/coming-5g-revolution-will-affect-environment/.

Comisión Europea. (2016). COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. Recuperado 12 de abril de 2022, de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016DC0588&from=es.

Congressional Research Service. (2019). Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress. crsreports.congress.gov. Recuperado 19 de marzo de 2022, de https://crsreports.congress.gov/product/pdf/R/R45485.

Consumer and Governmental Affairs. (2020). Wireless Devices and Health Concerns. fcc.gov. Recuperado 24 de marzo de 2022, de https://www.fcc.gov/consumers/guides/wireless-devices-and-health-concerns.

Comission Nationale Informatique & Libertes. (2018). Privacy Impact Assessment. Recuperado 16 de abril de 2022, de https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf.

Cooley, B. (2020). How 5G antennas will get built near you. CNET. Recuperado 1 de abril de 2022, de https://www.cnet.com/tech/mobile/how-5g-antennas-will-get-built-near-you/.

Curran, C. (2020, 30 enero). What Will 5G Mean for the Environment? University of Washington. Recuperado 26 de marzo de 2022, de https://jsis.washington.edu/news/what-will-5g-mean-for-the-environment/.

Department for Digital, Culture, Media & Sport. (2020). What is 5G? gov.uk. Recuperado 18 de marzo de 2022, de https://www.gov.uk/government/publications/telecommunications-security-bill-factsheets/factsheet-6-5g.

Department of Health and Social Care. (2019, 10 julio). NHS health information available through Amazon's Alexa. gov.uk. Recuperado 26 de marzo de 2022, de https://www.gov.uk/government/news/nhs-health-information-available-through-amazon-s-alexa.

El Acuerdo de París. (2020). Naciones Unidas. Recuperado 26 de marzo de 2022, de https://www.un.org/es/climatechange/paris-agreement#:~:text=El%20Acuerdo%20de%20Par%C3%ADs%20brinda,un%20ciclo%20de%20cinco%20a%C3%B1os.

Ericsson. (2021). Conceptualizing security in mobile communication networks – how does 5G fit in? Recuperado 17 de abril de 2022, de https://www.ericsson.com/en/security/a-guide-to-5g-network-security.

Espinosa, M. (2022). Subtel fiscalizará despliegue de redes 5G en aeropuertos, tras alertas por efectos en los aviones. Diario Financiero. Recuperado 21 de marzo de 2022, de https://www.df.cl/empresas/industria/subtel-fiscalizara-despliegue-de-redes-5g-en-aeropuertos-tras-alertas.

European Commission. (2016, 30 septiembre). 5G deployment could bring millions of jobs and billions of euros benefits, study finds. Shaping Europe's digital future. Recuperado 20 de marzo de 2022,https://digital-strategy.ec.europa.eu/en/library/5g-deployment-could-bring-millions-jobs-and-billions-euros-benefits-study-finds.

European Commission. (2020). Mergers: Commission clears acquisition of Fitbit by Google, subject to conditions. Recuperado 27 de marzo de 2022, de https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2484.

European Data Protection Board. (2021). Norwegian DPA: Intent to issue € 2,5 million fine to Disqus Inc. Recuperado 16 de abril de 2022, de https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-intent-issue-eu-25-million-fine-disqus-inc_en.

European Union Agency for Cybersecurity. (2020). ENISA Threat Landscape for 5G Networks Report. ENISA. Recuperado 2 de abril de 2022, de https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

Existence of standards. (2022). [Ilustración]. THE GLOBAL HEALTH OBSERVATORY. https://www.who.int/data/gho/data/indicators/indicator-details/GHO/existence-of-standards.

FAA Aviation Safety. (2021). SPECIAL AIRWORTHINESS INFORMATION BULLETIN. Recuperado 21 de marzo de 2022, de https://rgl.faa.gov/Regulatory_and_Guidance_Library/rgSAIB.nsf/dc7bd4f27e5f107486257221005f069d/27ffcbb45e6157e9862587810044ad19/$FILE/AIR-21-18.pdf.

Federal Communications Commission. (2022). America 's 5G Future. Recuperado 15 de abril de 2022, de https://www.fcc.gov/5G.

Federal Ministry of Transport and Digital Infrastructure. (2017). 5G Strategy for Germany. Recuperado 18 de abril de 2022, de https://www.bmvi.de/SharedDocs/EN/publications/5g-strategy-for-germany.pdf?__blob=publicationFile.

Grupo de Trabajo de Seguridad Cibernética. (2020). IoT・5G セキュリティ総合対策. Recuperado 10 de abril de 2022, de https://www.soumu.go.jp/main_content/000641510.pdf.

H. Lehne, P. (2005). Future Mobile Phones. telektronikk, 101. https://www.academia.edu/2933675/Interest_in_future_net-based_services_for_a_sample_of_Norwegian_interviewees.

IBM. (2021). Genere confianza en sus datos de IoT con blockchain. Recuperado 8 de abril de 2022, de https://www.ibm.com/es-es/topics/blockchain-iot

IEEE. (2018). 5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View. IEEE Access, 6. https://doi.org/10.1109/ACCESS.2018.2872781.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2021). Evitar vincular el dispositivo inteligente a otros aparatos de los que se desconoce su nivel de seguridad. INAI. Recuperado 18 de abril de 2022, de https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-261-21.pdf.

Instituto Federal de Telecomunicaciones. (2021). neutralidad DE LA RED. IFT México. Recuperado 17 de abril de 2022, de http://www.ift.org.mx/sites/default/files/neutralidad_de_la_red_v.pdf.

Instituto Federal de Telecomunicaciones. (2021). Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones establece el Comité Técnico en materia de Despliegue de 5G en México, como un órgano técnico de apoyo, de naturaleza consultiva y no vinculante, para propiciar una eficiente implementación de 5G en México y expide sus Reglas de Operación. IFT. Recuperado 12 de abril de 2022, de http://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/pift061021497acc.pdf.

Inter-American Development Bank, García Zaballos, A., Iglesias Rodriguez, E., Woo Kim, K., & Park, S. (2020). 5G The Driver for the Next-Generation Digital Society in Latin America and the Caribbean, IDB, https://publications.iadb.org/publications/english/document/5G_The_Driver_for_the_Next-Generation_Digital_Society_in_Latin_America_and_the_Caribbean.pdf.

International Agency for Research on Cancer. (2011). IARC CLASSIFIES RADIOFREQUENCY ELECTROMAGNETIC FIELDS AS POSSIBLY CARCINOGENIC TO HUMANS. Organización Mundial de la Salud. Recuperado 23 de marzo de 2022, de https://www.iarc.who.int/wp-content/uploads/2018/07/pr208_E.pdf.

International Commission on Non-Ionizing Radiation Protection. (2020). INTERNATIONAL COMMISSION ON NON-IONIZING RADIATION PROTECTION e.V. icnirp.org/. Recuperado 25 de marzo de 2022, de http://www.icnirp.org/cms/upload/publications/ICNIRPemfgdlesp.pdf.

International Telecommunication Union. (2012). Reglamento de las Telecomunicaciones Internacionales. ITU. Recuperado 13 de marzo de 2022, de https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.42.48.es.301.pdf.

International Telecommunication Union. (2020). ITU completes evaluation for global affirmation of IMT-2020 technologies. ITU. Recuperado 21 de marzo de 2022, de https://www.itu.int/en/mediacentre/Pages/pr26-2020-evaluation-global-affirmation-imt-2020-5g.aspx.

International Telecommunications Union. (2008). K.91: Guidance for assessment, evaluation and monitoring of human exposure to radio frequency electromagnetic fields. ITU. Recuperado 25 de marzo de 2022, de https://www.itu.int/rec/T-REC-K.91/en.

International Telecommunications Union. (2020). ITU-T K.70 (12/2020). ITU. Recuperado 25 de marzo de 2022, de https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14568&lang=en.

International Telecommunications Union. (2021). E-waste, circular economy and sustainable supply chain management. ITU. Recuperado 26 de marzo de 2022, de https://www.itu.int/en/ITU-T/studygroups/2017-2020/05/Pages/q7.aspx.

International Telecommunications Union. (2021). Climate change and assessment of digital technologies in the framework of the Sustainable Development Goals (SDGs) and the Paris Agreement. ITU. Recuperado 26 de marzo de 2022, de https://www.itu.int/en/ITU-T/studygroups/2017-2020/05/Pages/q9.aspx.

International Telecommunications Union. (2021). Setting Environmental Requirements for 5G. ITU. Recuperado 26 de marzo de 2022, de https://www.itu.int/en/ITU-T/climatechange/Pages/ictccenv.aspx.

International Telecommunications Union. (2021). Adaptation to climate change and low cost and sustainable resilient information and communication technologies (ICTs). ITU. Recuperado 26 de marzo de 2022, de https://www.itu.int/en/ITU-T/studygroups/2017-2020/05/Pages/q10.aspx.

International Telecommunications Union. (2022). Comisión de Estudio 5 del UIT-T – Medio ambiente y cambio climático. ITU. Recuperado 26 de marzo de 2022, de https://www.itu.int/es/ITU-T/about/groups/Pages/sg05.aspx.

Izan, G. (2020). Tu smart TV te está espiando: así es cómo sabe qué series ves. El Español. Recuperado 26 de marzo de 2022, de https://www.elespanol.com/omicrono/20200312/smart-tv-espiando-sabe-series-ves/473953871_0.html.

Khantimirov, R. (2021). What Does 5G Mean for Global DDoS Vulnerability? CyberSecurity Magazine. Recuperado 1 de abril de 2022, de https://cybersecurity-magazine.com/what-does-5g-mean-for-global-ddos-vulnerability/.

Luque Ordóñez, J. (2017). Espectro electromagnético y espectro radioeléctrico. AUTORES CIENTÍFICO-TÉCNICOS Y ACADÉMICOS. Recuperado 13 de marzo de 2022, de https://www.acta.es/medios/articulos/ciencias_y_tecnologia/062017.pdf.

Madnick, S. (2020). The dark side of 5G. MIT SLOAN EXPERTS. Recuperado 4 de abril de 2022, de https://mitsloan.mit.edu/experts/dark-side-5g.

Minister for Communications and the Arts. (2018). Government provides 5G security guidance to Australian carriers. Parliament of Australia. Recuperado 10 de abril de 2022, de https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/6164495%22.

Ministerio de Asuntos Económicos y Transformación Digital. (2021). BORRADOR DE ANTEPROYECTO DE LEY SOBRE REQUISITOS PARA GARANTIZAR LA SEGURIDAD DE LAS REDES Y SERVICIOS DE COMUNICACIONES ELECTRÓNICAS DE QUINTA GENERACIÓN. Recuperado 11 de abril de 2022, de https://avancedigital.mineco.gob.es/es-es/Participacion/Documents/5G_audiencia/Texto_APL_ciberseguridad_5G.pdf?csf=1&e=48JHOH.

Ministerio de Asuntos Económicos y Transformación Digital. (2017). Plan Nacional 5G. Gobierno de España. Recuperado 15 de abril de 2022, de https://avancedigital.mineco.gob.es/5g/paginas/medidas-5g.aspx.

Mucientes, E. (2016). Así se gestó el ciberataque más grave de los últimos 10 años. El Mundo. Recuperado 4 de abril de 2022, de https://www.elmundo.es/tecnologia/2016/10/22/580b10e5268e3e06158b45e0.html.

National Cybersecurity Center of Excellence. (2021, febrero). 5G Cybersecurity. NCCOE. Recuperado 16 de abril de 2022, de https://www.nccoe.nist.gov/sites/default/files/legacy-files/nist-5G-sp1800-33a-preliminary-draft.pdf.

Nokia. (2010). •Revista Cloud Computing. (2021). Recuperado 17 de abril de 2022, de https://onestore.nokia.com/asset/201049.

Oficina de Desarrollo de las Telecomunicaciones de la UIT. (2018). Sentando las bases para la 5G: Oportunidades y desafíos. ITU. Recuperado 20 de marzo de 2022, de https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-S.pdf.

Orange. (2020, 2 septiembre). Aviso del Consejo de Salud de los Países Bajos sobre la 5G (2020/09/02). Orange.com. Recuperado 25 de marzo de 2022, de https://radio-waves.orange.com/es/preguntas/aviso-del-consejo-de-salud-de-los-paises-bajos-sobre-la-5g/.

Organización Mundial de la Salud. (2005). Electromagnetic hypersensitivity. who.int. Recuperado 23 de marzo de 2022, de https://www.who.int/teams/environment-climate-change-and-health/radiation-and-health/non-ionizing/el-hsensitivity.

Organización Mundial de la Salud. (2020). Radiation: 5G mobile networks and health. who.int. Recuperado 24 de marzo de 2022, de https://www.who.int/news-room/questions-and-answers/item/radiation-5g-mobile-networks-and-health.

OXFORD ECONOMICS. (2019). THE ECONOMIC IMPACT OF RESTRICTING COMPETITION IN 5G NETWORK EQUIPMENT. https://www.scribbr.es/detector-de-plagio/generador-apa/new/report/.

Pandita, S. (2021). Case for Blockchain in 5G. HCL Technologies Limited. Recuperado 10 de abril de 2022, de https://www.hcltech.com/blogs/case-blockchain-5g.

Pretz, K. (2019). Will 5G Be Bad for Our Health? IEEE antenna and telecommunications experts address concerns over radio frequency exposure. IEEE Spectrum. Recuperado 15 de abril de 2022, de https://spectrum.ieee.org/will-5g-be-bad-for-our-health.

R. Prasad, A., Zugenmaier, A., Escott, A., & Cano Soveri, M. (2018). 3GPP 5G Security. 3GPP. Recuperado 17 de abril de 2022, de https://www.3gpp.org/news-events/1975-sec_5g.

Real Academia Española. (2021). Telecomunicación. https://dle.rae.es/. Recuperado 11 de marzo de 2022, de https://dle.rae.es/telecomunicaci%C3%B3n.

Revista Cloud Computing. (2021). ¿Qué sucede cuando los empleados abandonan sus dispositivos inteligentes en el trabajo? Recuperado 11 de abril de 2022, de https://www.revistacloudcomputing.com/2021/07/que-sucede-cuando-los-empleados-abandonan-sus-dispositivos-inteligentes-en-el-trabajo/.

Singh Sound, S. (2017). 1G, 2G,. . .& 5G: The evolution of the G's. mse238blog.stanford.edu. Recuperado 15 de marzo de 2022, de https://mse238blog.stanford.edu/2017/07/ssound/1g-2g-5g-the-evolution-of-the-gs/.

Statista. (2021). Aumento acumulado del PIB durante diez años si la tecnología 5G se despliega en América Latina según estimaciones de 2019, por país [Imagen]. Statista. https://es.statista.com/estadisticas/1189858/impacto-economico-tecnologia-5g-america-latina/.

The EU toolbox for 5G security. (2021). European Commission. Recuperado 6 de abril de 2022, de https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

United Nations. (2015). ¿Qué es el Acuerdo de París? unfccc.int. Recuperado 26 de marzo de 2022, de https://unfccc.int/es/process-and-meetings/the-paris-agreement/que-es-el-acuerdo-de-paris.

Wall, M. (2018). 5G: «A cyber-attack could stop the country». BBC. Recuperado 1 de abril de 2022, de https://www.bbc.com/news/business-45952693.

Wolfe, J. (2017, 24 julio). Roomba vacuum maker iRobot betting big on the «smart» home. Reuters. Recuperado 27 de marzo de 2022, de https://www.reuters.com/article/us-irobot-strategy-idUSKBN1A91A5?il=0.

World Economic Forum. (2020). The Impact of 5G: Creating New Value across Industries and Society. Recuperado 19 de marzo de 2022, de https://www.weforum.org/whitepapers/the-impact-of-5g-creating-new-value-across-industries-and-society.

Xinhua. (2017). 5G to drive 6.3t yuan economic output in China: report. ChinaDaily. Recuperado 21 de marzo de 2022, de http://www.chinadaily.com.cn/business/tech/2017-06/14/content_29733286.htm.

PARTE III:
INFRAESTRUCTURA Y CIBERSEGURIDAD

COMPARTICIÓN DE INFRAESTRUCTURA PARA LA CONECTIVIDAD UNIVERSAL

Aida HUERTA BARRIENTOS[9]
César MARTÍN RODRÍGUEZ[10]

[9]Doctora en Ingeniería por la UNAM. Actualmente es Secretaria de Posgrado e Investigación de la Facultad de Ingeniería, UNAM, aida.huerta@comunidad.unam.mx.
[10]Maestro en Administración de Negocios. Actualmente es Director General de Ultimate ORBIS Telecomm, cesar.martin@orbistelecomm.com.

COMPARTICIÓN DE INFRAESTRUCTURA PARA LA CONECTIVIDAD UNIVERSAL

Infrastructure Sharing for Universal Connectivity

Resumen

Las limitaciones de los modelos de negocio tradicionales de los operadores de redes de telecomunicaciones móviles a nivel global ya han sido analizadas por diversos autores, quienes coinciden en que, de acuerdo con los requerimientos actuales de servicios de telecomunicaciones, dichos modelos de negocios ya no son vigentes y se sugiere entonces la inclusión de esquemas de compartición de infraestructura para optimizar los costos de las redes de telecomunicaciones. El objetivo general de este artículo es presentar un esquema de compartición de infraestructura pasiva entre sectores como es la infraestructura asociada a la red carretera y a la red ferroviaria, susceptible de ser utilizada para propósitos de telecomunicaciones y contribuir así a alcanzar los objetivos del Programa de Cobertura Social del Gobierno Federal Mexicano promoviendo el incremento en la cobertura de las redes de transporte de altas capacidades, habilitadoras del acceso a los servicios de telecomunicaciones. Primero, se presenta la revisión de la literatura acerca de los esquemas de compartición de infraestructura para redes de telecomunicaciones móviles. Después, se describe la infraestructura pasiva

Abstract

The limitations of the traditional business models of mobile telecommunications network operators at a global level have already been analyzed by various authors, who agree that, according to the current requirements of telecommunications services, business models are no longer and then it is suggested the inclusion of infrastructure sharing schemes to optimize the costs of telecommunications networks. The general objective of this article is to present a passive infrastructure sharing scheme between sectors such as the infrastructure associated with the road network and the railway network, capable of being used for telecommunications purposes and thus contribute to achieving the objectives of the Mexican Federal Government Coverage Program, promoting the increase in the coverage of high-capacity transport networks, enabling access to telecommunications services. First, a review of the literature on infrastructure sharing schemes for mobile telecommunications networks is presented. Then, the passive infrastructure capable of being used for telecommunications in Mexico is described, among which we highlight: the road network and the railway network. Next, the advantages of the

susceptible de ser utilizada para telecomunicaciones en México, entre la que destacamos: la red carretera y la red ferroviaria. Enseguida, se analizan las ventajas del esquema de compartición de infraestructura pasiva entre sectores. Consideramos que, los resultados de este estudio pueden apoyar la toma de decisiones del Gobierno Federal y de los concesionarios y operadores de redes de telecomunicaciones para lograr la conectividad universal en las Zonas de Atención Prioritaria de Cobertura Social.

Palabras clave: infraestructura pasiva, infraestructura carretera, infraestructura ferroviaria, esquemas de compartición, cobertura social.

passive infrastructure sharing scheme between sectors are analyzed. We really believe that the results of this study can support the decision-making of the Mexican Federal Government and the concessionaires and operators of telecommunications networks to achieve universal connectivity in the Priority Attention Areas of Social Coverage.

Keywords: *pasive infrastructure, road infrastructure, railway network infrastructure, passive infrastructure sharing scheme; social coverage.*

I. Introducción

De acuerdo con el Diario Oficial de la Federación (DOF, 2020), en México el derecho de acceso a los servicios de telecomunicaciones y radiodifusión fue establecido explícitamente mediante el *Decreto por el que se reformaron y adicionaron diversas disposiciones de los artículos 6o., 7º., 27, 28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos en materia de telecomunicaciones* (en adelante El Decreto), cuyo objetivo estuvo orientado a reducir los costos de los servicios de telecomunicaciones para generar una mayor oferta que se tradujera en un beneficio concreto para la población en general, de ahí que es fundamental para los concesionarios desplegar, operar, mantener y actualizar infraestructura que incremente su capacidad y cobertura a fin de tener una amplia oferta competitiva de sus servicios. Es en esta dirección que, en nuestro país se requiere de condiciones que favorezcan los modelos de negocio de los concesionarios en relación con el despliegue de infraestructura.

El modelo de negocios tradicional de los operadores de redes de telecomunicaciones móviles considera que dichos operadores son propietarios de toda la red de capa física, sin embargo, este modelo de negocios ya no es vigente debido principalmente a fenómenos como la saturación del mercado que conlleva a una presión sobre los márgenes de ganancias y a la acelerada migración tecnológica (Frisanco *et al.,* 2008). Es en este sentido que, los operadores de red están replanteando sus modelos de negocios teniendo en cuenta el enfoque de

compartición de infraestructura con el objetivo de minimizar el gasto en capital (en inglés Capital Expenditures, en adelante CAPEX) y el gasto operativo (en inglés Operating Expenses, en adelante OPEX) asociados. Las mejores prácticas internacionales sugieren que la compartición de infraestructura puede darse en diversas vertientes como se describe enseguida.

Inmuebles

De acuerdo con el Diario Oficial de la Federación (DOF, 2020), se cuenta con experiencias internacionales de distintas autoridades que han promovido la presencia de más de un operador en inmuebles: Parlamento Europeo el Consejo de la Unión Europea (Directiva 2014/61/UE), República Federal Alemana (Ley para facilitar el desarrollo de redes digitales de alta velocidad), Órgano Regulador de Telecomunicaciones de Francia (Ley de Modernización de la Economía), Procuraduría General Distrital de Lisboa (Decreto 92/2017), Agencia Croata de Correos y Comunicaciones Electrónicas (Ordenanza sobre las condiciones técnicas de la red de comunicaciones electrónicas para edificios comerciales y residenciales, adoptada en diciembre de 2009) y la Secretaría de Telecomunicaciones de Chile (Ley 20.808 que Protege la libre elección de los servicios de cable, Internet o telefonía).

Obra civil

Así mismo, como lo indica el Diario Oficial de la Federación (DOF, 2020) países como España, Bahrein, Portugal, Suecia, Perú y Estados Unidos, ya han llevado a cabo acciones para establecer mecanismos de coordinación entre diferentes concesionarios para el despliegue de infraestructura a fin de reducir costos de forma conjunta. En la literatura científica, encontramos distintos estudios donde se propone el uso de métodos y técnicas de optimización para la compartición de infraestructura basados en el criterio de minimización de costos y de maximización de uso de recursos de red (Bousia *et al.,* 2015; Cano *et al.,* 2015; Antonopoulos *et al.,* 2015; Burhanudin and Asvial, 2018). Uno de los estudios que describe ampliamente los beneficios derivados de la compartición, las implicaciones regulatorias y legales y que presenta los posibles modelos para implementar los esquemas de compartición en la región de América Latina y el Caribe se presenta en Martínez *et al.,* (2020). Sin embargo, a pesar de que en la literatura y en las mejores prácticas internacionales encontramos interesantes propuestas para la compartición de infraestructura entre los diferentes operadores de redes de telecomunicaciones móviles, estas hacen énfasis en las redes de acceso dejando de lado lo correspondiente a las redes de transporte de altas capacidades, las cuales realmente son las habilitadoras de cobertura. Adicionalmente, en la literatura reciente no se aborda el uso de infraestructura pasiva cuyo objetivo inicial no fue para telecomunicaciones pero que, es susceptible de ser utilizada para fines de

telecomunicaciones, sobre todo para redes de transporte de telecomunicaciones. Además, tampoco se indica la normatividad técnica que debe cumplir dicha infraestructura para tales propósitos. Los estudios existentes se enfocan en análisis de costos, principalmente. Es en este contexto que, el objetivo general de este artículo es presentar un esquema de compartición de infraestructura pasiva basado en la infraestructura de la red carretera y la red ferroviaria, las cuales son susceptibles de ser utilizadas para propósitos de telecomunicaciones, y contribuir así a lograr los objetivos del Programa de Cobertura Social del Gobierno Federal Mexicano promoviendo el incremento en la cobertura habilitada de las redes de transporte de altas capacidades. Para propósitos de este estudio se entiende por infraestructura pasiva aquellos elementos no electrónicos al servicio de las redes públicas de telecomunicaciones que incluyen, de forma enunciativa más no limitativa, los derechos de vía, conductos, mástiles, zanjas, torres, postes, instalaciones de equipo y de alimentaciones conexas, seguridad, equipos auxiliares, sitios, predios, espacios físicos, ductos y canalizaciones; así como, fuentes de energía y sistemas de aire acondicionado. De acuerdo con el Artículo 3 de la Ley Federal de Telecomunicaciones y Radiodifusión, el término cobertura *universal* considera el acceso de la población en general a los servicios de telecomunicaciones determinados por la Secretaría de Comunicaciones y Transportes bajo condiciones de disponibilidad, asequibilidad y accesibilidad.

Este artículo se constituye por cinco secciones. En la sección 2, presentamos la revisión de la literatura acerca de los esquemas de compartición de infraestructura para redes de telecomunicaciones móviles. En la sección 3, describimos la infraestructura pasiva susceptible de ser utilizada para telecomunicaciones y a través de la cual puede lograrse la conectividad de localidades y municipios más alejados que no tienen actualmente ningún tipo de conectividad a redes de telecomunicaciones, entre las que destacamos: la red carretera y la red férrea. Se incluyen los aspectos técnicos existentes que deberán cumplirse para el aprovechamiento de dicha infraestructura. En la sección 4, se analizan las ventajas del esquema de compartición de infraestructura pasiva. En la sección 5, se analiza el Programa de Cobertura Social del Gobierno Federal de México y se sugiere la posibilidad de alcanzar sus objetivos a través de la compartición de infraestructura. Al final, se enuncian las conclusiones generales.

II. Revisión de la literatura

El modelo de negocios tradicional de los concesionarios de redes de telecomunicaciones móviles considera que dichos operadores son propietarios de toda la red de capa física, sin embargo, este modelo de negocios ya no es vigente debido principalmente a fenómenos como la saturación del mercado que conlleva a una presión sobre los márgenes de ganancias y a la acelerada migración

tecnológica (Frisanco *et al.,* 2008). Es en esta dirección, que en la última década los concesionarios de redes se han replanteado los modelos de sus negocios teniendo en cuenta el enfoque de compartición de infraestructura con el objetivo de minimizar el CAPEX y OPEX. En la literatura científica encontramos diferentes estudios que muestran algunas de las soluciones implementadas. Por un lado, en Frisanco *et al.,* (2008) se sugieren diferentes enfoques y soluciones técnicas para la compartición de redes de telecomunicaciones móviles y se analizan diferentes escenarios de un modelo de simulación indicando los beneficios de servicios gestionados para el caso de la compartición de recursos de la red. Como lo sugiere Meddour (2011), la compartición de infraestructura de redes móviles de telecomunicaciones es una medida importante para reducir costos, es una estrategia muy útil en la fase de despliegue, ya que permite, desplegar una cobertura de forma rápida, mientras que en el largo plazo permite desplegar una cobertura rentable, especialmente en áreas rurales y menos pobladas o marginadas. En el contexto de los mercados emergentes, tanto la compartición de infraestructura en áreas urbanas como rurales debe adoptarse como un imperativo para el crecimiento sostenido de las telecomunicaciones (Meddour, 2011). En última instancia, la compartición de redes móviles puede desempeñar un papel importante para aumentar el acceso a las Tecnologías de la Información y Comunicación (TIC), generar crecimiento económico, mejorar la calidad de vida y ayudar a los países en desarrollo y desarrollados a cumplir los objetivos establecidos por la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y los Objetivos de Desarrollo del Milenio establecidos por las Naciones Unidas (ODM). Por ejemplo, la industria de telecomunicaciones en China ha tenido un gran incremento en los últimos años, ofreciendo una mejor cobertura de redes de telecomunicaciones a medida que los esquemas de compartición de infraestructura se convirtieron en un requisito para la reducción de costos y cuidado del medio ambiente. Desde 2009, en China se estableció que en la construcción de una red de telecomunicaciones se deben compartir torres, postes de líneas de transmisión y las mismas líneas de transmisión -fibra óptica- (APEC, 2011).

Por otro lado, en Bousia *et al.,* (2015) se aborda el problema de la subutilización de las redes de telecomunicaciones móviles durante los períodos de bajo tráfico y se plantea un nuevo modelo de negocios de compartición de infraestructura que permite a los operadores de redes móviles que su tráfico sea ofrecido por otros operadores de redes móviles que se localicen en la misma área geográfica. Para esto, se propone un algoritmo de compartición de infraestructura para entornos multi operador, el cual permite la desactivación de radio bases subutilizadas durante los períodos de bajo tráfico y se lleva a cabo un análisis de costo beneficio. Otra herramienta de apoyo a la toma de decisiones en la compartición de infraestructura de operadores de redes coexistentes en una misma área geográfica se propone en Cano *et al.,* (2015). Se sugiere un modelo de

programación lineal entera mixta que tiene en cuenta aspectos tecno-económicos para alcanzar diferentes tasas de transmisión a través de configuraciones compartidas, los modelos de precios para los servicios ofrecidos a los clientes finales y las expectativas de retorno de inversión de los operadores móviles. Como salida del modelo se obtiene la mejor opción de compartición de infraestructura con base en la inversión realizada por los operadores de redes móviles. Las ventajas en términos energéticos de la combinación de ambos escenarios, compartición de infraestructura y el apagado de radio bases por subutilización se analiza en Antonopoulos *et al.,* (2015) utilizando el marco teórico de la Teoría de Juegos.

Recientemente, en Burhanudin and Asvial (2018), se propone una metodología regulatoria para la compartición de infraestructura para operadores de redes móviles en un contexto de Indonesia. Al llevar a cabo el Análisis de Impactos Regulatorios, se demostró que la regulación actual no es suficiente para permitir la compartición de infraestructura por lo que sugiere un nuevo esquema de regulación que favorezca un entorno de negocios sustentable para todos los operadores móviles, y no se favorezca al operador predominante. Además, en el *Informe sobre Compartición de Infraestructura* (2018) que sugiere Martínez *et al.,* (2020) se indica que, la compartición de infraestructura pasiva representa hasta un 16%-35% de CAPEX, y el ahorro de costos de infraestructura activa (excluyendo el espectro) es del 33%-35% de CAPEX y del 25% - 33% de OPEX. Del mismo modo, Martínez *et al.,* (2020) analizan los beneficios derivados de la compartición, las implicaciones regulatorias y legales y presentan los posibles modelos para implementar la compartición en la región de América Latina y el Caribe, al final del estudio presentan las recomendaciones para la hoja de ruta para la compartición de infraestructura que incluyen: recomendaciones técnicas, recomendaciones internas, recomendaciones regulatorias y recomendaciones políticas.

Específicamente en el contexto de México, en enero de 2020, se publicó en el Diario Oficial de la Federación el ACUERDO mediante el cual el Pleno del Instituto Federal de Telecomunicaciones emitió los Lineamientos para el Despliegue, Acceso y Uso Compartido de Infraestructura de Telecomunicaciones y Radiodifusión (DOF, 2020), en el cual se promueve el despliegue, se fomenta la compartición de infraestructura entre concesionarios, y se establecen las condiciones que permiten el acceso de concesionarios a elementos de infraestructura de otros concesionarios instalada en edificios, centros comerciales, fraccionamientos o cualquier inmueble con el propósito de que se brinden servicios de telecomunicaciones y radiodifusión en mejores condiciones de competencia y libre concurrencia, y con ello, impulsar que los usuarios cuenten con más y mejores servicios de telecomunicaciones y radiodifusión. Como se observa, las diferentes propuestas que encontramos en la literatura hacen énfasis en las redes de acceso dejando de lado lo correspondiente a las redes de transporte de altas capacidades. Desafortunadamente, no se aborda

el uso de infraestructura pasiva cuyo objetivo inicial no fue para telecomunicaciones; sin embargo, es susceptible de ser utilizada para propósitos de telecomunicaciones.

II.1. Infraestructura pasiva susceptible de ser utilizada para telecomunicaciones

Al día de hoy los concesionarios de telecomunicaciones han ampliado el despliegue de las redes en condiciones de competencia, atendiendo además sus compromisos de cobertura y penetración, sin embargo, la brecha digital en México continúa. De acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnología de la Información en hogares (en adelante ENDUTIH) publicada en junio de 2021, se logró mantener la tendencia a la reducción de la brecha digital, es decir, de las condiciones de desigualdad social que se asocian con la falta de acceso a las Tecnologías de la Información y la Comunicación tales como el Internet, la telefonía, la televisión o la computadora, durante 2020. Sin embargo, no ha sido posible que todos los habitantes de México ejerzan su derecho de acceso a los servicios de telecomunicaciones y radiodifusión. Es en esta dirección, que se requiere el despliegue infraestructura no solo en redes de acceso, sino,en redes de transporte que habiliten un mayor número de redes de acceso. Algunos de los retos que actualmente enfrentan los concesionarios de redes para reducir la brecha digital en México son: la gran dispersión geográfica de la población mexicana, la geografía accidentada a lo largo del territorio nacional y el desconocimiento de normatividad técnica que debe cumplirse para que la infraestructura de redes de otros sectores sea utilizada para propósitos de telecomunicaciones.

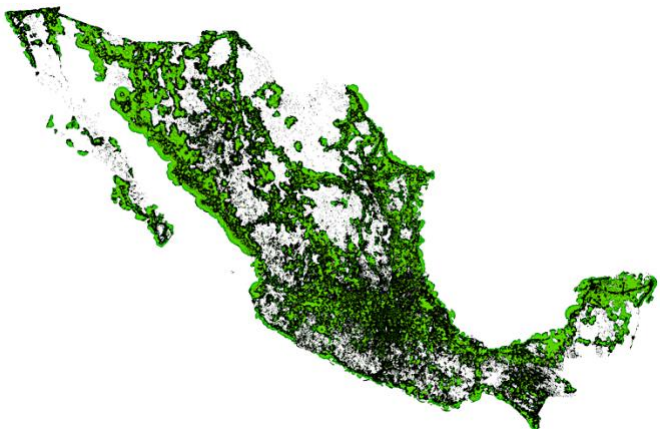


Fig. 1. Cobertura de redes de telecomunicaciones móviles considerando los tres operadores principales en México *versus* las localidades distribuidas espacialmente.

II.2 Red carretera

Una de las redes que es susceptible de ser utilizada para propósitos de telecomunicaciones de altas tasas de transmisión es la red carretera en México, a través del aprovechamiento de los derechos de vía para la instalación de fibra

óptica. Para que lo anterior sea posible, se debe cumplir con normatividad técnica que asegure la operatividad de dicha fibra óptica, como se describe enseguida.

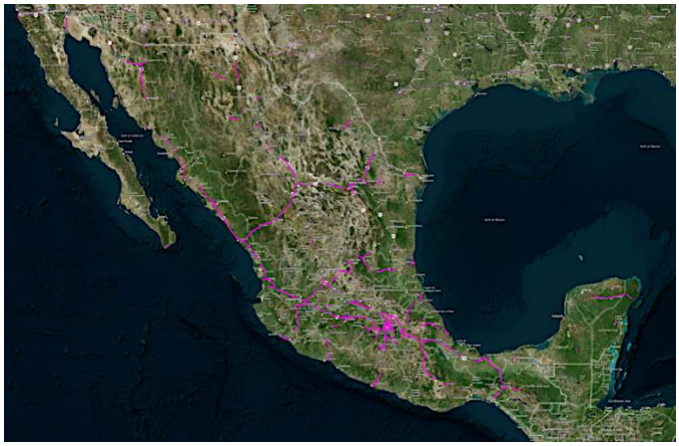


Fig. 2. Red carretera de peaje en México.

Normatividad técnica que debe cumplirse para que la infraestructura de la red carretera sea utilizada para propósitos de telecomunicaciones.

Son de aplicación, además de la normatividad legal vigente de obligado cumplimiento, las Normas Mexicanas y prescripciones técnicas, en su última edición, que a continuación se citan.

- N·CTR·CAR·1·08·007/11 – Tritubos para Fibra Óptica en el Acotamiento de Carreteras Nuevas.
- N·LEG·3 - Ejecución de Obras.
- N·CTR·CAR·1·08·008 - Registros para Tritubos para Fibra Óptica en Carreteras Nuevas.
- N·CTR·CAR·1·08·009 - Adosamiento de Tritubos a Puentes y Estructuras Similares.
- N·CTR·CAR·1·08·010 - Cruces de Tritubos entre Acotamientos.
- NMX-E-004-CNCP-2004 - Industria del plástico – Determinación de la Densidad de los Materiales Plásticos no Celulares – Método de Ensayo.
- NMX-E-166-1985 - Plásticos – Materias Primas - Densidad por Columna de Gradiente – Método de Prueba.
- NMX-E-135-CNCP-2004 - Industria del plástico – Índice de Fluidez de Termoplásticos por medio de Plastómero Extrusor – Método de Ensayo.
- NMX-E-029-CNCP-2005 - Industria del Plástico – Resistencia al Impacto de Tubos y Conexiones – Método de Ensayo.
- NMX-E-014-CNCP-2006 - Industria del Plástico – Resistencia al Aplastamiento en Tubos y Conexiones – Método de Ensayo.

• NMX-E-082-SCFI-2002 - Industria del Plástico – Resistencia a la Tensión de Materiales Plásticos – Método de Ensayo.

• NOM-130-ECOL-2000 -Sistemas de comunicación telefónica por red de fibra óptica - Especificaciones para la planeación, diseño, preparación del sitio, construcción, operación y mantenimiento.

En las especificaciones de cajas herméticas para empalmes de cables de fibras ópticas es aplicable la Norma Oficial Mexicana siguiente:

- NOM-I-7/27 -Establece los equipos y componentes eléctricos, métodos de prueba ambientales y durabilidad, parte 27 prueba ka; aspersión salina

Materiales para la canalización

a. Manejo de materiales

Para el manejo o montaje de cualquier material, se tendrá en cuenta lo indicado en las instrucciones del fabricante. Todos los materiales han de estar tratados contra la corrosión, especialmente los anclajes, soportes, bandejas porta-cables y demás elementos metálicos usados han de ser de acero inoxidable o galvanizados en caliente. Las bobinas se transportarán siempre de pie, nunca volcadas sobre los platos laterales. Nunca se realizará la descarga de la bobina haciendo rodar la bobina dejándola caer de forma que golpee con el suelo. Durante el tendido el cable siempre deberá deslizarse mediante poleas o rodillos. Nunca se permitirá que roce en el suelo u obstáculo alguno.

b. Materiales

Los materiales que se utilicen en la instalación de los registros para fibra óptica, cumplirán con lo establecido en las Normas aplicables del Libro CMT- *Características de los Materiales*, salvo que el proyecto indique otra cosa o así lo apruebe la Secretaría.

c. Tritubos

Se entiende por tritubo al conjunto de tubos flexibles, de polietileno de alta densidad (PE-80 PE-100), de color verde, de treinta y cuatro (34) milímetros de diámetro interior nominal, con paredes de tres (3) milímetros de espesor. Los tritubos se encuentran normalizados en la norma N – CTR – CAR-1-08-007/11.

Maquinaria, herramientas y equipos

a. Condiciones de uso

Los equipos, máquinas y herramientas estarán en perfectas condiciones de uso. Al efecto de comprobar su estado se procederá a la revisión de los mismos al comienzo de la obra.

b. Equipo zanjador

El equipo zanjador será capaz de ejecutar una excavación de seis (6) centímetros de ancho y treinta (30) centímetros de profundidad por debajo del nivel de subrasante. Estará equipado con dispositivos que depositen el material excavado en ambos lados de la microzanja, para su posterior traslado.

c. Maquinaria de tendido de la fibra óptica

Tendido por cabrestante de tiro. Este ha de estar dotado de un sistema de control automático que medirá y registrará la tensión máxima aplicada en cada momento en el extremo inicial del cable, no superando nunca la máxima tensión establecida para cada cable parando automáticamente al alcanzar está.

Fig. 3. Cabrestante de tiro.
Fuente: Guía de instalación de cables ópticos subterráneos. MT 2.33.14.

Tendido por impulsión neumática. El equipo principal se localiza en la entrada del cable al tubo, se trata de una oruga que empuja al cable por medio de unos rodillos a la vez que insufla aire a presión en el tubo para introducir el cable por impulsión.

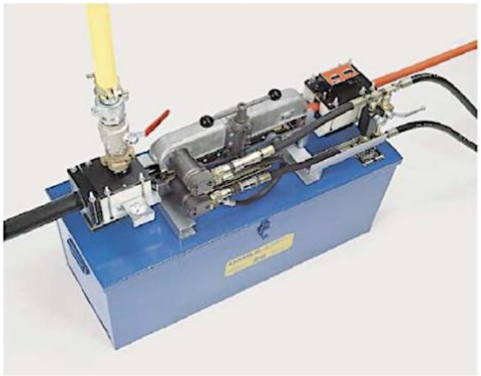


Fig. 4. Oruga de impulsión mecánica.
Fuente: Guía de instalación de cables ópticos subterráneos. MT 2.33.14.

d. Alza bobina con frenos

Con el objetivo de facilitar el tendido y dar garantías sobre el manejo del cable óptico, se deben utilizar alza bobinas con freno.

Fig. 5. Alza bobinas con freno.
Fuente: Guía de instalación de cables ópticos subterráneos. MT 2.33.14.

e. Caja de almacenamiento

Para realizar el tendido de una forma más organizada y evitar el roce del cable se debe utilizar una caja de almacenamiento en donde el cable quede depositado en una jaula giratoria a la que se puede acoplar el cabrestante de impulsión.

Fig. 6. Caja de almacenamiento.
Fuente: Guía de instalación de cables ópticos subterráneos. MT 2.33.14.

f. Equipos de comunicación

Se debe de comprobar que los equipos de comunicación funcionan correctamente y estén disponibles para atender cualquier incidencia, como puede ser la formación de cocas y/o posibles defectos en el

cable óptico o tubo efectúen la parada inmediata del proceso de tendido.

Instalación del ducto

Para la instalación de los tritubos para fibra óptica, se considerará lo señalado en la Cláusula D. de la Norma N-LEG-3, Ejecución de Obras. Las actividades que comprenden la instalación del ducto se detallan en la sección G de la norma N·CTR·CAR·1·08·007/11.

Prueba de vía para la instalación de ductos

Una vez terminado el relleno de la microzanja hasta el nivel de subrasante y conectados los tritubos a los registros, se realizarán pruebas de vía para comprobar que los ductos del tritubo son continuos en toda su longitud, es decir, que no tenga variaciones en su sección transversal provocada por deformaciones en su pared, ni ensambles defectuosos u otros daños que afecten su capacidad o que pongan en riesgo la integridad de la fibra óptica durante su colocación. Las especificaciones de las pruebas de vía se detallan en la sección G.10 de la norma N·CTR·CAR·1·08·007/11.

Prueba de hermeticidad para la instalación de ductos

Una vez comprobada la continuidad de los ductos del tritubo, se realizarán pruebas de hermeticidad para asegurar que los ductos del tritubo resistan la presión de soplado durante la instalación de la fibra óptica y no tengan grietas que pongan en riesgo la integridad de la misma después de su instalación. Las especificaciones de las pruebas de hermeticidad se detallan en la sección G.11 de la norma la norma N·CTR·CAR·1·08·007/11.

Tendido e instalación del cable de fibra óptica

Para el tendido e instalación del cable de fibra óptica, se recomienda tener en cuenta de forma general las siguientes actividades:

- Replanteos previos. Estudios previos de cada uno de los segmentos a tender para valorar y conocer las necesidades técnicas de los mismos. La información recabada durante el replanteo deberá atender los aspectos siguientes:
    - Método de tendido a utilizar;
    - Bobinas para cada segmento;
    - Material y maquinaria necesaria para el tendido del cable de fibra óptica;
    - Equipo humano que realizará los trabajos;
    - Medidas de seguridad y señalización;
    - Procedimiento de supervisión del tendido;

- Medidas medioambientales de aplicación;

- Se recomienda para el inicio de los trabajos contar con los permisos y autorizaciones necesarias.
- Se recomienda verificar todos los materiales suministrados cumplen con las especificaciones técnicas definidas previamente.
- Al finalizar la instalación, se deberán llevar a cabo los trabajos de limpieza y retirada de los restos de materiales y escombros.
- Se considera que la instalación de ductos ha sido realizada previamente conforme a la normatividad vigente.
- Verificación en el cable de fibra óptica antes del tendido. Con el objeto de detectar cualquier daño ocasionado en el núcleo óptico durante el proceso de transporte o almacenamiento se realizarán medidas reflectométricas en la tercera ventana y con un pulso ≤ a 100 *ns,* en la totalidad de las fibras de todas las bobinas. El criterio de aceptación en la atenuación especifica será < a 0.23 *dB/km* y además se observará la longitud óptica. Esta tiene que ser superior a la indicada en la placa de la bobina y tendrá en un valor que varía con el fabricante y el tipo de cable entre un 0.4% y 1%.

El tendido del cable es la acción propia de desplegar el cable de fibra óptica entre los extremos a conectar.

- Tendido de cabrestante automático. Para esta técnica es necesaria la utilización de un cabrestante automático con control de tensión. Se sitúa al final del tramo en cuestión y consiste en tirar de la fibra de forma automática, controlando la fuerza de tiro para evitar dañar el cable. Es necesario el uso de poleas para regular los radios de curvatura y la utilización de lubricantes para disminuir la fuerza de rozamiento de la cubierta del cable con la pared interior del conducto. Se suele utilizar para tendidos de cables especiales (gran sección y elevado peso), siendo desaconsejable su uso para tendidos de fibra óptica convencionales.
- Tendido mediante soplado. Este sistema se utiliza en tendidos de largas distancias y sin obstáculos intermedios. Se basa en eliminar el rozamiento del cable con el conducto haciendo flotar el cable en el interior del conducto mediante insuflación de aire a presión. En esta técnica se combinan dos sistemas para el tendido de la fibra óptica de una forma rápida y eficiente. Una fuerza de tracción se combina con una fuerza de empuje para hacer que el cable viaje como aire por el conducto. La unidad de soplado utiliza un sistema de potencia hidráulico y un compresor de aire para generar las fuerzas de empuje y tracción.

Supervisión del tendido e instalación del cable de fibra óptica

Con el objeto de garantizar la instalación correcta del cable óptico, se recomienda la supervisión del tendido, su instalación, la realización de empalmes, colocación de cajas y accesorios de fibra óptica y la correcta ejecución de las medidas ópticas finales. Será responsabilidad del supervisor, verificar que se utilizan los medios técnicos, materiales y humanos necesarios para la instalación del cable.

Medidas finales en el cable de fibra óptica

Entendemos por medidas finales los resultados obtenidos en las pruebas de atenuación óptica, reflexión óptica, dispersión cromática y dispersión por modo de polarización.

Aceptación de la instalación de los empalmes

Con base en la Recomendación UIT-T L.12 Empalmes de fibra óptica, para que un empalme sea aceptado el valor de la media aritmética será inferior a 0.10 *dB* y los valores absolutos en cualquiera de los dos sentidos inferior a 0.20 *dB* en segunda y tercera ventana. Las pérdidas de inserción en un conector se evaluarán juntamente con el empalme que une la fibra al pigtails, la pérdida del conjunto será inferior a 0.60 *dB* en ambas ventanas. La atenuación específica será medida tramo a tramo. En 1,300 *nm* será inferior a 0.38 *dB/km*. y para 1,500 *nm* inferior a 0.25 *dB/km*.

III. 3. Red ferroviaria

Otra de las redes que es susceptible de ser utilizada para propósitos de telecomunicaciones de altas tasas de transmisión es la red ferroviaria en México, a través del aprovechamiento de los derechos de vía para la instalación de fibra óptica. Para que lo anterior sea posible, se debe cumplir con normatividad técnica que asegure la operatividad de dicha fibra óptica, como se describe enseguida.

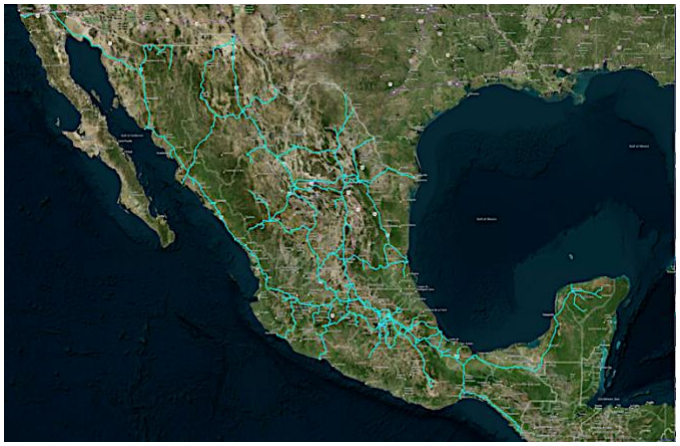


Fig. 7. Red ferroviaria en México.

Normatividad técnica que debe cumplirse para que la infraestructura de la red ferroviaria sea utilizada para propósitos de telecomunicaciones

- Recomendación UIT-T L.10 (2002). Cables de fibra óptica para aplicaciones en conductos y galerías.
- Recomendación UIT-T L.12 (2000). Empalmes de fibra óptica.
- Recomendación UIT-T L.26 (2002). Cables de fibra óptica para aplicaciones aéreas.
- Recomendación UIT-T L.34 (1998). Instalación de cables de fibra óptica de hilo de guarda.
- Recomendación UIT-T L.35 (1998). Instalación de cables de fibra óptica en la red de acceso.
- Recomendación UIT-T L.13 (2003). Empalmes de cubiertas y organizadores de cables de fibra óptica en planta exterior.
- Recomendación UIT-T K.33 (1996). Límites para la seguridad de las personas en relación con el acoplamiento en el sistema de telecomunicaciones de instalaciones de energía eléctrica c.a. y de instalaciones ferroviarias electrificadas en c.a. en condiciones de avería.
- Recomendación UIT-T K.53 (2000). Valores de las tensiones inducidas en las instalaciones de telecomunicación para establecer las responsabilidades de los operadores de telecomunicaciones y de transporte de energía eléctrica en corriente alterna y de ferrocarriles electrificados.

Materiales para la canalización

a. Manejo de materiales

De forma similar que en el caso del tendido de cable de fibra óptica en el acotamiento de carreteras.

b. Cables

El núcleo del cable que transporta a la fibra óptica puede tener diferentes configuraciones: tubo ajustado, fibra suelta en el tubo, de cinta y fibra suelta en surco. Esta última, es la configuración más utilizada. La cubierta y armadura de los cables depende de factores como el diseño del cable, tipo de infraestructura a utilizar y método de instalación. Por ejemplo, para aplicaciones aéreas se recomienda el uso de cables totalmente diélectricos o con armadura de cinta corrugada de acero cuando se entierran directamente o se instalan en conductos. Otra alternativa para estos cables aéreos es la de los cables de hilo de puesta a tierra de fibra óptica (en inglés Optical

Ground Wire, en adelante OPGW). En este caso, tienen que tomarse precauciones para evitar problemas en el sistema de señalización o en la línea de alimentación de la vía ferroviaria, Recomendación UIT-T L.56 (05/2003).

c. Tipos de infraestructura

El tipo de infraestructura a utilizar depende del tipo de instalación y el entorno (rural o urbano). La instalación puede ser en conducto, directamente enterrada o aérea. Para elegir el tipo de instalación se debe realizar un estudio de impacto medioambiental, de la reglamentación en cada región y factores económicos. Siempre que sea posible se debe utilizar la infraestructura ya existente.

Maquinaria, herramientas y equipos

a. Condiciones de uso:
   De forma similar que en el caso del tendido de cable de fibra óptica en el acotamiento de carreteras.
b. Herramientas:
   Herramientas para empalme y terminación.
   Herramientas para remover cubiertas de la fibra óptica.
   Herramientas necesarias para la preparación del empalme-cierre.
c. Equipo zanjador:
   De forma similar que en el caso del tendido de cable de fibra óptica en el acotamiento de carreteras.
d. Maquinaria de tendido de fibra óptica:
   De forma similar que en el caso del tendido de cable de fibra óptica en el acotamiento de carreteras.
e. Equipos de comunicación:
   De forma similar que en el caso del tendido de cable de fibra óptica en el acotamiento de carreteras.

Instalación en conductos

Para la instalación de fibra óptica en vías ferroviarias en conductos se pueden utilizar diferentes diseños de cable:

- Cable totalmente dieléctrico.
- Cable con armadura metálica.

Por lo general la instalación de estos conductos puede ser elaborada por una compañía ferroviaria o por un proveedor local de telecomunicaciones. Dependiendo del diseño del cable a escoger se instalará en el conducto mediante cualquiera de los métodos tradicionales. Se recomienda la utilización de cables armados en el caso en que los cables se depositen en una zanja de cemento cubierta posteriormente con tapa.

Instalación en cables directamente enterrados

Para este tipo de instalación se recomienda elegir un cable diseñado para proteger a las fibras ópticas de choques externos, ataques de los roedores o cualquier otra condición ambiental de riesgo. Debería considerarse la posibilidad de armar los cables con cintas corrugadas de acero o cualquier otro tipo de armadura. Dependiendo del diseño del cable se utilizará alguno de los métodos tradicionales de instalación.

Fig. 8. Instalación de cables directamente enterrados.
Fuente: Broadband applications & construction manual of Commscope.

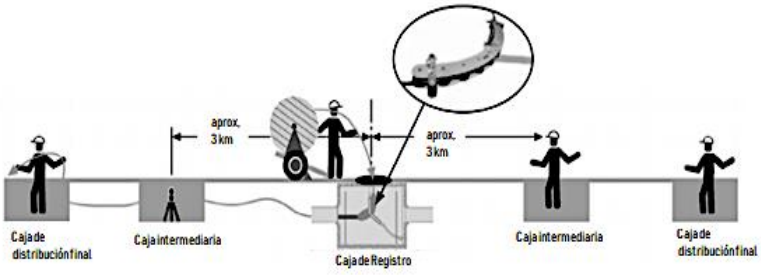


Fig. 9. Ubicación de cajas: de registro, intermedia y distribución final.
Fuente: Broadband applications & construction manual of Commscope.

Instalación aérea

En instalaciones aéreas se recomienda la utilización de cables totalmente dieléctricos y armados en contra de pájaros u otros animales, todo en función de las condiciones medioambientales. En caso de no usar cables totalmente dieléctricos se recomienda utilizar los cables de hilos de puesta tierra de fibra óptica (OPGW) los cuales se deben tener las precauciones para evitar cualquier problema en el sistema de señalización o en la línea de alimentación. Se tendrá en cuenta la Recomendación UIT-T L.34 - Instalación de cables de fibra óptica de hilo de guarda. Generalmente se usan los postes de las líneas ferroviarias de suministro eléctrico

para colgar y sujetar el cable, pero también suelen utilizarse otros postes que pertenecen al proveedor de telecomunicaciones.

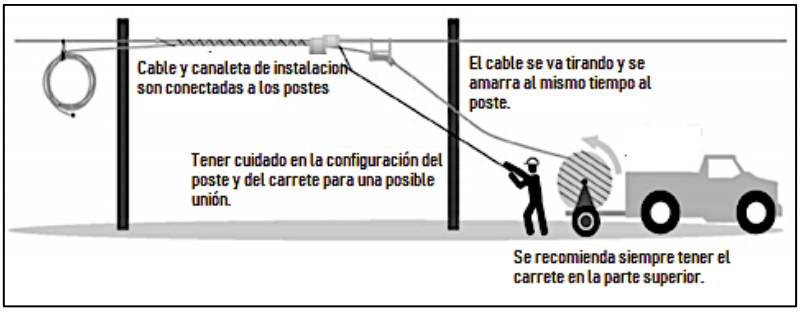


Fig. 10. Instalación aérea.
Fuente: Broadband applications & construction manual of Commscope.

En cuanto al material de los postes para la alimentación de las vías ferroviarias se recomienda que sean de cemento o hierro. Si existen o se necesitan postes adicionales deberían ser de madera, cemento, acero, fibra o plástico en función del coste y del estudio de impacto medio ambiental. En caso de que se utilicen los postes el suministro eléctrico ferroviaria para la instalación del cable óptico, este puede ser colgado del lado de la vía o del lado exterior. Se recomienda que, la altura mínima desde el nivel del suelo (cuando el cable está instalado en el lado exterior) o desde la vía (cuando el cable se ha instalado en el lado de la vía) debe ser superior a cinco metros e inferior o igual a 10 metros. La separación horizontal del conductor eléctrico activo dependerá del diseño de la línea de postes teniendo en cuenta los requisitos de seguridad para las operaciones. En cuanto a la longitud de un vano o distancia entre postes puede depender de las características del tendido y del diseño de cable, también se recomienda que la flecha nominal del cable no supere el 3% debido a que el cable debe suspenderse de todos los postes de forma adecuada en función del diseño de cable y de las características del tendido es necesario el uso de abrazaderas o poleas. Para los trabajos de instalación de cable en los postes y pruebas de control al principio y al final de cada tramo se suministra una longitud adicional de cable. Esta longitud adicional garantiza la capacidad de instalación y reinstalación mediante cajas de conexiones. Algunas veces es necesaria una longitud adicional de cable para realizar los trabajos de instalación en el suelo. Las cajas y el remanente de cable se sitúan en los postes de la siguiente manera. Estas cajas de unión mantienen las características eléctricas y mecánicas del cable de fibra óptica ya sea durante la instalación como en operación.

Casos particulares

Cuando es necesaria la instalación del cable óptico por túneles y puentes se requiere protección adicional o precauciones especiales como las cubiertas ignífugas. Para el caso de la instalación de cable óptico por túneles debe estar fijado

mediante un soporte a la pared con grapas o utilizando conductos. En cuanto a la instalación del cable óptico en puentes se utilizan conductos.

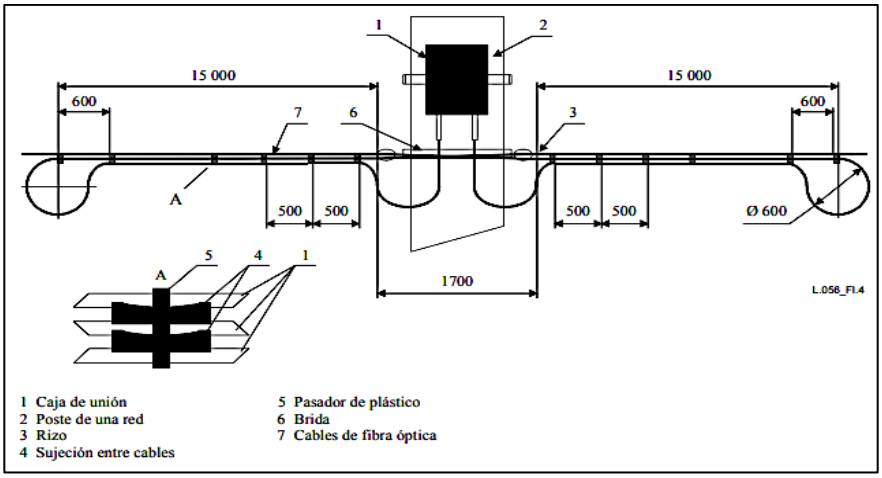


Fig. 11. Instalación de cables de fibra óptica a lo largo de las vías ferroviarias.
Fuente: UIT-T L.56.

Supervisión del tendido e instalación del cable de fibra óptica

De forma similar que en el caso del tendido de cable de fibra óptica en el acotamiento de carreteras.

Medidas finales en el cable de fibra óptica

De forma similar que en el caso del tendido de cable de fibra óptica en el acotamiento de carreteras.

Aceptación de la instalación de los empalmes

De forma similar que en el caso del tendido de cable de fibra óptica en el acotamiento de carreteras.

IV. Ventajas del esquema de compartición de infraestructura

Como lo sugiere Martínez *et al.,* (2020), la compartición de infraestructura origina una serie de beneficios sociales y económicos:

- Reduce el costo y tiempo de implementación de las redes y los costos operativos, además de acelerar potencialmente el tiempo de comercialización, con impactos positivos en cobertura.
- Crea beneficios ambientales positivos al reducir la duplicación de redes.
- Mejora la provisión de servicios y crea incentivos para que los operadores extiendan sus redes.

- Reduce la barrera derivada de la obtención de permisos y del pago de derechos por concepto de uso de derechos de vía.

Adicionalmente, el aprovechamiento de derechos de vía de redes carreteras y ferroviarias permitirá mejorar las capacidades en las redes de transporte, crear circuitos redundantes que permitan mejorar la disponibilidad operativa de las redes de telecomunicaciones de altas capacidades y habilitar la cobertura en localidades muy dispersas desde el punto de vista geográfico.

V. Programa de cobertura social del Gobierno Federal de México

El Programa de Cobertura Social del Gobierno Federal de México (en adelante Programa) tiene como objetivo establecer las bases para promover el incremento en la cobertura de las redes y la penetración de los servicios de telecomunicaciones y radiodifusión incluyendo banda ancha e Internet, bajo condiciones de disponibilidad, asequibilidad y accesibilidad, en las Zonas de Atención Prioritaria de Cobertura Social (STC, 2019), las cuales se determinaron con base en los siguientes criterios:

- Localidades de alta y muy alta marginación.
- Localidades con alta presencia de población indígena y afromexicana.
- Localidades alejadas de las zonas con servicio de Internet.
- Localidades incluidas en el “Decreto por el que se formula la Declaratoria de las Zonas de Atención Prioritaria en cumplimiento a la Ley General de Desarrollo Social”.
- Localidades que son cabeceras municipales sin cobertura de servicio de Internet.
- Localidades con solicitud de atención ciudadana de acceso a Internet.

De esta forma, se contabilizan 7 537 localidades en las que viven 4.8 millones de habitantes. Dicho Programa puede ser aprovechado por el Instituto Federal de Telecomunicaciones para establecer a los concesionarios las obligaciones de cobertura geográfica, poblacional o social y de conectividad en sitios públicos. De forma tal que, serán los concesionarios de telecomunicaciones y radiodifusión los responsables de ampliar el despliegue de las redes en condiciones de competencia, atendiendo además sus compromisos de cobertura y penetración (SCT, 2019). Sin embargo, lo anterior no es posible si no se realiza bajo un esquema de aprovechamiento de infraestructura existente que sea susceptible de ser utilizada para propósitos de redes de telecomunicaciones, como es el caso de la red

carretera y la red ferroviaria, debido principalmente a la dispersión geográfica de las Zonas de Atención Prioritaria de Cobertura Social, ver la Figura 17.

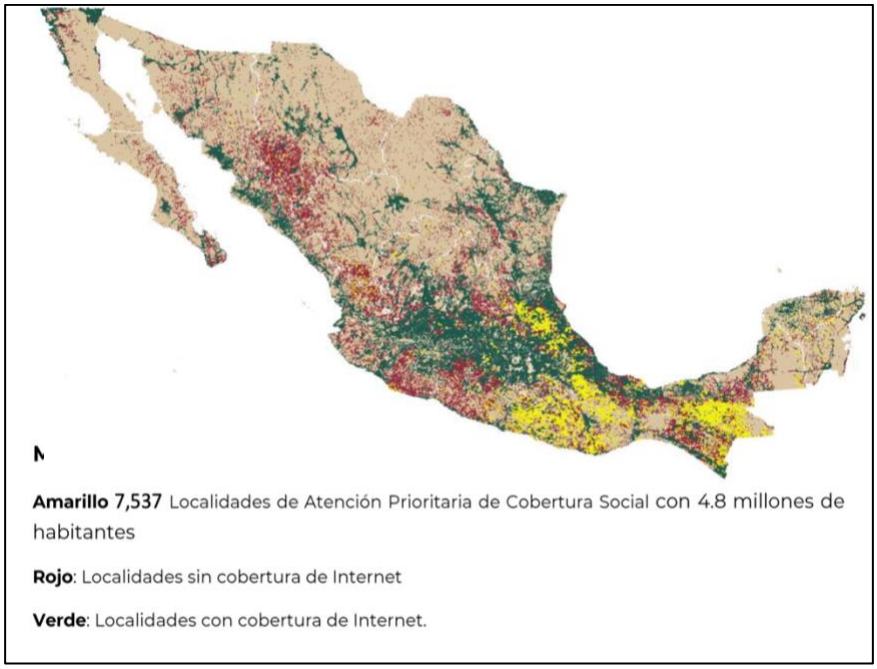


Fig. 12. Localidades de Atención Prioritaria de Cobertura Social, 2021-2022. Fuente: SCT (2021).

VI. Conclusiones

Se presentó un esquema de compartición de infraestructura pasiva entre sectores como es la infraestructura asociada a la red carretera y a la red ferroviaria en México, susceptible de ser utilizada para propósitos de telecomunicaciones, con base en la cual podrían enfrentarse los retos para reducir la brecha digital en México como son la gran dispersión geográfica de la población mexicana, la geografía accidentada a lo largo del territorio nacional y el desconocimiento de normatividad técnica que debe cumplirse para que la infraestructura de redes de otros sectores sea utilizada para propósitos de telecomunicaciones. Entre las ventajas que implica la compartición de infraestructura encontramos el uso de derechos de vía para realizar obras de ingeniería civil y conductos en diferentes municipios y estados federales de México. Además, a través del esquema de compartición de infraestructura pasiva podrían reducirse considerablemente los costos de despliegue para las redes de transporte de telecomunicaciones de altas capacidades y habilitadoras de cobertura, tal y como ya se hace en países como Brasil (UIT, 2008). Las mejores prácticas sugieren que en el caso de redes móviles, la compartición de infraestructura puede desempeñar un papel importante para aumentar el acceso a las tecnologías de la información y la comunicación (TIC),

generar crecimiento económico, mejorar la calidad de vida y ayudar a los países en desarrollo y desarrollados a cumplir los objetivos establecidos por la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y los Objetivos de Desarrollo del Milenio establecidos por las Naciones Unidas (ODM). Consideramos que, los resultados de este estudio pueden apoyar la toma de decisiones del Gobierno Federal y de los concesionarios y operadores de redes de telecomunicaciones para lograr la conectividad universal en las Zonas de Atención Prioritaria de Cobertura Social.

VII. Referencias

Antonopoulos, A., E. Kartsakil, A. Bousia, L. Alonso, and C. Verikoukis. (2015). Energy-efficient infrastructure sharing in multi-operator mobile networks. IEEE Communications Magazine, vol. 53 (5), May 2015.

APEC. (2011). Survey Report on Infrastructure Sharing and Broadband Development in APEC Region Asia, 2011. https://www.apec.org/Publications/2011/09/Survey-Report-on-Infrastructure-Sharing-and-Broadband-Development-in-APEC-Region.

Bousia, A., E. Kartsakli, A. Antonopoulos, L. Alonso, and C. Verikoukis. (2015). Game-theoretic infrastructure sharing in multioperator cellular networks. IEEE Transactions on Vehicular Technology, vol. 65(5), June 2015.

Burhanudin B. and Asvial, M. (2018). Regulatory framework analysis of infrastructure sharing for mobile operators in Indonesia by using regulatory impact analysis approach, in 2018 International Conference on Applied Information Technology and Innovation (ICAITI), September 2018.

Cano, L., A. Capone, G. Carello, and M. Cesana. (2015). Evaluating the performance of infrastructure sharing in mobile radio networks, in *2015 IEEE International Conference on Communications (ICC)*, June 2015.

DOF. (2020). ACUERDO mediante el cual el Pleno del Instituto Federal de Telecomunicaciones emitió los Lineamientos para el Despliegue, Acceso y Uso Compartido de Infraestructura de Telecomunicaciones y Radiodifusión. https://www.dof.gob.mx/nota_detalle.php?codigo=5583940&fecha=15/01/2020.

Frisanco, T., P. Tafertshofer, P. Lurin, and R. Ang. (2008). Infrastructure sharing and shared operations for mobile network operators: from a deployment and operations view, in *IEEE Network Operations and Management Symposium (NOMS),* April 2008.

Martínez Garza, R., Iglesias rodríguez, E., García Zaballos, A. (2020). Transformación digital: compartición de infraestructura en América Latina y el Caribe. Banco Interamericano de Desarrollo.

https://publications.iadb.org/publications/spanish/document/Transformacion-digital-Comparticion-de-infraestructura-en-America-Latina-y-el-Caribe.pdf.

Meddour, D. (2011). On the Role of Infrastructure sharing for Mobile Network Operators in Emerging Markets," Italia, 2011. https://www.sciencedirect.com/science/article/abs/pii/S1389128611000776.

SCT. (2021). Secretaría de Comunicaciones y Transportes. Programa de Cobertura Social 2021-2022. https://www.gob.mx/cms/uploads/attachment/file/687804/211209_PCS_2021-2022_vf.pdf.

SCT. (2019). Secretaría de Comunicaciones y Transportes. Programa de Cobertura Social 2019. Octubre 2019. https://www.gob.mx/sct/acciones-y-programas/programa-de-cobertura-social.

UIT. (2008). Ampliación del acceso abierto a las redes troncales de fibra nacional en los países en desarrollo. Ginebra: UIT.

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014L0061&from=es

https://www.cr-online.de/bgbl116s2473.pdf.

http://www.autoritedelaconcurrence.fr/doc/jo_lme.pdf.

https://dre.pt/home/-/dre/107785482/details/maximized.

https://www.hakom.hr/UserDocsImages/2011/propisi_pravilnici_zakoni/Pravilnik%20o%20tehnièkim%20uvjetima%20za%20elektronièku%20ko

EXPERIENCIAS EN LA GESTIÓN DE ACTIVOS FÍSICOS. CASO: REDES DE CÓMPUTO CORPORATIVO EN UNA FIRMA DE MANUFACTURA

Adrián LÓPEZ MARTÍNEZ[11]

[11]Maestro en Ingeniería de Operaciones Estratégicas por la Universidad Autónoma de Yucatán. Ingeniero en Electrónica y Comunicaciones por la Universidad Autónoma de Nuevo León. Registro ORCID 0009-0007-0185-0487. Contacto: adrianloma@hotmail.com.

EXPERIENCIAS EN LA GESTIÓN DE ACTIVOS FÍSICOS. CASO: REDES DE CÓMPUTO CORPORATIVO EN UNA FIRMA DE MANUFACTURA

Physical Asset Management Experiences in Case: Corporate Computer Networks in a Manufacturing Firm

Resumen

La gestión de activos es la administración de bienes físicos de una firma o compañía tales como: maquinaria, vehículos, equipamiento, planta de producción, edificios e infraestructura.

El desarrollo de activos físicos ha sido un sello distintivo de la actividad humana desde tiempos remotos. Por ejemplo, la rueda, lo que significa que también debió haber artesanos que estuvieran familiarizados con el rodamiento, del que depende la rueda, al igual que todas las herramientas para su construcción. Por ende, el mantenimiento y apoyo logístico para estos “activos” debió haber existido desde una fecha muy temprana.

Diversas Universidades han desarrollado sus propios enfoques sobre el tema, bajo títulos como: Logística, Ingeniería en Sistemas, Ingeniería de Obras Públicas, Infraestructura y mantenimiento o llanamente Costos. El papel de la administración de activos es aportar una combinación de conocimiento técnico y conocimiento comercial para satisfacer de manera efectiva y eficiente las necesidades de negocio en su conjunto.

Esta ponencia presenta una introducción a la gestión estratégica del ciclo de vida de un activo, la evaluación de negocio, la concepción de los proyectos, los horarios de planeación financiera y la continuidad

Abstract

Asset management is the administration of physical assets of a firm or company such as machinery, vehicles, equipment, production plant, buildings, and infrastructure.

The development of physical assets has been a hallmark of human activity since ancient times. For example, the wheel, which means that there must also be craftsmen who were familiar with the bearing, on which the wheel depends, as well as all the tools for its construction. Therefore, maintenance and logistical support for these "assets" must have existed from early dates.

Several universities have developed their own approaches to the subject, under degrees such as Logistics, Systems Engineering, Public Works Engineering, Infrastructure, and Maintenance or simply Costs. The role of asset management is to bring a combination of technical knowledge and business knowledge to meet business needs effectively and efficiently as a whole.

This paper presents an introduction to the strategic management of the life cycle of an asset, business evaluation, project conception, financial planning schedules and asset continuity. General principles of technology asset management in the case of a corporation's computer network are reviewed.

del activo. Se revisan los principios generales de la gestión de activos tecnológicos en el caso de la red de cómputo de una corporación.
Después, el documento presenta 10 puntos de control entregables, con detalles técnicos valiosos. Aprendizajes recabados al haber realizado la renovación de activos en catorce cuartos de comunicación en diferentes edificios en la misma firma corporativa o compañía.

Palabras clave: gestión de activos físicos, procesos del ciclo de vida, ISO 55000, fiabilidad, infraestructura.

The document then presents 10 deliverable checkpoints, with valuable technical details. Lessons learned from having conducted renovation of assets in fourteen communication rooms in different buildings in the same corporate firm or company.

Keyword: *physical asset management, life cycle processes, ISO 55000, reliability, infrastructure*.

I. Introducción

Entre el 3 000 y el 2 500 a.C. el uso de la rueda se había extendido desde suiza al Indo continente pasando por Mesopotamia en forma de piezas macizas tripartitas cuya peculiar forma de construcción, era idéntica desde Zúrich a Iraq según Piggot (1983).

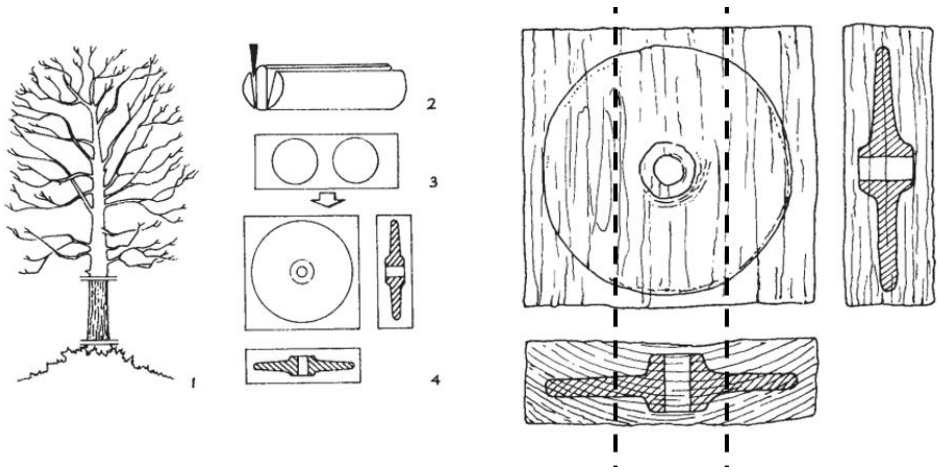


Figura 1. Diagrama básico de la construcción de una rueda tripartita a partir del tronco de un árbol. Fuente: Piggot (1983).

El uso de la rueda y su evolución llevó a la humanidad a mejorar las interacciones que tenían sus pobladores en todas partes del mundo, se crearon trabajos más especializados y el florecimiento de industrias cada vez más específicas como, la creación de rodamientos muy económicos para el comercio o

ligeras y muy fuertes, digamos la última gama para la guerra para su uso en cuadrigas. Tener información de cuántas ruedas estaban disponibles, dónde existían los materiales y los artesanos que las fabricaran debió ser fundamental para mantener sus flotillas en servicio y reponer los activos que se fueran dañando. La gestión de los activos da seguimiento a la vida y mantenimiento de los equipos o activos físicos de una organización. Los tipos de activos incluyen vehículos, computadoras, muebles y maquinaria de producción y soporte.

La gestión de activos fijos puede influir en cómo las organizaciones supervisan equipos y vehículos. Evaluar su estado y mantenerlos en buen funcionamiento, de esta manera, se minimizan las pérdidas de inventario, las fallas de los equipos, el tiempo de inactividad, y mejoran el desempeño de una organización.

Sin una adecuada gestión de activos fijos, una organización puede experimentar infracciones de seguridad o medioambientales. No cumplir con los estándares regulatorios o de conformidad y, por tanto, pérdida de contratos. Este trabajo, tiene la finalidad de presentar una introducción a la gestión estratégica del ciclo de vida de una red de telecomunicaciones como activo y propone 10 puntos de control entregables, cuando se considera su renovación.

II. Ciclo de vida de un activo

Una ilustración básica del rol de los activos físicos y de la gestión de activos dentro de una organización o firma se muestra en la figura 1 donde se ilustra que el componente principal es la demanda del cliente que conduce a los objetivos de negocio y sus planes de negocio.

La gestión de activos sirve para proporcionar activos que soportan las operaciones del negocio. Esta actividad requiere un sistema de gestión de activos para su planeación, adquisición, manteamiento y logística. Como lo muestra la figura 2. No olvidar que otros servicios de soporte como tecnologías de información, financieros, y legales también son requeridos en todas estas actividades.

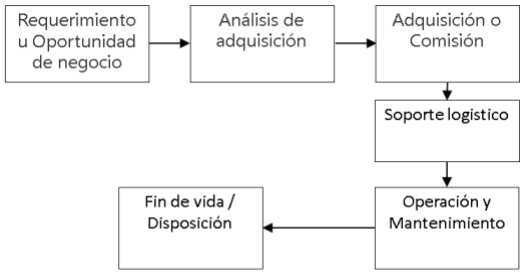


Figura 2. Ciclo de vida de un activo.
Fuente: Elaboración propia.

- Requerimiento de negocio. Identificación de oportunidades de negocio o necesidades operativas,
- Análisis de adquisición, física y financiera—selección de opciones,
- Adquisición, incluyendo la implementación a operaciones,
- Soporte logístico para aprovisionamiento, como instalaciones de mantenimiento, consumibles y partes de reemplazo,
- Operación, mantenimiento y disposición.

Los gestores de activos están involucrados en todos los aspectos del ciclo de vida del activo por las siguientes razones:

- Asistir a la organización a identificar y a adquirir los activos requeridos para soportar los objetivos de negocio;
- Proporcionar conocimiento que aporte al proceso de presupuesto de capital y los costos de operación sobre todo el ciclo de vida del activo;
- Asegurar que los sistemas empleados por la firma brinden el soporte al activo durante su vida útil;
- Y para evitar sorpresas en la implementación operativa.

Según la norma internacional ISO 55000, la gestión de activos busca maximizar la relación calidad-precio para asegurar el mejor retorno de la inversión.

II.1. Planeación estratégica de activos

Los negocios de activos de uso intensivo requieren una detallada planeación que sea originado en el área de planeación de capital y presupuesto, tomando en cuenta:

- Activo (y capacidad asociada) desarrollo de planeación e implementación,
- Planeación de continuidad de activo e implementación,
- Mantenimiento e instalaciones logísticas de soporte, desarrollo y gestión,
- Desarrollo de caso de negocio para los presupuestos relacionados al capital.

En el área de presupuesto operativo se involucran decisiones relacionadas con:

- Sistemas y procedimientos relacionados a los activos en toda la organización,
- Sistemas de control de inventario para consumibles y partes de remplazo,
- Desarrollo y gestión de tercerización de mantenimiento,
- Concientización y gestión de complimiento a regulaciones,
- Desarrollo de caso de negocio para los presupuestos operativos.

Los gestores de activos necesitan ser capaces de proporcionar el estado de la situación de los activos y ser consciente de los factores como edad y condición de la flota de activos, el rol evolutivo de los activos en los negocios y los desarrollos en términos técnicos y de las expectativas de servicio. La imagen estratégica de la gestión de activos se puede resumir en la figura 3, donde la doble flecha apuntando arriba y abajo indica la naturaleza del flujo en el proceso de planeación.

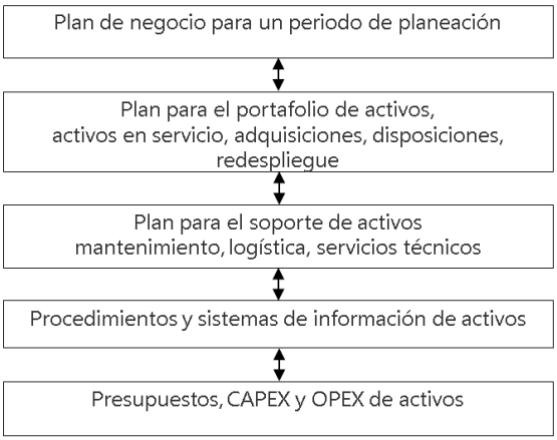


Figura 3. Elementos de planeación de activos estratégicos.
Fuente: Elaboración propia.

II.2. Preguntas básicas de gestión de activos

La gerencia de activos necesita continuamente proporcionar respuestas a preguntas básicas de cualquier activo como:

- ¿Cómo funciona el activo?
- ¿Es seguro en su operación?
- ¿Soporta los objetivos de negocio?

En relación con los objetivos de negocio se tiene que adquirir el adecuado:

- Equipamiento por tipo y ubicación.
- Instalaciones de soporte, edificios, logísticos, tipo y ubicación.
- Recurso humano dedicado a soporte en cantidad y calificado.
- Sistemas de información y procedimientos de gobernanza, gestión de riesgos, gestión de cambio, monitoreo de desempeño y mejora.

Una correcta planeación requiere desarrollar un caso con las siguientes actividades para el soporte y el nivel apropiado de gestión:

- Edificios, planta, maquinaria, equipamiento: comprar o vender, rentar o terminar arriendo,
- Instalaciones para el activo, expandir, reducir, consolidar o reubicar,
- Personal de soporte a activos, reclutar, reducir, entrenar, subcontratar, o contratar internamente.

II.3. Peligros de una gestión de activos deficiente

En negocios de uso intensivo de activos, es esencial estructurar la organización, para que el desarrollo, adquisición y operación de los activos sea conducida efectivamente.

Funciones de negocio como ventas, operaciones, finanzas y gestión de recursos humanos están siempre muy bien documentadas en la estructura de negocio, donde la gestión define sus actividades y áreas de responsabilidad, pero la gestión de activos es una "área gris," por debajo de la competencia de gerencia superior, pero por encima del nivel de mantenimiento.

La carencia de un enfoque de la gestión de activos puede conducir a problemas de pobre comunicación entre operaciones y mantenimiento por un lado y, la "gerencia superior" del otro. Esto se aplica tanto al entendimiento de las situaciones físicas y a los pasos financieros necesarios para atender problemáticas actuales o potenciales. Desencadenando pérdidas de negocio que aparecen como una falta de la disponibilidad de activos y finalmente en la espiral de muerte de activos.

Como ejemplo, un ingeniero de monitoreo identifique un problema de disponibilidad de equipo, como falta de "interfaces, puertos o transceptores" en un equipo de telecomunicación. Pero en una visión general, no es evidente de forma inmediata, si esto es un problema temporal con el que es mejor vivir con él, si se requiere comprar más transceptores aumentando la capacidad de la infraestructura con conmutadores más potentes, problemas de fiabilidad de proveedor o si también se requiere aumentar el cableado de fibras ópticas que soportan la espina dorsal.

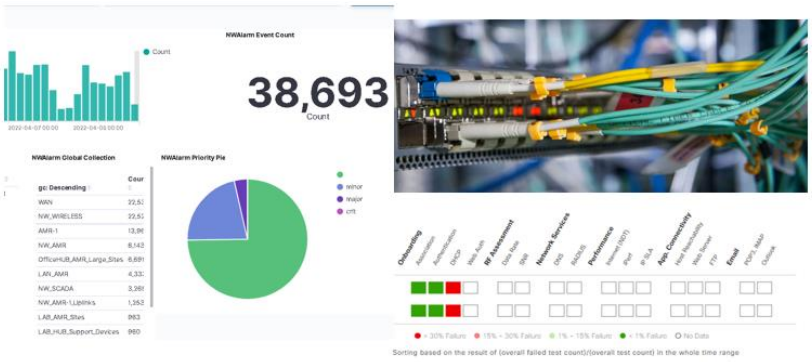


Figura 4. Sistemas de gestión a incidentes, y equipos de conmutación.
Fuente: Elaboración propia.

Para obtener la mejor solución se requerirá de un análisis, del plan de operación del negocio y el plan de la gestión de activos. La continua recurrencia de problemas de este tipo indica el rol esencial que juega el gestor de activos.

III. Del concepto a la aprobación de proyecto

El desarrollo de negocio es un rol importante de la alta gerencia. La planeación de desarrollo requiere confidencialidad, conforme los planes son discutidos lo que podría influenciar la dirección en general de los negocios, pero que están aún en estado de incertidumbre. Un grupo de desarrollo de negocios es normalmente establecido para generar, asesorar, y monitorear principales desarrollos potenciales.

El grupo de desarrollo de negocio es un grupo de nivel de alta gerencia que:

- Identifica las necesidades de desarrollo de negocio,
- Examina las opciones que cumplen las necesidades,
- Establecen prioridades,
- Asesoran los retornos financieros, recursos y restricciones,
- Planean el impacto de desarrollos en los negocios,
- Inician grandes proyectos de desarrollo,
- Tiene la responsabilidad de la estrategia de desarrollo de capacidad del negocio (qué tan rápido y en qué puntos).

III.1. Comienzo de Proyecto

La lógica detrás de los proyectos de activos de uso intensivo puede ser uno o más de los siguientes:

- Renovación o actualización de activos existentes.
- Creación de capacidad, expansión, reducción o consolidación.
- Reducción del costo de proceso.
- Mejora de procesos en cantidad o calidad.
- Eliminación de cuellos de botella.
- Desarrollos técnicos, interna y externamente.
- Respuesta a cambios regulatorios.

III.2. Tipos de adquisiciones o desarrollos

Multitud de tipos diferentes de adquisición de activos o procesos de desarrollo pueden ser identificados de la siguiente manera:

- Adquisición de repisa-estante (sin modificaciones).
- Desarrollo de negocio, pero no adquisición primaria.
- Diseño incorporación al seleccionar elementos de repisa/estante.
- Diseño desde pizarra, usando tecnología estandarizada.
- Introducción de cambio técnico (reacondicionamiento).

- Diseño con tecnología de desarrollo.
- Investigación y desarrollo.

Una adquisición desde repisa-estante, es una donde se adquiere un producto existente, sin diseño o involucrar modificaciones. Con las adquisiciones desde repisa, los requerimientos de soporte logístico debieran estar debidamente cubiertos, y comúnmente están disponibles como una parte estándar dentro del paquete de adquisición.

III.2.1. Complejidad del proyecto

Factores para tomar en cuenta cuando se considera el desarrollo de un proyecto, incluir lo siguiente.

- Tamaño y alcance y urgencia;
- Costo y nivel de aprobación requerido;
- Interdependencia con otros proyectos y escala de tiempos semanas, meses o años;
- Familiaridad – este proyecto es similar a proyectos anteriores o cual es el porcentaje de novedad.
- Proveedores involucrados (existentes, nuevos, uno o muchos);
- Cambio, extensión de capacidad instalada.
- Ambiental, herencia, aspectos políticos-corporativos.

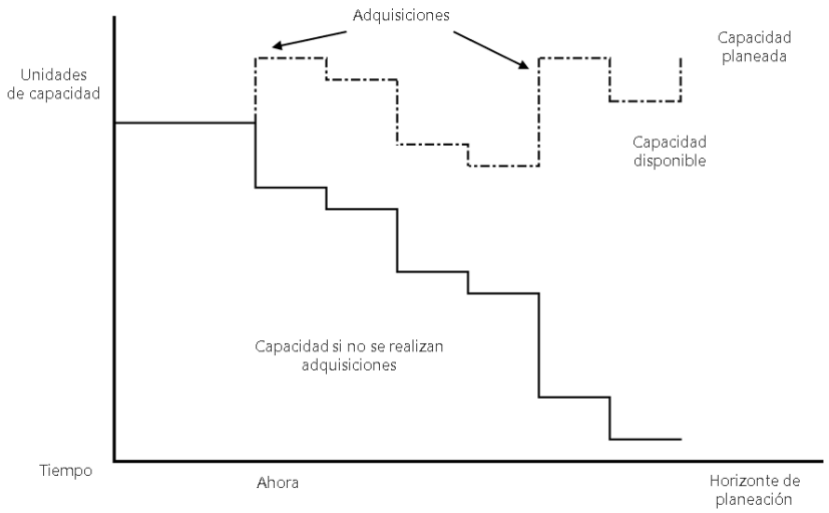


Figura 5. Plan de Desarrollo de activos.
Fuente: Elaboración propia.

Las etapas del desarrollo de grandes proyectos son las siguientes:

- Iniciación de proyecto.
- Análisis de requisitos de capacidad.

- Análisis de pre-factibilidad: identificar opciones.
- Análisis de viabilidad: plan detallado.
- Aprobación del proyecto.
- Implementación y pruebas unitarias.
- Aceptación final.

IV. Estrategia de adquisición

Al considerar las opciones de adquisición y desarrollo es importante asegurar si es factible desde el punto de vista de entrega. Un equipo de desarrollo puede ser sobre optimista, al evaluar qué capacidades tienen los proveedores, pueden proporcionar y qué proyectos se pueden ejecutar internamente, dados el tiempo y el presupuesto destinado.

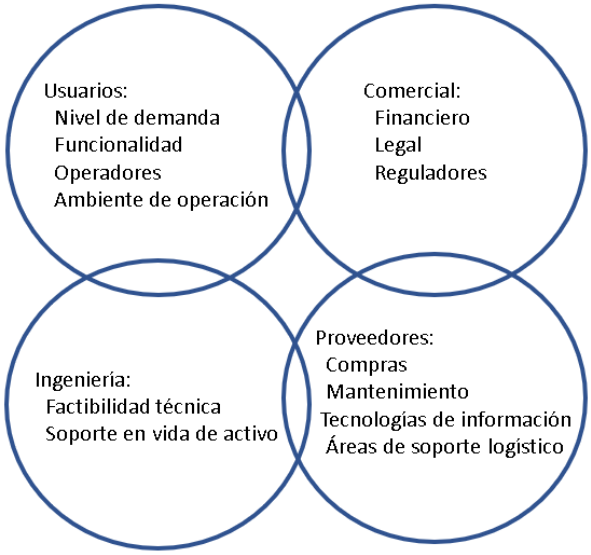


Figura 6. Involucrados en la estrategia de adquisición.
Fuente: Elaboración propia.

Existen peligros al asumir que las adquisiciones son de repisa, cuando en realidad requieren adaptaciones para cubrir las necesidades de la firma. En ese caso es aconsejable tomar la adaptación como un proyecto por separado, y solo proceder con el proyecto principal cuando se esté seguro de que las necesidades pueden ser cumplidas con los parámetros adecuados para el negocio.

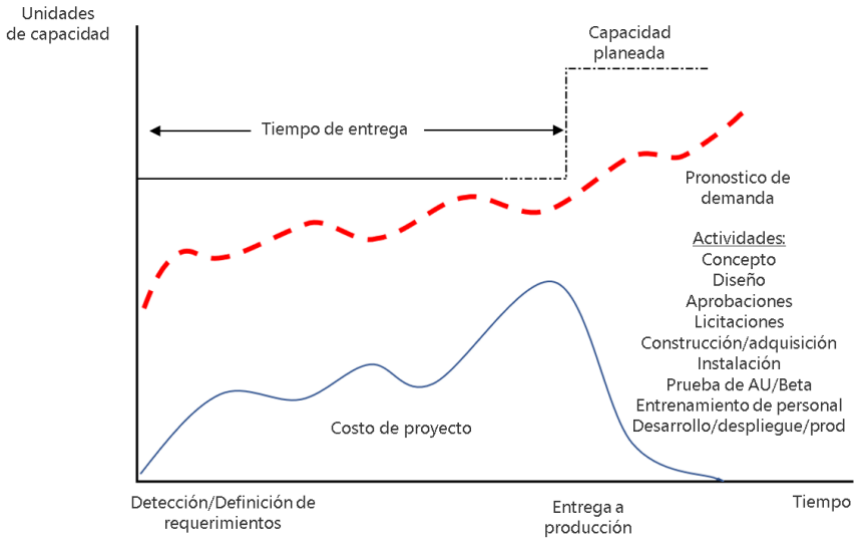


Figura 7. Tiempos de entrega de actividades para bienes de capital.
Fuente: Elaboración propia.

V. Conocimiento íntimo de los activos

Una gestión de activos exitosa depende de que los gerentes tengan un claro entendimiento de los activos usados para físicamente operar y dar servicio al negocio y también mantenerlo rentable.

V.1 Resumen de activos físicos

El resumen de los activos físicos clave debe ser establecido y mantenido como una parte del documento de planeación estratégica de gestión de activos. Este resumen puede incluir listas, mapas, diagramas de flujo, agrupaciones geográficas u organizacionales, planes, imágenes satelitales, fotografías, imágenes de videovigilancia a varios niveles de detalle.

El resumen debe proporcionar un entendimiento de la localidad y la naturaleza de los activos y pudiera indicar también su condición actual, como se muestra en la tabla 1.

Activo	Cantidad
Enrutadores de corazón	3 (-1)
Enrutadores de distribución	4
Conmutadores de entrada oficina	4

Circuitos de área ancha	2
Proveedores de Internet	2
Transceptores, LC de 10 giga corta distancia	22
Fibras ópticas de columna vertebral, MDF 111-112	12 (-8)
Presupuesto anual de capital	260,000 USD
Presupuesto de mantenimiento	85,000 USD
Presupuesto de renovación de 12 fibras MDF 112-211	$ 4800 USD

Tabla 1. Resumen de activos en una red de computo.
Fuente: Elaboración propia.

V.2. Conocimiento del activo

Sumado a la información contenida en el resumen de activos físicos, los gerentes de activos deben tener disponible el acceso a todos los detalles adicionales con respecto a los activos. Aspectos importantes como los enumerados a continuación.

Conciencia de los activos clave/críticos:

- Dibujos, con nombre clave, identificador y ubicación.
- Manuales de operación y mantenimiento.
- Diagrama de bloques de los grandes flujos de producción, sistemas.
- Condición del activo, tiempo restante de vida útil, valor en libros.
- Historia reciente, última reparación, modificación o fecha de actualización, problemas y planes conocidos.
- Criticidad de los activos desde el punto de vista de servicio.
- Concientización de individuos expertos o equipos que tienen conocimiento total y detallado de un tipo particular de activo.

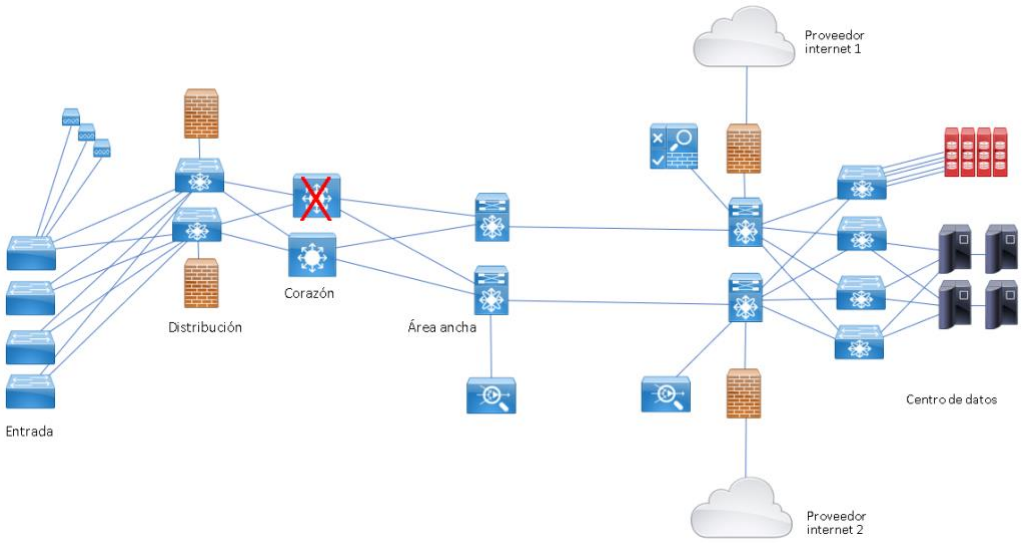


Figura 8. Diagrama de bloques capa 3 con un activo fuera de servicio.
Fuente: Elaboración propia.

Las siguientes premisas pueden ser usadas para crear un diagrama de bloques:

1.- La función de cada componente o bloque tiene que ser identificada.

2.- Cada bloque tiene que ser físicamente identificable.

3.- Los bloques tienen que ser mutuamente independiente (tanto como sea razonablemente posible).

4.- Enlaces, cableados y acoplamientos, tienen que ser asignados a bloques específicos o formar su propio bloque cuando sea justificable.

5.- Cada bloque mantenga la preferencia en un solo enfoque, capa 1, diagrama de flujo por aplicativo o capa 3, que es el más común en la infraestructura de redes de cómputo mostrado en la figura 8.

VII. Planeación de continuidad de activo

Cada activo tendrá su propio ciclo de vida, pero la situación general es más compleja de lo que pudiera sugerirse si se utiliza una visión basada en ciclos de vida de los activos individuales, o por el tipo de activos de manera independiente. Las “entradas a capacidad” de los principales tipos de activos son frecuentemente traslapados, de la misma forma que el soporte a los activos de sistemas o instalaciones. Y su renovación requiere la participación de múltiples partes interesadas.

VI.1. Factores en la planeación de continuidad de activo

VI.1.1. Financiera

Al mantener la continuidad activos es necesario el aprovisionamiento financiero para la compra de nuevos artículos conforme la flotilla envejece y los fabricantes descontinúan su producción y soporte.

Es muy probable que la mayoría de los artículos en la flotilla tengan edades similares y en este caso se tendrá que aprovisionar financieramente contra el tiempo cuando muchos los remplazos sean debidos. Las cantidades compradas en cierto tiempo pudieran involucrar negociaciones para el capital disponible y descuentos por el volumen adquirido. Idealmente la gerencia necesita saber cuánto tiempo durará un artículo de forma individual antes de necesitar remplazarlo. En la práctica se toma en consideración de forma individual la condición del activo y los requerimientos de servicio cuando se toma una decisión de reemplazo.

VII. Terminología de planeación de activos

Como se mencionó en el apartado anterior, la gerencia financiera necesita un estimado para saber cuándo reemplazar cada tipo de activo. Esta información puede estar contenida en el plan de gestión de ciclo de vida de activos, y de forma detallada en el inventario de activos.

También se deben registrar los montos de utilización del activo; así como, los años en operación, la versión del sistema operativo, la última vez que se reinició el activo, el estado del diagnóstico de arranque.

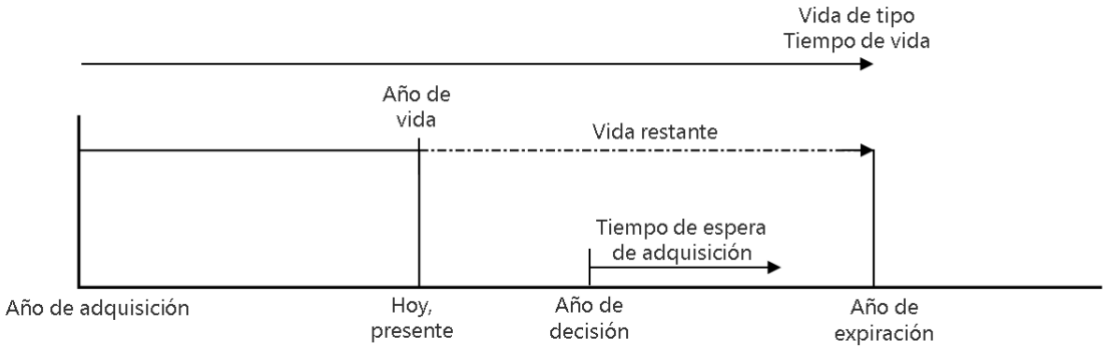


Figura 9. Calendario de planeación, adquisición y vida.
Fuente: Elaboración propia.

Año de adquisición, es el año cuando el activo fue adquirido, usualmente también asumido es el año cuando inicia su vida operativa. Este puede ser registrado en la base de datos de activos.

Edad o año de vida, mide la edad del activo, año de vida es la edad +1. Entonces el primer año de vida es 1, el segundo año es año 2, y así consecutivamente.

Año de vida= año corriente -años de adquisición +1.

Vida de tipo, es el número de años en las que un tipo dado de activo es asumido que durará para los propósitos planeados. Un término alternativo es vida estimada útil. Este concepto es útil en la planeación de flotillas de activos similares. Para activos más grandes de puede basar el plan con la evaluación de la vida restante de cada activo en particular. La vida de tipo puede variar con la aplicación y el tipo de ambiente donde opera el activo. Para flotillas de activos es aconsejable asignar una “vida de tipo” a cada clase de activo. Una guía posible está dada por los calendarios de depreciación publicados por las autoridades fiscales.

Vida restante, es el número de años que se espera un activo dure a partir de la fecha presente, o el día en que se presenta el análisis.

VIII. 10 entregables de consultoría de renovación de activos/infraestructura de red

La documentación acerca de la gestión de proyectos de tecnologías de información es muy basta y compleja. Ahondar los detalles metodológicos está fuera del alcance de esta publicación. Buenos puntos de partida son las metodologías definidas en PMBOK, ITIL o TOGAF, cuyos enfoques ya están definidos en otros medios de difusión y consulta.

Esta sección se delimitará a definir generalidades de los entregables que son usualmente intercambiados tanto por la firma que recibe los servicios de consultoría, como por la firma que los brinda cuando se proponen actualizar la infraestructura de redes de cómputo.

VIII.1. Accesos, físico, lógico, inventario de responsabilidad y diagramas

Contar con los diagramas lógico y físico; así como, sus versiones en estado actual en producción y futuro son indispensables para entender cuál es la estrategia que las dos firmas tienen contemplada ejecutar. En la industria se le conoce como FCAPS por sus siglas en inglés de Fallas, Configuración, Autorización, Desempeño y Seguridad, que son los parámetros básicos de gestión de desempeño e inventario mínimo necesarios para atender el estado y servicio brindado a los usuarios de la firma.

Fallas, el sistema de gestión utilizado por la firma para detectar errores o desviaciones del estado de servicio de un activo en producción, es soportado por el protocolo SNMP y funciones de registro de sistemas (Syslog), y trampas (Traps).

Configuración, contar con la definición de cuáles son los fabricantes de los activos y modelos aprobados para brindar servicios, contar con una base de datos que contenga los archivos en producción, inicio, al igual que el inventario de los sistemas operativos de los activos.

Autorización, control de acceso basado en roles, define que usuarios se encuentran en nivel 1- nivel 7, o nivel 15 al asociar usuarios con dominios y roles se

mejora la gestión de la infraestructura. Un dominio es el conjunto de recursos físicos y virtuales, y los roles de usuario determinan los privilegios a los que se tiene acceso dados, como los comandos y acciones que un usuario puede ejecutar en un enrutador.

Desempeño (en inglés, “Performance”), entender el desempeño de la red incluye obtener el histórico del CPU, desconexiones y saturación de circuitos e interfaces, contar un usuario para entrar al sistema que haga el caminado de MIB, OID que son todos los parámetros relacionados con el activo, estado de interfaces, niveles de errores, descartes, cantidad de bytes trasmitidos y dispersión característica de las tramas de red trasmitidas, tiempo de producción, estos sistemas de generación de estados históricos de desempeño ayudan a encontrar cuáles son los cuellos de botella y los puntos más frágiles a atender en una red.

Seguridad, entender la postura de la firma que recibe los servicios, cuáles son las cadenas de autorización y mando para los incidentes de seguridad, entender cuáles son los servidores de traducción de nombre dominio y direcciones de protocolo de Internet, cuáles son las políticas de configuración y seguridad de acceso a la red, obtener del cliente la postura de cuando se permite la conexión lógica y físico a la red, cuáles son los puntos de entrada; así como, saber los puntos de choque para la aplicación de políticas.

VIII.2. Listado de órdenes de trabajo y listado de compra de activos

El listado de los enunciados de trabajo contratado. Al comparar las órdenes de trabajo con los activos a actualizar, la función de esta tarea es coordinar las actividades que se pueden ejecutar o se pueden mandar a espera de ejecución. Tener preparada la definición de uniformidad en activos, el listado de proveedor/canal, cuáles son los esquemas de financieros de activos, números de serie y números de rastreo de envíos para manejar los inventarios que ayudan a planear el estado de tránsito, consumo y puesta en servicio de los activos e incluso su resguardo, evitando perdidas de material “recibido, pero mal inventariado”. Es importante resaltar que, en muchos casos los activos son fabricados en esquema “empuje”. Es decir, los activos son de una especialidad tal que el fabricante solo los manufactura cuando se han acumulado una cantidad suficiente para la producción en lote definido en su centro de ensamblado final, también ocurre que los “proveedor de canal” tienen un inventario reducido, dando a lugar a un tiempo de espera más largo, Morra (2021) mencionó el motivo de la escasez mundial de microprocesadores que afectó a los fabricantes de equipos de telecomunicaciones retrasando las fechas de entrega para los modelos de enrutadores y conmutadores considerados de estantería.

Numero de serie	Nombre de activo	Etiqueta de estado	Año adquisición	Prioridad	Fecha programada de renovación	Activo a desarrollar
cuarto	v1c21-bs1	mandar a-c21-br1	2004	1	1/30/2022	usar BR
cuarto	v1c22-bs1	mandar a-c22-br1	2004	1	1/30/2022	usar BR
0702Z156	v1d2c-04as1	en_uso	2003	1	11/30/2021	igual igual modelo 9300_24
0815N5E6	v1d2c-21as1	en_uso	2004	1	11/30/2021	igual igual modelo 9300_24
0842yrfc	la222-as1	en_uso	2004	1	11/30/2021	C9407B + 3 tarjetas
0842yrde	la222-as2	mandar a la222-as1 (Consolidar)	2004	1	1/30/2022	mandar a "as" mas cercano

Tabla 2. Enunciados de trabajo y fechas de entrega.
Fuente: Elaboración propia.

VIII.3. Costeo de fibras, cableados y mano de obra

Al identificar la adquisición de fibras y cableados es necesario seguir con las políticas de procedimientos de trabajos seguros en alturas, espacios confinados e incluso llegar a la negociación de contratos de instalación, el uso de escaleras y arrendamiento de plataformas tipo tijeras. La tabla 3 es una referencia para las capacidades de fibras ópticas y tipo de transductores modernos usados en redes de área local basada en los estándar ISO/IEC 11801:1995-2010, las celdas resaltadas en color gris destacan los materiales más recientes y comúnmente utilizados en redes de área local, al momento de escribir esta esta publicación.

Categoría fibra modo múltiple (espectro 850nm)	Color de camisa/cable	Color de conector	Distancia maxima con SFP 1GbE	Distancia maxima con SFP 10GbE	Distancia maxima con SFP40GbE	Distancia maxima con SFP100GbE	Año de lanzamiento al mercado
OM1	Naranja	beige	275m	33m	/	/	1988
OM2	Naranja	negro	275m	82m	/	/	1989
OM3	Azul aqua	azul	/	300m	100m	70m	2002
OM4	Azul aqua	no definido	/	550m	150m	150m	2009
OM5	Verde limon	no definido	/	550m	150m	150m	2014
Trasnductor Cisco	No aplica	No aplica	GLC-SX-MMD	SFP-10G-SR	QSFP-40G-SR4	QSFP-100G-SR4-S	No aplica

Categoría fibra modo sencillo (espectro 1310nm)	Color de camisa/cable	color de conector	Distancia maxima con SFP 1GbE	Distancia maxima con SFP 10GbE	Distancia maxima con SFP 40GbE	Distancia maxima con SFP 100GbE	Año de lanzamiento al mercado
OS1 Interior	Amarillo	no definido	2 km	2 km	2 km	2 km	2010
OS2 Exteriores	Amarillo	no definido	10 km	10 km	10 km	10 km	2010
Trasnductor Cisco	No aplica	No aplica	GLC-LH-SMD	SFP-10G-LR	QSFP-40G-LR4	QSFP-100G-LR4-S	No aplica

Tabla 3. Capacidades de fibras ópticas y transductores.
Fuente: Elaboración propia.

VIII.4. Análisis y limpieza de configuraciones

Los incidentes de alto impacto o primera prioridad tienen su raíz en el desconocimiento del propósito de cada segmento de la red o un levantamiento incompleto. Por eso la importancia de eliminar líneas en el archivo de configuración, pero que no realizan ninguna operación. Por ejemplo, la definición de rutas estáticas que apuntan a circuitos que ya no existen.

VIII.5. Construcción de redundancia y cableados especiales

Gestionar las órdenes de compra para la adquisición de los nuevos cableados de conexión cobre UTP, fibras intercampus, de acuerdo con los diagramas futuros en

el mapa de ruta de desarrollo. Contar con esta tabla ayuda a comunicar cuáles son las fibras que requieren adquirirse y cuáles se reutilizarán.

Origen							Destino							
Nombre de dispositivo origen	Modelo origen	Numero de serie	Puerto origen	Ubicación de origen	Tipo de terminación de fibra en origen	Tipo de cable /fibra	Nombre dispositivo destino	Modelo destino	Numero de serie	Puerto destino	ubicación de destino	Tipo de terminación de fibra en destino	Tipo de transductor	Notas
AL61D-VR1	9500	37240RM	Twe 1/0/1	AL61D	LC	fibra	AL61D-CR1	C4500X	201303UB	Ten_1/9	AL61D	LC	10 G LR	enlace subida
AL61D-VR1	9500	37240RM	Twe 1/0/2	AL61D	LC	fibra	F51D-CR1	C4500X	201303RW	Ten_1/9	F151D	LC	10 G LR	enlace subida
AL61D-VR1	9500	37240RM	Twe 1/0/3	AL61D	LC	fibra	al61d-r1	C4506	1435G0KP	Gig_3/9	AL31D	LC	10 G LR	enlace subida
AL61D-VR1	9500	37240RM	Twe 1/0/4	AL61D	LC	fibra	F15-R1A	C4506	0725011A	Gig_5/1	F511	LC	10 G LR	enlace subida
AL61D-VR1	9500	37240RM	Twe 1/0/5	AL61D	LC	fibra	al823-gs1	C2900	88912PF	Gig_0/51	AL4	LC	1 G LR	enlace bajada
AL61D-VR1	9500	37240RM	Twe 1/0/6	AL61D	LC	fibra	AL61D-VR2	9500	37254DA	Twe 1/0/6	AL61D	LC	10 G SR	enlace con gemelo redundante
AL61D-VR1	9500	37240RM	Twe 1/0/7	AL61D	LC	fibra	AL61D-VR2	9500	37254DA	Twe 1/0/7	AL61D	LC	10 G SR	enlace con gemelo redundante

Tabla 4. Hoja de adquisición de cableados.
Fuente: Elaboración propia.

VIII.6. Presentación de cambios

El entender los procedimientos formales; así como, las fechas donde ocurren las juntas de control de cambios. Tener identificado al grupo de aprobadores de cambio, los líderes técnicos, al igual que las partes interesadas en donde sucedan las modificaciones para la aceptación de riesgos, entender quiénes son los líderes técnicos que tienen conocimiento histórico acerca del portafolio de proyectos.

VIII.7. Listado de materiales en sitio

Hacer el inventario de estatus de los activos también forma parte de las restricciones al ejecutar un plan de renovación de activos. En administración de proyectos se le denomina el BOM, por sus siglas en ingles de "*Bill of materials*". Entender cuál es el espacio disponible en los racks del cuarto de comunicaciones, disposición de elevadores de chasis, capacidad de enchufes para conectar cables de poder e incluso disponibilidad de potencia para no violar los cortacircuitos eléctricos, auditar fibras ópticas, conectores solicitados.

VIII.8. Ejecución

Unos días antes de la ejecución se espera haber realizado una junta con el equipo técnico de cableado para identificar riesgos o retos técnicos a considerar tales como limitaciones de cableado o disponibilidad de recursos humanos para dar soporte al cambio sugerido. Es imperativo obtener el estado de las funciones y estatus operativo del activo. Registras cuál es el estado de cada uno de los protocolos e interfaces, tablas de rute y conmutación y enumerar los comandos y actividades a ejecutar en la ventana de mantenimiento, junto con las hojas de corte.

Las hojas de corte sirven para guiar a los técnicos en sitio encargados de mover y conectar los cables físicamente, apoya los trabajos del inventario de cableados. Esta hoja puede considerarse una subsección de la tabla 4 donde se hicieron las órdenes de nuevos cableados, en ocasiones solo se adquirirán los cables de parcheo que tienen una terminación deferente a la utilizada. Un ejemplo de hoja de corte para transición descritos en la tabla 5.

Interfaces dispositivo a demoler AL61D-VR1 C-4500 N.Serie:0725011A	Nombre dispositivo destino	Modelo destino	Numero de serie	Nuevo Puerto	Tipo de terminación en destino
Gig_1/1	AL61D-VR1	9500	37240RM	Twe 1/0/1	LC
Gig_1/2	AL61D-VR1	9500	37240RM	Twe 1/0/2	LC
Gig_2/3	AL61D-VR1	9500	37240RM	Twe 1/0/3	LC
Gig_2/6	AL61D-VR1	9500	37240RM	Twe 1/0/4	LC
Gig_3/1	AL61D-VR1	9500	37240RM	Twe 1/0/5	LC
Gig_3/3	AL61D-VR1	9500	37240RM	Twe 1/0/6	LC
Gig_3/4	AL61D-VR1	9500	37240RM	Twe 1/0/7	LC

Tabla 5. Hoja de corte para transición a nuevo activo.
Fuente: Elaboración propia.

VIII.9. Validaciones

Después de ejecutar todas las modificaciones dictadas en el plan de cambios, y verificar las comprobaciones de cada paso ejecutado se espera realizar una validación del servicio que identifique en cada una de las capas OSI la comprobación en que aún existe la redundancia diseñada y en caso de no obtener el estatus deseado conviene también indicar cuáles serán los pasos necesarios para regresar al estado anterior a la modificación y regresar el servicio en las mismas o similares condiciones para que sigan soportando los servicios brindados del negocio.

VIII.10. Estrategias y consejos de campo

Contar con carpetas que incluyan las fechas de los levantamientos de los estados actuales, y mapas de ruta futuros. Registrar cada una de las juntas celebradas para recabar las observaciones, acuerdos y actividades requeridas junto con sus responsables utilizando el versionado de documentos.

Programar el software de emulador de consola para guardar un registro de todos los comandos ejecutados y todos los dispositivos a los que se dispone de responsabilidad, este registro debe incluir el nombre de dispositivo, y dentro del archivo incluir la fecha, hora y el registro de todas las salidas de los comandos ejecutados. Esto forma los respaldos y los estados en puntos del tiempo mientras dure el compromiso o contrato de prestación de servicios y así limitar las responsabilidades.

Acerca de las ventanas de mantenimiento, se recomienda que sean siempre menores de cuatro horas continuas de trabajo fuera de horario regular. Dado que es más fácil mantener la concentración de la cuadrilla en cuatro horas dividiendo el cambio en dos jornadas nocturnas, en contra de realizar cambios en una sola jornada de 8 horas.

IX. Conclusiones y recomendaciones

Este documento pretende dar una introducción a la gestión de activos físicos y las motivaciones que un negocio o institución debiera evaluar y concientizar de la visión estratégica necesaria para gestionar adecuadamente el ciclo de vida de los activos e infraestructura tecnológica. Incluye el lenguaje de planeación de proyectos para iniciar discusiones pertinentes a la renovación de activos. La sección de diez entregables es también un resumen mínimo de los documentos a intercambiar y los procedimientos para asegurar un entendimiento de la estrategia a seguir en la gestión redes de cómputo corporativo. Se proporcionan en la tabla 3, el listado de materiales de fibra óptica, transductores modernos y cuál es su desempeño. Se mencionan recomendaciones para ejecutar migraciones exitosas y transparentes para los usuarios, evitando errores de planeación, que dañan la imagen de profesionalismo con el que el departamento de tecnologías de información administra proyectos y brinda sus servicios.

La carencia de un enfoque de la gestión de activos conduce a problemas de coordinación de los departamentos de operaciones, planeación por un lado y la “gerencia superior” del otro. Desencadenando perdidas de negocio maquillados como fallas de servicio, que producen resultados que bajo rendimiento operativo del negocio.

En una futura entrega se volverán a revisar esos esos diez entregables con actividades técnicas más detalladas como la automatización de la lectura de salidas de comandos ejecutados, como detectar fallos a configuraciones redundantes, con software y scripts de automatización y por último, cómo resolver problemas de espacio físico y logístico con respecto a los cableados de cobre e interfaces físicas.

Reconocimientos

Se agradece al por INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación por la invitación a participar en el foro, a la Facultad de Ingeniería Química de la Universidad Autónoma de Yucatán (UADY) por la infraestructura y al Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCyT) por las facilidades para el desarrollo de esta investigación.

X. Glosario

- **BOM** del inglés Bill Of Materials, en español listado de materiales es un inventario completo de los materiales directos de fabricante, ensamblados, sub ensamblados, partes y componentes, así como las cantidades de cada uno para manufacturar un producto o entregar un proyecto.

- **CAPEX** del inglés Capital Expenditure, en español, Gasto en Capital, es la inversión en capital o inmovilizado fijo que realiza una compañía ya sea para adquirir, mantener o mejorar su activo no corriente.
- **CPU** del inglés Central Procesor Unit, en español, Unidad de Procesamiento Central, es el chip de silicio dentro de un ordenador u otros dispositivos programables, que interpreta las instrucciones de un programa informático mediante la realización de las operaciones básicas aritméticas, lógicas y de entrada/salida del sistema.
- **FCAPS** del inglés fault, configuration, accounting, performance and security es un acrónimo de los cinco niveles de gestión de la red: Fallas, Configuración, Contabilidad, Desempeño y Seguridad.
- **ICMP** del inglés Internet Control Message Protocol, en español, Protocolo de Mensajes de Control de Internet es un protocolo de reporte de errores que dispositivos de red como enrutadores utilizan para generar mensajes a las direcciones origen, cuando algún problema se evita la entrega de paquetes IP.
- **ISO/IEC** 11801:1995-2010 estándar conjunto especificado por la Comisión Electrotécnica Internacional y la Organización Internacional de Normalización que especifica el cableado genérico para usarse en instalaciones comerciales, la cual contenga uno o varios edificios en un campus. Especifica: la estructura y la configuración mínima de cableado.
- **ITIL** del inglés Information Technology Infrastructure Library, en español, Biblioteca de Infraestructura de Tecnologías de Información. Es un conjunto de estándares que definen la selección, la planeación, entrega y mantenimiento del ciclo de vida de los servicios de IT en una firma corporativa o negocio.
- **MIB** del inglés Management Information Base, en español, Base de Información de Gestión es una base de datos utilizada para manejar las entidades en una red de comunicaciones.
- **OID** del inglés Object Identifiers, en español, Identificador de objeto es un mecanismo identificador estandarizado por la ITU, Unión Internacional de Telecomunicaciones y la ISO/IEC para nombrar cualquier objeto, concepto, o "cosa" en una computadora.
- **OPEX** del inglés Operational Expenditure, en español, Gasto Operativo es el dinero que una compañía u organismo gasta continuamente en el día a día para operar su negocio.
- **OSI** es un modelo conceptual que proporciona una base común para la coordinación de los estándares definidos por la ISO que ayudan al desarrollo de los sistemas de interconexión de información.

- **PMBOK** del inglés Project Management Body of Knowledge (PMBOK® Guide), en español, Cuerpo de Conocimientos de la Gestión de Proyectos, información de soporte e instrucciones que ayudan a los profesionales administradores de proyectos a aplicar los estándares del instituto de administración de proyectos.
- **SNMP** del inglés Simple Network Management Protocol, en español, Protocolo Simple de Gestión de Red, es usado para la gestión y monitoreo de dispositivos conectados en redes basadas en el protocolo de Internet.
- **SYSLOG** es un protocolo usado en sistemas de cómputo utilizado para mandar eventos o registros de datos a una ubicación central para su resguardo.
- **TCP/IP** del inglés Transmission Control Protocol/Internet Protocol, en español, Protocolo de Control de Transmisión/Protocolo de Internet es un sistema de protocolos que hacen posibles servicios informáticos, transmisión de video y audio, transferencia de datos, entre computadoras que están conectados en red.
- **TOGAF** del inglés The Open Group Architecture Framework, en español, El marco de arquitectura de grupo abierto es un esquema de arquitectura empresarial que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura de información empresarial.
- **SNMP** trap es un tipo de mensaje del protocolo SNMP empleado por un agente monitoreado para mandar un mensaje no solicitado al gestor central notificando acerca de un evento importante en el sistema. a Diferencia del resto de mensajes que son enviados después de su expresa solicitud por el gestor.
- **UTP** del inglés Unshielded Twisted Pair, en español, Par Trenzado sin Blindaje es un cable de cobre contiene de dos hasta 1800 pares sin blindaje o armadura con una cubierta de plástico exterior.

XI. Referencias

Al-shawi, Marwan y Laurent, Andre. *Designing for Cisco Network Service Architectures (ARCH) Foundation Learning Guide: CCDP ARCH 300-320*, 4th Edition. San Jose, California, Cisco Press, 2016.

Blanchard, Benjamin, *Logistics Engineering & Management*, Harlow, Essex, Pearson education, 2014.

Edgeworth, Brad. Hucaby et al., *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide*. San Jose, California, Cisco press, 2019.

Gulati, Ramesh, *Maintenance and Reliability Best Practices*, New York, New York: Industrial Press, Incorporated, 2012.

International Organization for Standardization, *Systems engineering — System life cycle processes (ISO/IEC no. 15288:2002)*, 2002, https://www.iso.org/standard/27166.html.

International Organization for Standardization, *Asset management — Overview, principles and terminology (ISO standard no. 55000:2014)*, 2014, https://www.iso.org/standard/55088.html.

International Organization for Standardization, *Asset management — Guidance on the alignment of financial and non-financial functions in asset management (ISO/TS no. 55010:2019),* 2019, https://www.iso.org/standard/72700.html.

Meyers, Mike, *CompTIA Network+ Certification All-in-One Exam Guide*, Seventh Edition (Exam N10-007), New York, New York, McGraw-Hill Education, 2018.

Morra, James, *Broadcom Tightens Strings on Supply Amid Global Chip Scramble*, 2021, https://www.electronicdesign.com/technologies/analog/article/21174341/electronic-design-broadcom-ceo-tightens-strings-on-supply-amid-global-chip-scramble.

O'Connor, Patrick, *Practical Reliability Engineering*, New York, New York, Wiley, 2012.

Piggott, Stuart, *The earliest wheeled transport from the Atlantic coast to the Caspian Sea*, Ithaca, Nueva York, Cornell University Press, 1983.

CIBERSEGURIDAD EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

Juan JOSÉ LÓPEZ ÁVILA[12]
Irma PÉREZ HERNÁNDEZ[13]

[12]Doctor en Tecnologías de la Información. Centro de Idiomas y de Autoacceso. Universidad Veracruzana. ORCID 0000-0003-3812-4693. javila@uv.mx.
[13]Doctora en Educación. Facultad de Ingeniería Mecánica. Universidad Veracruzana. ORCID 0000-0001-9278-6946. irmaperez@uv.mx.

CIBERSEGURIDAD EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

Cibersecurity in Higher Education Institutions

Resumen

El avance vertiginoso de las tecnologías genera retos importantes en las instituciones de educación superior, hablando de la seguridad de sus procesos, el manejo de información íntegra, confiable y disponible para su uso, protección de usuarios y activos tecnológicos e infraestructura; así como, la toma de decisiones para el diseño, desarrollo e implementación de nuevos sistemas y tecnologías. El objetivo de este escrito es presentar un estado del conocimiento sobre las medidas de ciberseguridad que las instituciones educativas están tomando para ofrecer sistemas confiables, minimizar riesgos, establecer estrategias para la seguridad y las medidas regulatorias que están adoptando las instituciones de educación superior. Se ha realizado una investigación documental de las producciones realizadas al respecto en América Latina, España, destacando el hecho de que la producción del conocimiento al respecto aún es limitada, se identificaron áreas de oportunidad, dada la escasa literatura de ciberseguridad en el entorno universitario.

Abstract

The vertiginous advance of technologies generates important challenges in higher education institutions, speaking of the security of their processes, the management of comprehensive, reliable and available information for their use, protection of users and technological assets and infrastructure, as well as the taking decisions for the design, development and implementation of new systems and technologies The objective of this paper is to present a state of knowledge on the cybersecurity measures that educational institutions are taking to offer reliable systems, minimize risks, establish security strategies and the regulatory measures that higher education institutions are adopting. A documentary investigation of the productions carried out in this regard in Latin America, Spain has been carried out, highlighting the fact that the production of knowledge in this regard is still limited, areas of opportunity were identified, given the scarce cybersecurity literature in the university environment.

Palabras clave: amenazas, ciberseguridad, gestión de riesgos, educación, IES.

Keywords: *threats, cybersecurity, risk management, education, HEI.*

I. Introducción

La definición de seguridad sufre una transformación para agregar cualidades tecnológicas que hoy identificamos como ciberseguridad; mantener la confianza y seguridad en la utilización de las Tecnologías de la Información y la Comunicación (TIC). "*La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno" (*ITU, 2010*).*

La creciente necesidad de las organizaciones e instituciones de proteger sus sistemas e infraestructura de ataques maliciosos; así como, del uso indebido de la información que es generada y almacenada en ellos y que se distribuye mediante la interconexión de todos sus elementos obliga a definir estrategias que permitan disponer de planes de acción remediales y contar con medidas preventivas anticipando y evitando cualquier eventualidad que ponga en riesgo el funcionamiento tecnológico y operativo de la institución.

La Organización Internacional para la Estandarización (ISO) desarrolló los estándares de la familia 27000 referentes a la seguridad de la información; la implementación de dichos estándares no es obligatoria en ninguna empresa ni organismo público, sin embargo, cada día es más común que se exija la certificación dentro de las organizaciones en algunos de estos estándares con la finalidad de garantizar la calidad de las medidas adoptadas y su eficiencia.

La seguridad de la información abarca todos los aspectos desde la seguridad de la infraestructura de comunicaciones, seguridad en la red, seguridad en Internet, hasta la protección de la información de la infraestructura critica.

Según datos de la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES), en el año 2019, el porcentaje de instituciones de educación superior (IES) que tenían implementada alguna iniciativa relacionada con ciberseguridad fue del 15%, el 14% se encuentra en proceso de implementación de un proyecto; en lo que respecta al año 2020, el porcentaje de IES que tuvo implementación de alguna iniciativa relacionada con la Ciberseguridad fue del 25%,

y el 11% se encontraba en proceso de implementar; es decir 1 de cada 3 IES que respondieron a la pregunta, informaron que tienen alguna solución activa o en etapa de implementación Ciberseguridad (ANIUES, 2020).

Debido a la importancia que genera dentro de las organizaciones mantener seguro su ciberespacio, el presente documento explora diferentes estudios realizados identificando las medidas adoptadas y resultados obtenidos, se describen algunas investigaciones realizadas en América Latina en relación al concepto de ciberseguridad y finalmente se generan algunas conclusiones, que evidencian la carencia de aplicación de estrategias formales y auditables que garanticen la eficiencia de las mismas.

II. Metodología

En el presente texto se plantea una investigación documental logrando un acercamiento al estado del conocimiento generado a través de la producción científica en América Latina y España respecto a cómo las universidades gestionan los riesgos en materia de ciberseguridad. La búsqueda de información se basó en recursos como *Dialnet, Reserarchgate, Google Scholar, Google Books*, fuentes de información CONRICyT de la biblioteca virtual de la Universidad Veracruzana, que cuenta con bases de datos como EbscoHost, IEEE Xplore, ACM Digital Library, de igual forma dentro de la biblioteca virtual se consultaron libros electrónicos de E-libro. Se combinaron criterios de búsqueda de conceptos como amenazas, seguridad informática, ciberseguridad, cibereducación, educación superior. Se estipuló un periodo de tiempo para búsqueda de 10 años (2011 a la fecha), teniendo como principal fuente artículos científicos.

La información localizada fue administrada en el gestor de referencias bibliográficas el cual permitió generar las referencias y el apéndice.

III. Marco teórico-conceptual

Con el propósito de enmarcar y clarificar la terminología utilizada que abarca este trabajo de investigación, se incluyen una serie de conceptos que se relacionan y se mencionan a lo largo del documento.

El incesante incremento del uso de la tecnología en todos los ámbitos de la sociedad nos hace cada vez en mayor medida dependientes de las Tecnologías de Información y Comunicación (TIC) y a la vez vulnerables ante los incontables riesgos que supone el uso de dispositivos e infraestructuras inherentes a la transformación digital.

III.1. La ciberseguridad

La ciberseguridad es una ciencia diseñada para proteger la computadora y todo lo relacionado con ella (Patterson & Winston-Proctor, 2019), en términos generales la ciberseguridad es el conjunto de estrategias que se emplean para resguardar el correcto uso de la infraestructura tecnológica (computadoras, servidores, los dispositivos móviles, sistemas de información, las redes y los datos) de ataques maliciosos.

Derivado del término ciberseguridad se desprenden categorías como: seguridad de la red, de las aplicaciones, de la información, seguridad operativa, la recuperación ante sucesos, y la capacitación de los usuarios.

III.2. Amenazas, vulnerabilidades y ataques a la seguridad

Los términos de amenaza, vulnerabilidad y ataque se encuentran directamente relacionados debido a que un atacante aprovecha las vulnerabilidades de un sistema o infraestructura para realizar amenazas y/o atacar, provocando daños operativos. La vulnerabilidad es toda aquella debilidad de un sistema informático (Monsalve, 2018). *Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota* (INCIBE, 2021).

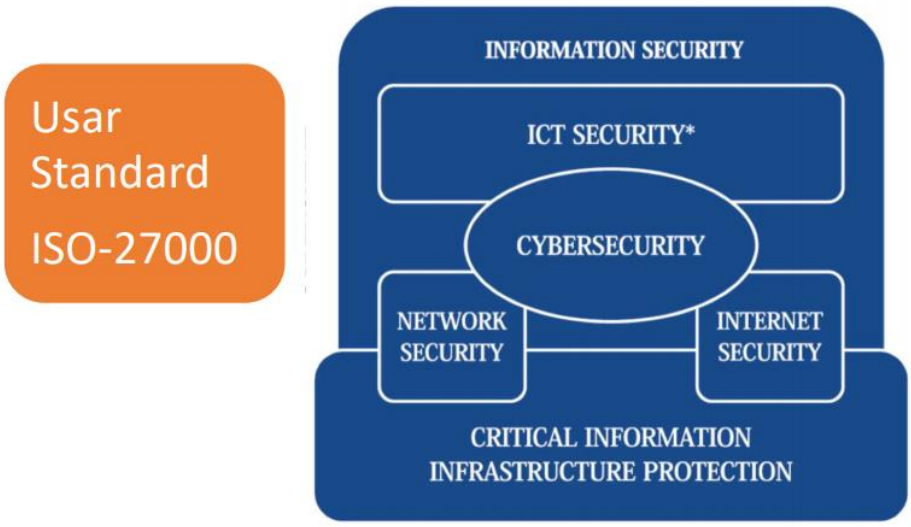
Se considera como amenaza a la seguridad informática, cualquier acción que pone en riesgo la infraestructura tecnológica de una organización poniendo en riesgo su información y/o activos*. La amenaza pone en peligro los sistemas aprovechando sus vulnerabilidades. Amenaza: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad* (INCIBE, 2021).

Las amenazas son originadas por los ataques a la seguridad o ciberataques:

Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema (INCIBE, 2021).

III.3. Estándares ISO de seguridad de la información

El origen de los estándares de la familia ISO/IEC 27000 que tiene como propósito generar una perspectiva y soporte encaminado a responder por la seguridad de la información, el cual abarca todas las posibles aristas de la ciberseguridad como se puede representar en la siguiente imagen (ANUIES, 2020).



III.4. Activo de información

Un activo de información en el contexto de la norma ISO/IEC 27001 es: "algo que una organización valora y por lo tanto debe proteger". "*Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización"* (ANIUES, 2020).

IV. Análisis de resultados

IV.1. Descripción de estudios

En este apartado se presenta el análisis de las investigaciones realizadas en torno a lo que las IES han propuesto o implementado en relación con la ciberseguridad de sus activos de información. El orden de análisis de los documentos es en primer lugar los artículos científicos ordenados cronológicamente, posteriormente las tesis doctorales, mencionando el nombre del autor, el año en que se realizó el trabajo de investigación, los objetivos y los resultados que se obtuvieron, se podrá consultar información adicional al respecto, en el cuadro de resumen que se anexa al final del capítulo.

IV.2. Artículos científicos

En el año 2014 un escrito de Cayón Peña y García Segura, estudia las principales Estrategias de Ciberseguridad (EC) publicadas hasta ese momento, principalmente en el ámbito educativo, se resalta la importancia que tiene la educación, formación, entrenamiento y sensibilización de todos los actores que intervienen en la ciberseguridad de las instituciones educativas, en la recopilación que realizan del

Centro de Cooperación y Excelencia para la Ciberdefensa de la OTAN se visualizan las EC publicadas por país, se listan 53 países que generaron estrategias, destacando que potencias económicas iberoamericanas como México, Colombia y Chile, no figuran. Por otra parte, Estados Unidos estableció desde al año 2012 una plataforma llamada *National Initiative for Cibersecurity Education* (NICE) la cual busca promover el desarrollo de capital humano en temas de ciberseguridad.

En general los países que participan definiendo EC proponen lo siguiente: creación de portales informativos, personal especializado en ciberseguridad, educación formal a los estudiantes mediante la incorporación de la competencia de ciberseguridad en todos los niveles educativos, tomar en cuenta la experiencia de otros países, coordinación entre el sector público y privado, involucrar a las IES tanto públicas como privadas a la hora del diseño y redacción de EC, programas de entrenamiento para adultos mayores y para niveles básicos educativos.

La conclusión de esta investigación radica en verificar el avance de los países en el diseño de EC, sugiriendo que las mismas se enmarquen en una estrategia de ciberseguridad nacional, lo que en México sucede en el año 2017.

En la investigación de Hernández Jaimes y Prada Angarita publicada en el año 2014, muestran la importancia y el resultado de realizar un análisis del tráfico de la red de una institución universitaria, ya que esta actividad permite detectar anomalías, visualizando posibles ataques, lo que minimiza los ataques maliciosos. Los autores recolectan datos del servidor principal del campus universitario utilizando un monitor de desempeño incluido en el sistema operativo del mismo servidor, midiendo valores de tráfico de entrada y salida en diferentes intervalos de horario, obteniendo valores constantes que se tomarían como base para detectar situaciones anormales en condiciones diferentes. El modelo propuesto genera una EC para monitorear valores estandarizados en la institución que darían la base para generar análisis continuos, permitiendo detectar a tiempo fallas en la seguridad de los sistemas institucionales y el acceso a la información.

Por otra parte, en el año 2017, Anchundia-Betancourt realiza una investigación sobre el estado del conocimiento de la ciberseguridad en los sistemas de información en el contexto universitario, en el documento se expresa que el desarrollo de Políticas o Estrategias de Ciberseguridad no es una tarea fácil, y basa en acciones variadas, incluyendo estrategias generadas por grupos multidisciplinarios, contribuyendo a crear un ciberespacio universitario seguro promoviendo la cultura de ciberseguridad.

Se analiza el caso particular de Ecuador donde se promulgaron políticas que han dispuesto el uso obligatorio de las Normas Técnicas Ecuatorianas para la Gestión de Seguridad de la Información, que contemplan un conjunto de directrices para viabilizar la implementación de la seguridad de la información en las entidades públicas, además del uso de las normas internacionales para los Sistemas de

Gestión de Seguridad de la Información (SGSI), para gestionar la seguridad de los activos de información de las instituciones en general.

Una investigación de carácter cuantitativo realizada en México en el año 2018, por Gordón Revelo y Pacheco Villamar donde analizan estrategias de seguridad informática basadas en metodología *open source* llamada OSSTMM (es un documento que reúne de forma estandarizada y ordenada diversas verificaciones y pruebas que se pueden realizar para una auditoría informática) para la red interna de una IES, se enfoca en aplicar una auditoría de seguridad informática utilizando una prueba de *hacking*. Dado que las IES poseen información de personal administrativo, docentes y estudiantes se hace hincapié en la necesidad de contar con herramientas que permitan evaluar el estado actual de la seguridad de las redes de datos.

La metodología aplicada permitió detectar que la IES no disponía de una protección adecuada apoyada con IPS/IDS, antivirus bajo licencia para la detección de posibles amenazas, no se disponía de políticas de respaldos tanto de la información como en la infraestructura de suministro y protección eléctrica, se encontraron y cuantificaron riesgo de seguridad física, seguridad en wireless y seguridad en las comunicaciones. Se analizaron además controles de confidencialidad, privacidad, integridad, alarma, autenticación, entre otros. Se cuantificaron vulnerabilidades en la intranet.

Dando a conocer los resultados obtenido a la IES recomendando analizar estrategias que permitan regularizar la seguridad lógica operacional factores humanos, los factores analizados son los físicos, redes inalámbricas, servicios, aplicaciones, y redes de datos, encontrando como resultados, que la mayoría de los elementos de la intranet evaluada, tienen riesgos altos de ser vulnerados y de sufrir ataques de seguridad informática. Los autores proponen la aplicación de estrategias, tales como: la creación de barreras entre el activo de información y la amenaza, la disminución de las brechas de seguridad tratada de manera individual para cada activo de información lo que garantizaría la confiabilidad, integridad y disponibilidad de la información.

Un tema importante de mencionar al hablar de ciberseguridad es la ingeniería social en el documento de Acosta Pineda, del año 2018 elaborado en Colombia, se hace referencia a la ingeniería social en instituciones de educación superior, se menciona que existen técnicas de ingeniería social basadas en computadoras y basadas en el recurso humano, la primera técnica se caracteriza por hacer uso de herramientas informáticas para la realización de los ataques y la segunda técnica se basa en aprovechar las características de las personas como: curiosidad, deseo, codicia, miedo incluso la bondad, en la investigación se menciona que el 50% de las IES que formaron parte del estudio, fueron víctimas de ataques, la suplantación de identidad, el phishing, ataques a sitios web se anotan como los ataques para utilizados.

Se realiza un estudio de vulnerabilidades a cinco IES, analizando que las técnicas de suplantación de identidad fueron viables en todas las instituciones, en tres de las cinco instituciones no había seguridad en la documentación, cuatro no contaban con procedimientos de control, en tres de las instituciones se pudo obtener la ubicación de los equipos de cómputo y en las cinco instituciones se obtuvo información relevante y no contaban con accesos restringidos a salas de reuniones.

En todas las instituciones analizadas, tienen una unidad encargada de la gestión de los servicios tecnológicos, sin embargo, su orientación hacia la seguridad se basa en el componente físico, desatendiendo el recurso humano; mismo que, puede ser la puerta de entrada para un ataque a la institución.

Por tanto, se hacen recomendaciones basadas en diferentes autores: desarrollo e implementación de políticas y planes de seguridad, capacitación, copias de seguridad, autenticación, monitoreo, almacenamiento en la nube, actualización periódica de dispositivos.

En el estudio de Morales Carrillo (2019) realizado en Ecuador se da a conocer el aspecto de seguridad en los sistemas distribuidos mediante la aplicación de la norma ISO 27032-2012, utilizaron herramientas como Shodan, Nessus y Acunetix, que permitieron conocer y analizar posibles amenazas y defensas, en los niveles de seguridad de los sitios, sistemas o servicios webs. Utilizaron una metodología Análisis Modal de Fallos y Efectos (AMFE) se brindó soluciones de mitigación de riesgos.

Para el desarrollo de la investigación se trabajó con cuatro IES elaborando cuestionarios basados en la norma mencionada aplicando un método cuantitativo. Para identificar los riesgos de las vulnerabilidades detectadas generaron la matriz AMFE determinando mediante la probabilidad de ocurrencia y el impacto, el nivel de riesgo de las vulnerabilidades, emitiendo acciones de mitigación.

Aplicaron herramientas de escaneo de vulnerabilidades como Shodan, Nessus, y Acunetix, mismas que permiten realizar escaneo de la red o por enlace web de los sistemas de las IES públicas, en donde obtuvieron vulnerabilidades ya clasificadas.

En el análisis realizado clasificaron las vulnerabilidades del dominio seguridad de información, de seguridad de aplicaciones y seguridad de las redes, detectando en todas las clasificaciones vulnerabilidades altas. En cuanto a las vulnerabilidades detectadas por las tres herramientas aplicadas (Shodan, Nessus y Acunetix), las vulnerabilidades más altas son de aplicación, seguido de red y datos.

Se menciona la elaboración del plan de acción (que no se detalla), en donde se consideran estrategias de mitigación y criterios de aceptación de la matriz de riesgo AMFE, permitiendo mejorar la seguridad de los sistemas distribuidos de estas instituciones públicas y, de esta manera, disminuir los riesgos encontrados.

Leguizamón-Páez, Bonilla-Díaz y León-Cuervo (2020) analizaron la implementación de la herramienta alternativa Honeypot al esquema de seguridad

informática existente en una IES, permitiendo encontrar fallas de seguridad pertenecientes a los servidores de la universidad debido a ataques informáticos.

La herramienta utilizada mostró información de los eventos capturados visualizando datos relevantes para identificar la procedencia del ataque; así como, las actividades realizadas por el mismo. Honeypots genera la captura los archivos maliciosos que intentaron aprovechar un fallo de seguridad, y permitió ver cómo los scripts desarrollados protegen ampliamente los servidores. Los autores diseñaron una nueva distribución de red para registrar información sobre los diferentes ataques y permitir establecer soluciones efectivas.

En la investigación metodológica de Mena Mosquera (2020) desarrollada en Colombia, plantea la importancia de implementar planes de auditorías de seguridad a los diferentes sistemas de gestión de la seguridad de la información, bajo la norma ISO/IEC 27001:2013. En Colombia reconocen una serie de leyes y normas que rigen los delitos informáticos como son: Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013, Ley 1273 DE 2009, BS 7799-3:2006, NTC 27001:2006, ISO 27002:2005, ISO/IEC 27001:2005.

Se menciona que este país definió cinco dimensiones estratégicas (DE) que determinan los campos de acción de la política nacional de seguridad digital, las cuales son: Gobernanza de la seguridad digital, Marco legal y regulatorio de la seguridad digital, Gestión sistemática y cíclica del riesgo de seguridad digital, Cultura ciudadana para la seguridad digital y Capacidades para la gestión del riesgo de seguridad digital.

Los autores citados en este documento introducen términos concernientes a la ciberseguridad como son la ingeniería social, análisis y evaluación de riesgos, uso de metodologías como son OWASP, MARGERIT, Análisis Modal de Fallos y Efectos (AMFE), es TOPSIS y COBIT, implementación de normas ISO/IEC 27001, ISO 27007:2011, ISO 27002:2015, ISO 25023, ISO/IEC 27002:2009, NTE ISO/NEC 27001:2013 ISO 17799.

La finalidad de esta investigación es documentar de qué manera algunas IES están implementando controles, metodologías y políticas que permitan evaluar los riesgos a los que están expuestos los datos y la información confidencial.

Aguilar Torres, Gallegos García, Delgado Vargas, De Abiega L'Eglisse y Salinas Rosales (2021) hablan sobre la importancia de la educación en ciberseguridad, haciendo referencia a las principales amenazas en el ciberespacio; presentan una recopilación del trabajo que están haciendo las universidades en el quehacer de la formación de recursos humanos expertos en este tema, presentando las instituciones que tienen programas de posgrado, diplomados y grupos de investigación enfocados en la ciberseguridad en México, Centro de Estudios Superiores Navales, Centro de Investigación y de Estudios Avanzados, Instituto Nacional de Astrofísica Óptica y Electrónica, Instituto Politécnico Nacional, Universidad Anáhuac, Universidad Autónoma de Nuevo León, Universidad en

Internet, Universidad Iberoamericana, Universidad La Salle, Universidad Nacional Autónoma de México, Universidad Tecnológica de México, Universidad del Valle de México, Tecnológico de Monterrey.

Los autores presentan un panorama que hace referencia a la necesidad que se tiene de formar recursos humanos expertos en ciberseguridad.

Salazar Mata, Balderas Sánchez, García Aldape y Cruz Navarro (2020) plantean un proyecto que pretende implementar la metodología OWASP como estrategia de pruebas de penetración con herramientas de software libre como KALI Linux, con la finalidad de fortalecer la seguridad informática del Sistema de Información Escolar (SII), realizando las pruebas de intrusión, elaborando un plan de monitoreo, prevención y control en la seguridad informática para estos sistemas.

Se definen seis fases: identificación del contexto, elección y configuración de la herramienta, determinación de las pruebas, aplicación del modelo de penetración, evaluación de resultados y plan de acción.

De los resultados obtenidos en las pruebas, generaron un plan de acción con las siguientes recomendaciones: formar recurso humano involucrando estudiantes, implantar y evaluar un manual de mejores prácticas, plantear un programa de capacitación al personal encargado del centro de cómputo y a estudiantes, buscando el apoyo del COZCyT y de ANUIES, realizar divulgación del Manual, crear un laboratorio de seguridad, de pentesting o hacker ético. En una etapa posterior un proyecto de cómputo forense.

IV.2.1. Tesis doctorales

Vicente Cestero (2016) en su tesis doctoral de la Universidad Politécnica de Madrid realiza un análisis de gestión de riesgos en los sistemas de información (SI) tomando como base la metodología MAGERIT, adoptando las normas ISO/IEC 27000. La herramienta de números borrosos trapezoidales se utilizó para modelar el juicio probabilístico de los expertos en sistemas de ayudando a la decisión cuando la información que se maneja es imprecisa.

Propone un método interactivo analista experto para la extracción de juicios probabilísticos borrosos de expertos sobre un evento, además, propone una aritmética adecuada que mejore las aritméticas borrosas usuales, simplificando los algoritmos utilizados en el análisis de riesgos en los sistemas de la información, y funciones de similitud que mejoren las funciones.

Con el modelo propuesto, se pueden valorar las probabilidades de fallo, las probabilidades de amenazas y la degradación que puede sufrir los activos atacados, obteniendo indicadores de impacto y riesgo, presentando un modelo de reducción de riesgos en los sistemas de información consistente en la reducción de las dependencias entre los activos.

Avellán Zambrano y Zambrano Bravo (2019) en su tesis titulada *Ciberseguridad y su aplicación en las instituciones de educación superior públicas de Manabí*.

Este documento pretende determinar el nivel de ciberseguridad utilizando la norma ISO 27032-2012 para identificar los riesgos, amenazas y vulnerabilidades de los sistemas distribuidos. Mediante la metodología Análisis Modal de Fallos y Efectos (AMFE), evaluando el nivel de riesgos en información, redes y aplicaciones, utilizaron las herramientas de escaneo de vulnerabilidades Shodan, Nessus y Acunetix en los sistemas distribuidos de las IES públicas.

Los resultados obtenidos son reportes de las diferentes categorías de vulnerabilidades que permitieron brindar recomendaciones para mitigar las inseguridades en el ciberespacio, que permite determinar sugerencias de mejora en aspectos de integridad, disponibilidad y confiabilidad de la información.

Medidas recomendadas: estandarizar la gestión de calidad de los procesos de seguridad de la información mediante normas ISO 9000, uso de herramientas de monitoreo de acceso a los sistemas de información (Norma ISO/IEC), emplear las normas de control interno 410-09, utilizar la norma ISO/IEC 27032, elaborar un plan de seguridad para el desarrollo, prueba y retroalimentación de las aplicaciones, realizar pruebas de *pentest* para verificar las medidas de seguridad de las aplicaciones: red, plataforma de alojamiento, sistema web, emitir informes periódicos sobre el estado de ciberseguridad, simulación de escenarios simulados de ataques, elaborar indicadores de prevención y respuestas frente a ataques cibernéticos, capacitación, uso de software legal, etcétera.

IV.3 Análisis de resultados

De las investigaciones descritas en el apartado anterior el análisis resultante concluye que cinco documentos realizan revisión documental, tres documentos realizan una investigación aplicativa donde se emplean herramientas de software, dos documentos realizan investigación de campo y tres documentos utilizan normas y metodologías para identificar riesgos y proponer planes de acción. A continuación, se resume la información:

(Cayón Peña y García Segura, 2014). Este documento realiza un análisis documental que concluye con una serie de recomendaciones y acciones para la implementación de la ciberseguridad.

(Hernández Jaimes & Lina, 2014). En este estudio se realiza un análisis estadístico del tráfico de la red de una institución, utilizando una herramienta propia del Sistema Operativo de los servidores con los que cuenta la IES.

(Anchundia-Betancourt, 2017). Realiza una revisión documental del estado del conocimiento acerca de la ciberseguridad en los sistemas de información de las universidades, resaltando el papel protagónico de las instituciones de educación para tratar de semas de seguridad informática.

(Gordón Revelo y Pacheco Villamar, 2018). Mediante una metodología definida se realiza una investigación de campo obteniendo valores requeridos para realizar una auditoría de seguridad informática.

(Acosta Pineda, A. Bohada, y Lorena Pineda, 2018). Documento que integra la revisión documental de ingeniería social.

(Morales Carrillo, Avellán Zambrano, Mera Cantos, y Zambrano Bravo, 2019). Realizan la revisión de unas de las normas de seguridad de la información, utilizando herramientas de software para analizar el estado de la seguridad en una institución.

(Leguizamón-Páez, Bonilla-Díaz, y León-Cuervo, 2020). En este estudio se implementa una herramienta de software que complementa el esquema de seguridad informática.

(Mena Mosquera, 2020). Realiza una investigación documental del estado actual de la auditoría informática en los SI de educación superior.

(Aguilar Torres, Gallegos García, Delgado Vargas, Abiega L'Eglisse, y Salinas Rosales, 2021). Investigación documental del aporte de algunas universidades en formación en ciberseguridad.

(Salazar Mata, Balderas Sánchez, García Aldape, y Cruz Navarro, 2020). Investigación aplicativa con el uso de herramientas de software libre para generar resultados, proponiendo un plan de acción.

(Vicente Cistero, 2016). Tesis doctoral que utiliza una metodología para generar datos que apoyan en la detección de riesgos en los SI.

(Avellán Zambrano & Zambrano Bravo, 2019). Tesis doctoral que determina el nivel de seguridad mediante la norma ISO 27032-2012 y la metodología AMFE.

V. Conclusiones

La ciberseguridad es una práctica y a la vez conjunto de estrategias que se encuentran en continua evolución, debido al avance vertiginoso de las tecnologías cada día aparecen nuevas formas de ataques, la búsqueda de información realizada visualiza que actualmente existen pocos estudios enfocados a este tema, el cual es de interés general y particularmente de las instituciones educativas ya que en su camino a la transformación digital maneja cada vez mayor cantidad de datos sensibles, lo que requiere de soluciones de seguridad informática fiables y funcionales.

Las aportaciones de los documentos identificados en este trabajo de investigación permiten concluir que, en todos los casos de estudio, las instituciones no cuentan con un plan de acción elaborado para minimizar daños o riesgos en sus sistemas e infraestructura.

También se pudo identificar que existen normas que, aunque no son leyes marcan la pauta para establecer metodologías que permitan identificar

vulnerabilidades. Los documentos que utilizaron alguna herramienta de software para el análisis de la red y sus sistemas permitieron demostrar que dichas herramientas facilitan el camino para identificar las fallas en los activos de información y por ende realizar esfuerzos para mantener el ciberespacio con menos riesgos de ataques.

De las revisiones documentales se puede observar la carencia y necesidad de organismos especializados en ciberseguridad que apoyen a las instituciones en el mejoramiento integral de la seguridad. El requerimiento de personal calificado que dé solución y apoye en la prevención.

Finalmente se puede afirmar que no es posible conseguir el 100% de seguridad, sin embargo, las IES deben estar preparadas ante posibles afectaciones contando con un plan de acción que se mantenga actualizado, haciendo participes a todos los empleados y alumnos mediante capacitaciones constantes y campañas de sensibilización, ya que, gran parte de los ataques se originan de las brechas abiertas por los mismos usuarios de las tecnologías.

VII. Referencias

Acosta Pineda, S., A. Bohada, J., & Lorena Pineda, M. (2018). Ingeniería Social en Instituciones de Educación Superior. *Revista Colombiana de Tecnologías de Avanzada (RCTA)*, 52-61. Obtenido de https://www.researchgate.net/publication/339506131_INGENIERIA_SOCIAL_EN_INSTITUCIONES_DE_EDUCACION_SUPERIOR.

Aguilar Torres, G., Gallegos García, G., Delgado Vargas, K. A., Abiega L'Eglisse, A. F., & Salinas Rosales, M. (2021). Educación en Ciberseguridad. En *Hacia una tecnología educativa con sentido humano para una educación sin distancia y de bienestar en México* (págs. 111-122). México: Corporación Universitaria para el Desarrollo de Internet. Obtenido de https://redlate.net/publicaciones/.

Anchundia-Betancourt, C. E. (2017). Ciberseguridad en los sistemas de información de las universidades. *Dominio de las Ciencias*, 201-212. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6102849.

ANIUES. (2020). *Estado Actual de las TIC en las Instituciones de Educación Superior en Mexico.* Obtenido de https://estudio-tic.anuies.mx/Estudio_ANUIES_TIC_2020.pdf.

ANUIES. (2020). Ciberseguridad en las Instituciones Educativas. Obtenido de https://recursosdigitales.anuies.mx/wp-content/uploads/2020/05/anuiesticc_v2.pdf.

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). *¿Que sabemos de ciberseguridad?* Madrid: CSIC. Obtenido de https://elibro.net/es/ereader/bibliotecauv/172144?page=1.

Avellán Zambrano, N. V., & Zambrano Bravo, M. F. (05 de 2019). Ciberseguridad y su aplicación en las Instituciones de educación superio púbilcas de Manabí. Ecuador. Obtenido de http://repositorio.espam.edu.ec/bitstream/42000/1032/1/TTMTI3.pdf.

Cayón Peña, J., & García Segura, L. A. (2014). La importancia del componente educativo en toda estrategia de ciberseguridad. *Estudios en seguridad y defensa*, 5-13. Obtenido de https://esdeguerevistacientifica.edu.co/index.php/estudios/article/view/9/4.

Craigen, D., Diakun-Thibault, N., & P. R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 13-21.

Gordón Revelo, D. S., & Pacheco Villamar, R. (2018). Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior. *ReCIBE. Revista electrónica de Computación, Informática*, 1-21. Obtenido de ttps://www.redalyc.org/articulo.oa?id=512255650001.

Hernandez Jaimes, A., & Lina, P. A. (2014). Validación de la caracterización estadística del tráfico de red de un servidor web de un campus universitario como mecanismo de un sistema de detección de intrusos. *Ingeniería y Desarrollo*, 65-79. Obtenido de ttps://www.redalyc.org/articulo.oa?id=85230428005.

INCIBE, I. N. (2021). *Glosario de términos de ciberseguridad.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf.

ITU, U. I. (Noviembre de 2010). *Ciberseguridad*. Obtenido de https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx.

Leguizamón-Páez, M. A., Bonilla-Díaz, M. A., & León-Cuervo, C. A. (2020). Analysis of computer attacks through Honeypots in the District University Francisco José de Caldas. *Ingeniería y competitividad*, 1-13. Obtenido de https://www.redalyc.org/articulo.oa?id=291365765002.

Mena Mosquera, A. J. (15 de 12 de 2020). *Estado actual de la auditoria de seguridad en los sistemas de información de Educación Superior.* Obtenido de Tecnológico de Antioquia, Institución Universitaria: https://dspace.tdea.edu.co/bitstream/handle/tdea/1391/Informe%20Auditoria%20seguridad.pdf?sequence=1&isAllowed=y.

México, G. d. (2017). *Gobierno de México.* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

Monsalve, J. C. (2018). CIBERSEGURIDAD: PRINCIPALES AMENAZAS EN COLOMBIA (INGENIERÍA SOCIAL, PHISHING Y DoS). *Universidad Piloto de Colombia*, 1-10.

Morales Carrillo, J. J., Avellán Zambrano, N., Mera Cantos, J. S., & Zambrano Bravo, M. (2019). Ciberseguridad y su aplicación en las Instituciones de Educación Superior. *Revista Ibérica de Sistemas e Tecnologias de Información*, 438-448. Obtenido de https://www.proquest.com/openview/7bdb0c8eba16e5afd00ea4d3397ad815/1?pq-origsite=gscholar&cbl=1006393.

Patterson, W., & Winston-Proctor. (2019). *Behavioral cybersecurity: Applications of personality.* CRC Press.

Salazar Mata, J., Balderas Sánchez, A., García Aldape, H., & Cruz Navarro, c. (2020). Implementación de una estrategia de pentesting con software libre. *Revista de divulgación científica y tecnológica.*, 22-30. Obtenido de https://www.eumed.net/uploads/articulos/6e7ad2f07d822d9d6e7c50f66f2d75d2.pd.

Standars, I. 2. (2017). *The ISO 27000 Directory*. Obtenido de http://www.27000.org/iso-27002.htm.

Vicente Cistero, E. (2016). Análisis y gestión del riesgo en los sistemas de información: un enfoque borroso. *Universidad Politécnica de Madrid*. Madrid. Obtenido de http://oa.upm.es/44529/.

Apéndice A. Resumen de investigaciones consultadas

Se integra una tabla con la siguiente información de las investigaciones consultadas: número, autor(es) y año, metodología utilizada, participantes y contexto, aportaciones.

Núm.	Autor(es), año y lugar	Metodología	Participantes y contexto	Aportaciones
1	Cayón y Peña (2014), Colombia.	Estudio cualitativo	53 países, análisis del componente educativo en la estrategia de ciberseguridad (EC).	Los dos primeros países que publicaron su EC fueron E.E.U.U y Rusia en el 2003, 31 países incorporan el componente educativo dentro de sus EC.
2	Hernández y Prada (2014), Colombia.	Estudio cuantitativo	Servidor web de un campus universitario, medición y análisis de valores de tráfico de entrada y salida, durante tres meses y una semana.	El hallazgo más importante es que el tráfico por hora de entrada y salida tiene una media y una desviación estándar que puede considerarse estadísticamente invariable en el tiempo, dado que puede utilizarse en la detección de situaciones atípicas que sugieren presencia de amenazas o ataques cibernéticos.
3	Archundia-Betancourt (2017), Ecuador.	Estudio cualitativo	Sector universitario, Estado actual del conocimiento de la ciberseguridad en los sistemas de información.	La universidad debe tener un papel protagónico en el establecimiento de una cultura de ciberseguridad que exige una labor de capacitación de todos los sectores de la sociedad; uno de los desafíos más importantes es lograr un compromiso real de los Estados en la generación de políticas públicas específicas, y en la construcción de una cultura de ciberseguridad, este es un rol que definitivamente, debe liderar la universidad.
4	Gordon y Pacheco (2018), México.	Cuantitativo	Institución de educación superior, auditoría de seguridad informática, mediante la aplicación de la metodología OSSTMM para identificar brechas de seguridad, utilizando como tipo de prueba el Hacking ético.	Se encontró que la institución de educación superior no lleva un control adecuado de políticas de seguridad informática y aplicación, obteniendo como principal hallazgo los valores de evaluación de riesgo, equivalente al 72,15% de seguridad, equivalente a una seguridad informática media.

Núm.	Autor(es), año y lugar	Metodología	Participantes y contexto	Aportaciones
5	Bohada y Pineda (2018), Colombia.	Cualitativo	Instituciones de Educación Superior, estudio sobre la Ingeniería Social y sus antecedentes, las vulnerabilidades que poseen las IES y que pueden ser objeto de ataque, y estrategias propuestas en favor de la protección de la información, así como recomendaciones generales y significativas.	La suplantación de identidad ha sido la técnica puerta de entrada a ataques de ingeniería social en las IES, Por tanto, el tomar medidas para minimizar, contribuirá a contrarrestar este tipo de ataques. El desarrollo de políticas y planes de protección de la información, unido con procesos continuos de capacitación ayudarán a mejorar la confidencialidad, integridad y disponibilidad de la información de las IES.
6	Morales, Avellan, Mera y Zambrano (2019).	Cuantitativa	Instituciones de educación superior, las cuales comparten la preocupación de la protección de sus datos en el ciberespacio, por no contar en sus sistemas con normas de ciberseguridad, al utilizar la norma ISO 27032-2012, directrices en ciberseguridad y las herramientas Shodan, Nessus y Acunetix, que permitieron conocer y analizar posibles amenazas y defensas, en los niveles de seguridad de los sitios, sistemas o servicios webs. Además, con la metodología Análisis Modal de Fallos y Efectos (AMFE) se brindó soluciones de mitigación de riesgos.	La evaluación de los riesgos en los procesos de documentación en los dominios de ciberseguridad basados en la norma ISO/IEC 27032 en el dominio de seguridad de la información, tuvo un total de 12 vulnerabilidades, en seguridad de las aplicaciones, se registró un total de 14 vulnerabilidades, por último, en cuanto a la seguridad de las redes, se hallaron 8 vulnerabilidades, Todos estos datos permitieron tomar acciones correctivas y establecerlas en el plan de acción para la mitigación de los mismos. En cuanto a las herramientas aplicadas, se pudo apreciar que Acunetix fue la más eficaz y óptima en resultados, puesto que mostraba más evidencias de riesgos en vulnerabilidades de nivel alto que las demás. Las propuestas definidas en el plan de acción permitirán a las instituciones involucradas, mejorar la seguridad en la información, redes y aplicaciones que estas administran, aplicando técnicas y recomendaciones mostradas previo a los análisis efectuados con las herramientas de análisis de vulnerabilidad. Finalmente, como medida de solución se efectuó un plan de acción para cada institución objeto de estudio que le permita desarrollar medidas de control y estrategias.
7	Leguizamón-Páez, Miguel A.; Bonilla-Díaz, María A.;	Cualitativo*	Diseño e implementación de la herramienta Honeypots como complemento alternativo al	Identificación de diferentes patrones y formas de atacar.

Núm.	Autor(es), año y lugar	Metodología	Participantes y contexto	Aportaciones
	León-Cuervo, Camilo A. (2020), Bogotá Colombia.		esquema de seguridad informática existente en la Universidad Distrital Francisco José de Caldas como proyecto que contribuye al análisis y detección de ataques a la seguridad de la red y los elementos de cómputo en la institución.	Detección fallas de seguridad en los servidores de la universidad debido a ataques informáticos. Diseño de una nueva red de distribución para registrar información sobre los diferentes ataques y permitir la aplicación de soluciones efectivas.
8	Mena Mosquera, A. J. (2020), Antioquia.	Cualitativo	Documenta de qué manera algunas IES están implementando controles, metodologías y políticas que permitan evaluar los riesgos a los que están expuestos los datos y la información confidencial.	Concentración de información que da a conocer diferentes normas y metodologías para los SGSI.
9	Aguilar Torres, Gallegos García, Delgado Vargas, Abiega L'Eglisse, & Salinas Rosales, (2021), México.	Cualitativo	Documento que analiza la participación y aportes de las universidades de México, en materia de ciberseguridad.	Documenta las principales amenazas en el ciberespacio, presenta las instituciones que tienen programas de posgrado, diplomados y grupos de investigación enfocados en la ciberseguridad.
10	Salazar Mata, J., Balderas Sánchez, A., García Aldape, H., & Cruz Navarro, (2020), México.	Cualitativa	Vinculación de trabajos de investigación y prueba con el Laboratorio de Software Libre (LabSol) del Centro Zacatecano de Ciencia y Tecnología (COZCyT). Investigación de tipo aplicativo, partiendo de un análisis contextual de la situación actual, para la preparación del escenario para la implementación de pruebas de penetración, utilizando la guía OWASP v3.0 y la metodología OSSTMM v2.1., considerando la herramienta Kali Linux.	Generación de un plan de acción recomendaciones para formar recurso humano. Propuesta para implantar y evaluar un manual de mejores prácticas, programas de capacitación al personal Propuesta de creación de un laboratorio de seguridad, de pentesting o hacker ético. Se propone un proyecto de cómputo forense.
11	Vicente Cistero, E. (2016). Madrid.	Cualitativo / Cuantitativo	Se proporciona información sobre las normas internacionales relativas al análisis y gestión de riesgos en los SI. Se describe la metodología de análisis y gestión de riesgos MAGERIT, utilizada en España.	Ejemplo ilustrativo de una unidad administrativa que utiliza un SI para el desarrollo de sus tareas internas y para la prestación de servicios de atención administrativa a los ciudadanos (administración electrónica).

RETOS DE CIBERSEGURIDAD PARA MÉXICO

Salim Daniel SIGALES MONTES[14]

[14]Salim Sigales es un experto en áreas de tecnologías de la información, telecomunicaciones y seguridad de la información. Su investigación se enfoca en los retos de ciberseguridad que enfrenta México, con especial atención en la prevención de ciberataques en sectores críticos.

RETOS DE CIBERSEGURIDAD PARA MÉXICO

Cybersecurity Challenges for Mexico

Resumen

A lo largo de la historia, la comunicación ha sido esencial para la sociedad humana, permitiendo intercambiar ideas, emociones e intenciones. La voz fue la primera forma de comunicación, seguida por la escritura. Luego, surgieron otros medios como el correo, la comunicación impresa, las telecomunicaciones y la tecnología de la información. Todos estos medios han sido vehículos para transmitir información. siendo este último término el considerado como el activo más importante para las compañías.

Hoy en día la telefonía celular, las computadoras y los satélites son herramientas tecnológicas que tienen una gran importancia. Sin embargo, con estas tecnologías llegaron ventajas y riesgos para la información. Siendo esto último lo que daría paso al surgimiento de la ciberseguridad. Termino que ganó importancia a través de los años. Por ejemplo, durante el 2022 fuimos testigos de la guerra cibernética de mayor magnitud.

Si bien México se reconoce por ser una nación pacifica en términos de conflictos bélicos, esto no exime a nuestra nación de ser un objetivo en presente y futuro, por lo que se deben existir esfuerzos

Abstract

Throughout history, communication has been essential for human society, allowing the exchange of ideas, emotions and intentions. The voice was the first form of communication, followed by writing. Later, other media such as mail, print communication, telecommunications and information technology arose. All these media have been vehicles for transmitting information. being this last term the one considered as the most important asset for the companies.

Today cell phones, computers and satellites are technological tools that are of great importance. However, with these technologies came benefits and risks to information. The latter being what would give way to the emergence of cybersecurity. I end up gaining importance over the years. For example, during 2022 we witnessed the largest magnitude cyber war.

Although Mexico is recognized for being a peaceful nation in terms of war conflicts, this does not exempt our nation from being a target in the present and future, so there must be efforts to protect our nation's critical infrastructure and to be able to face to the Cybersecurity Challenges for Mexico, which range from

para proteger la infraestructura crítica de nuestra nación y poder hacer frente a los retos de ciberseguridad para México, que van desde capacitar a sectores vulnerables en términos de ciberseguridad, la disminución de ciberdelitos, la preparación para hacer frente a las amenazas avanzadas, afrontar la desinformación con la llegada de la Inteligencia Artificial; así como, las implicaciones que representarían los ordenadores Cuánticos, el cifrado cuántico y la ciberseguridad en el espacio exterior.

training vulnerable sectors in terms of Cybersecurity, reducing cybercrimes, preparing to deal with advanced threats, dealing with disinformation with the arrival of artificial intelligence, as well as the implications that would represent Quantum Computers, Quantum Encryption and Cybersecurity in outer space.

Palabras clave: guerra cibernética, Inteligencia Artificial, ordenadores cuánticos, cifrado cuántico, espacio exterior.

Keywords: *cyber warfare, artificial intelligence, quantum computers, quantum encryption, outer space.*

I. Introducción

Antes de comenzar primero debemos responder a la pregunta ¿qué es la ciberseguridad? Y para responder a ello, haremos referencia a la definición de dicho termino por parte del *National Institute Of Standards and Technology* (NIST), quien la define como la capacidad de proteger y defender el uso del ciberespacio de los ataques cibernéticos. Por lo que, podemos entender que la ciberseguridad se encarga de proteger y defender las redes, sistemas, programas e información. Siendo esta última en la que se deben destinar mayores esfuerzos para preservar sus características de confidencialidad, integridad y disponibilidad ante los ataques cibernéticos. Cabe mencionar que el término de ciberseguridad se enfoca en la protección del mundo digital. Caso contrario a la seguridad de la información que se aboca a la protección de la información sin importar en los medios que esta se encuentre, lo anterior puede ser tanto en medios físicos, como en medios digitales.

Hoy en día la ciberseguridad va ganando mayor importancia y es sabido que la información se considera el activo más importante para las empresas y para todo lo que hacemos en nuestra vida personal. Es por ello, que la materialización de una amenaza puede llevar consigo un impacto económico, operativo, emocional y social. Y como muestra de lo antes mencionado, hagamos énfasis en los impactos económicos estimados gracias al estudio realizado por la empresa Accenture, en donde se estimó un valor económico

en riesgo, debido a ciberataques directos e indirectos para un periodo de cinco años que van del 2019 al 2023 y que se dimensionó en 5.2$ billones de USD a nivel global.

En otro ámbito durante 2019 y 2022 derivado de la nueva normalidad existente por la pandemia, las empresas en México y en otras naciones se han visto obligadas a reinventar la arquitectura de su infraestructura tecnológica, en donde la red corporativa se ha extendido hasta el hogar de los colaboradores, en donde las actividades no exigen un contacto físico o presencial para la entrega de servicios. Y pese al cambio tan repentino que dio la forma en la que operaba la industria, todo indicaba que las mismas se habían adaptado rápidamente al cambio sin mayor inconveniente. Sin embargo, muy pocas realmente estaban preparadas para hacer frente a lo que estaba por venir, ya que, muchas transaccionaban información sensible sin controles de ciberseguridad adecuados. Ello se vio reflejado desde los impactos en la continuidad del negocio, hasta la afectación por la exposición de información sensible en redes sociales, y sobre todo pérdidas económicas que en algunos casos derivaron en el cierre de empresas. Y esto solo representa una pequeña fracción de los impactos asociados a los ataques cibernéticos que experimentó la población mundial durante la pandemia, lo cual tenía sentido, ya que el consumo a través de Internet se potencializó y, por ende, la demanda y uso de las tecnologías de las información y telecomunicaciones. Lo anterior ya representaba un gran reto para la industria con la implementación de mayores y mejores controles de seguridad. A continuación, haremos alusión al estudio realizado por la Asociación de Internet de México a una muestra de 410 usuarios de Internet. De esto sabemos que durante 2021 el 53% de ellos fueron víctimas de una vulneración (ver ilustración 1. Víctimas de alguna vulneración).

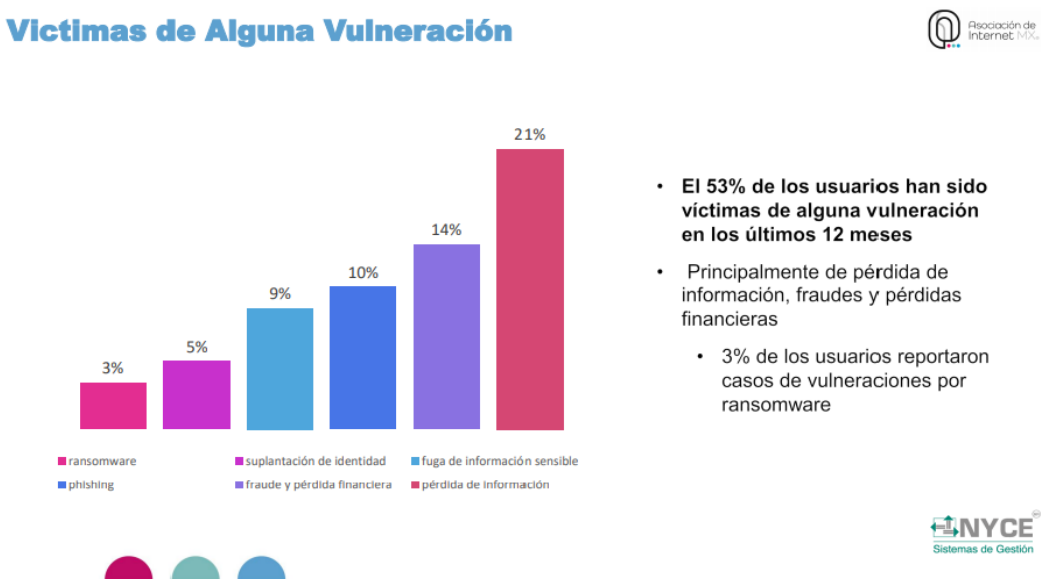


Ilustración 1. Víctimas de alguna vulneración.
Fuente: Asociación de Internet MX

Lo antes mencionado no lo fue todo. Ya que durante el primer trimestre de 2022 cuando la población mundial comenzaba a regresar a la normalidad a la que estábamos acostumbrados durante años, se suscitó de manera apresurada un conflicto entre Rusia y Ucrania, que daría paso a una guerra cibernética de mayores magnitudes, misma que, se ha desarrollado durante el primer trimestre del presente año y que ha mostrado una serie de estrategias utilizadas para afectar infraestructura clave de una nación, poniendo a prueba la ciberseguridad. Y en lo que nos focalizaremos como parte importante de los retos de ciberseguridad para México.

II. Objetivo

El siguiente documento tiene como finalidad puntualizar los desafíos y retos de ciberseguridad a los que nuestra nación se enfrenta en el presente y que enfrentará en los próximos años. Todo ello con la finalidad de concientizar a la ciudadanía y coadyuvar a los organismos pertinentes a sumar esfuerzos para aumentar la madurez de nuestra nación en dicha materia y con ello disminuir los impactos que se puedan derivar a consecuencia de ataques cibernéticos intencionados a nuestra nación.

III. Cultura de ciberseguridad

Aumentar la educación, formación y concientización aspectos básicos esenciales de ciberseguridad. Tanto a la ciudadanía, sector académico, sector privado e instituciones públicas para aumentar la confianza de la interacción en el mundo digital.

1) El 51% de los encuestados reporta utilizar la misma contraseña en cuentas personales y laborales.
2) El 68% de los usuarios no utiliza un segundo factor de autenticación.
3) El 33% de niñas, niños y adolescentes no recibe capacitación en su escuela sobre los peligros de Internet.
4) Los delitos cibernéticos contra menores aumentaron un 157% con base en un estudio de la Guardia Nacional.
5) El 26% de los encuestados no sabe cuál es la autoridad competente para reportar problemas de ciberseguridad.
6) El 53% de los usuarios encuestados reportaron que fueron vulnerados:
    - *Ransomware,*
    - *Phishing,*
    - Suplantación de identidad,
    - Fraude y pérdida financiera,
    - Fuga de información sensible,
    - Pérdida de información.
7) El 10% de los usuarios realizan respaldos de su información y el 38% lo hace cuando se acuerda. Y el 37% verifica los respaldos.
8) El 27% de usuarios realiza respaldos en nube.

III.1. Disminución de ciberdelitos

Aumentar la participación de la ciudadanía, del sector académico, sector privado e instituciones públicas para coadyuvar a disminuir los actos ilegales realizados por un atacante cibernético en el mundo digital y que se llevan a cabo a través de las redes y tecnologías de comunicación e información.

1) En 2021 la Guardia Nacional reportó un aumento en las denuncias relacionadas a ciberdelitos, 2 898 denuncias durante 2020, ello significó más del doble con relación a 2019.
2) Accenture estimó un valor económico en riesgo debido a ciberataques entre 2019 y 2023 de 5.2 billones de USD.

III.2. Ciberseguridad en infraestructura crítica

El Estado mexicano debe implementar una estrategia para proteger la infraestructura critica basada en las amenazas del mundo cibernético actual,

para lo cual se deben priorizar los sectores, de energía, banca, infraestructura digital, administración pública y del espacio. Así como, del resto de infraestructura crítica que pueden verse afectadas en su continuidad ante un incidente de ciberseguridad. La infraestructura crítica es definida por la European Critical Infraestructure (ECI) como un activo, sistema o parte del mismo y el cual es esencial para mantener las funciones críticas de la sociedad, la salud, la seguridad, el bienestar económico o social de las personas, y cuya perturbación o destrucción supone un impacto considerable en una nación como resultado de la falta de mantenimiento de dichas funciones (ver tabla 0-1. Infraestructura Crítica ECI).

NÚMERO	SECTOR	SUBSECTOR	TIPO DE ENTIDAD
I	**Energía	Electricidad	
		Calefacción y refrigeración urbana	
		Petróleo	
		Gas	
		Hidrógeno	
II	**Transporte	Aire	
		Ferrocarril	
		Marítimo	
		Carretera	
III	**Banca		Entidades de crédito
IV	Infraestructuras de los mercados Financieros		
V	Salud		
VI	Agua potable		
VII	Aguas residuales		

VIII	**Infraestructura Digital		Los proveedores de puntos de intercambio de Internet
			Los proveedores de servicios de DNS
			Los registros de nombres del dominio de primer nivel
			Los proveedores de servicios de computación en nube
			Los proveedores del servicio de centros de datos
			Los proveedores de redes de distribución de contenidos
			Los proveedores de servicios de confianza
			Los proveedores de redes públicas de comunicaciones electrónicas
IX	**Administración Pública		Las entidades de la administración pública de las administraciones centrales
X	**Espacio		Los operadores de infraestructuras terrestres, poseídas, gestionadas y explotadas por los Estados miembros o por entidades privadas, que apoyan la prestación de servicios espaciales, excluidos los proveedores de redes públicas de comunicaciones electrónicas

Tabla 0-1. Infraestructura Crítica ECI.
Fuente: Elaboración propia

A continuación, se anexan algunas gráficas que muestran una disrupción en el servicio crítico energético en una localidad de Ucrania, durante

el presente conflicto bélico con Rusia (ver Gráfica IT energía afectada). De igual forma, se anexa una gráfica que muestra otra disrupción en Ucrania, pero esta última al servicio de la banca y la cual se presentó durante el mismo conflicto bélico entre las naciones antes mencionadas (ver Gráfica red bancaria afectada). En otro ámbito podemos apreciar gráficas adicionales que demuestran la disrupción del servicio satelital (ver gráfica de red satelital) y una disrupción del servicio de internet en el país atacado (ver gráfica de disrupción significante de Internet), lo cual demuestra que dichos servicios críticos son clave para cualquier atacante.

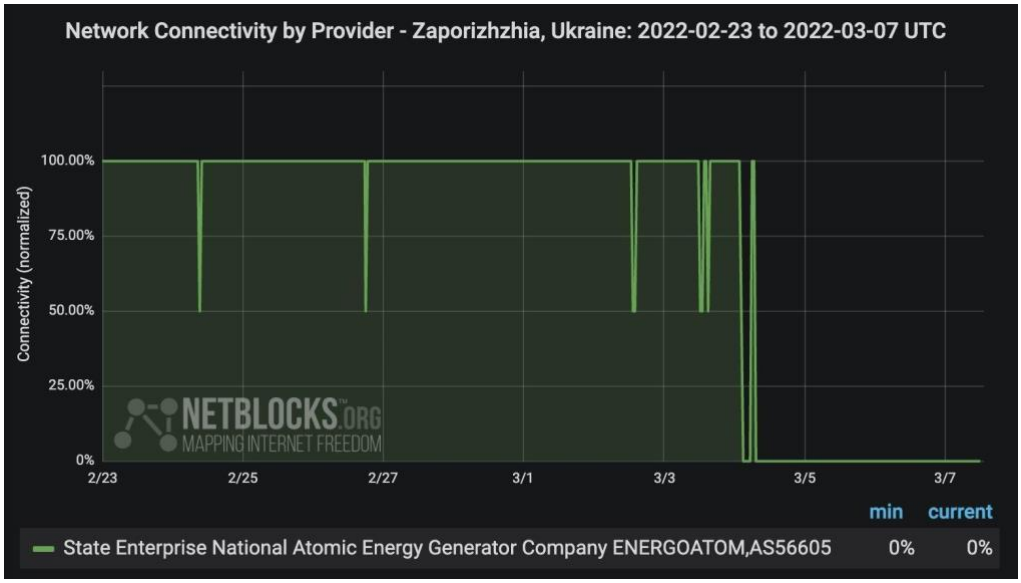


Ilustración 2. Gráfica IT energía afectada.
Fuente: Netblocks.

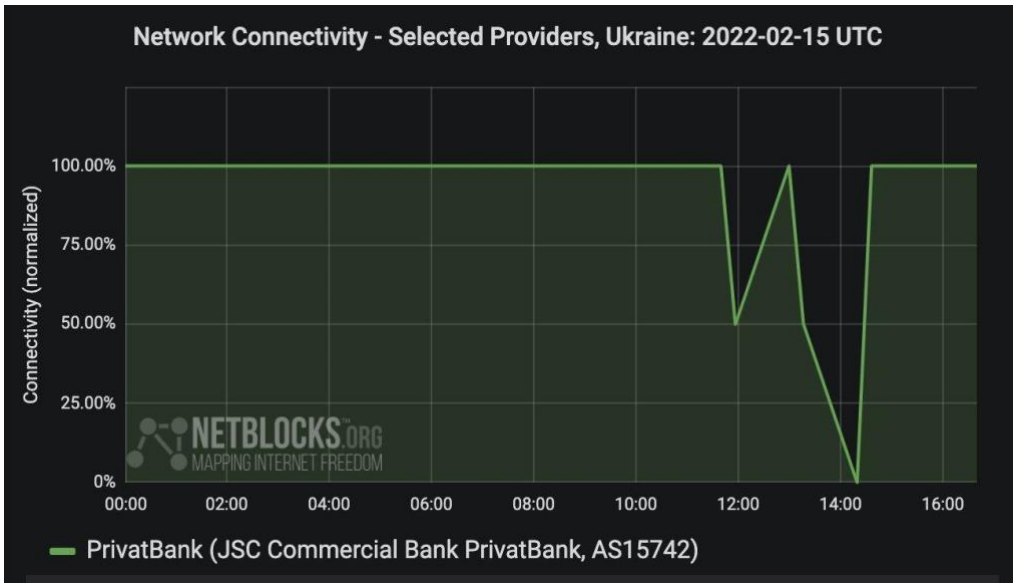


Ilustración 3. Gráfica red bancaria afectada.
Fuente: Netblocks

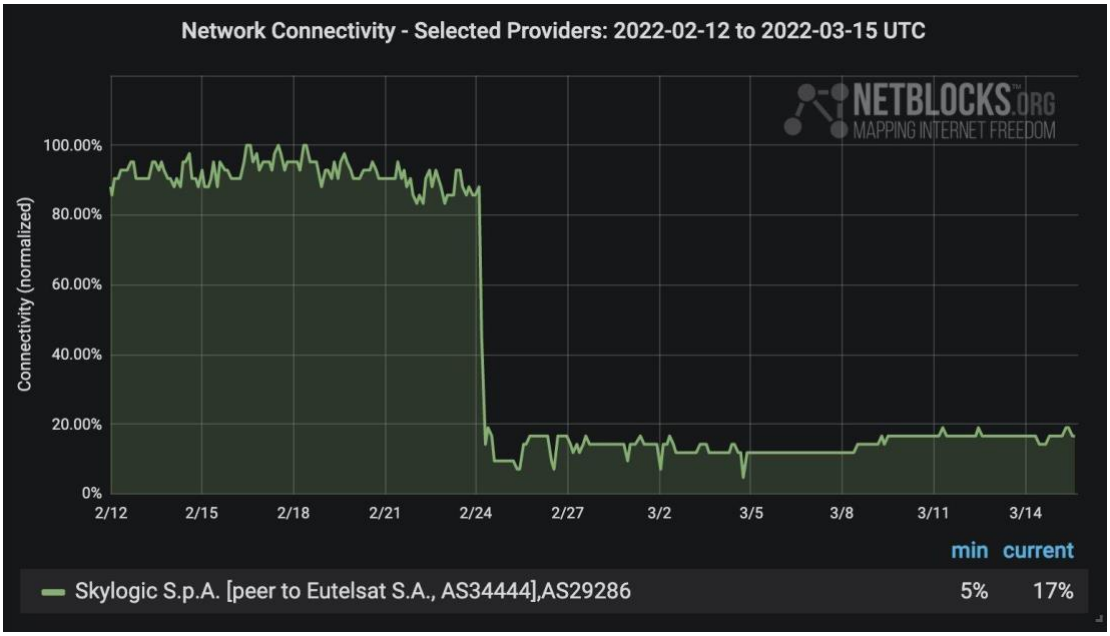


Ilustración 4. Gráfica red satelital afectada.
Fuente: Netblocks.

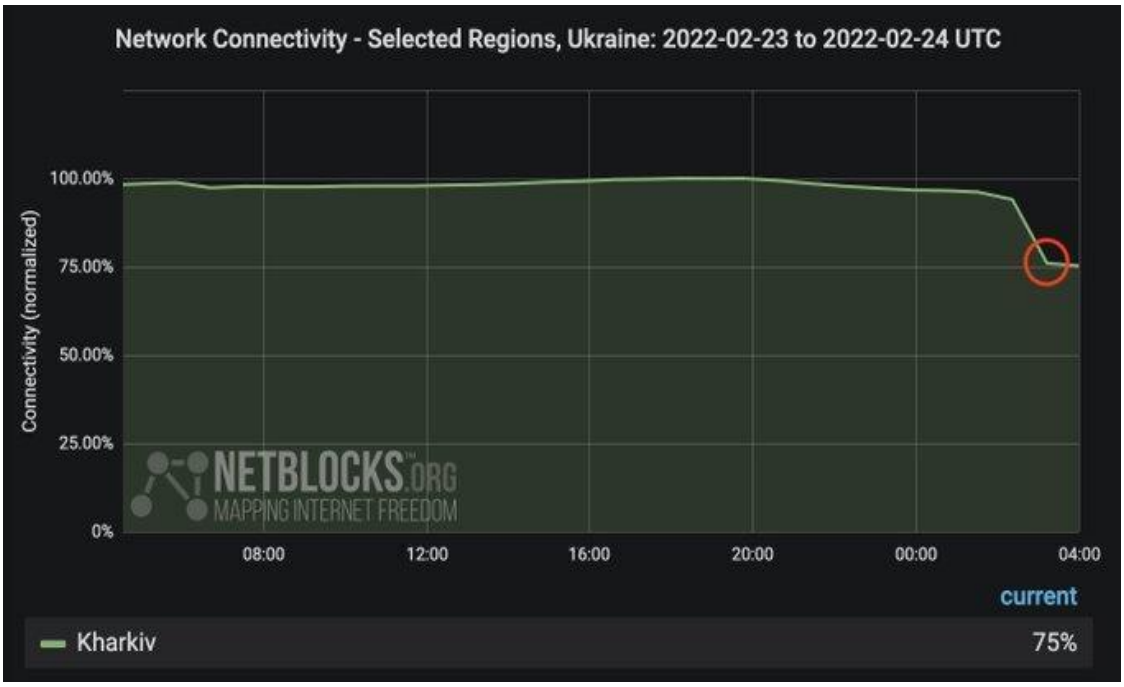


Ilustración 5. Gráfica de disrupción significante de internet.
Fuente: Netblocks.

IV. Amenazas persistentes avanzadas

El Estado mexicano debe aumentar esfuerzos para promover buenas prácticas de ciberseguridad en los sectores civil, académico, público y privado para hacer frente a las amenazas que son las responsables de grandes impactos económicos.

IV.1. Spear phishing

Ataque de *phinging* altamente dirigido a personas, organizaciones o empresas específicas. Actividad que podrá ser tipificado con base en nuestro Código Penal Federal como:

- **Fraude** Art. 386.
- **Falsedad** Art. 234 al 246.

IV.2. Rasomware as a service (RAAS)

Kits de *malware* para llevar a cabo ataques de *ransomware*, los cuales tienen por objetivo cifrar archivos de la víctima. El RaaS está disponible en la web oscura, lo cual lo hace peligroso ya que está disponible a toda persona sin necesidad de conocimientos avanzados. Sin embargo, el uso del mismo sirve para realizar actividades ilícitas que serán tipificadas como alguno(s) de los siguientes delitos con base en nuestro Código Penal Federal:

- **Traición a la patria** Art. 123.
- **Espionaje** Art. 127 a 129.
- **Terrorismo** Art. 133 a 135.
- **Sabotaje** Art. 140.
- **Delitos en materia de vías de comunicación** Art. 167 a 168.
- **Revelación de secretos** Art. 210, 211, 211 bis.
- **Acceso no autorizado a Sistemas de Cómputo** Art. 211 bis 1 al 211 bis 7.
- **Robo** Art. 367, 368.
- **Delitos en materia de derecho de autor** Art. 24.

IV.3. LOLBAS (Living off the Land Binaries and Scripts)

Un método que hace un mal uso de los programas existentes en una computadora, por ejemplo, programas del sistema operativo, para funciones dañinas o para malware. Estos archivos pueden ser:

- Binarios.

- Scripts.
- Bibliotecas.

Estos archivos deben estar disponibles en el sistema de forma predeterminada o pueden instalarse a través de fabricantes de software confiables o fuentes de código abierto. Y los cuales se utilizará por un atacante cibernético para realizar funciones tales como:

- Ejecución de código de programa o scripts,
- Lectura del tráfico de la red o las actividades de los usuarios,
- Proceso de volcado de memoria,
- Leer los datos de inicio de sesión,
- Operaciones de archivos como descargas y cargas de archivos.

IV.4. Ataque DDoS de rescate (RDDOS)

Intento de extorsión a una persona u organización amenazándolos con un ataque de denegación de servicio distribuido (DDoS), ataque que tiene por objetivo agotar los recursos de una aplicación, sitio web o red para que los usuarios legítimos no puedan consumir los servicios.

- **Delitos contra la paz y seguridad de las personas** (amenazas) Art. 282 y 283.

V. Computadora cuántica criptográfica relevante

Debemos implementar estratégicas que coadyuven a implementar algoritmos capaces de soportar una amenaza post cuántica en los Sistemas de Seguridad Nacional (NSS, por sus siglas en inglés), sistemas que transportan información militar o de inteligencia clasificada o confidencial. Lo cual hoy en día la Agencia de Seguridad Nacional considera devastador para su nación, ya que, este tipo de computadoras serían capaces de vulnerar los algoritmos de claves públicas y firmas digitales. Lo cual, en términos cotidianos, se utilizan para el cifrado e intercambio de información de manera segura.

Naciones que participan en la carrera cuántica:

- ✓ China
- ✓ Estados Unidos
- ✓ Alemania
- ✓ Rusia
- ✓ India

VIII. Consideraciones de ciberseguridad en el espacio exterior

Se deben aumentar las capacidades de ciberseguridad para los activos críticos ubicados en el espacio exterior. Actualmente el sistema satelital mexicano se conforma por los siguientes satélites:

- Morelos I
- Morelos II
- Morelos III
- Solidaridad I
- Solidaridad II
- EUTELSAT 115 West A (Satmex 5)
- EUTELSAT 113 West A (Satmex 6)
- QuetzSat 1
- Mexsat 3

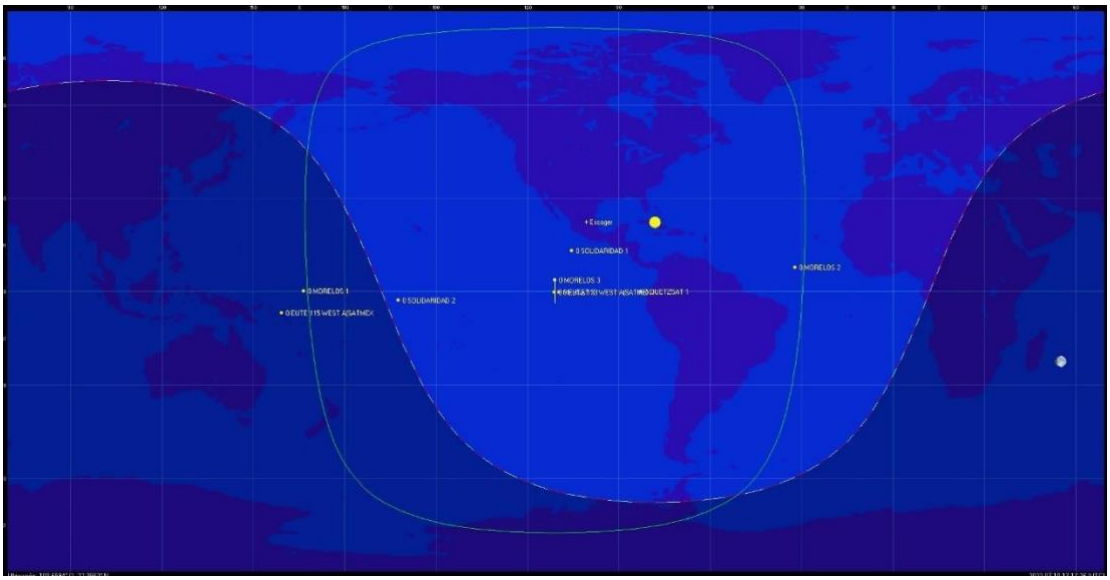


Ilustración 6. Sistema Satelital Mexicano.
Fuente: Orbitron.

Actividades cibernéticas maliciosas que afectan un satélite:

- Inyección de código malicioso,
- Ataques de DDoS,
- Bloquear o enviar comandos no autorizados para orientación y control.

Algunos controles de seguridad para los satélites son:

- Protección contra accesos no autorizados,
- Protección contra interferencia,
- Protección de sistemas terrestres,
- Protección de sistemas de procesamiento de información,
- Gestión de riesgos de cadena de suministro,

- Cifrado cuántico,
- Protección en la gestión de actualizaciones.

Invertir en investigación y desarrollo de cifrado cuántico para garantizar la confidencialidad, integridad y disponibilidad de la información transaccionada en los satélites. Lo cual garantice la continuidad de funciones como:

- ✓ Tareas de seguridad nacional.
- ✓ Servicios de telefonía y banda ancha.
- ✓ Apoyo en desastres naturales.
- ✓ Educación a distancia.
- ✓ Telemedicina.
- ✓ Comunicación en zonas rurales.

En 2016, China colocó el primer satélite cuántico, el que solo proporciona las claves de cifrado, y para 2024 España estima colocar satélites 5G de distribución de claves cuánticas (QKD), el cual es un método seguro de intercambio de claves basado en las leyes cuánticas de la física en lugar de la complejidad computacional.[23]

Se considera que las tecnologías cuánticas determinarán que naciones seguras y cuáles no. Y los gobiernos no permitirán que se vendan estas tecnologías lo cual es un gran reto para nuestra nación.

VII. Uso dual de la Inteligencia Artificial

El pasado 7 de marzo en una conferencia de seguridad internacional, se exploró que el uso de las tecnologías de Inteligencia Artificial (IA) para diseñar nuevos fármacos, se podría utilizar para generar armas bioquímicas. Por lo tanto, debemos responder a las preguntas:

¿Cuáles son los impactos actuales sobre el uso dual de la IA en términos de ciberseguridad? Y para dar respuesta a ello lo primero que nos viene a la mente es la aplicación inversa de la Inteligencia Artificial en cuestiones de ciberseguridad para:

- Generar intrusiones,
- Generación de malware,
- Generación de fraudes,
- Hacer contrainteligencia,

[23]https://www.google.com/amp/s/www.elespanol.com/omicrono/tecnologia/20210515/constelacion-satelites-espanoles-cifrado-cuantico-blindar-defensa/581193099_0.amp.html.

- Analizar y explotar las vulnerabilidades de una víctima,
- Analizar comportamientos de los objetivos para ejecutar ciberataques más efectivos por parte de un atacante,
- Generación de correo malicioso,
- Generación de desinformación,
- Suplantación de identidad.

Hoy en día se tiene registro de impactos en ciberseguridad debido al uso dual de la IA y dentro de lo cual destacan los siguientes:

- La desinformación.
- La suplantación de identidad.

Por ejemplo, en los últimos meses se habla mucho del término *Deep Fake*, que es una técnica que hace uso de la Inteligencia Artificial, específicamente del aprendizaje profundo (*Deep Learning*) y el cual es utilizado frecuentemente para la elaboración de material video grafico falso, actividad que puede encaminar a una persona a incurrir en el delito, como por ejemplo en el código penal para el estado de Jalisco en su artículo 143-Quáter, se tipifica como suplantación de identidad a quien por medios electrónicos o a través de Internet, se atribuya los datos de otra persona, generando con ello un daño moral o al patrimonio, al obtener un lucro indebido, lo que se sancionará con prisión de tres a ocho años y multa de mil a dos mil salarios mínimos. Un ejemplo de este tipo de actividades ilícitas con estas tecnologías es el caso que suscitó, según el *Wall Street Journal*, donde el CEO de una compañía inglesa transfirió 220 000 euros por orden de un software que imitaba la voz de su jefe de origen alemán.

Como podemos ver el uso dual de la Inteligencia Artificial supone un gran reto para México. Por ello, ahora debemos responder a la pregunta ¿cómo debe el Estado mexicano prevenir el uso dual de la IA en términos de ciberseguridad? Y para dar respuesta a ello se propone lo siguiente:

El Estado mexicano debe destinar esfuerzos para fomentar el uso ético de IA dentro de los sectores civil, académico, público y privado. Y de lo que podemos priorizar lo siguiente:

- ✓ Promover una cultura responsable del uso de las tecnologías de información y comunicación para mitigar el mal uso de la IA.
- ✓ Fomentar la elaboración de un código de conducta para capacitación de personal, sobre el uso ético de la IA en empresas que desarrollan este tipo de tecnologías.

- ✓ Implementar y controlar el acceso a tecnologías de desarrollo de IA para mitigar los usos indebidos de estas.
- ✓ Crear canales de comunicación con las autoridades federales o estatales para reportar usos indebidos de IA.
- ✓ El sector académico debe canalizar esfuerzos en la formación ética temprana de profesionales de ciberseguridad. Sobre los impactos del uso dual de la IA.

Antes de finalizar debemos tener presente que la llegada de este avance tecnológico supone un gran reto para México, ya que, lo que se origina en el mundo virtual, se puede extender al mundo real. Por lo que se debe culturizar, educar y concientizar a la población sobre los riesgos del uso dual de esta tecnología.

VIII. Conclusiones

Con base en lo presentado a lo largo de este documento, es importante que el Estado mexicano identifique los aspectos críticos de la nación, para que se diseñen estrategias que ayuden a hacer frente en alguna contingencia que ponga en riesgo la estabilidad del país, como lo son los sectores de banca, infraestructura digital, energía, transporte, administración pública e infraestructura espacial. Fortaleciendo todas aquellas áreas de oportunidad que se identifiquen en términos de ciberseguridad. Con base en este estudio hemos podido confirmar que no solo la tecnología evoluciona constantemente, ya que, también las estrategias y tácticas de los atacantes cibernéticos evolucionan al mismo ritmo y en ocasiones más rápido. Por lo que, el Estado mexicano debe incursionar en este campo, y estar un paso adelante. Con la implementación de medidas preventivas y ofensivas en caso de que las estrategias de la nación se vean comprometidas. Como bien sabemos los tiempos reactivos y proactivos son conceptos del pasado. Hoy en día vivimos en la era de la predicción, en donde gracias a las nuevas Tecnologías de la Información y Comunicación tenemos la oportunidad de anticiparnos a los hechos futuros.

Por otro lado, hemos comprobado que otras naciones están realizando una fuerte inversión en lo que se refiera a la seguridad cibernética, ya que, este dominio ha ganado terreno, demostrando que es un pilar de toda nación, lo que supone un riesgo potencial para quienes no estén preparados y por el contrario da poder a quienes estén a la vanguardia. Por lo que, nuestra nación no debe perder de vista contar con planes y medidas para enfrentar la era de la computación cuántica. Ya que esta supone riesgos en mundo digital e

incluso para los secretos de esta y cualquier otra nación. Por lo que se deben tomar medidas oportunas para no tener dependencia de terceros. Ya que, nuestro país cuenta con gente muy capaz para lograrlo.

En otro ámbito nuestra nación sigue su desarrollo en lo que compete al dominio del espacio exterior, si bien, México no es una potencia en este tipo de desarrollo tecnológico, es importante que todo proyecto tecnológico de este tipo cuente con controles de seguridad que garanticen su objetivo principal, sin poner en riesgo todas aquellas operaciones para las que brindan servicio. Ya que hoy en día dicha tecnología espacial es un pilar para un gran número de servicios críticos y necesarios que son utilizados por la sociedad civil día a día.

Sin embargo, el no contar con las medidas en este campo virtual, da la oportunidad a que una amenaza externa pueda explotar cualquier vulnerabilidad derivando en impactos económicos y a la seguridad nacional.

Adicionalmente la Inteligencia Artificial ha demostrado que no solo revolucionó nuestra era, por el contrario, ha puesto a prueba rápidamente a diversos sectores debido a que perdieron de vista que no solo traería beneficios a la sociedad, por el contrario, trajo nuevos retos debido a los malos usos que se le dan. Y para lo cual pocos estaban preparados. Por ejemplo, los primeros indicios han sido el uso de la Inteligencia Artificial para la generación de código malicioso sin la necesidad de tener conocimientos previos en temas de lenguajes de programación y computación. Pero todo ello fue debido a las pocas o nulas restricciones que se implementaron en esta nueva tecnología para mitigar el uso dual de la misma. Sobre todo, considerando que la Inteligencia Artificial sería utilizada en contra de nuestra misma especie. Ya que, vienen tiempos en los que se generarán nuevas armas químicas, herramientas que ayudarán a una persona mal intencionada a explotar vulnerabilidades tecnológicas de todo tipo. E incluso harán más difícil distinguir lo que es real o no. Ya que esta tecnología desde sus inicios demostró sus capacidades para alterar la realidad. Por lo que, nuestra nación debe prepararse para hacer frente a nuevas amenazas que vienen acompañando cada una de las nuevas tecnologías. Porque hay que tener presente que si bien hoy en día ya se comienzan a implementar controles para que la Inteligencia Artificial bloqueé o no proceda a peticiones que tienen como finalidad un mal uso, eso no quita que el ámbito militar y la ciberdelincuencia lo utilicen para tareas ofensivas constantes para la búsqueda y explotación de vulnerabilidades que pueden generar daños en el mundo cibernético y extenderse al mundo real.

Por último, debemos tener presente que las Tecnologías de la Información y Comunicación, son herramientas que nos ayudan a resolver y realizar procesos complejos. Pero como pudimos analizar en este documento, estos avances tecnológicos en las manos equivocadas pueden ser utilizados

de manera inadecuada. Por lo que hay mucho trabajo que realizar por parte de todos los habitantes de nuestra nación, para que juntos podamos educar y preparar a los futuros habitantes de México, quienes se deben mantener a la vanguardia de los cambios y exigencias tecnológicas mundiales.

XI. Referencias

Anónimo, “Historia de la Comunicación Humana”, disponible en: https://www.caracteristicas.co/historia-de-la-comunicacion-humana/ (fecha de consulta: 19 de marzo de 2022).

AIMX, “Estudio de Ciberseguridad AIMX 2021”, disponible en: https://irp.cdn-website.com/81280eda/files/uploaded/Estudio%20de%20Ciberseguridad%20AIMX%202021%20%28Pu%CC%81blica%29%2020210614.pdf (fecha de consulta: 19 de marzo de 2022).

Gómez, Vicente, “ESTUDIO COSTE DEL CIBERCRIMEN EN ESPAÑA”, disponible en: https://slideplayer.es/slide/17720821/ (fecha de consulta: 19 de marzo de 2022).

Vérgara, Jesus, “¿Qué países invierten más en Computación Cuántica?”, disponible en: https://neuroons.com/es/que-paises-invierten-mas-en-computacion-cuantica/ (fecha de consulta: 19 de marzo de 2022)

NSA, “Quantum Computing and Post-Quantum Cryptography”, disponible en: https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF (fecha de consulta: 19 de marzo de 2022).

Mink, Alan, “Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration”, disponible en: https://www.nist.gov/publications/quantum-key-distribution-qkd-and-commodity-security-protocols-introduction-and (fecha de consulta: 19 de marzo de 2022).

González, Izan, “La constelación de satélites españoles con cifrado cuántico para blindar a Defensa”, disponible en: https://www.elespanol.com/omicrono/tecnologia/20210515/constelacion-satelites-espanoles-cifrado-cuantico-blindar-defensa/581193099_0.html (fecha de consulta: 19 de marzo de 2022).

Rodríguez Ansorena, Tomás, “El fin de la realidad”, disponible en: https://nuso.org/articulo/el-fin-de-la-realidad/ (fecha de consulta: 19 de marzo de 2022).

NIST, “spear phishing”, disponible en: https://csrc.nist.gov/glossary/term/spear_phishing (fecha de consulta: 19 de marzo de 2022).

Anónimo, “Ransomware as a service (RaaS), una nueva amenaza a tu seguridad”, disponible en: https://protecciondatos-lopd.com/empresas/ransomware-as-a-service-raas/ (fecha de consulta: 19 de marzo de 2022).

Anónimo, “¿Qué es un ataque DDoS de rescate?”, disponible en: https://www.cloudflare.com/es-es/learning/ddos/ransom-ddos-attack/ (fecha de consulta: 19 de marzo de 2022).

Urbina Fabio, Lentzos Filippa e Invernizzi Cédric Dual use of artificial-intelligence-powered drug discovery”, disponible en: https://www.nature.com/articles/s42256-022-00465-9 (fecha de consulta: 19 de marzo de 2022).

INFOTEC
Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación

En su composición se usaron los tipos Arial 10.5/12/16. Gotham Condensed 12/22/32
Times New Roman Regular / Italic 12/13

La elaboración, producción, diseño, formación y edición estuvo a cargo de la Dirección Ejecutiva (**DE**) y la Dirección Adjunta de Innovación y Conocimiento (**DAIC**)