La ciber seguridad

en el mundo contemporáneo

UAEH®

Universidad Autónoma del Estado de Hidalgo

La ciberseguridad
en el mundo contemporáneo

Universidad Autónoma del Estado de Hidalgo

División de Extensión de la Cultura

La ciberseguridad en el mundo contemporáneo

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

Pachuca de Soto, Hidalgo, México

2024

Primera edición electrónica: 2024.

Abasolo 600, colonia Centro, Pachuca de Soto, Hidalgo, México, C.P. 42000.
Dirección electrónica: editor@uaeh.edu.mx.

ISBN: 978-607-482-860-3

Hecho en México/*Printed in México*

Este libro fue dictaminado por pares académicos.

Se agradecen los comentarios y sugerencias del Cuerpo de Asesores, ya que permitieron darle un mejor rumbo a esta publicación. De igual manera, se agradece profundamente a los dictaminadores del proceso evaluador, quienes con sus observaciones y comentarios enriquecieron esta obra, así como al equipo de coordinadores de esta obra: M. en C. Gonzalo Alberto Torres Samperio, Dr. Edgar Olguín Guzmán, Dr. Omar Domínguez Ramírez, Dr. Eduardo Cornejo Velázquez, y Dr. Joselito Medina Marín, quienes también organizaron el coloquio de Ciberseguridad.

Índice

Presentación

DR. OCTAVIO CASTILLO ACOSTA
RECTOR DE LA UAEH

La Universidad Autónoma del Estado de Hidalgo se enorgullece en presentar este notable compendio de ensayos y estudios titulado "La ciberseguridad en el mundo contemporáneo", el cual forma parte del esfuerzo permanente que realiza nuestra institución por ofrecer un producto académico de análisis e investigación en torno al tema de cada edición de la Feria Universitaria del Libro (FUL). Por esta razón, el presente compendio es una parte muy valiosa de nuestra misión de contribuir al avance del conocimiento y la innovación en temas cruciales para nuestra sociedad contemporánea.

En una era donde la tecnología y la digitalización han transformado todos los aspectos de nuestra vida diaria, la forma en que nos comunicamos, trabajamos, aprendemos y nos entretenemos, hasta cómo manejamos nuestras finanzas y accedemos a servicios esenciales, resulta fundamental tomar a consideración de manera rigurosa los desafíos y amenazas a los que nos enfrentamos.

La ciberseguridad se ha convertido en una preocupación global de primer orden. Los ataques cibernéticos, las brechas de seguridad y el robo de datos personales y corporativos son fenómenos cada vez más comunes y sofisticados. Estos eventos no solo ponen en riesgo nuestra información, también amenazan la estabilidad económica, la seguridad nacional y la confianza pública en las tecnologías digitales.

Como institución académica comprometida con el desarrollo y la protección de nuestra sociedad, la UAEH ha asumido el desafío de liderar iniciativas que fortalezcan la comprensión y la capacidad de respuesta ante estas amenazas. Este libro reúne una muestra de la obra de destacados académicos y expertos en el campo. Los lectores se encontrarán con un análisis exhaustivo de diversos aspectos de la ciberseguridad, desde los fundamentos teóricos y técnicos hasta las implicaciones legales, éticas, sociales y disciplinares.

Cada uno de los autores que ha contribuido trae consigo una vasta experiencia y un profundo conocimiento. Sus investigaciones y reflexiones nos ofrecen una visión integral y multifacética de la ciberseguridad. Este texto no solo es una obra académica, sino también un llamado a la acción. Estoy seguro de que nuestros lectores, desde estudiantes hasta profesionales y responsables en la elaboración de políticas públicas, tendrán una importante herramienta para reflexionar y considerar cómo pueden contribuir y participar en los contextos que este tema lleva implicados. La seguridad en el entorno digital es una responsabilidad compartida. Todos tenemos un papel que desempeñar, ya sea mediante la adopción de buenas prácticas de seguridad, el apoyo a la educación y la promoción del debate sobre estos temas, o la participación en iniciativas de investigación y desarrollo.

Expresar mi más sincero agradecimiento a todos los que han hecho posible la publicación de este libro. En primer lugar, a los autores, por su valiosa contribución y dedicación. Agradezco también al equipo editorial y a todos los colaboradores que han trabajado arduamente para que esta obra vea la luz. Un agradecimiento especial a los organizadores de la 36° Feria Universitaria del Libro, por brindarnos este espacio para compartir y celebrar el conocimiento. Sin duda, este libro servirá de inspiración para que más personas se involucren y conozcan todas las aristas de la ciberseguridad y de ese modo continúen generándose propuestas y proyectos que propicien un entorno digital más seguro y confiable.

Amor, orden y progreso
Dr. Octavio Castillo Acosta
Rector.

Presentación

DR. OTILIO ARTURO ACEVEDO SANDOVAL

La educación en ciberseguridad es esencial para prevenir ataques y minimizar los daños.

Hoy en día la tecnología está al alcance de casi todo el mundo, esta influye en la sociedad en aspectos tan variados como la agricultura, educación, política, trabajo o transporte, se trata de una herramienta que ha modificado la forma en la que la sociedad se desenvuelve; se emplea para comunicarnos, viajar, aprender, en resumen, para facilitar nuestra vida.

Las herramientas informáticas forman parte de la actividad cotidiana del ser humano, millones de datos circulan por la red todos los días en todo el mundo procedentes de servidores de sistemas de correo electrónico, redes sociales, herramientas para videollamadas, aplicaciones bancarias, entre otras; la creciente dependencia de las tecnologías digitales, aunque beneficiosas, pero podemos ser objeto a las estafas de ingeniería social, ataques de malware y al robo de contraseñas, lo que permite tener acceso a información sensible y a base de datos las cuales terminan vendiéndose al mejor postor en la darkweb.

Un ciberataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema Informático o dispositivo digital.

La falta de seguridad puede tener consecuencias desastrosas, el propio ser humano es el eslabón más débil de la cadena, James Scott investigador y cofundador del Instituto de Tecnología de Infraestructura Critica y del Centro de Estudios de Operaciones de Influencia Cibernética en Estados Unidos de Norteamérica reportó, que el reisomwer es único entre los delitos cibernéticos, porque para que el ataque sea exitoso, requiere que la víctima se convierta en cómplice voluntario después del hecho, por lo que se requiere educar a las personas en las buenas prácticas sobre el cuidado de la información personal, y el uso seguro de los medios de comunicación, almacenamiento de información y dispositivos digitales para establecer un primer obstáculo a los ataques de ingeniería social.

Se sabe que el objetivo de la ingeniería social es manipular o persuadir a las personas para que revelen información sensible o secreta que no debería ser revelada, descarguen un programa de computadora malicioso, visiten sitios web construidos como centros de recolección de información, envíen dinero a delincuentes o cometan serios errores poniendo en riesgo los activos o seguridad tanto personal como empresarial.

En cuestiones de ciberseguridad México se encuentra en el lugar 84 de 160 a nivel mundial con un índice de seguridad cibernética de 37.66 puntos sobre 100 cifras que deben alarmar tanto a dependencias gubernamentales como a las empresas.

De acuerdo con un estudio realizado el año 2022 denominado “el estado de reisonwer” indico que 200 organizaciones en México, el 74 % fue víctima de reisonwer, pagando un promedio de 482,446 dólares, solo en 2021 este tipo de ataque creció un 600 %.

Ejemplos de ataques cibernéticos en México, se tiene el realizado al Instituto Mexicano del Seguro Social, la secretaria de Hacienda y Crédito Publico, Petróleos Mexicanos, Banco de México, la Lotería Nacional, la Comisión Nacional de Seguros y Finanzas, entre otros. Expertos en ciberseguridad aseguran que lejos de que vayan a desaparecer estos ciberataques, están en aumento y tanto las dependencias gubernamentales como las empresas privadas en México tienen que protegerse.

La ciberseguridad desempeña un papel cada vez mas relevante en nuestra sociedad digital, su principal objetivo es proteger los sistemas tecnológicos y los datos privados contenidos en los mismos de cualquier tipo de amenaza, desde hackers maliciosos hasta virus informáticos, ataques de phishing o robo de identidad.

El futuro de la ciberseguridad dependerá de la capacidad para innovar y desarrollar soluciones que aprovechen estas tecnologías emergentes y mitiguen sus riesgos asociados. La ciberseguridad no solo son metodologías y herramientas tecnológicas, que eviten o mitiguen el riesgo de ciberataques, constituye un factor fundamental para la estrategia operativa, tanto de empresas, como de gobiernos, y de los hombres y mujeres a nivel personal, es tal la dimensión de la gravedad que se requiere de tres componentes estratégicos: el legal, el tecnológico y por supuesto el ético, que garanticen el resguardo y cumplimiento de los derechos humanos.

Es importante concienciar a la sociedad sobre la importancia de la ciberseguridad y fomentar una cultura de buenas prácticas en el uso de la tecnología; por tal motivo, la Universidad Autónoma del Estado de Hidalgo se ha caracterizado por abordar temas de actualidad y que

preocupan a miles de personas a nivel nacional e internacional; en esta ocasión, a través de la 36 edición de la Feria Universitaria del Libro presenta el libro "La ciberseguridad en el mundo contemporáneo" destacados académicos e investigadores presentan un análisis desde una perspectiva de su área de conocimiento sobre la visión que tienen sobre: i) Ingeniería Social y sus impactos en la Ciberseguridad; ii) El Método Cualitativo como Alternativa en Peritajes para Dispositivos de Interferencia de Señal; iii) Ciberseguridad; ¿Necesidad o Moda? El amplio espectro de la ciberseguridad; iv) La Ciberseguridad en la Adopción de la Industria 4.0; v) El proceso de democratización del internet y el surgimiento de la ciberseguridad; y vi) Ciberseguridad, Regulación y ética, Imprescindibles en la sociedad actual, el presente libro tiene el propósito de fomentar la seguridad de los datos personales, preservar la integridad de los dispositivos IoT, salvaguardar la privacidad de las redes de comunicación y el intercambio de datos, y garantizar el funcionamiento adecuado y continuo de los sistemas de información.

Uno de los principales beneficios de la ciberseguridad es la protección de nuestros datos personales, depende de cada uno de nosotros en disminuir el riesgo de ser afectados por un ciberataque, por lo que es recomendable el uso de contraseñas seguras, la encriptación de datos y la actualización constante de software, son algunas medidas que se deben tomar para proteger la información.

Ingeniería Social y sus impactos en la Ciberseguridad

Adolfo Arreola García[1][Anáhuac México, UNAM]

[1]Es profesor investigador en la Universidad Anáhuac México y profesor en la Facultad de Estudios Superiores Acatlán, dependiente de la Universidad Nacional Autónoma de México (UNAM). De igual manera, se desempeña como consultor independiente en política y estrategia de ciberseguridad. Sus líneas de investigación se enfocan en temas de seguridad nacional, ciberseguridad en todos los ámbitos, transformación digital y tecnología aplicada a la seguridad nacional. Es Doctor en Seguridad Internacional por la Universidad Anáhuac México.
Para contacto: adolfoarreola@yahoo.com.mx

Abstract. A pesar del creciente desarrollo de la tecnología, los sistemas continúan siendo vulnerables a la manipulación, la propaganda y el engaño. Esto no solamente es el resultado de una expansión de la superficie de ataque, las filtraciones de información o de un diseño que no considera a la ciberseguridad como algo prioritario, sino también de las vulnerabilidades humanas. Como resultado de esa amalgama entre tecnología y el ser humano, todos los sistemas tecnológicos incluyendo aquellos más avanzados dependen, en algún momento dado, de la acción humana, lo que conlleva de origen una vulnerabilidad independientemente de la plataforma tecnológica que se utilice o de los medios tecnológicos de protección implementados y convierte el arte de *hackear* al ser humano en un vector de ataque atractivo, redituable y efectivo. Bajo este contexto es pertinente cuestionarse ¿Cuáles son las características que convierten a la ingeniería social en una amenaza para la ciberseguridad? ¿Cómo se pueden mitigar los efectos negativos de la ingeniería social en la ciberseguridad?, que serán los ejes rectores de este trabajo. Por supuesto, que se requiere mayor investigación sobre el comportamiento humano en internet, para contar con elementos de juicio y toma de decisiones que den vida a modelos de ciberseguridad reforzados y enfocados en las acciones humanas en el entorno digital.

Keywords: ingeniería social, persuasión, engaño, manipulación, ciberseguridad

1. Introducción

El uso inicial de la ingeniería social puede vincularse con la llegada de la revolución industrial en el siglo XVIII. De hecho, en sus inicios la ingeniería social fue emparentada con la resolución de conflictos al interior de las empresas, privilegiando la intervención racional entre el capital y el trabajo. En ese momento, un buen negociador o mediador debía contar con habilidades sociales (relacionadas con la mejora industrial) que permitieran encontrar soluciones rápidas y eficientes a los problemas industriales [1]. Aunque ese es su origen, en el presente es conocido que la frase de ingeniería social se utilizó por primera vez en un ensayo del holandés J.C. Van Marken, pero fue difundido y popularizado posteriormente por Émile Cheysson [2].

En consecuencia, el término de ingeniera social tuvo su mayor impulso en EE.UU. tras la publicación del libro "*Social Engineering*" de William Howe Tolman (1909) que es el vivo ejemplo del esfuerzo por entender los problemas al interior de las empresas. De facto, la acción definida fue conocida, a carencia de mejor término, como “mejora industrial” y buscaba entender el sistema para lograr la máxima eficiencia y estudiar los problemas entre “vida y mano de obra de manera científica” [3]. Fue hasta 1990 cuando el concepto evolucionó para referirse a personas que llamaban por teléfono para engañar a otras con el objetivo de que revelaran información sensible o personal. Fue hasta ese momento cuando la ingeniería social se convirtió

en la herramienta preferida para hackear al ser humano, debido a sus características de bajo costo, riesgo mínimo y enorme ganancia que la hacen atractiva como vector de ciberataque.

Hoy en día y de forma general, se sabe que el objetivo de la ingeniería social es manipular o persuadir a las personas para que revelen información sensible o secreta que no debería ser revelada, descarguen un programa de computadora malicioso, visiten sitios *web* construidos como centros de recolección de información, envíen dinero a delincuentes o cometan serios errores poniendo en riesgo los activos o seguridad tanto personal como empresarial.

De esta forma, los correos electrónicos, las pláticas informales amistosas, las supuestas amenazas de las autoridades o una oferta demasiado buena para ser verdad se convierten en tácticas efectivas de ingeniería social que incluso podrían significar el comienzo de un ciberataque de mayores proporciones. Se puede aducir que, la ingeniería social es una práctica constante de engaño, defraudación y manipulación, que invita a tomar decisiones sin pensar.

Los impactos de la manipulación, propaganda y engaño en sistemas de seguridad no son desconocidos, pero siguen siendo un dolor de cabeza para los encargados, ya que su efectividad no ha disminuido, sino, por el contrario, ha ido en aumento. De hecho, de acuerdo con Malcolm Coxall las técnicas manipuladoras podrían incluir "el uso de falacias lógicas y técnicas de propaganda, implicando la supresión de información o exclusión de puntos de vista" para lograr que la gente no preste atención a ciertos argumentos o se enfoque en otra cosa [4]. Aunque cercanas, la manipulación y la persuasión no deben ser entendidas ni utilizadas como sinónimos. En un intento por mostrar la diferencia, es conveniente exponer las ideas de Dave Lakhani exponiendo la diferencia que existe entre persuasión y manipulación al decir que:

> La verdadera persuasión se basa en la verdad, la honestidad, la curiosidad y la capacidad de contar una buena historia y obtener los criterios de persuasión de aquellos a los que esperas persuadir para que puedas cumplir con sus expectativas fácilmente. La manipulación siempre es mala, y nunca funciona a largo plazo. [5]

Palabras en las que se expone el carácter negativo de la manipulación y lo positivo de la persuasión. En apoyo a lo antes expresado, Christopher Hadgany [6] afirma y agrega que influencia [persuasión] es "lograr que alguien desee hacer algo que quieres que haga", mientras que manipulación es "lograr que alguien haga lo que tú deseas".

La expansión de la superficie de ataque es otro elemento que abona a la dificultad para proteger de manera eficiente a los sistemas en el mundo digital y se suma a las vulnerabilidades existentes en el ser humano e incluso se puede afirmar que, adiciona algunas otras que serán aprovechadas por los ciberdelincuentes debido a la ignorancia de los usuarios finales acerca de las fortalezas y debilidades de los nuevos dispositivos integrados al sistema. Aunado a lo anterior, las filtraciones de información se constituyen en un claro ejemplo de que los sistemas de última

generación siguen conformándose sin tener en consideración la ciberseguridad desde el diseño ni las debilidades humanas al momento de implementar las actividades. Esto debe de cambiar y hay que poner al centro al ser humano como el objeto/sujeto de la ciberseguridad; porque es víctima de la ingeniería social.

Es por ello que, el objetivo del presente documento es identificar cuáles son las características que convierten a la ingeniería social en una amenaza a la ciberseguridad. Lo anterior se hace desde un enfoque cualitativo, para lograr identificar, a través de los diversos documentos consultados, aquellas características que hacen de la ingeniería un problema de ciberseguridad. De igual forma, el análisis del discurso, la revisión bibliográfica y el análisis comparativo son métodos útiles para lograr el objetivo propuesto. Al final, se busca una explicación para el comportamiento, características y motivaciones de las personas para engañar, persuadir o manipular a otros seres humanos a partir de lo expresado por terceros, así como de los detalles de la ingeniería social.

La organización y desarrollo del presente trabajo incluye en primera instancia una breve descripción de los términos de ciberseguridad e ingeniería social; se continúa con una clasificación de los ataques de ingeniería social y sus objetivos; posteriormente, se proporcionan algunas de las razones que justifican porque la ingeniería social es una amenaza para la ciberseguridad, y se termina emitiendo algunas conclusiones sobre el tema desarrollado y breves recomendaciones sobre como mitigar los efectos de los ataques de ingeniería social. De esta forma, se aportan algunos datos que permiten conocer un poco más sobre la ingeniería social y se reconoce la necesidad de continuar investigando sobre los pormenores y alcances de los ataques con ingeniería social en una época en la que sus capacidades se han visto potencializadas con el uso de la inteligencia artificial (IA). Lo importante es cuidar la fragilidad humana con ciberseguridad.

2. Como entender la ciberseguridad

La ciberseguridad con mucha frecuencia es relacionada única y estrictamente con temas tecnológicos; sin embargo, el concepto es por sí mismo un reflejo de las diferentes aristas que tiene el término de seguridad en el mundo material. Es decir, la ciberseguridad debe ser garantizada en los diferentes ámbitos del poder de los Estados o político-social; dicho de otra forma, económico, político, social, militar, tecnológico, psicológico y diplomático. Al tener la ampliación de la definición de ciberseguridad se pueden incorporar los elementos geográficos, virtuales, humanos, informáticos y tecnológicos, que de alguna forma coinciden con las capas del ciberespacio[1] que al fin y al cabo es el objeto de la ciberseguridad. En este sentido, algunos

[1] El *National Institute of Standards and Technology* (NIST) lo define al ciberespacio como "un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de

autores mencionan que el ciberespacio se compone de: "geografía, red física, red lógica, ciberpersona y persona" [7] incluyendo los diversos elementos inmersos en el ciberespacio; algunos otros lo hacen desde tres capas principales física, lógica y social.

Debido a lo anterior, la definición de ciberseguridad debe incluir diversos elementos ubicados en el ciberentorno y reconocer que el ser humano es un punto central en dicho sistema. Desde nuestro punto de vista y después de la revisión bibliográfica realizada, la definición más completa que se encontró es aquella que se establece en la Resolución 181 de la Unión Internacional de Telecomunicaciones (UIT) de 2010, que a la letra dice:

> 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. [8]

Definición en la cual se pueden resumir los elementos constitutivos de las diversas capas que componen al ciberespacio y la importancia del ser humano.

De esta forma, desde la definición de ciberseguridad se afirma que, de una forma u otra, se protegen todos los flancos con instrumentos diversos para tener un sistema de protección integral, multidisciplinario, multicapas y holístico. Se debe enfatizar que, es de particular importancia incluir al ser humano, dado que, por experiencia y estadística, es particularmente importante para preservar la ciberseguridad, por ser en este caso el blanco primario de los ataques de ingeniería social.

3. Definir la ingeniería social

El concepto de ingeniería social surge en la segunda mitad del siglo XX como una forma de poder solventar los problemas existentes entre trabajadores y empleadores. La ingeniería social nace con 2 propósitos principales, 1) esfuerzo para influir en actitudes, relaciones y acciones sociales y 2) como un medio llevar programas de modificaciones sociales a las clases trabajadoras que posteriormente evoluciona siendo "vinculada con la propaganda y prácticas de manipulación que buscaban controlar la opinión pública" [9], palabras en donde se puede ver la convergencia de manipulación y persuasión.

sistemas de información que incluyen Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados" [50]. Definición que es una guía inicial para posteriores desarrollos.

Hasta ahora no se cuenta con una definición de ingeniería social única, pero es a partir de las más populares que se puede interpretar su alcance e identificar los elementos básicos que la componen. De acuerdo con Christopher Hadgany la ingeniería social es "cualquier acto que influye en una persona para que realice una acción que puede o no ser lo mejor para él o ella" [10] que, aunque muy general, conlleva el hecho que la ingeniería social no siempre es negativa. Segundo, para Kevin Mitnick (2002) [11], la ingeniería social utiliza la persuasión y la influencia, por lo que se convierte un conjunto de técnicas empleadas para convencer y persuadir a la gente de que soy alguien que en realidad no soy; por lo general, el objetivo será obtener información sensible que me dé oportunidad de realizar algún movimiento o transacción ilegal para mi propio beneficio [12].

Tercero, para Richard Kissel la definición de ingeniería social queda como "el intento de engañar a algún individuo para que revele información (por ejemplo, una contraseña) que puede ser utilizada para atacar los sistemas o redes" [13]. Mientras que para Sara Granger en su página Social *Enginering Fundamentals*, *Part I: Hacker Tactics*, la ingeniería social se define como "el arte y la ciencia de hacer que la gente cumpla con tus deseos" [14]. Todos teniendo en común hacer que otro haga algo por nosotros, aún a pesar de su voluntad por medio de la persuasión, manipulación o engaño.

Por lo tanto, debido a esa inexistencia de una definición universal y considerando los pormenores que detallan las antes mencionadas, la definición que aquí será adoptada fue brindada por Paul Grassi, Michael Garcia y James Fenton en 2017; en sus palabras dice:

> El acto de engañar a un individuo para que revele información confidencial, obtener acceso no autorizado o cometer fraude al asociarse con el individuo para ganar credibilidad y confianza. [15]

Término que incorpora los elementos distintivos de la ingeniería social que tiene por objetivo engañar, para comprometer información sensible, hacerse con credenciales de acceso u obtener beneficios económicos con o sin la participación de la víctima. Con base en ello, se debe repensar qué hacer para mitigar los impactos de los ataques de ingeniería social y preguntarse si ¿será suficiente con educar a los usuarios? O ¿debe adoptarse un modelo mixto/ecléctico de ciberseguridad? Lo cual parte de una revisión de los vectores de ataque conocidos de la ingeniería social.

4. Hackear al ser humano: tipos de ataques y objetivos

En el contexto actual, hackear al ser humano se ha convertido en una alternativa muy atractiva para quienes buscan hacerse con información sensible, utilizar medios no técnicos de infiltración a los sistemas de ciberseguridad o simplemente burlar las tecnologías más sofisticadas al utilizar al eslabón más débil como la puerta de entrada.

En consecuencia, se deben de conocer algunos de los muchos detalles que se encuentran en los diversos formatos o tipos de ataques de ingeniería social para implementar medidas que puedan contrarrestar el logro de su principal objetivo, que es engañar la voluntad humana. Con ello se busca proteger al usuario mientras navega en internet o maneja (de forma segura) información personal, profesional o institucional sensible. Particularmente, en una sociedad que promueve hacer nuestra vida pública y contar a todos sobre el diario acontecer.

Conocer los tipos de ataques de ingeniería social es una condición indispensable para comprender sus alcances, costos y objetivos. En este sentido, de acuerdo con Kaspersky [16] los tipos de ataques de ingeniería social incluyen, aunque no se limitan, a: el anzuelo (*baiting)*, *pretexting*, *phishing*, *vhising*, *smishing*, *spam* y hackeo del correo electrónico. Kaspersky [17] deja en claro que los planes sencillos incluyen un ciclo de ataque bien determinado con entrada, robo de información y salida del sistema; mientras que los ataques más sofisticados requieren de entablar una relación con la víctima y un periodo de tiempo más prolongado para lograr el objetivo.

Al final, se debe de recordar que, los ataques con ingeniería social son difíciles de contrarrestar por haber sido diseñados para tomar ventaja de las debilidades humanas que surgen de la curiosidad, el antagonismo, el desprecio, el respeto por la autoridad y el deseo de ayudar. Es empleando las emociones humanas como se rompe el cerco de seguridad.

Las tácticas del engaño provocado con ingeniería social requieren del empleo de motivadores básicos que inviten al usuario a brindar la información voluntariamente a fin de evitar la violencia física o ataques de fuerza bruta. De acuerdo con el Dr. Robert Cialdini estos motivadores son: reciprocidad, orientación social, consistencia, aceptación, autoridad y tentación [18]. Dichos elementos antes citados son considerados la columna vertebral de los ataques de ingeniería social y se correlacionan con los rasgos característicos de la complejidad de dichos actos. Remarcando que la efectividad de dichos ataques se fundamenta en la recolección de información de fuentes abiertas puesta por la víctima en diversos lugares o medios.

En relación con su propósito, es bien sabido que el principal objetivo de la ingeniería social es "explotar al eslabón más débil de la organización, el usuario" [19] para colarse en cualquier sistema de seguridad. Esto se logra al apoderarse (a través del engaño) de información sensible de alto valor que puede ser explotada posteriormente para obtener beneficios económicos, tecnológicos, políticos y bajo algunos contextos dañar la reputación de las personas, organizaciones e incluso Estados.

En consecuencia, la persistencia existente para hackear al ser humano se convierte en uno de los argumentos para considerar a la ingeniería social como una amenaza a la ciberseguridad. Lo anterior se ve respaldado y amplificado por las tendencias observadas durante los últimos años, en donde los ataques con ingeniería social siguen al alza. Por ejemplo, Irina Shimko *et al*. (2023) [20] mencionan para 2022 que:

- El 48,63% de los correos electrónicos en todo el mundo y el 52,78% en el sector ruso de Internet fueron spam.
- El 29,82% del spam provino de Rusia.
- Nuestro antivirus de correo electrónico bloqueó 166 187 118 archivos adjuntos maliciosos.
- El sistema antiphishing impidió 507 851 735 intentos de seguir enlaces de phishing.
- 378 496 intentos de seguir enlaces de phishing estaban vinculados con cuentas de Telegram robadas.

Irina Shimko *et al.* [21] resaltan además que los cibercriminales aprovechan eventos mundiales de gran relevancia como medios de engaño (caso el mundial de Qatar 2022, lanzamiento de la película Batman, las nominaciones a los premios Oscar, el conflicto entre Rusia-Ucrania, la pandemia entre otros). Momentos en que los usuarios bajan la guardia dada la importancia de los eventos y las emociones que estos exaltan. Por ello, es conveniente reflexionar sobre la importancia e impacto de los ataques de ingeniería social para los sistemas de ciberseguridad, así como en las variantes que podrían adoptar para lograr sus objetivos.

En breve, existen cuatro vectores principales de ataques con ingeniería social: *smishing*, *vishing*, *phising* y usurpación de identidad; y, las estadísticas muestran que los ataques con estos vectores no han disminuido, sino simplemente adaptado sus tácticas a las nuevas realidades.

5. ¿Por qué la ingeniería social es una amenaza para la ciberseguridad?

Muchas son las razones que pueden esgrimirse para aseverar que la ciberseguridad sufre debido a la amenaza que representa la ingeniería social; pero, al final, todas ellas se orientan a hacer notar que el ser humano es débil y fácil de engañar. Particularmente, esto se realiza con base en el hecho de que es complejo mantener al elemento humano permanentemente consciente de la importancia de su actuar seguro en sus actividades realizadas en el ciberespacio, al mismo tiempo que se suprime su tendencia natural a confiar en otros, ser curioso o tener miedo a ciertas cosas.

Además, es preciso señalar que existen algunos rasgos característicos que les dotan de la complejidad que presumen los ataques de ingeniería social, entre ellos se encuentran que: enaltecen las emociones, falsifican la dirección del remitente, muestran peticiones extrañas de amigos, vinculan a sitios web no profesionales, son demasiado bueno para ser verdad, traen consigo documentos adjuntos sospechosos, muestran un remitente cuestionable, toman ventaja de la urgencia, atemorizan al usuario y se niegan a contestar nuestros cuestionamientos. Elementos que, separados son de por sí difíciles de detectar, conjugados se convierten en un medio exitoso para infiltrarse en cualquier sistema.

De esta manera, en este apartado se mencionará primeramente el hecho de que la ingeniería social ataca al eslabón más débil que es el ser humano; posteriormente, se menciona que existen diversos vectores de ataque y técnicas que son utilizados por la ingeniería social para llevar a cabo sus ciberataques; continuando con la mención de la importancia de la inteligencia artificial en la construcción de ataques de ingeniería social y su dificultad para ser detectados. Finalizando con algunas estadísticas sobre la probada efectividad de los ataques con ingeniería social.

No es nuestra intención hablar de todas las aristas de la ingeniería social como amenazas a la ciberseguridad, sino simplemente dar algunas muestras de los impactos que genera y la forma en que trastoca a la sociedad internacional. Recordando que, la complejidad de los ataques de ingeniería social incluye la huella digital existente de la víctima, que es la base de la construcción del ataque.

5.1. La ingeniería social ataca el eslabón más débil de la cadena de seguridad

Como ha sido expresado, la ciberseguridad conceptualizada de forma integral y holística incluye al ser humano como parte fundamental del sistema. De hecho, desde esta perspectiva, los elementos del ciberentorno que deben ser objeto de la ciberseguridad incluyen información, equipos, procesos, lugar geográfico y personas. De esta forma, la ciberseguridad se convierte en un concepto holístico, sistémico e integral que cubre aspectos geográficos, informáticos,

tecnológicos y humanos. Siendo este último elemento el objetivo primario de la ingeniería social que busca explotar las debilidades, las emociones y vicios de los seres humanos para poder acceder a los sistemas ciber seguros [22], [23], [24] y materia de protección intensiva/exhaustiva.

De esta forma se puede afirmar que, todo sistema de ciberseguridad es tan seguro como lo es su eslabón más débil [25] y que los ciberataques de todo tipo, incluyendo los de ingeniería social, se concentrarán en este punto. Por lo tanto, siendo esto una realidad innegable, en el caso que nos atañe, el ser humano debe ser educado para tomar conciencia de los riesgos y hacer todo lo posible para preservar la ciberseguridad ante ataques de ingeniería social. Lo anterior hace imprescindible "formar a sus empleados [usuarios] en medidas higiénicas de ciberseguridad" [26] y emprender medidas para la concienciación en ciberseguridad de usuarios finales, proveedores y terceras partes.

Lo anterior es necesario, ya que según Cristian Borghello "las técnicas de engaño conocidas mundialmente y vigentes desde los inicios de la humanidad, sólo deben ser adaptadas al nuevo medio por el cual las personas maliciosas apuntan a concretar sus ataques" [27] que enfatiza la continuidad de las debilidades humanas. Esto además remarca que "toda persona padece las mismas debilidades dentro y fuera del sistema informático o de la red de trabajo" [28] que llevan los riesgos hasta la vida personal y el entorno familiar.

De esta manera, el ser humano se convierte en la primer línea de defensa o de ataque de un sistema de ciberseguridad, por lo que es preciso educarlo en las diversas técnicas de ingeniería social y prepararle para adoptar las mejores prácticas de protección. Además, para fortalecer la defensa y debido a que la ingeniería social se basa en el engaño e influencia, deben ser revisados y comentados con lujo de detalle los seis principios de la persuasión enunciados por Robert Cialdini, Roselle Wissler y Nicholas Schweitzer que incluyen: la aceptación, la autoridad, la escasez, la consistencia, la reciprocidad y la aceptación social [29] para construir un sistema consciente sobre el impacto de los ataques de ingeniería social y sabedor de las debilidades propias. El autoconocimiento es esencial para una buena lectura de las personalidades y comunicación efectiva en la ingeniería social.

Particularmente, dicha revisión detallada debe hacerse porque dichos principios de la persuasión son utilizados por un ingeniero social hábil y exitoso para tener influencia efectiva en las personas, cambiar opiniones, manipular decisiones y vulnerar cualquier sistema de seguridad. Ante esta situación, es preciso enfatizar que los seis principios serán utilizados de manera conjunta para tener el mayor impacto posible en las víctimas, tanto para bien como para mal [30]. En resumen, no se puede olvidar que la ingeniería social tendrá por objetivo al ser humano en todo momento y que bombardeará constantemente la psique de los usuarios, buscando doblegar incluso al mejor, más consciente y más preparado.

Esto enfatiza un rasgo característico de los sistemas de ciberseguridad, el cual indica que la ofensiva solamente requiere de un error/negligencia/oportunidad para infiltrarse y la defensa debe ser efectiva en todo momento. Lo que lleva a pensar que, sin importar el vector de ataque, la fortaleza de un sistema radica en su propia defensa.

5.2. La ingeniería social tiene una gran variedad de vectores y técnicas de ataque

Para comprender la importancia de los vectores de ataque de la ingeniería social es preciso definir lo que se debe de entender como vector de ataque, ya que este es frecuentemente confundido con la técnica o medios de ataque. De esta forma, para nosotros el vector de ataque será el medio por el cual un ciberatacante hace llegar un programa malicioso a la víctima. Con base en esta definición se puede afirmar que los medios que utiliza la ingeniería social como vectores principalmente son: el correo electrónico, las vulnerabilidades del sistema, navegadores web, puntos de venta, aplicaciones digitales, malas configuraciones de programas, credenciales comprometidas o robadas, contraseñas débiles, carencia de cifrado, trabajadores o personal interno y debilidades en la cadena de suministro.

En el mismo tenor, aunque poco distantes de lo antes señalado, desde el punto de vista de la compañía de ciberseguridad Cloudfare, los vectores de ataque se clasifican como "ataques de ingeniería social, el robo de credenciales, el aprovechamiento de vulnerabilidades y la insuficiente protección contra las amenazas internas" [31]. Los medios anteriores se combinan o complementan a través de una diversidad de técnicas que de acuerdo con algunas clasificaciones se centran en acciones de reconocimiento, desarrollo de un recurso, acceso inicial, ejecución, persistencia, escalada de privilegios, evasión de sistemas de defensa, credenciales de acceso, descubrimiento y movimiento lateral, entre otras. Todas ellas son categóricas y pudieran englobar algunas otras más específicas como: ver por encima del hombro, spam, búsqueda en la basura, pharming, entre otras.

De esta manera, debido a las múltiples combinaciones posibles, se hace evidente la complejidad de los ataques que pudieran ser elaborados a partir de la información obtenida por medio de la ingeniería social. Para mostrar lo citado y la necesidad de elegir apropiadamente la herramienta/medio de ataque, por ejemplo, el phising se realiza a través del correo electrónico, el smishing por medio de mensajes SMS, pero el vishing se lleva a cabo por medio de la telefonía utilizando la voz. Esta variación en los medios hace que el escenario cambie, el ciberatacante se adapte y al final estos ataques sean una variante del mismo en diversos medios de comunicación que hacen menos o más compleja la tarea.

A lo anterior habría que sumar ataques por medio de fuerza bruta para intentar adquirir los privilegios de una cuenta; aquellos enviados por medio de documentos adjuntos con programas maliciosos que se ejecutan poco después de que el usuario abre el correo; las amenazas internas que se han convertido en un medio muy redituable para obtener información sensible ya sea de forma voluntaria o involuntaria o como el elemento vital que permite voluntariamente que se lleve a cabo un ciberataque, y por supuesto el más letal en los últimos años el ransomware. No serán los únicos vectores ni técnicas que se empleen por los ingenieros sociales, pero son una muestra del peligro que representan; que, dicho de paso, se ha visto incrementado exponencialmente por el uso de inteligencia artificial.

5.3. Con el empleo de la Inteligencia Artificial (IA) se potencializa el peligro que representa la ingeniería social

La llegada de la inteligencia artificial y su empleo por los ciberdelincuentes para mejorar la redacción y estructura del mensaje preparado para convencer y/o persuadir a las víctimas en turno es algo que se ha venido experimentando durante los últimos años. El detalle puesto por la inteligencia artificial en las palabras y el alcance de estas han logrado que los ciberataques, en particular los de ingeniería social, tengan mayor tasa de éxito.

Esto es particularmente cierto porque la inteligencia artificial generativa es capaz de ser entrenada para copiar el estilo de redacción, la voz y el lenguaje natural de cualquier persona. De acuerdo con Mariano Manfredi "es importante conocer cómo la IA está siendo utilizada en estos ataques [ingeniería social] y tomar medidas de seguridad para proteger nuestra información personal" [32]. Lo anterior es un llamado a reconocer las capacidades que trae consigo la IA y que son utilizadas para desarrollar más y mejores ataques de ingeniería social.

De conformidad con Mariaia (2022) "un ejemplo notable de un ataque de ingeniería social con IA es el robo de 35 millones de dólares, en el que los delincuentes utilizaron un sistema de *chatbot* que se hizo pasar por una empleada de la empresa y engañó a otra empleada" [33]. Es muy preocupante que la inteligencia artificial esté siendo utilizada para hacer más sofisticados y casi indetectables los ataques de ingeniería social que ahora no solamente utilizan el *phishing*, sino también los *deep fake*[2] o, como el ejemplo, los *chatbots*. Incluso este tipo de usos ha despertado el interés de las potencias mundiales en tecnología y representa una de las nuevas áreas que debe ser estudiada a través de la geopolítica.

En este sentido, por ejemplo el presidente ruso Vladimir Putin expresó que, la Inteligencia Artificial (IA) "es el futuro, no sólo para Rusia, sino para la humanidad", ya que trae consigo "oportunidades colosales, pero también amenazas difíciles de predecir" y que "quien sea capaz de liderar esta esfera liderará el mundo" [34]; afirmaciones que permiten recordar la importancia del desarrollo tecnológico en IA para la nueva realidad internacional y su conexión con visiones geopolíticas previas. De igual forma, de las palabras de Putin se infiere que las potencias mundiales harán uso de la inteligencia artificial para generar ataques de ingeniería social mucho más efectivos y complejos que les permitan contar con la ventaja en el campo de batalla.

De hecho, la sociedad internacional considera necesario contar con un marco jurídico que regule el empleo de la IA como arma de engaño y ataque; incluso, personajes como Bill Gates o Elon Musk, o instituciones como el Parlamento Europeo, hayan comenzado a evaluar y advertir sobre

[2] Es una técnica de inteligencia artificial que se basa en la síntesis de imágenes; puede ser una imagen, un vídeo o sonido que imita lo que hace cualquier persona.

los riesgos de la IA [35]. Desde otra perspectiva, pero confirmando la tendencia en el uso de la IA por los diferentes actores del sistema internacional, el barómetro de Allianz 2023 pone a los ciberincidentes en el primer lugar de los riesgos que enfrentan las empresas [36], lo cual lleva a pensar que potencialmente la mayoría de ellos serán iniciados con ingeniería social debido a su bajo costo, gran impacto y probada efectividad.

5.4. La ingeniería social es un ataque con probada efectividad

La ingeniería social representa una preocupación para los sistemas de ciberseguridad, dado que es un método de ataque que ha dejado en claro su efectividad y eficacia. Que, además, como se mencionó arriba, cuando se combina con la IA potencializa sus impactos negativos a tal grado que "se ha llegado a estimar que un ciberataque global pudiera llegar a generar pérdidas de 50 billones de dólares" [37]. Algo que habla de la importancia de contar con medidas preventivas, correctivas y de mitigación/corrección de los daños causados por ataques de ingeniería social.

En los números se sabe que la tendencia en la cantidad de ataques de ingeniería social va en aumento y que durante el 2021 fue responsable del 98% de los ataques. De acuerdo con Carolina González Valenzuela (2022) [38]:

> Más del 70 % de las violaciones de datos comienzan con phishing o ingeniería social. Google registró más de 2 millones de sitios web de phishing en 2021. Aproximadamente el 43 % de los correos electrónicos falsos suplantan a grandes organizaciones como Microsoft.

Estadísticas que son un ejemplo claro del impacto que tienen los ataques con ingeniería social en los diversos ámbitos del quehacer humano y las compañías que suelen ser los mejores o más sustanciosos blancos.

Según la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés), la ingeniería social cuesta a las organizaciones 1.600 millones de dólares en todo el mundo [39]. De hecho, el mismo FBI afirma que "los cibercriminales robaron $6.9 mil millones de dólares en 2021, utilizando ingeniería social" [40]. Cantidades que con mucha seguridad irán en aumento durante los próximos años.

Esto enfatiza los riesgos que trajo consigo el uso intensivo de los medios digitales durante la pandemia, particularmente por la ampliación de la superficie de ataque y la suma masiva de usuarios con poca cibercultura. De esto se puede inferir que, las principales razones que hicieron

de la ingeniería social un medio idóneo de ataque a partir del 2021 fueron las condiciones de trabajo en línea adoptadas durante la pandemia.

Cabe señalar que la población más vulnerable a los ataques de ingeniería social fue la de los adultos mayores y por supuesto la de los analfabetas digitales que tuvieron que adoptar nuevos hábitos de comunicación, compra, estudio, convivencia y trabajo sin una concienciación suficiente y oportuna sobre los riesgos que trae consigo la transformación digital. El informe del FBI *Internet Crime Report 2022*, reportó que "51,829 personas se vieron afectadas en 2021 por filtraciones de datos, lo que representa un aumento del 14% con respecto al año anterior" [41] estadísticas que hablan del éxito y costo de los ataques con ingeniería social.

Las estadísticas aquí presentadas hablan por sí solas del serio impacto que tiene la ingeniería social en la economía y la confianza de los usuarios de los servicios de internet, comercio electrónico, actividades financieras, medios de comunicación y teletrabajo. Por desgracia, los ataques de ingeniería social pueden quebrantar cualquier tipo de sistema de ciberseguridad que, aunque utiliza lo último en tecnología de protección, olvida el fortalecimiento de la computadora más perfecta, el ser humano.

Por ello, se debe adoptar un modelo de ciberseguridad holístico, integral y sistémico que busque privilegiar las medidas preventivas en lugar de las reactivas a partir de una estrategia basada en el conocimiento preciso, oportuno y detallado del entorno, factores y actores.

En resumen, la ingeniería social ha sido y sigue siendo un tipo de ataque exitoso que se encuentra en el arsenal de los ciberdelincuentes. A partir de la tendencia mostrada en los últimos años se puede predecir que los ataques con ingeniería social irán en aumento, serán más sofisticados, recurrirán a la inteligencia artificial como un medio de sofisticación/mejora y pondrán en jaque a los diversos medios y herramientas de ciberseguridad.

5.5. Dificultad para detectar ataques de ingeniería social pone en riesgo la ciberseguridad

Los ataques de ingeniería social son particularmente difíciles de contrarrestar, ya que están diseñados a modo y/o personalizados para aprovechar las debilidades y emociones humanas como son la curiosidad, el respeto por la autoridad, el deseo por ayudar, la empatía con otros seres humanos, la urgencia y el temor a perder una oportunidad, cometer un error, faltar a un compromiso o aparecer en listas negras de diversas instituciones financieras.

Del mismo modo, los ataques de ingeniería social son particularmente efectivos debido a que no se cuenta en gran parte de las empresas u organizaciones con sistemas que detecten y monitoreen cambios de conducta o hábitos de los usuarios en tiempo real. En caso contrario, cambios bruscos en la forma de actuar, operar, escribir, navegar, transmitir y responder pueden ser indicadores tempranos de que un ataque de ingeniería social está llevándose a cabo. Sin embargo, dado que el ser humano está expuesto tanto dentro de la empresa como fuera de ella a los ataques de ingeniería social, para eficientar la protección y monitoreo de la conducta el sistema de ciberseguridad es preciso considerar que el usuario está en todo momento como potencial blanco de potenciales delincuentes que busquen manipular su mente.

De acuerdo con James Mackay existen cinco señales típicas que avisan de un potencial ataque de ingeniería social y estas son: un anexo o enlace inesperado, una petición inusual, una petición o demanda urgente, una oferta demasiado buena para ser verdad y una petición de alguien que no reconoces [42]. Señales que, como se ha expuesto, no se presentan únicamente a través de medios digitales de comunicación, sino también por medio de ataques en persona. En este sentido, Rafael Marín recuerda la existencia de algunas estrategias de gestión de riesgos que tienen impacto en la ingeniería social que ya se encuentran disponibles, como son MAGERIT, ISO 31000, ISO 27001 entre otras [43].

Al final, es muy difícil detectar los ataques con ingeniería social porque manipulan nuestra conducta en el diario acontecer en cualquier ámbito de la vida a partir de nuestra propia información; demostrando que mientras no se tenga un sistema de ciberseguridad que detecte los cambios de conducta, emociones y hábitos, los correos maliciosos, las nuevas técnicas de engaño, los exploits y las vulnerabilidades de los usuarios y/o sistema en tiempo real, la detección de los ataques de ingeniería social serán un dolor de cabeza y un gran hoyo en el bolsillo de personas, organizaciones y Estados.

6. Como mitigar los efectos de la ingeniería social en la ciberseguridad

Ante los ataques de ingeniería social no todo está perdido, tanto los individuos como las organizaciones o Estados pueden adoptar medidas de mitigación de los efectos de un ataque. A continuación se presentan algunos de los consejos que pueden servir para contrarrestar o mitigar los efectos negativos generados por los ataques de ingeniería social. No son una fórmula precisa ni mágica que deba ser adoptada al pie de la letra, sino una visión generalizada de las buenas prácticas empleadas a nivel internacional como una técnica efectiva.

La primera recomendación se centra en la educación digital y en la construcción de una cultura de ciberseguridad incluyente, que busquen fortalecer al elemento humano de la ciberseguridad. Para tal efecto, es preciso incorporar programas que brinden información precisa y oportuna a

la población sobre los riesgos e impactos negativos que tienen los ataques con ingeniería social en el día a día. Lo anterior recuerda que "la herramienta más eficiente con la que cuentan las organizaciones para contrarrestar la ingeniería social es la concientización" [44], que pide tres cosas: que el usuario identifique la importancia de su labor, esté consciente del valor de la información y la responsabilidad que tiene para con el buen uso del sistema.

También, sería conveniente implementar protocolos de respuesta ante ataques de ingeniería social que conlleven la participación activa de los ciudadanos y establezcan con claridad el rol que cada uno debe asumir para romper el ciclo de los ataques. De esta forma se asume que la ciberseguridad es un trabajo de todos, por todos y para todos.

La segunda recomendación está orientada a la selección del capital humano. Es preciso que para minimizar la amenaza que representan los actores amenaza internos se cuente con un proceso de selección de personal más eficiente; así como, con un protocolo de seguimiento y vigilancia de las conductas esperadas en los miembros del equipo. Estas medidas son un intento por acotar la contratación de personas que buscan solamente obtener beneficios ilegales a partir de su función dentro de una organización y por identificar conductas potencialmente lesivas. No se pide contar con una bola de cristal para leer la mente de los trabajadores o predecir ataques, sino contar con un sistema de ciberinteligencia que permita tomar decisiones informadas en relación con la conducta de los miembros de la organización y el buen funcionamiento interno.

Una tercera recomendación tiene que ver con los hábitos de higiene digital que deben ser generados en todos y cada uno de nosotros. Lo que enfatiza la importancia de la cibercultura y las buenas prácticas en el ciberespacio.

Lo anterior pide, no solamente la concientización del personal para que evite entre otras cosas dar clic en documentos adjuntos de correos electrónicos desconocidos o sospechosos, seguir las cadenas enviadas por redes sociales, verificar la seguridad de la red wifi y de los sitios web que se visitan, confiar en personas que acaba de conocer o sospechar de tratos demasiado buenos para ser verdad; sino, también conlleve buenas prácticas para la actualización/adquisición de tecnología de ciberseguridad como antivirus o firewalls, el establecimiento de políticas de cuidado de la información y borrado seguro, la salvaguarda de las contraseñas, la observación del entorno antes de hacer uso de los dispositivos electrónicos, la actualización programada del sistema operativo y la verificación de la seguridad que ofrecen tanto las redes como los sitios web.

Finalmente, sabedores de que los ataques con ingeniería social no son un fenómeno exclusivo del mundo digital, se debe extender la protección o círculo de seguridad más allá del área de

trabajo y a diversos escenarios del mundo físico. Esta medida busca contrarrestar el pensamiento popular que prioriza la seguridad en el lugar de trabajo, pero olvida la seguridad en nuestro entorno familiar o social. Lo anterior se fundamenta en el hecho de que los ingenieros sociales utilizan las noticias, las tendencias en redes, los temas populares, los personajes de moda, los líderes mundiales, las catástrofes mundiales y todo aquello que atraiga la atención de grandes audiencias para hackear al ser humano.

Como sustento de lo anterior, Borghello menciona que "la lluvia de correos sobre las tormentas en Europa del 2007 confirma la efectividad de la Ingeniería Social" dado que permitió la propagación del programa malicioso Nuwar que logró conformar una gran *Botnet* con millones de usuarios infectados [45].

Otro ejemplo sería lo que informa Kaspersky, según Tatyana Kulykova *et al*. (2021) [46], en diferentes informes realizados para los años 2020 y 2021 indicando que los cibercriminales utilizaron los eventos deportivos como la Eurocopa de fútbol, los Juegos Olímpicos en Tokio y la Fórmula 1 para lograr sus objetivos diseñando sitios web fraudulentos de venta de boletos y suscripciones de acceso por internet. Todo lo cual se ve fortalecido con lo mencionado por It Digital Security (2023) [47] que afirma "los ataques de phishing se incrementaron a nivel mundial casi un 50% en 2022".

En el mismo sentido y fortaleciendo la visión de la posverdad que agrega un grado de complejidad a la interpretación de la vida y genera incertidumbre, Elías Todorovich habla de la creación de una nueva realidad a partir de las redes sociales que se convierten en referencias indiscutibles, ya que "no se les cree ni a los científicos de primera línea, referentes en sus disciplinas, pero sí, se cree en un mensaje que llega por Whatsapp sin la más mínima referencia, sin autoría, imposible de chequear" [48]. Lo que genera el caldo de cultivo para los ataques con ingeniería social porque alteran las emociones, genera desinformación y aumenta la incertidumbre.

Todo lo antes citado permite asumir que "la tecnología persuasiva tiene como objetivo cambiar el comportamiento de personas a través de diferentes técnicas de persuasión e influencia social" [49] que se ve complementada con otras actividades de ingeniería social para motivar la reacción inconsciente del elemento humano. En breve, los ataques de ingeniería social no han cesado, sino por el contrario, han ido en aumento alrededor del mundo con nuevas tácticas e instrumentos de engaño. La cuestión es si con las medidas actuales se podrán minimizar los impactos inferidos por los ataques de ingeniería social o si es preciso contar con un programa intensivo de capacitación/educación en tácticas de ingeniería social de alcance nacional e incluso internacional que motive que el usuario brinde el debido valor a la protección de su

información. Paradógicamente, sería utilizar las mismas tácticas de ingeniería social para impulsar al usuario como la primer línea de defensa.

7. Conclusiones

La complejidad y efectividad de los ataques de ingeniería social hacen pensar que no existe tecnología capaz de proteger a los sistemas informáticos; y dejan en claro que tampoco existen expertos o usuarios que estén exentos de este tipo de ataques. Esto reafirma que la ingeniería social está aquí para quedarse y ser utilizada profusamente con fines diversos.

Se puede asumir que la ingeniería social es el uso premeditado y malicioso de técnicas y medios preexistentes para manipular la mente, acciones y opiniones de las personas con el objetivo de lograr que realicen tareas que de otra forma no estarían dispuestas a realizar. Lo anterior enfatiza que la ingeniería social no es un fenómeno nuevo ni exclusivo del mundo digital; de hecho, tiene una larga historia de éxito en el mundo físico.

Los ingenierios sociales se han adaptado a los cambios de escenarios, medios y tecnología mucho más rápido y eficientemente que la sociedad en general, a tal grado que hoy se puede hablar de la ingeniería social no solamente como el arte, sino como la ciencia para hackear el ser humano. Esto les ha permitido tomar ventaja de las vulnerabilidades humanas por más tiempo, reducir los costos de sus embates, disfrutar de una impunidad casi perenne y obtener jugosas ganancias.

A partir de la tendencia mostrada en los últimos años se puede predecir que los ataques con ingeniería social irán en aumento, serán más sofisticados, recurrirán a la inteligencia artificial como un medio de sofisticación/mejora y pondrán en jaque a los diversos medios y herramientas de ciberseguridad. En consecuencia, la educación o concienciación sobre los impactos negativos de la ingeniería social es la única forma efectiva de prevenirla y contrarrestarla; esta educación no debe ser necesariamente técnica, sino más bien comprensible para todos los usuarios.

Finalmente, la posible solución a los desafíos de la ciberseguridad no es solamente de carácter tecnológico, sino también incluye la concientización, educación y capacitación. Lo antes citado permite afirmar que los problemas de la ciberseguridad dependen de tres elementos principales: la tecnología, los procesos y las personas. Desde la perspectiva antroprocéntrica, el individuo es quién cierra el círculo de las fortalezas y vulnerabilidades, convirtiéndose no sólo en la primera línea de defensa, sino también en el mayor riesgo a la ciberseguridad.

8. Recomendaciones

Es preciso educar a las personas en las buenas prácticas sobre el cuidado de la información personal y el uso seguro de los medios de comunicación, almacenamiento de información y dispositivos digitales para establecer un primer obstáculo a los ataques de ingeniería social. Sería un gran paso construir una cibercultura (seguridad y confianza en la red) desde las primeras etapas de la educación formal.

Se requiere de la formación de capital humano que tenga voluntad para hacer el bien, defender, proteger, educar y empoderar a otros para que comprendan los riesgos que trae consigo la ingeniería social, identifiquen sus capacidades para contener los daños, reconozcan sus vulnerabilidades y aprendan a defenderse por sí mismos en un entorno que utiliza la información como un arma.

Es necesario generar una consciencia sobre los impactos políticos, sociales y económicos de los ataques de ingeniería social en los tomadores de decisiones y creadores de políticas públicas a fin de que se instauren las medidas pertinentes para salvaguardar la integridad de las personas por medio de alianzas o colaboraciones público-privadas. En este sentido, escuchar las demandas de la sociedad es un elemento esencial para lograr el objetivo propuesto.

Referencias

1. Tolman, W. H.: *Social engineering: A record of things done by American industrialists employing upwards of one and one-half million of people*, pp.iii-iv. McGraw Publishing Company (1909).
2. Torres, A T. D. O., & López Rodríguez, D. J. P.: *Diseño e implementación de un plan de concientización frente a la ingeniería social para la empresa promociones y cobranzas Beta SA,* p.38. (Bachelor's thesis, Universidad Piloto de Colombia) (2018).
3. Tolman, W. H.: *Social engineering: A record of things done by American industrialists employing upwards of one and one-half million of people*, p.iii. McGraw Publishing Company (1909).
4. Coxall, M.: *Human Manipulation-A Handbook*. Malcolm Coxall-Cornelio Books, p.207 (2013).
5. Lakhani, D.: *Persuasión*. Editorial AMAT, p.2 (2018).
6. Hadnagy, C.: *Social engineering: The art of human hacking*. John Wiley & Sons, p.178. (2010).
7. ARMY TRAINING AND DOCTRINE COMMAND FORT MONROE VA.: *Cyberspace Operations Concept Capability Plan 2016-2028.* Army, US, p.8. *(2010).*
8. Unión Internacional de Telecomunicaciones (UIT): Resolución 181. Recomendación UIT–T X.1205. *UIT*. http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx (2010). Accedido el 03 de octubre de 2023.
9. Arreola G., A.: Phishing a la pesca de tu información. *Revista Consultoría*. p.29, https://issuu.com/chelafm/docs/cic_299_digital/30 (sep de 2017). Accedido el 03 de octubre de 2023.
10. Hadnagy, C.: *Social engineering: The art of human hacking*. John Wiley & Sons, p.20. (2010).
11. Mitnick, K.: How to hack people. *BBC NewsOnline*. http://news.bbc.co.uk/2/hi/technology/2320121.stm (2002). Accedido el 03 de octubre de 2023.
12. Mitnick, K.: How to hack people. *BBC NewsOnline*. http://news.bbc.co.uk/2/hi/technology/2320121.stm (2002). Accedido el 03 de octubre de 2023.
13. Kissel, R. (Ed.): *Glossary of key information security terms*. Diane Publishing, p.185. (2011).
14. Granger, S.: *Social engineering fundamentals, part I: hacker tactics*. Security Focus, December, 18, p.1. (2001).

15. Grassi, P. A., Garcia, M. E., & Fenton, J. L.: *Digital identity guidelines*. NIST special publication, 800, 63-3, p.54. (2017).
16. Kaspersky: Maneras de evitar ataques de ingeniería social. *Kaspersky*. https://www.kaspersky.es/resource-center/threats/how-to-avoid-social-engineering-attacks (s.f.). Accedido 22 de septiembre de 2022.
17. Kaspersky: Maneras de evitar ataques de ingeniería social. *Kaspersky*. https://www.kaspersky.es/resource-center/threats/how-to-avoid-social-engineering-attacks (s.f.). Accedido 22 de septiembre de 2022.
18. Cialdini, R. B.: *The science of persuasion*. Scientific American, 284(2), 76-81, pp.74-79. (2001).
19. López Grande, C. E.: *Ingeniería social: el ataque silencioso*. Revista Tecnológica: no. 8, p.39. (2015).
20. Shimko, I. *et al*.: El spam y el phishing en 2022. *SecureList.* https://securelist.lat/spam-phishing-scam-report-2022/97582/ (2023). Accedido el 24 de septiembre de 2023.
21. Shimko, I. *et al*.: El spam y el phishing en 2022. *SecureList.* https://securelist.lat/spam-phishing-scam-report-2022/97582/ (2023. Accedido el 24 de septiembre de 2023.
22. García, A. A.: *Ciberseguridad: ¿Por qué es importante para todos?*. Siglo XXI Editores México. (2019).
23. Martín, R. M.: El componente humano, el eslabón más débil en la ciberseguridad. *Capital humano: revista para la integración y desarrollo de los recursos humanos*, (359), 18. (2020).
24. Gutierrez Arevalo, F. R.: *Ciberseguridad e ingeniería social de la mano del ciberdelincuente*. Repositorio Institucional Universidad Piloto de Colombia. (2020).
25. García, A. A.: *Ciberseguridad: ¿Por qué es importante para todos?*. Siglo XXI Editores México. (2019).
26. Ayerbe, A.: La ciberseguridad en el sector energético. *Análisis del Real Instituto Elcano* (ARI), (3), 1, pp. 7 y 8. (2020).
27. Borghello, C.: *El arma infalible: la Ingeniería Social*. ESET Latinoamérica, p.2. (2009).
28. Borghello, C.: *El arma infalible: la Ingeniería Social*. ESET Latinoamérica, p.2. (2009).
29. Cialdini, R. B., Wissler, R. L., & Schwietzer, N. J.: *Science of Influence*. Disp. Resol. Mag., 9, 20, p.2. (2002).
30. Cialdini, R. B., Wissler, R. L., & Schwietzer, N. J.: *Science of Influence*. Disp. Resol. Mag., 9, 20, p.4. (2002).
31. Cloudfare.: ¿Qué es un vector de ataque? *Cloudfare.* https://www.cloudflare.com/es-es/learning/security/glossary/attack-vector/. Accedido el 21 de septiembre de 2023. (s.f.).
32. Manfredi, M.D.: . Cómo la IA está siendo utilizada en ataques de ingeniería social y cómo protegernos. *Linkedin*. https://www.linkedin.com/pulse/c%C3%B3mo-la-ia-est%C3%A1-siendo-utilizada-en-ataques-de-social-manfredi/?originalSubdomain=es. (3 de febrero de 2023). Accedido el 21 de septiembre de 2023.
33. Mariaia.: La inteligencia artificial y los ataques de ingeniería social. *Lascosasdeinternet*. https://lascosasdeinternet.com/tech-development/la-inteligencia-artificial-y-los-ataques-de-ingenieria-social/. (20 de diciembre de 2022). Accedido 21 de septiembre de 2023.
34. Putin, V.: Putin: Leader in Artificial Intelligence Will Rule World. *U.S. News*. https://www.usnews.com/news/business/articles/2017-09-01/putin-leader-in-artificial-intelligence-will-rule-world#close-modal. (2017). Accedido 21 de septiembre de 2023.
35. Bentley, P. J., Brundage, M., Häggström, O., & Metzinger, T.: *Should we fear artificial intelligence?* European Parliamentary Research Office. 2018. (2018).
36. Allianz.: Allianz Risk Barometer. *Allianz*. https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html. (Enero de 2023). Accedido el 21 de septiembre de 2023.
37. Blanco, J. M., & Cohen, J.: *Inteligencia artificial y poder*. Real Instituto Elcano, ARI, 93, p.3. (2018).
38. González, C.: ¿Qué es la Ingeniería Social y en qué consisten estos ataques? *Computer Hoy*. https://computerhoy.com/tecnologia/ingenieria-social-consisten-estos-ataques-1152941. (11 de diciembre de 2022). Accedido el 21 de septiembre de 2023.
39. González, C.: ¿Qué es la Ingeniería Social y en qué consisten estos ataques? *Computer Hoy*. https://computerhoy.com/tecnologia/ingenieria-social-consisten-estos-ataques-1152941. (11 de diciembre de 2022). Accedido el 21 de septiembre de 2023.
40. Smith, S. Z.: Cybercriminals Stole $6.9 Billion In 2021, Using Social Engineering To Break Into Remote Workplaces. *Forbes*. https://www.forbes.com/sites/zacharysmith/2022/03/22/cybercriminals-stole-69-billion-in-2021-using-social-engineering-to-break-into-remote-workplaces/?sh=10baa9226cf5. (22 de marzo de 2022). Accedido el 21 de septiembre de 2023.
41. Smith, S. Z.: Cybercriminals Stole $6.9 Billion In 2021, Using Social Engineering To Break Into Remote Workplaces. *Forbes*. https://www.forbes.com/sites/zacharysmith/2022/03/22/cybercriminals-stole-69-billion-in-2021-using-social-engineering-to-break-into-remote-workplaces/?sh=10baa9226cf5. (22 de marzo de 2022). Accedido el 21 de septiembre de 2023.
42. Mackay, J.: Cómo Detectar Las Señales De Un Ataque De Ingeniería Social. *Metacompliance*. https://www.metacompliance.com/es/blog/phishing-and-ransomware/signs-of-a-social-engineering-attack. (s.f.). Accedido el 24 de septiembre de 2023.
43. Marín Jiménez, R.: *Estudio de metodologías de ingeniería social*. openaccess.uoc.edu, p.71. (2018).
44. Berenguer Serrato, D.: *Estudio de metodologías de Ingeniería Social*. openaccess.uoc.edu, p.28. (2018).
45. Borghello, C.: *El arma infalible: la Ingeniería Social*. ESET Latinoamérica, p.4. (2009).

46. Kulikova, T. *et al*.: Spam y phishing en el tercer trimestre de 2021. *SecureList*. https://securelist.lat/spam-and-phishing-in-q3-2021/95710/. (01 de noviembre de 2021). Accedido el 24 de septiembre de 2023.
47. Anonimo.: Los ataques de phishing se incrementaron a nivel mundial casi un 50% en 2022. *It Digital Security*. https://www.itdigitalsecurity.es/actualidad/2023/04/los-ataques-de-phishing-se-incrementaron-a-nivel-mundial-casi-un-50-en-2022#:~:text=El%20phishing%20sigue%20siendo%20uno,fueron%20educaci%C3%B3n%2C%20finanzas%20y%20gobierno. (21 de abril de 2023). Accedido el 24 de septiembre de 2023.
48. Todorovich, E.: *La pandemia de las Redes sociales.* RADI, Empresas y Servicios de Ingeniería, 9(17), p.93. (2021).
49. Todorovich, E.: *La pandemia de las Redes sociales.* RADI, Empresas y Servicios de Ingeniería, 9(17), p.91. (2021).
50. National Institute of Standards and Technology (NIST).: Information Security. *NIST*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. (septiembre de 2012), B3. Accedido el 28 de septiembre de 2023.

El Método Cualitativo como Alternativa en Peritajes para Dispositivos de Interferencia de Señal

Daniel A. Ramírez Contreras [1] y Omar A. Domínguez Ramírez [2]

[1] Fiscalía General de la República, Servicios Periciales, Pachuca, Hidalgo, México
[2] Universidad Autónoma del Estado de Hidalgo, Instituto de Ciencias Básicas e Ingeniería, Mineral de la Reforma, Hidalgo, México
daniel.ramirezc@fgr.org.mx, omar@uaeh.edu.mx

Resumen. El constante desarrollo y avance tecnológico han llevado a un aumento en el uso de bloqueadores de señales por parte de grupos criminales para cometer delitos. En respuesta, se han implementado medidas legales para penalizar la fabricación, comercialización y uso de estos dispositivos, como se evidencia en México con la incorporación de los artículos 190 bis a la Ley General de Telecomunicaciones y Radiodifusión, y 168 TER a la Ley del Código Penal Federal. A pesar de estas sanciones, la investigación forense relacionada con el uso de bloqueadores de señales enfrenta limitaciones. Organismos internacionales como el Instituto Nacional de Estándares y Tecnología (NIST) y el Grupo de Trabajo Científico sobre Evidencia Digital (SWGDE) no han desarrollado procedimientos específicos acordes a la legislación mexicana para investigar delitos que involucran a estos dispositivos. Esta deficiencia representa un desafío para el sistema de justicia penal, que depende de la prueba pericial para esclarecer hechos delictivos. En este contexto, este capítulo propone una alternativa basada en el método cualitativo para fortalecer el trabajo experto en telecomunicaciones y electrónica, particularmente en demostrar la acción de bloquear señales de radiocomunicaciones. Esta alternativa no sólo permite un uso más eficiente de los recursos económicos, sino que también brinda un sólido respaldo científico y técnico a las autoridades responsables de tomar acciones penales o sancionatorias. Una de las limitaciones identificadas es la falta de equipos necesarios, como analizadores de espectro y frecuencímetros, así como la escasez de infraestructura para instalar una cámara anecoica, que proporcione un ambiente controlado para realizar mediciones. Estos recursos tienen un coste importante y su ausencia dificulta la realización de pruebas en dispositivos de interferencia de señales. El enfoque cualitativo propuesto en este trabajo supone un ahorro económico considerable al mitigar la necesidad de estos equipos y recursos de infraestructura. En resumen, el método cualitativo presentado en este artículo proporciona una alternativa eficaz y bien fundada para fortalecer el trabajo de expertos en el campo de las telecomunicaciones y la electrónica, particularmente en la demostración de la acción de bloqueo de señales de radiocomunicaciones resultantes de interferencias de señal causadas por la superposición de ondas electromagnéticas. Además de contribuir al ahorro de recursos económicos, esta propuesta ofrece apoyo científico y técnico a las autoridades encargadas de emprender acciones legales contra el uso ilícito de bloqueadores de señales.

Keywords: Bloqueador de señal, Investigación forense, Método cualitativo, Analizador de espectro, Cámara anecoica, Interferencia de señal, Ondas electromagnéticas, Legislación Mexicana, Uso ilícito.

1. Introducción

En un entorno de constante evolución tecnológica y avance de las existentes, es evidente el impacto que estas innovaciones tienen en diversas áreas de la sociedad. Lamentablemente, también se han convertido en herramientas utilizadas por grupos delincuenciales para cometer actos ilícitos. Un ejemplo destacado de esto son los bloqueadores de señales, dispositivos diseñados para interferir en las comunicaciones de radio-comunicación y dificultar el auxilio o rastreo de personas y/o vehículos al cometerse un delito. Conscientes de esta problemática, las autoridades han promulgado medidas legales para sancionar las acciones relacionadas con el uso de bloqueadores de señal. En este sentido, el 24 de enero de 2020 se adicionaron el artículo 190 bis a la Ley General de Telecomunicaciones y Radiodifusión, y el artículo 168 TER al Código Penal Federal en México, estableciendo penas de 12 a 15 años de prisión para aquellos particulares que fabriquen, comercialicen, adquieran, instalen, porten,

usen y operen equipos de bloqueo, cancelación o anulación de señales de radiocomunicación. No obstante, a pesar de la existencia de estas sanciones penales, se evidencia una falta de procedimientos específicos en la investigación forense relacionada con el uso de bloqueadores de señal. Organismos de investigación internacionales, tales como el Instituto Nacional de Estándares y Tecnología (NIST) y el Grupo de Trabajo Científico sobre Evidencia Digital (SWGDE), no han desarrollado protocolos que se ajusten a la legislación mexicana para investigar delitos que involucren el uso de estos dispositivos. Esta carencia representa un desafío significativo para el sistema de justicia penal mexicano, el cual depende de pruebas periciales para esclarecer hechos delictivos.

En vista de esta problemática, el presente trabajo tiene como objetivo presentar una alternativa basada en el enfoque cualitativo para fortalecer el trabajo pericial en el ámbito de las telecomunicaciones y la electrónica. Específicamente, se busca demostrar la acción de bloquear señales de radiocomunicación mediante la implementación de procedimientos, herramientas y pasos sustentados en un enfoque científico y técnico. Esta metodología propuesta no solo promueve un uso más eficiente de los recursos económicos, sino que también brinda un respaldo sólido a las autoridades encargadas de ejecutar acciones penales o sancionatorias. En las siguientes secciones, se explorarán en detalle las limitaciones actuales en la investigación forense relacionada con el uso de bloqueadores de señal, se expondrá la propuesta del método cualitativo como alternativa y se discutirán los beneficios que este enfoque puede aportar al sistema de justicia penal. Además, se presentarán ejemplos y casos de estudio que respalden la eficacia y aplicabilidad de este enfoque en la demostración de la acción de bloquear señales de radiocomunicación.

Revisión de literatura

La revisión de literatura realizada para este trabajo, se basó en la consulta de diversas fuentes de información fidedignas y oficiales. Se consultaron sitios web de renombre y organizaciones especializadas en el tema investigado. Entre las fuentes consultadas se encuentran el Instituto Nacional de Estándares y Tecnología (NIST), el Grupo de Trabajo Científico sobre Evidencia Digital (SWGDE), el Instituto Nacional de Justicia (NIJ) y el Poder Judicial de la Federación en México. Sin embargo, no se encontraron antecedentes específicos sobre el tema investigado en estas fuentes.

No obstante, se encontró una publicación relevante en el sitio web de Rohde & Schwarz (https://www.rohde-schwarz.com/). El artículo titulado "EMC SYSTEM SOLUTIONS FROM ROHDE & SCHWARZ Customized EMC test system solutions" aborda el tema de las pruebas de compatibilidad electromagnética (EMC) y ofrece soluciones de Rohde & Schwarz para medir la interferencia electromagnética (EMI) y la susceptibilidad electromagnética (EMS). El artículo presenta sistemas de prueba que cumplen con la norma EN IEC 61000-4-3, los cuales evalúan la inmunidad de los equipos eléctricos y electrónicos (EUT) frente a campos electromagnéticos de alta frecuencia. Estos sistemas de prueba ofrecen suministros para diferentes tamaños de EUT

e intensidades de campo, con configuraciones flexibles que permiten pruebas en rangos de frecuencia específicos.

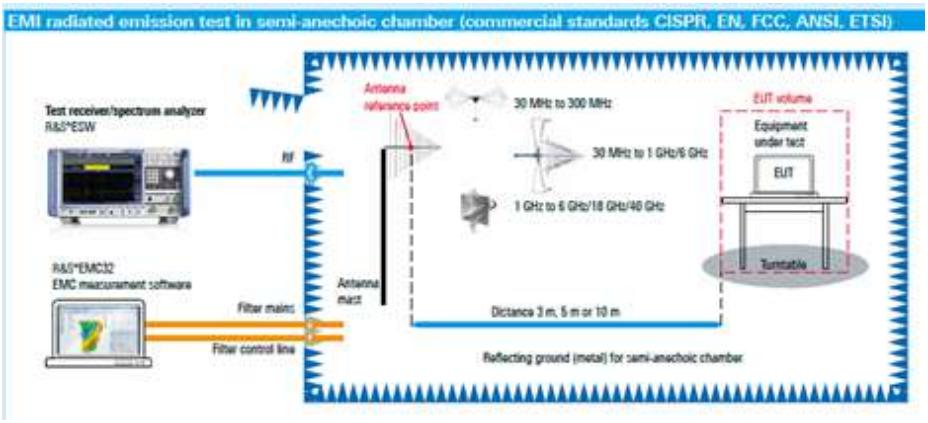

Fig. 1. Pruebas utilizando cámara anecoica.. Homepage: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/EMC-Solutions_bro_en_5215-0511-62_v0300.pdf

Fig. 2. Pruebas utilizando cámara anecoica. Homepage: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/EMC-Solutions_bro_en_5215-0511-62_v0300.pdf

Adicionalmente, se encontró otro estudio relevante encargado por el grupo GSMA Latinoamérica y disponible en su página web (https://www.gsma.com/ latinamerica/wp-content/uploads/2017/12/Reporte-Jammers-2017-Espan%CC%83ol.pdf). GSMA es una organización que representa a operadores móviles y compañías relacionadas, y el informe titulado "Inhibidores de señal Uso de Jammers en prisiones" proporciona información sobre los principios básicos de la propagación de las ondas radioeléctricas y las características de los dispositivos de bloqueo de señal, así como mediciones de campo realizadas con un analizador de espectro. Las mediciones se presentan en forma de gráficas que muestran la intensidad de la señal en decibeles (dB) en función de la frecuencia en MHz.

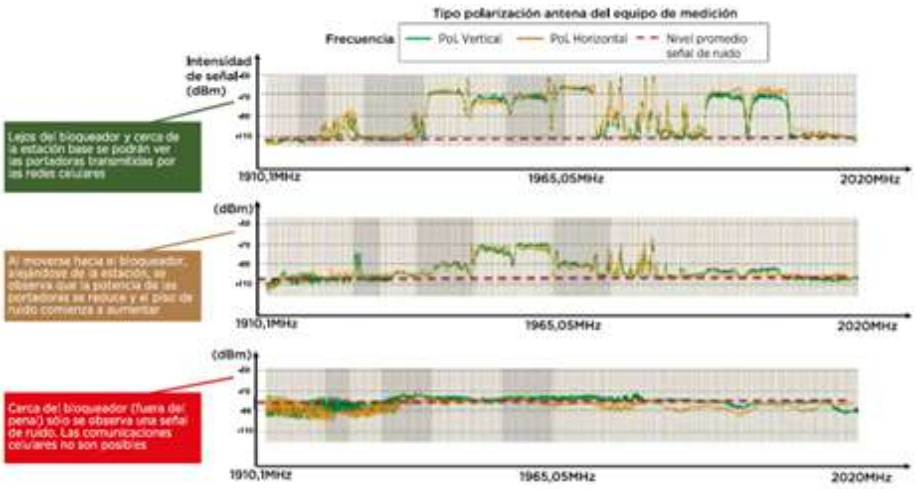

Fig. 3. Spectrum analyzer measurements. Homepage https://www.gsma.com/latinamerica/wp-content/uploads/2017/12/Reporte -Jammers-2017-Espan%CC%83ol.pdf, p. 16

En cuanto a las normativas relevantes, se destaca la Norma Oficial Mexicana NOM-220-SCFI-2017, la cual establece los requisitos y especificaciones para los equipos de bloqueo de señales de telefonía celular, radiocomunicación o transmisión de datos e imagen en centros de readaptación social, establecimientos penitenciarios o centros de internamiento. Esta norma hace referencia a la Disposición Técnica IFT-010-2016, que proporciona las especificaciones técnicas y condiciones de operación para los equipos de bloqueo de señales, así como los métodos de prueba para verificar el cumplimiento de dichas especificaciones. La disposición técnica menciona los equipos de medición necesarios, como el analizador de espectro, antenas patrón o de referencia calibradas, acoplador de impedancias, preamplificador, medidor de potencia de RF y una cámara anecoica.

En México, la Norma Oficial Mexicana NOM-220-SCFI-2017 establece las especificaciones y requerimientos de los equipos de bloqueo de señales de telefonía celular, radiocomunicación y transmisión de datos e imagen en centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores. El objetivo de esta norma es asegurar que los equipos importados y comercializados en México cumplan con las especificaciones y métodos de prueba establecidos en la Disposición Técnica IFT-010-2016. La Disposición Técnica IFT-010-2016 establece las especificaciones técnicas y condiciones de operación para los equipos de bloqueo de señales en los centros mencionados anteriormente. También define los métodos de prueba para verificar el cumplimiento de dichas especificaciones. Esta disposición es aplicable a todos los equipos de bloqueo de señales que bloqueen, cancelen o anulen de manera permanente las señales de telecomunicaciones dentro de los centros penitenciarios.

Para realizar las mediciones necesarias, la Disposición Técnica IFT-010-2016 menciona algunos equipos de medición que se deben utilizar, como un analizador de espectro, antenas de referencia calibradas, acoplador de impedancias, preamplificador, medidor de potencia de RF y una cámara anecoica.

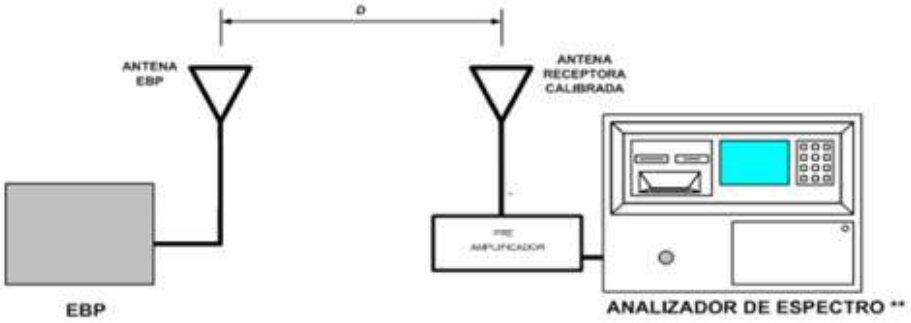

Fig. 4. Configuration for the measurement of radiated emissions. Disposición Técnica IFT-010-2016, pp. 19. (2016)

$$[P_T]_W = \frac{\left[[E]_{\frac{V}{m}}[D]_m\right]^2}{30[G]} \qquad (1)$$

Donde: $[P_T]_W$: Potencia de salida del transmisor, en Watt

$[E]_{\frac{V}{m}}$ Intensidad de campo eléctrico en Volt/metro.

$[D]_m$ Distancia en metros entre las dos antenas.

[G] Ganancia numérica de la antena del EBP

En el contexto de las mediciones de potencia de salida del transmisor (PT), se utiliza la ecuación 1, que relaciona la potencia de salida, la intensidad de campo eléctrico (E), la distancia entre las antenas (D) y la ganancia numérica de la antena del equipo de bloqueo de señales (G).

El marco conceptual del presente trabajo proporciona una base teórica para abordar científicamente el problema relacionado con el funcionamiento de los bloqueadores de señales. Se presentan conceptos clave de la teoría electromagnética, como banda de frecuencias, bloqueo de señales, interferencia, entre otros. La comprensión de estos conceptos es fundamental para comprender el funcionamiento de los bloqueadores de señales y su impacto en las telecomunicaciones. Además, se mencionan conceptos relacionados con las ondas electromagnéticas, como frecuencia, longitud de onda, velocidad de propagación e interferencia.

Banda de frecuencias: porción del espectro radioeléctrico comprendido entre dos frecuencias determinadas [3].

Bloqueo de señales: *i*mpedimento del flujo normal en el canal descendente (Downlink) de señales de telefonía celular, de radiocomunicación o de transmisión de datos e imagen en las bandas que se utilicen para la recepción en los dispositivos o equipos terminales inalámbricos móviles o fijos y las estaciones que proporcionan el servicio [12].

Efectos de la interferencia: ocurren cuando dos o más ondas coherentes se traslapan. Si dos ondas coherentes de la misma amplitud se superponen, ocurre interferencia destructiva total (cancelación o, en el caso de la luz, oscuridad) cuando las ondas están fuera de fase 180°. La interferencia constructiva total (reforzamiento o, en el caso de la luz, brillantez) ocurre cuando las ondas están en fase [1].

Equipo de bloqueo de señales: dispositivos que impiden que los equipos terminales inalámbricos móviles o fijos se puedan comunicar con las estaciones de radio del operador móvil a través del canal descendente (Downlink), impidiendo la recepción y transmisión de señales de telefonía celular, de radiocomunicación o de transmisión de datos e imagen [12].

Equipo bajo prueba (EBP): unidad representativa de un modelo de bloqueador de señales sobre el que laboratorios de prueba lleva a cabo pruebas para verificar el cumplimiento con las especificaciones de la presente disposición técnica [12].

Espectro radioeléctrico: espacio que permite la propagación, sin guía artificial, de ondas electromagnéticas cuyas bandas de frecuencias se fijan convencionalmente por debajo de los 3,000 gigahertz [3].

Frecuencia: número de ciclos por segundo que efectúa una onda del espectro radioeléctrico, cuya unidad de medida es el Hertz [3].

Interferencia: Efecto de una energía no deseada debida a una o varias emisiones, radiaciones, inducciones o sus combinaciones sobre la recepción en un sistema de radiocomunicación, que se manifiesta como degradación de la calidad, falseamiento o pérdida de la información que se podría obtener en ausencia de esta energía no deseada [6].

Magnitud escalar: no tiene una dirección en el espacio. Son escalares muchos conceptos de la física, como longitud, tiempo, temperatura, masa, densidad, carga y volumen; cada uno tiene una escala o tamaño, pero no una dirección asociada [1].

Magnitud vectorial: es un concepto de la física que implica una dirección y solo se especifica por completo si se proporcionan su magnitud (es decir, su tamaño) y una dirección. Muchos conceptos físicos, como el desplazamiento, la velocidad, la aceleración, la fuerza y la cantidad de movimiento, son cantidades vectoriales [1].

Ondas radioeléctricas u ondas hertzianas: Ondas electromagnéticas, cuya frecuencia se fija convencionalmente por debajo de 3 000 GHz, que se propagan por el espacio sin guía artificial [6].

Ondas coherentes*:* son ondas que tienen la misma forma, la misma frecuencia y una diferencia de fase constante (esto es, la cantidad por la que las crestas de una onda se adelantan o atrasan respecto de las de la otra, no cambia en el tiempo) [1].

Radiocomunicación: *toda telecomunicación transmitida por ondas radioeléctricas* [6].

Radiación (radioeléctrica): flujo saliente de energía de una fuente cualquiera en forma de ondas radioeléctricas, o esta misma energía [4].

Servicio de radiocomunicación: *s*ervicio definido en esta sección que implica la transmisión, la emisión o la recepción de ondas radioeléctricas para fines específicos de telecomunicación [6].

Telecomunicación: toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos [6].

Además, es importante destacar que la interferencia de señales se encuentra dentro del campo de conocimiento que obedece a las leyes de Maxwell, es decir, la teoría electromagnética. Según esta teoría, las ondas electromagnéticas son perturbaciones de energía que se propagan en un medio y tienen la característica fundamental de no necesitar un medio para su propagación, pudiendo viajar tanto en el vacío como en otros medios con dos niveles energéticos perpendiculares entre sí. Estos niveles energéticos son el campo eléctrico (E) y el campo magnético (B), y se consideran vectores debido a que tienen magnitud, dirección y sentido.

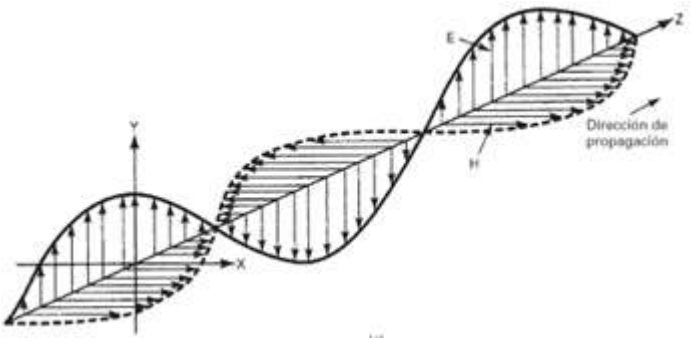

Fig. 5. Onda Electromagnética. Tomasi, W. Sistemas de Comunicaciones Electrónicas. 2a. ed. México: Prentice Hall Hispanoamericana, 2000

Las ondas electromagnéticas pueden clasificarse según su frecuencia, abarcando una amplia gama de frecuencias que se encuentran especificadas en el Cuadro Nacional de Atribución de Frecuencias (CNAF) publicado por el Instituto Federal de Telecomunicaciones en México.

Las principales características de las ondas electromagnéticas son las siguientes: **i)** no requieren un medio de transmisión y pueden propagarse en el vacío; **ii)** su velocidad de propagación depende del medio físico en el que se encuentren, siendo de aproximadamente 300.000 km/s en el vacío; **iii)** se componen de un campo eléctrico (E) y un campo magnético (B), que están definidos por vectores perpendiculares entre sí; **iv)** se caracterizan por su amplitud (A), frecuencia (f), longitud de onda (λ) y velocidad de propagación (v); **v)** la dirección de propagación está relacionada con la perpendicular al plano definido por los campos eléctrico y magnético; y **vi)** son susceptibles a interferencias y ruido.

Las magnitudes que determinan las características de las ondas electromagnéticas son:

La frecuencia (f) de una onda es el número de ciclos por segundo. Entonces,

$$f=1/T \qquad (2)$$

Si T está en segundos, entonces *f* se encuentra en Hertz (Hz), donde:

$$1Hz = 1\ s^{-1} \qquad (3)$$

Las partes superiores de la onda, como los puntos A y C, se llaman crestas. Las partes inferiores, como los puntos B y D, se denominan valles. Al pasar el tiempo, las crestas y los valles se mueven a la derecha con una rapidez y, que es la rapidez de la onda. La amplitud de una onda es la máxima perturbación experimentada durante un ciclo de vibración, la distancia y_0. La longitud de onda (λ) es la distancia a lo largo de la dirección de propagación entre puntos correspondientes de la onda, por ejemplo, la distancia AC. En un tiempo T, una cresta que se mueve con rapidez v recorrerá una distancia λ hacia la derecha. Por consiguiente,

$$s=vt \quad (4)$$

$$\lambda = vt = v/t \quad (5)$$

$$v = f\lambda \quad (6)$$

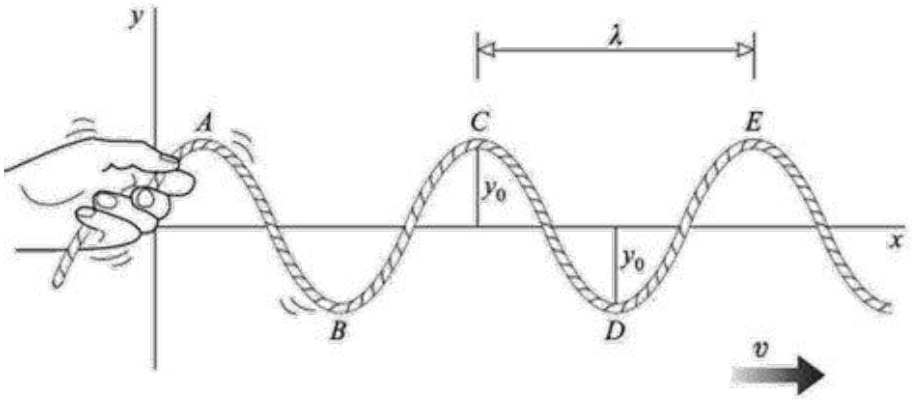

Fig. 6. Magnitudes de onda. Bueche, F. J., Hecht, E., José Hernán Pérez Castellano, & Elizabeth, A. Física general. Mcgraw Hill/Interamericana 2007

En cuanto a la interferencia de ondas, se pueden consultar diversas fuentes bibliográficas para comprender la matemática básica y el método del paralelogramo utilizado para calcular la superposición de ondas. Algunas de estas fuentes incluyen el libro "Introduction to Electrodynamics" de Griffiths (2014) y "Advanced Engineering Mathematics" de Zill, Wright y Cullen (2011), que presentan información relevante sobre este tema. También se puede recurrir al libro "Fundamentos de la Teoría Electromagnética" de Reitz, Milford, Blumovicz Perelberg y Santiago (1996), el cual proporciona una base teórica sólida para comprender la interferencia de ondas electromagnéticas.

En el siguiente ejemplo como lo señala (P. Feynman et al., 1963/2018, p. 615) utilizando métodos trigonométricos para encontrar el efecto de dos fuentes a un cierto ángulo particular en el caso más general, donde los dos osciladores tienen un desfase intrínseco y las intensidades en el caso más simple A1 y A2 son iguales, encontramos que tenemos que sumar dos cosenos que tienen la misma frecuencia, pero con fases diferentes. Matemáticamente, debemos encontrar la suma R de dos ondas, donde:

$$R = A_1\, cos(\omega t + \varphi_1) + A_2\, cos(\omega t + \varphi_2) \quad (7)$$

Utilizando la identidad trigonométrica:

$$cos\, A + cos\, B = 2cos\tfrac{1}{2}(A + B)cos\tfrac{1}{2}(A - B) \quad (8)$$

Simplificando, se obtiene,

$$R = 2Acos\tfrac{1}{2}(\varphi_1 - \varphi_2)cos\,(\omega t + \tfrac{1}{2}\varphi_1 + \tfrac{1}{2}\varphi_2) \quad (9)$$

Se observa que se tiene una onda oscilatoria con una nueva fase y amplitud. En general se tiene el siguiente resultado:

$$A_R = 2Acos\frac{1}{2}(\varphi_1 - \varphi_2) \qquad (10)$$

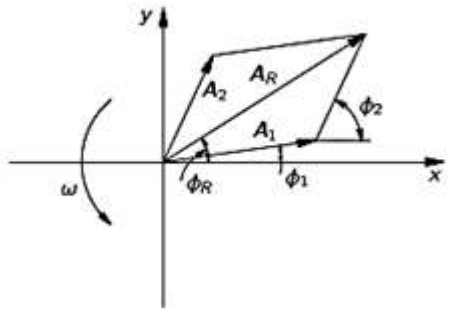

Fig. 7. Método geométrico para combiner dos ondas. P. Feynman, R., Leighton, R. B., & Sands, M. Lecciones de física de Feynman I (E. Oelker & H. Espinosa, Trans.; Primera, Vol. I, p. 615) [Review of Lecciones de física de Feynman I]. Fondo de Cultura Económica. (Original work published 1963) 2018

Lo anterior demuestra matemáticamente la superposición de ondas, como se aprecia en la fórmula (9) lo que da como resultante una nueva onda, originándose así la interferencia. Además, es importante considerar la clasificación de la interferencia de ruido propuesta por Poisel (2011). El autor divide la interferencia de ruido en tres categorías: ruido de banda ancha, ruido de banda parcial y ruido de banda estrecha. Estas clasificaciones se aplican a un bloqueador que puede ocupar una parte o todo el espectro utilizado por el sistema antibloqueo (AJ). El ruido de banda ancha y el ruido de banda parcial se refieren a situaciones en las que las señales de bloqueo ocupan parte del espectro, mientras que el ruido de banda estrecha está asociado con la interferencia del seguidor, donde se intenta seguir un objetivo AJ con salto de frecuencia. En el diseño de bloqueadores, Poisel (2011) menciona varias técnicas para generar interferencia. Estas técnicas incluyen:

- ***Bloqueo por ruido.*** En esta, la portadora emitida por el bloqueador es modulada por una señal aleatoria de ruido. El ruido que se introduce puede ocupar todo el ancho de banda o solo una parte de la señal.

- ***Bloqueo por ruido de banda ancha.*** Esta técnica introduce energía a través de todo el ancho del espectro de frecuencias en el que opere el objetivo. La eficiencia de este tipo de bloqueo depende del nivel de potencia y de la distancia entre el bloqueador y el objetivo. La capacidad de un canal corrompido por dicho ruido viene dada por:

$$C = W_{SS}log_2\left[1 + \frac{R}{P_T}\right] \qquad (11)$$

- ***Bloqueo por ruido de banda parcial (PBN).*** *Introduce energía a través de una parte específica del espectro, es decir, si se conoce la parte del espectro donde se encuentran los canales de sincronización, introduce ruido en esa parte, por lo que el desperdicio de potencia se reduce al mínimo, está dada por:*

$$P_{e_2} = \frac{1}{2}exp\left[-\frac{1}{2}\frac{R}{P_N + J}\right] \qquad (12)$$

De igual modo, se tienen más tipos de técnicas de comunicación AJ, las dos predominantes de uso generalizado son el espectro ensanchado de secuencia directa (DSSS) y el espectro

ensanchado por salto de frecuencia (FHSS). Un tercer tipo, llamado salto de tiempo (TH), la cual está comenzando a emerger como una técnica viable". Por otra parte, es necesario considerar también de la teoría de comunicaciones por radio que para poder radiar ondas radioeléctricas al medio como lo hace un bloqueador de señal, los elementos mínimos necesarios que se deben tener para tal efecto son los siguientes:

Oscilador: es un circuito que produce una señal senoidal a una frecuencia determinada.

Amplificador RF: circuito que sirve para amplificar las señales que se aplican a la entrada.

Antena: dispositivo que tiene la función de emitir o recibir desde o hacia el espacio ondas electromagnéticas.

Fig. 8. Diagrama de bloques simplificado de un bloqueador de señal.

2. Origen del método cualitativo

El método cualitativo encuentra sus raíces en la investigación antropológica y sociológica a finales del siglo XIX y principios del siglo XX. Pioneros como Bronislaw Malinowski y Franz Boas utilizaron técnicas de observación participante y análisis cualitativo para comprender las culturas y sociedades desde una perspectiva inmersiva y contextual. El método cualitativo, aunque es más comúnmente utilizado en las ciencias sociales y humanidades, también puede encontrar aplicaciones en las ciencias exactas. Aunque su uso en estas disciplinas puede ser menos frecuente. En el ámbito de la física, por ejemplo, se han llevado a cabo estudios cualitativos para comprender la conducta de partículas subatómicas en experimentos de física de altas energías (Carter, 2010). Estos enfoques cualitativos permiten explorar la interacción entre las partículas y comprender los procesos subyacentes desde una perspectiva más detallada. En la química, el enfoque cualitativo se ha utilizado para analizar y describir las propiedades y comportamiento de las sustancias químicas, especialmente en la identificación de compuestos desconocidos (Wagner, 2005). La observación detallada, las pruebas cualitativas y el razonamiento inductivo se combinan para obtener conclusiones sobre la composición y características de las sustancias químicas.

Por otra parte, como lo menciona Sampieri (2014) la palabra "cualitativa" (del latín qualitas) hace referencia a la naturaleza, carácter y propiedades de los fenómenos (Niglas, 2010), así también Baena (2017) menciona entre las características de la investigación cualitativa tiene: como elementos de estudio las variables, los datos generalmente son recogidos en un solo momento, su postura epistemológica es el cientificismo apoyado en las ciencias naturales, física, matemáticas y estadística. Se basa en métodos de recolección de datos no estandarizados. donde el investigador comienza examinando los hechos en sí y en el proceso desarrolla una teoría coherente para representar lo que observa (Esterberg, 2002)

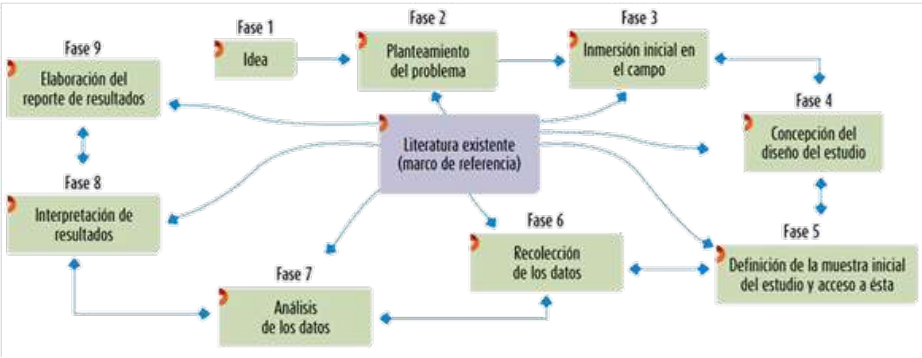

Fig. 9. Proceso cualitativo. Sampieri, R. H., Collado, C. F., & Lucio, M. P. B. Metodología de la investigación McGraw-Hill 2014.

***Investigaciones cualitativas**:* se basan más en una lógica y proceso de explorar y describir, y luego generar perspectivas teóricas [10].

***Método comparative**:* es el procedimiento que se realiza con la intención de encontrar semejanzas y diferencias entre dos o más objetos que se analizan [7].

Método descriptivo: Se utiliza con el propósito de señalar las características del fenómeno que se estudia y presentar los hechos tal como se observan [7].

3. Descripción del método

El método utilizado en este estudio cualitativo se centra en vincular los conceptos abstractos de interferencia por la superposición de ondas electromagnéticas con indicadores empíricos, específicamente la ausencia o presencia de señal en los dispositivos telefónicos como variable dependiente. El objetivo es medir el impedimento de la señal de telefonía celular causado por la

interferencia de ondas radioeléctricas generada por un dispositivo conocido como jammer, inhibidor o bloqueador de señal, considerado como la variable independiente.

El método cualitativo se desarrolla de la siguiente manera:

Hipótesis: el análisis cualitativo revelará que el uso de un bloqueador de señal afecta la presencia o ausencia de señal en un teléfono celular, y que esta relación está influenciada por la potencia de emisión del bloqueador de señal, el rango de frecuencias bloqueadas y la distancia entre el bloqueador de señal y el teléfono celular.

1***.- Descripción de las características de los dispositivos telefónicos:*** se detallan las características de los dispositivos telefónicos que serán utilizados como variables dependientes en las pruebas de funcionamiento. La información se obtiene consultando las páginas del fabricante para realizar la comparación.

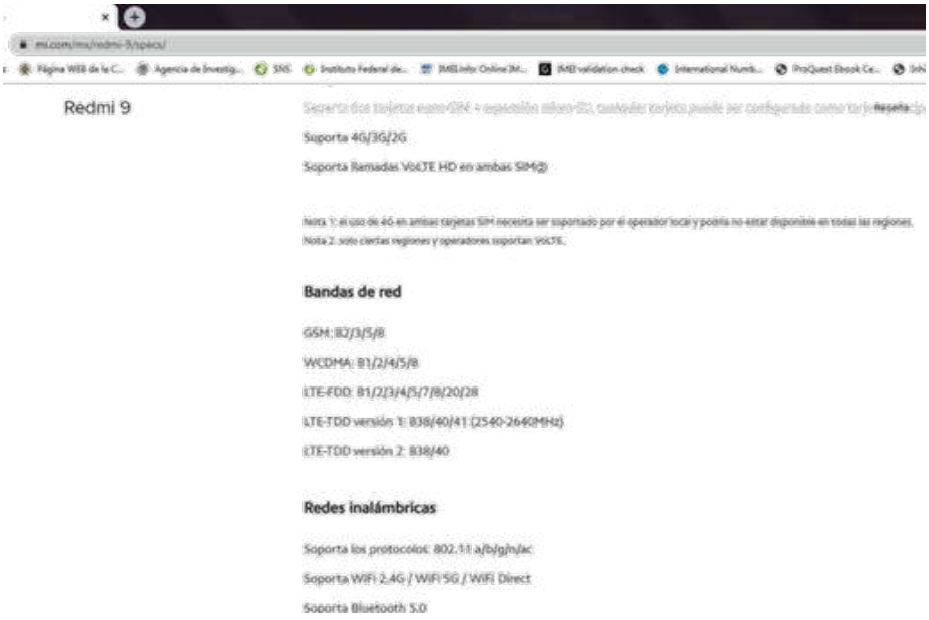

Fig. 10. Especificaciones técnicas del teléfono.

2***.- Prueba previa de funcionamiento de los dispositivos telefónicos:*** se realiza una prueba inicial para comprobar el funcionamiento de los dispositivos telefónicos seleccionados como variables dependientes. Se documenta fotográficamente la prueba, evidenciando la presencia de señal de telefonía, wifi y GPS.

Fig. 11. Prueba inicial de funcionamiento a variable dependiente.

Fig. 12. Prueba inicial funcionamiento variable dependiente.

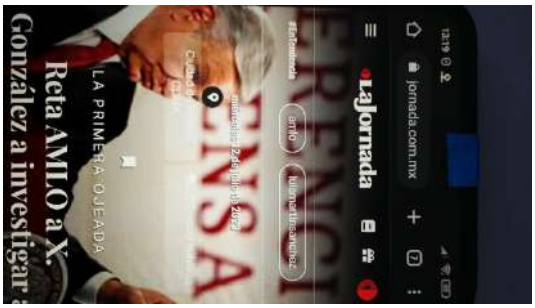

Fig. 13. Prueba inicial funcionamiento variable dependiente de la señal de WiFi.

Fig. 14. Prueba inicial de funcionamiento a variable dependiente señal GPS.

Fig. 15. Prueba inicial de funcionamiento variable dependiente señal de telefonía.

3.- ***Análisis de las características del bloqueador de señal:*** se examinan las características del objeto de estudio, considerado como la variable independiente (bloqueador de señal). Se extrae el bloqueador de su embalaje y se realiza una fijación fotográfica desde diferentes ángulos.

Fig. 16. Bloqueador de señal con accesorio para transporter.

Fig. 17. Bloqueador de señal vista frontal.

Fig. 18. Bloqueador de señal acercamiento a su selector de bandas.

Fig. 19. Vista lateral del bloqueador se observa interruptor de encendido/apagado.

Las especificaciones técnicas del bloqueador de señal se obtuvieron de la página de internet siguiente: https://es.made-in-china.com/co_chinanecom/product_Fast-Charging-Handheld-16-Antennas-Cell-Phone-Signal-Blocker_uooyyroerg.html. Donde proporciona las siguientes especificaciones técnicas:

"Rango de frecuencia: 2G 3G 4G 5G WiFi GPS Lojack 315 MHz 433/868MHz

Frecuencia: 100-6000MHz

batería de litio recargable integrada: 12000 mAh

tiempo de funcionamiento de la batería: 2.5 horas

fuente de alimentación: batería de litio recargable

Descripción de Producto

Las bandas de 16 portátiles de alta potencia Jammer/Blocker

Vodasafe P16N

Descripción breve:

Vodasafe jammer portátil P16N-5G su último modelo en el mercado, se adapta a dispositivo de bolsillo mediante, puede efectivamente bloquear CDMA, GSM, 3G UMTS, LTE 4G, 5G móvil, GPS, WIFI/Bluetooth, Lojack, el control remoto, radio VHF/UHF, podría bloquear todos los tipos de teléfonos Android, tablets, Smartphones, iPhones, ganar teléfonos walkie -talkie, etc. Este jammer portátil podría funcionar para redes inalámbricas 2G, 3G, 4G, WiMax, WIFI, Bluetooth, GPS Lojack, control remoto, las señales de radio VHF/UHF, podría elegir este modelo que se va a trabajar de forma estable y fiable. El blocker podría crear una zona muy tranquila que te rodea y evitar fugas de información en las zonas sensibles.

Portátil Jammer bandas Vodasafe 16p16N características:

** Cubre dieciséis bandas de frecuencia Jamming todo tipo de dispositivo inalámbrico*

** Antena oculta con tapa*

** Tamaño compacto y fácil de transportar*

** Cada banda puede activar/desactivar sin afectar el funcionamiento de otras bandas*

** Potente batería recargable y pueden ser utilizadas al aire libre*

** Un buen sistema de refrigeración No sé no puede trabajar mucho tiempo*

** Puede ser utilizado en el vehículo directamente, con cargador de coche para móviles de uso*

** Apoyar el uso, mientras que la carga de batería*

** Solo interfiriendo descendente y no la interceptación de la estación base.*

Lo anteriormente descrito se observa en las siguientes imágenes:

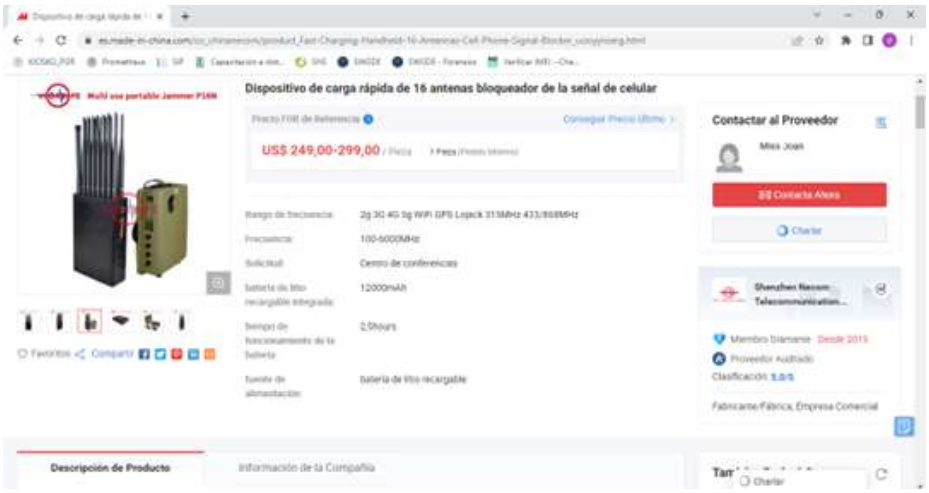

Fig. 20. Consulta en internet especificaciones del bloqueador

Fig. 21. Características técnicas en internet del bloqueador

4.- ***Prueba de funcionamiento del bloqueador de señal:*** se coloca el teléfono celular (variable dependiente) a una distancia que permita su manipulación con respecto al bloqueador de señal (variable independiente). Se enciende el bloqueador de señal y se documenta por escrito y fotográficamente la reacción de la variable dependiente durante la prueba.

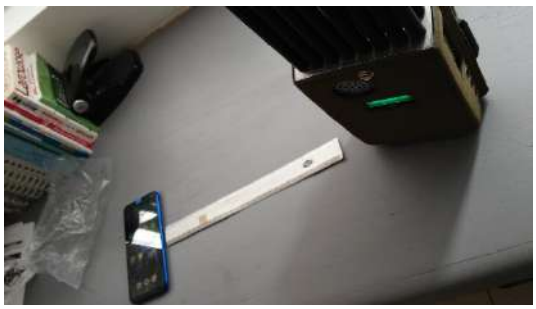

Fig. 22. Se enciende el bloqueador de señal.

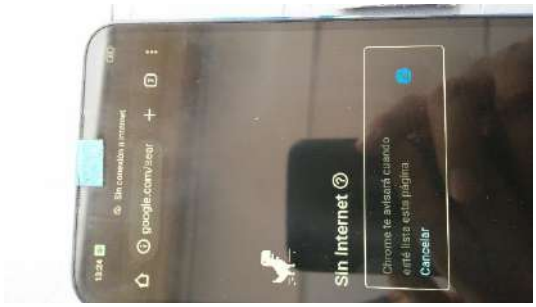

Fig. 23. Variable dependiente pierde señal de Wi Fi.

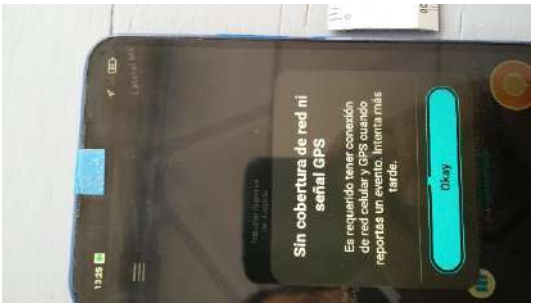

Fig. 24. La variable dependiente pierde señal de GPS.

Fig. 25. La variable dependiente pierde señal de telefonía.

5***.- Prueba de alcance del bloqueador:*** opcionalmente, se realiza una prueba de distancia para determinar el alcance del bloqueador. Se aleja el teléfono celular de manera gradual y se monitorea constantemente el indicador de señal en la pantalla. Una vez que se aprecia la presencia de señal, se realiza una llamada telefónica para verificar que la frecuencia dejó de ser interrumpida, confirmando así el alcance del bloqueo del aparato.

6.- ***Apagado del bloqueador de señal:*** se apaga el bloqueador de señal y se confirma que las variables dependientes recuperan la señal de manera automática. Este proceso se documenta fotográficamente y por escrito.

Fig. 26. Vista general del bloqueador de señal.

Fig. 27. Bloqueador apagado.

Fig. 28. Variable dependiente recupera señal.

7.- ***Conclusiones:*** se concluye que al activar el bloqueador de señal (variable independiente), se afecta el funcionamiento de los teléfonos celulares (variables dependientes), dando como resultado la pérdida de señal de telefonía, Wi-Fi y GPS. Esto confirma cualitativamente la interferencia de señal causada por la superposición de ondas electromagnéticas. Se especifica que un bloqueador de señal transmite señales en el espectro radioeléctrico, para lo cual requiere un oscilador, un amplificador y una o varias antenas según la banda de frecuencias que se desee transmitir.

Nota: no se omite señalar que las fijaciones fotográficas de las pruebas han sido obtenidas cumpliendo con el debido proceso legal y en estricto apego a lo estipulado en el artículo 168 ter del Código Penal Federal. Estas fijaciones fueron obtenidas aprovechando la solicitud de la autoridad ministerial, quien otorgó la autorización expresa y por escrito, debidamente acreditada para poder llevar a cabo las pruebas de funcionamiento del bloqueador de señal. Es importante destacar que el respeto a los procedimientos legales y el cumplimiento de las normas establecidas garantizan la integridad y validez de las pruebas recabadas, asegurando así el debido proceso en la investigación correspondiente. Cabe hacer mención que el método cualitativo en peritajes a bloqueadores de señales lo comencé a utilizar desde el 26 de abril del 2018 en las investigaciones correspondientes.

4. Resultados

El presente estudio cualitativo tuvo como objetivo medir el efecto de la interferencia por la superposición de ondas electromagnéticas en la señal de telefonía celular, utilizando un bloqueador de señal como variable independiente y los dispositivos telefónicos como variables dependientes. A continuación, se presentan los resultados obtenidos durante el desarrollo del estudio.

En primer lugar, se describieron las características de los dispositivos telefónicos utilizados en las pruebas. Se consultaron las páginas del fabricante para comparar y confirmar la información relevante. Los dispositivos telefónicos seleccionados como variables dependientes presentaron características similares en términos de frecuencia de operación, capacidad de conectividad y funciones. Posteriormente, se llevó a cabo una prueba previa de funcionamiento de los dispositivos telefónicos. Durante esta prueba, se verificó que los dispositivos contaban con señal de telefonía, wifi y GPS al momento de realizar la prueba. Se documentaron fotografías que mostraban los indicadores de señal activos en los dispositivos. Luego, se procedió a analizar las características del bloqueador de señal utilizado como variable independiente. Se extrajo el bloqueador de su embalaje y se realizaron fijaciones fotográficas desde diferentes ángulos para obtener una documentación detallada de su estructura física.

A continuación, se realizó la prueba de funcionamiento del bloqueador de señal en presencia de los dispositivos telefónicos. Se colocó un teléfono celular a una distancia que permitiera su manipulación con respecto al bloqueador de señal, y se activó el bloqueador pulsando la tecla de encendido en la posición "on". Durante la prueba, se documentaron por escrito y fotográficamente las reacciones de los dispositivos telefónicos. Se observó que al activar el bloqueador de señal, los dispositivos perdieron la señal de telefonía, wifi y GPS, lo que indicó la interferencia causada por la superposición de ondas electromagnéticas. Se llevó a cabo una prueba adicional para determinar el alcance del bloqueador de señal. Se alejó el teléfono celular de manera gradual, monitoreando constantemente el indicador de señal en la pantalla. Una vez que se apreció la presencia de señal, se realizó una llamada telefónica para confirmar que la frecuencia dejó de ser interrumpida. De esta manera, se estableció el alcance de bloqueo del aparato. Finalmente, se apagó el bloqueador de señal y se confirmó que los dispositivos telefónicos recuperaron la señal de manera automática. Se documentó fotográficamente y por escrito este proceso de restauración de la señal.

En conclusión, los resultados obtenidos en este estudio cualitativo demostraron que al manipular el bloqueador de señal (variable independiente), se afectó el funcionamiento de los dispositivos telefónicos (variables dependientes), dando como resultado la pérdida de señal de telefonía, wifi y GPS. Esto confirmó la interferencia de señal causada por la superposición de ondas electromagnéticas generada por el bloqueador. Se destacó que el bloqueador de señal transmitió

señales en el espectro radioeléctrico utilizando un oscilador, un amplificador y antenas, lo que provocó la interferencia en la comunicación de telefonía, wifi y GPS. Además, se realizó una comparativa con equipos bloqueadores similares encontrados en internet para validar la estructura física y características del bloqueador utilizado en el estudio. Se constató que el objeto de estudio se ajustaba a los estándares y especificaciones de los bloqueadores de señal existentes en el mercado. Es importante mencionar que todas las pruebas se llevaron a cabo en un entorno controlado, esto es, con línea de vista al exterior y sin obstáculos que pudieran interferir con la propagación de las ondas electromagnéticas. Esto permitió descartar posibles influencias externas en la pérdida de señal, como edificios, muros o tipo de construcción.

En resumen, los resultados obtenidos en este estudio cualitativo respaldan la hipótesis planteada, demostrando que la activación del bloqueador de señal provoca la interferencia en la señal de telefonía celular. Estos hallazgos son relevantes para comprender y abordar el problema de la interferencia electromagnética en el contexto de las telecomunicaciones y su impacto en la comunicación inalámbrica. Cabe señalar que este estudio ofrece una perspectiva cualitativa, por lo que se recomienda llevar a cabo investigaciones adicionales que complementen estos resultados y proporcionen un análisis más exhaustivo de la interferencia de señal en diferentes entornos y condiciones. Es importante resaltar, los resultados obtenidos en este estudio respaldan la efectividad del bloqueador de señal como un dispositivo capaz de interferir en la comunicación de telefonía celular. Estos hallazgos contribuyen al campo de las telecomunicaciones y pueden ser de utilidad para el desarrollo de estrategias y soluciones destinadas a minimizar los efectos de la interferencia electromagnética en las redes de comunicación inalámbrica.

Discusión

Los resultados obtenidos en este estudio cualitativo respaldan la hipótesis planteada y proporcionan evidencia sólida de que la activación de un bloqueador de señal tiene un efecto directo en la interferencia de la señal de telefonía celular. Al vincular los conceptos abstractos de interferencia por la superposición de ondas electromagnéticas con indicadores empíricos, como la ausencia de señal en los dispositivos telefónicos, se ha demostrado de manera concluyente que los bloqueadores de señal son capaces de interrumpir la comunicación inalámbrica. El método cualitativo utilizado en este estudio permitió medir y observar los efectos de la interferencia de señal en un entorno controlado. Se llevaron a cabo pruebas exhaustivas de funcionamiento y se documentaron fotográfica y de manera escrita las respuestas de los dispositivos telefónicos antes, durante y después de la activación del bloqueador de señal. Estas pruebas confirmaron de manera consistente que la señal de telefonía, Wi-Fi y GPS se veía afectada negativamente por la presencia del bloqueador. Los resultados también destacan la importancia de considerar las características y especificaciones del bloqueador de señal utilizado. La comparativa con equipos similares disponibles en el mercado validó que el bloqueador utilizado en este estudio cumplía con los estándares y características comunes de los bloqueadores de señal existentes. Esto asegura la reproducibilidad y generalización de los

resultados obtenidos. Es relevante mencionar que este estudio se enfocó en un entorno controlado y libre de obstáculos que pudieran afectar la propagación de las ondas electromagnéticas. Sin embargo, es necesario tener en cuenta que, en situaciones reales, como entornos urbanos o con estructuras físicas complejas, la interferencia de señal puede variar debido a la presencia de obstáculos y condiciones ambientales específicas. Por lo tanto, es recomendable llevar a cabo investigaciones adicionales en entornos diversos para obtener una visión más completa de la interferencia de señal en diferentes escenarios. En cuanto a las implicaciones prácticas, los resultados de este estudio tienen importantes implicaciones para el diseño y desarrollo de estrategias de mitigación de la interferencia electromagnética. La comprensión de cómo los bloqueadores de señal afectan la comunicación inalámbrica puede contribuir al desarrollo de soluciones más efectivas y eficientes para combatir el uso no autorizado de dispositivos bloqueadores y garantizar la integridad de las redes de telecomunicaciones. Este estudio proporciona evidencia sustancial de que los bloqueadores de señal tienen un impacto directo en la interferencia de la señal de telefonía celular. En perspectiva los resultados respaldan la necesidad de regulaciones y medidas de seguridad más estrictas para prevenir el uso indebido de estos dispositivos, así como para fomentar la investigación y desarrollo de tecnologías que minimicen los efectos de la interferencia electromagnética en las comunicaciones inalámbricas. En prospectiva recomienda efectuar investigaciones adicionales en diferentes entornos y condiciones para ampliar el conocimiento sobre este tema y explorar soluciones más específicas y adaptadas a escenarios reales.

5. Conclusiones

En este estudio, se empleó un método cualitativo para investigar los efectos de los bloqueadores de señal en la interferencia de la señal de telefonía celular. Los resultados obtenidos respaldan de manera concluyente la hipótesis planteada y demuestran que la activación de un bloqueador de señal tiene un impacto directo en la comunicación inalámbrica. La relevancia e impacto de este estudio radican en su contribución al campo de investigación de las telecomunicaciones y la interferencia electromagnética. Los bloqueadores de señal son dispositivos que plantean desafíos significativos para la seguridad de las redes de telecomunicaciones y la integridad de las comunicaciones inalámbricas. Comprender cómo funcionan y cómo afectan la señal de telefonía celular en prospectiva es fundamental para desarrollar estrategias efectivas de mitigación y garantizar la continuidad de los servicios de telecomunicaciones. Este estudio ha proporcionado evidencia sólida de que los bloqueadores de señal tienen la capacidad de interrumpir la comunicación inalámbrica al causar interferencia en las ondas electromagnéticas. Los resultados obtenidos respaldan la necesidad de establecer regulaciones más estrictas para prevenir el uso indebido de estos dispositivos y proteger la integridad de las redes de telecomunicaciones. Además, este estudio destaca la importancia de considerar las características y especificaciones de los bloqueadores de señal utilizados, así como el entorno en el que se llevan a cabo las pruebas. Se recomienda llevar a cabo investigaciones adicionales en entornos diversos para obtener una comprensión más completa de la interferencia de señal en diferentes escenarios. En términos prácticos, los hallazgos de este estudio pueden guiar el

desarrollo de estrategias y soluciones tecnológicas más efectivas para contrarrestar la interferencia electromagnética. Esto tiene implicaciones directas en la protección de la infraestructura de telecomunicaciones y la garantía de una comunicación inalámbrica confiable y segura. En resumen, este estudio ha contribuido significativamente al campo de investigación de las telecomunicaciones al proporcionar evidencia sólida de los efectos de los bloqueadores de señal en la interferencia de la señal de telefonía celular. Sus hallazgos tienen implicaciones prácticas importantes para la seguridad de las redes de telecomunicaciones y la continuidad de las comunicaciones inalámbricas. Se recomienda continuar investigando y desarrollando soluciones para mitigar la interferencia electromagnética y garantizar la integridad de las redes de comunicación en un mundo cada vez más dependiente de la tecnología inalámbrica.

Referencias

51. Bueche, F. J., Hecht, E., José Hernán Perez Castellano, & Elizabeth, A. (2007). Física general. Mcgraw Hill/Interamericana.
52. Esterberg, K. G. (2002). Qualitative methods in social research. Nueva York, EE. UU.: McGraw- Hill.
53. Ley Federal de Telecomunicaciones y Radiodifusión.
54. José Manuel Huidobro, Javier Luque Ordóñez, (2014). Comunicaciones por radio. Ra-Ma.
55. Niglas, K. (2004). The combined use of qualitative and quantitative methods in educational research. Tallin, Estonia: Tallin Pedagogical University.
56. Reglamento de Radiocomunicaciones. (2020). International Telecommunication Union. Recuperado el 24 de julio de 2023, de https://www.itu.int/es/publications/ITU-R/pages/publications.aspx?parent=R-REG-RR-2020&media=electronic
57. Rodríguez P. (1999). Metodología jurídica. Oxford University Press, Reimp (2006).
58. Poisel, R. (2011). Modern communications jamming principles and techniques. Artech House,
59. P. Feynman, R., Leighton, R. B., & Sands, M. (2018). Lecciones de física de Feynman I (E. Oelker & H. Espinosa, Trans.; Primera, Vol. I, p. 615) [Review of Lecciones de física de Feynman I]. Fondo de Cultura Económica. (Original work published 1963)
60. Sampieri, R. H., Collado, C. F., & Lucio, M. P. B. (2014). Metodología de la investigación McGraw-Hill.
61. Tomasi, W. (2003). Sistemas de Comunicaciones Electrónicas: Prentice-Hall.
62. Disposición Técnica IFT-010-2016; especificaciones y requerimientos de los equipos de bloqueo de señales de telefonía celular, de radiocomunicación o de transmisión de datos e imagen dentro de centros de readaptación social.
63. Carmines, E. G., & Zeller, R. A. (1991). Reliability and Validity Assessment. Sage Publications.
64. Carter, T. (2010). Exploring particle interactions: A qualitative approach. Physics Education, 45(2), 139-145. doi: 10.1088/0031-9120/45/2/008
65. Wagner, C. (2005). Qualitative chemical analysis of unknown substances. Journal of Chemical Education, 82(11), 1662-1665. doi: 10.1021/ed082p1662

Ciberseguridad; ¿Necesidad o Moda?

El amplio espectro de la ciberseguridad

Domínguez-Jiménez Ismael[1,2 [0000−0003−0959−5875]], Mendoza-Gamiño Alejandro[2 [0000-0001-5473-5078]] y Sánchez-Ruiz Melecio[2 [0009-0005-0342-8736]]

[1] Ingeniería de Software - Escuela Superior de Tlahuelilpan
Universidad Autónoma del Estado de Hidalgo
[2] Colegio de Posgrado – Torre de Posgrado, Ciudad del Conocimiento
Universidad Autónoma del Estado de Hidalgo

Resumen. La cantidad de información que viaja a través de Internet y que almacenamos en los distintos dispositivos locales y remotos (laptops, móviles, proveedores de correo electrónico, repositorios de datos, entre otros), se incrementa cada día más y a un ritmo exponencial y con ello la necesidad de protección de la información.

Seguramente han escuchado la frase "han hackeado mi cuenta …", más de una vez. Aquí surge la pregunta: ¿De verdad se tiene conocimiento acerca de que es la ciberseguridad y de que tratan sus áreas o solo se adoptan estos términos en nuestro lenguaje por moda a causa de la tecnología?

En este capítulo se dará un panorama general de las áreas que integran a la ciberseguridad, resaltaremos la importancia de incorporarla en nuestras vidas mediante la educación y daremos un enfoque en el individuo y su ética como principal factor en la protección de la información. Finalmente, responderemos a la pregunta: ¿La Ciberseguridad es una moda o es una necesidad?

Keywords: Ciberseguridad · Esteganografía · Criptografía · Informática forense · Encriptación · Ingeniería Social · Hacking.

1. Introducción

La era de la información ha llegado para quedarse y está más vigente que nunca, prácticamente en todos los rubros de nuestra vida cotidiana. Todos los días se envía información personal, sensible, no solo de personas sino de las organizaciones. Hoy en día, hay más información en la nube que en los hogares de las personas y que en instalaciones de las empresas.

De la misma manera, en que ha crecido la cantidad de información en internet, también ha crecido la necesidad de protección de los datos y el riesgo de que caigan en manos de personas malintencionadas. Del buen uso o mal uso de la información puede depender el éxito, fracaso o integridad de las personas y empresas.

La probabilidad de que los sistemas de seguridad y algoritmos criptográficos que nos protegen hoy sigan vigentes manteniendo, es cada vez más baja. Lo anterior se debe a la mejora continua de las capacidades de las computadoras, siendo cada vez más rápidas y de mayor capacidad, lo

que implicaría que en un momento no muy lejano se podrán descifrar, corromper, calcular, estimar las claves privadas de varios sistemas criptográficos actuales.

2. Áreas de la Ciberseguridad

La palabra Ciberseguridad es un término relativamente reciente en el ámbito de la computación y de las tecnologías de la información y se da debido al aumento de vulnerabilidades, amenazas y problemas de seguridad de los datos digitales que se transmiten en la Web.

No se tiene una fecha exacta respecto del surgimiento de esta palabra, sin embargo, se hizo popular a partir de la década de los 90′s comenzando a utilizarse cada vez más a medida que la era de la información digital se fue consolidando.

En general, podemos decir que la ciberseguridad se refiere al conjunto de prácticas, técnicas y medidas diseñadas para proteger la información digital de las personas y organizaciones de ataques malintencionados. Dicha información se puede encontrar en internet, teléfonos inteligentes, computadoras, servidores, dispositivos de almacenamiento (como discos duros y Memorias USB), servidores virtuales, servidores de aplicaciones, entre muchos otros medios.

Las prácticas y técnicas de protección de la información pueden ser implementadas en distintos niveles y en distintas áreas específicas que van desde aspectos tecnológicos, legales y logísticos hasta éticos.

Es importante tener claridad sobre la temática de la ciberseguridad y sus áreas de estudio con el fin de valorar la necesidad de personas calificadas y especializadas en distintas áreas para salvaguardar la información y para reflexionar acerca de las actividades que implica proteger a información en este mundo digital (figura 1).

Dentro de las áreas que conforman la ciberseguridad se pueden listar:

- Criptografía
- Criptología
- Esteganografía
- Informática forense
- Ingeniería social
- Hacking

Fig. 1. Temas de ciberseguridad

Las áreas mencionadas a su vez contienen distintos tópicos, cada uno con su complejidad, por ejemplo; la *criptología* como ciencia se divide en dos ramas; la *criptografía*, la cual se encarga del ocultamiento de la información mediante la implementación de códigos y algoritmos de cifrado tanto simétricos como asimétricos (de llave pública y privada), y el criptoanálisis, que en sentido opuesto, trata de descifrar los mensajes en clave, intentando corromper el criptosistema [11].

Cristof Paar y Jan Pelzl en su libro Understanding Criptography realizan una clasificación de las áreas de la criptografía, como se muestra en la figura 2.

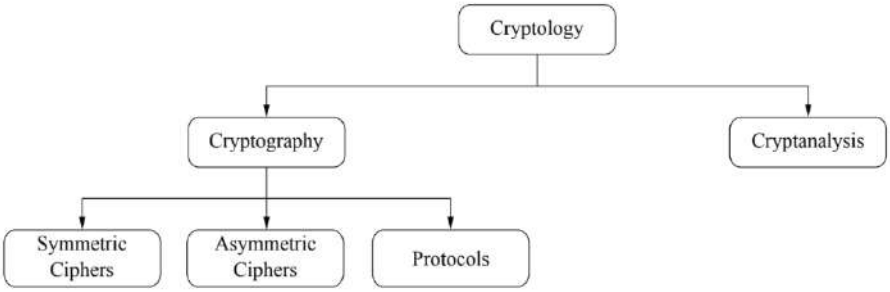

Fig. 2. Áreas de la criptología

La criptografía trata temas de cifrado clásicos (Cesar, Pigpen, Vigenére entre muchos otros) y modernos (RSA, Diffie-Hellman, AES, DES, Blockchain). Estos últimos aún están vigentes y ayudan a proteger nuestra información.

Pocas personas saben que el algoritmo de llave privada-publica RSA, es usado en aplicaciones de bancos para generar tokens que caducan en poco tiempo (entre 15-20 segundos), estos

números están basados en relaciones de primalidad. Esto es un claro ejemplo de la influencia de la criptografía y por ende de la ciberseguridad en nuestras vidas, a pesar del desconocimiento de los usuarios.

El algoritmo criptográfico moderno *blockchainse* puso de moda, principalmente por su uso en las *criptomonedas*, sin embargo, al momento no es tan utilizado en la transmisión de información en la Web como lo es RSA, MD5.

El *criptoanálisis* trata temas de análisis matemático, implementar ataques incluyendo de *fuerza bruta* y temas *de ingeniería social* (ver figura 3) [11].

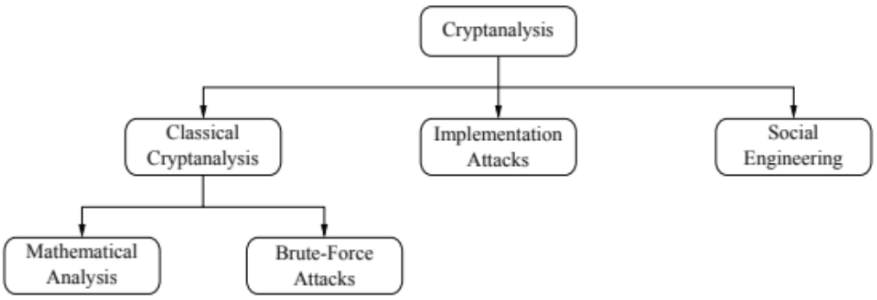

Fig. 3. Criptoanálisis y sus áreas (imagen tomada de [11])

Hasta este punto ya es posible vislumbrar la amplia gama de temas relacionados al menos, con la criptología como subárea de la ciberseguridad.

La Ingeniería Social (IS) también ha tenido su crecimiento debido al aumento en cuanto a la interacción de las personas en el mundo digital.

Las formas, acciones y herramientas que usamos los ciber usuarios, son estudiadas no solo por personas que procuran mejorar en cuanto a la protección de la información, sino también por los ciberdelincuentes quienes analizan el comportamiento de las personas en el uso del internet y plataformas digitales, ideando formas para obtener la información de sus víctimas o generar situaciones para que ellas mismas las compartan de forma voluntaria sin que se den cuenta del engaño (figura 4).

Fig. 4. Estudio de comportamientos humanos en la ingeniería social

También existe el área de la Informática Forense, que se encargan del estudio de las causas y mecanismos que fueron utilizados para vulnerar un sistema o extraer información de manera indebida. Usa cualquier tipo de indicio como Logs, registros, bit´acoras de acceso, procesos, historiales y otros medios para conocer como fue corrompido un mecanismo de seguridad.

Al momento se han explicado, a grandes rasgos, las áreas principales de la ciberseguridad, sin embargo, al ser una disciplina fuertemente relacionada con la tecnología, se encuentra en constante cambio. Los tópicos descritos al momento no son los únicos, pero son considerados los más relevantes. Se han explicado brevemente para dar una idea de la gran gama de temas que son parte de la ciberseguridad.

3. Educación y ética

La formación de recursos humanos altamente capacitados en materia de ciberseguridad en México aún es una utopía.

Se han hecho algunos intentos para mantener al día a profesionales de ciencias computacionales y en temas de ciberseguridad incluyendo algunas materias en maestrías de informática o se han ofrecido diplomados de actualización en informática forense, criptografía, ingeniería social solo por mencionar algunos temas, los cuales no son suficientes para tener un grado de especialización adecuado para mitigar los riesgos de accesos indebidos a la información.

3.1. Educación en ciberseguridad en el México

Al momento no existe un programa de licenciatura o maestría en México lo bastante completo que ofrezca un nivel de especialización suficiente para atender, mitigar o prevenir los potencialmente presentes delitos informáticos.

En la Tabla 1, se muestran algunos programas educativos a nivel maestría y especialidad que se ofrecen en México.

ENTIDAD	**IES**	**PROGRAMA**
CDMX	UNAM	Diplomado en ciberseguridad
EDO DE MEXICO	UNAM	Diplomado en ciberseguridad aplicada
CDMX	IPN	Especialidad en Seguridad informática
EDO DE MEXICO	ITESM	Maestría en ciberseguridad
CDMX	La Salle	Maestría en ciberseguridad

Tabla 1. Principales programas en ciberseguridad (o relacionados) en México

4. Educación en ciberseguridad en el Extranjero

La organización denominada Association of Computing Machinery(ACM) y el Comité para la Educación en Computación en Colegios Comunitarios (CCECC por sus siglas en inglés), emitió la primera guía para programas educativos en ciberseguridad en el año 2017 (ver figura 4. A partir de entonces la CCECC a continuado con la actualización de la guía [3].

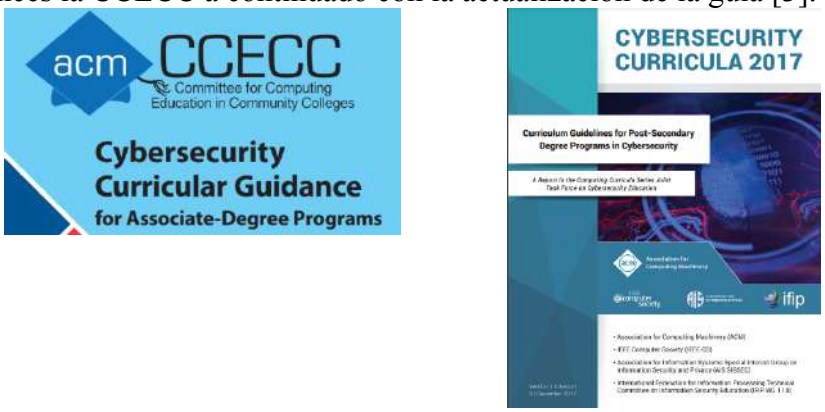

Fig. 5. Guía de diseño curricular para programas en ciberseguridad elaborada por la ACM y la CCEC

La ACM es referente mundial para la creación de programas en computación y ciberseguridad. Lleva a cabo estudios de necesidades de empresas de manera frecuente y la gran mayoría de universidades públicas de prestigio en el mundo se apoyan de los estudios guía que realiza.

En los Estados Unidos de América la preocupación por la formación de especialistas en materia de ciberseguridad ocasionó que desde hace ya algunos años surgieran organizaciones académicas para apoyar en la creación de programas de estudio como *The National Centers of Academic Excellence in Cybersecurity (NCAE-C)*, quien es apoyado ´por distintas instituciones líderes en seguridad nacional, como lo son;

- Cybersecurity and Infrastructure Security Agency (CISA)
- National Cryptologic School (NSA)
- Federal Bureau of Investigation (FBI)
- National Institute of Standards and Technology (NIST)
- National Initiative on Cybersecurity Education (NICE)
- National Science Foundation (NSF)
- Department of Defense Office of the Chief Information Officer (DoD-CIO)
- U.S. Cyber Command (USCYBERCOM)

La NCAE-C, congrega a especialistas, universidades y establece estándares curriculares para la creación de programas educativos en materia de ciberseguridad. En contraste, en México se han hecho pocos esfuerzos.

Fig. 6. Centros Nacionales de Excelencia académica en temas de ciberseguridad en EUA

Debemos tener en cuenta que debido a la amplia gama de tópicos que están incluidos en la ciberseguridad, y que esta puede ser abordada desde distintas trincheras, la ciberseguridad es hoy en día una área multidisciplinaria e incluso transdisciplinaria. De acuerdo con GitHub; la plataforma más grande de código en todo el mundo, la ciberseguridad está soportada por 3 pilares: la gente, la tecnología y los procesos (figura 7).

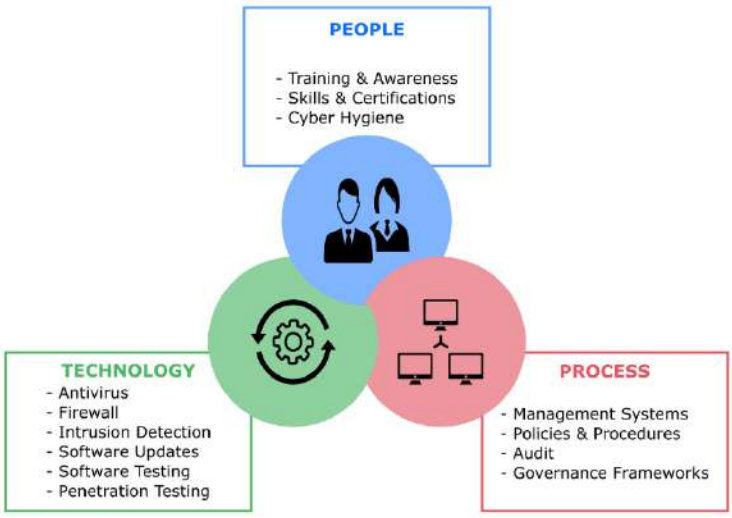

Fig. 7. Pilares de la Ciberseguridad (Fuente: GitHub)

Lo que muestra claramente que las acciones para asegurar la seguridad de la información con la Ciberseguridad deben de realizarse desde distintos ámbitos, que van desde la capacitación del personal, definición de procedimientos y políticas organizacionales, la implementación de aspectos tecnológicos de vanguardia, por mencionar algunos [7].

Dentro de poco, se reconoceráinevitablemente que se necesitan especialistas en ciberseguridad; ingenieros de software con conocimientos amplios en el aseguramiento de la calidad de software (SQA), científicos computacionales para el desarrollo de nuevos métodos criptográficos, administradores de bases de datos, científico de datos para analizar e interpretar la información, especialistas en gestión empresarial, quienes podrán implementar mecanismos de mitigación de riesgos.

5. Necesidad de protección de datos en México

En la sección anterior realizamos una breve comparación respecto de la formación de especialistas en ciberseguridad entre México y Estados Unidos. Hemos podido constatar que la hermana unión americana ha tomado con mayor seriedad el tema de la educación en ciberseguridad.

Esta situación resulta hasta cierto punto una inexplicable ironía, o es que acaso guardamos información de nuestros correos, aplicaciones, archivos en servidores que se encuentran en México.

Acaso, ¿tenemos empresas de tecnología en el territorio nacional que sean competidores serios frente Amazon, Azure o Google cloud... y que nos ofrezcan la infraestructura para albergar nuestros sitios Web, bases de datos, archivos y repositorios para atender las necesidades digitales? La respuesta es **No…** de hecho, mucha de nuestra información está justamente en servidores que se encuentran en territorio estadounidense. Entonces, los mismos riesgos que enfrenta EUA, nuestro principal proveedor de servicios digitales, los tenemos y tendremos en México.

Podemos pretender que los ciberataques solo se dan fuera de nuestro territorio y que los casos más sonados de hackeo no pueden pasar en nuestro país, incluso que solo son producto de la ciencia ficción, sin embargo, esto no es verdad, debido a que usamos la misma tecnología y nuestra información está en servidores norteamericanos, los ataques cibernéticos

Como para muestra solo basta un botón, algunos datos fueron compartidos en el *International Data Corporation - Cybersecurity Forum México*, el 27 de septiembre de 2022, donde se mencionó que México tiene el primer lugar de intentos de ciberataque con ochenta y cinco mil millones, al menos en la primera mitad del año 2022, seguido de Brasil y Colombia con 31.5 mil millones y 6.3 mil millones respectivamente en el mismo periodo [9].

6. La adopción social de términos lingüísticos en ciberseguridad

¿Alguna vez has escuchado o visto la frase "*Amigos, han hackeado mi cuenta, sí les escriben, no soy yo..."* ?, seguramente más de una vez. Los términos, tecnicismos y anglicismos derivados de la disciplina de la ciberseguridad, se han adoptado más por moda dentro de nuestro lenguaje. ¿Realmente se sabe qué significa "*hackear"?* La mayoría de las personas que han usado este término, seguramente no saben qué significa.

Muchos de los ataques o acceso indebidos a las cuentas personales de correo y redes sociales, se deben al descuido por parte de los usuarios y la falta de cultura de protección digital.

Un ejemplo es el uso de contraseñas de alguna forma se pueden "obviar", que son sencillas y no reúnen requisitos mínimos de creación como lo son el uso de caracteres alfanuméricos y con una extensión grande. Asímismo es frecuente que se dejen sesiones abiertas en computadoras de acceso público y oficinas. Muchos de los accesos indebidos se han dado de parte de personas muy cercanas a las personas y organizaciones.

¿Cuándo accedemos a la Web, leemos los acuerdos de privacidad? ¿Sabemos exactamente qué información nuestra comparten?... A pesar de que estamos en la era de la información, aún se necesita educación para consumir contenido digital de Internet de manera segura, pues frecuentemente compartimos nuestra información de manera voluntaria.

Este tipo de fenómenos sociales son los que analiza más a detalle el área de Ingeniería Social, y es este tipo de "conocimiento" el que se usa por parte de empresas y personas malintencionadas para crear publicidad y anuncios engañosos, de tal forma que nosotros mismos instalamos software sospechoso, que comparten información y recursos de nuestras computadoras.

Entonces... ¿Hay un grupo de hackers asechando e irrumpiendo la seguridad de nuestra información?, o simplemente no hemos tenido los cuidados necesarios para salvaguardar nuestra secrecía (Figura 8).

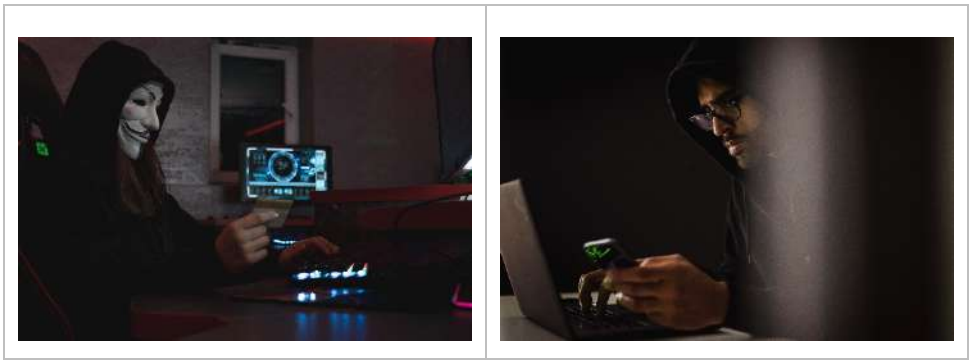

Fig. 8. Representación gráfica de la idea popular de un *hackeo*

Se siguen usando solo la cuenta y contraseña como mecanismo de acceso a los sistemas digitales a pesar de que se nos sugiere activar la autenticación de dos factores *2F*. En otras palabras, la gran mayoría de accesos indebidos a nuestra privacidad y causas de ciberdelitos a ciudadanos, se deben en su gran mayoría, a descuidos, dar poca importancia a la protección de datos y a la de educación cibernética por parte de las personas y empresas.

7. Conclusiones

La ciberseguridad como un área emergente e innovadora ha surgido para quedarse, dando respuesta a una necesidad innegable de proteger la información digital tanto personal como organizacional. Esta área ha sido poco valorada hasta el momento, pues a pesar de que su terminología ya es adoptada en nuestro lenguaje, pocas empresas invierten en tener infraestructura adecuada, especialistas en ciberseguridad, protocolos, planes de contingencia, mecanismos de roles y permisos para proteger su activo más importante; su información.

Es de suma importancia invertir no solo en educación computacional sino también en fomento a una cultura digital y el fomento a los valores y ética de las personas. Se habla poco acerca del individuo y su ética como primer frente para proteger los datos, sin embargo, es factor importante, pues muchos de los ataques, fugas de información, daño en sistemas informáticos y sus datos, ocurren a causa de personas cercanas.

La ciberseguridad es una necesidad poco valorada, sin embargo, tarde o temprano será seriamente considerada y adoptada por todos. Es importante difundir y socializar su importancia para incorporarla en nuestras vidas cuanto antes y no esperar que sucedan daños y fugas de información, que nos hagan valorarla.

Referencias

66. Anderson, R.J.: Security Engineering: A Guide to Building Dependable Distributed Systems (2020)
67. Baksi, A.: Classical and Physical Security of Symmetric Key Cryptographic Algorithms. Computer Architecture and Design Methodologies, Springer Nature Singapore (2022), https://books.google.com.mx/books?id=ZWRXEAAAQBAJ
68. On Cybersecurity Education, J.T.F.: Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, New York, NY, USA (2018)
69. Erickson, J.: Hacking: The Art of Exploitation (2008)
70. Force, C.T.: Computing Curricula 2020: Paradigms for Global Computing Education. Association for Computing Machinery, New York, NY, USA (2020)
71. Fumy, W.: Internet Security Protocols. Springer Berlin Heidelberg (1998)
72. Github: Security concepts: The three pillars (2020), https://github.com/
73. Hadnagy, C.: Social Engineering: The Science of Human Hacking. Wiley Publishing, 2nd edn. (2018)
74. (IDC), I.D.C.: International data corporation - cybersecurity forum Mexico 2022. https://www.idc.com/getdoc.jsp?containerId=prLA49766122 (03 octubre de 2022), accessed: 29 de Noviembre de 2023.
75. Karl Larew, The Codebreakers: The Story of Secret Writing. By David Kahn. (New York: Macmillan Company. 1967. Pp. xvi, 1164. $14.95.), The American Historical Review, Volume 74, Issue 2, December 1968, Pages 537–538, https://doi.org/10.1086/ahr/74.2.537
76. Paar, C., Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners. Springer Publishing Company, Incorporated, 1st edn. (2009)
77. Rao, U.H., Nayak, U.: Cryptography. A press, Berkeley, CA (2014)
78. Service, N.S.A.S.: National centers of academic excellence in cybersecurity (2020), https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/
79. Stallings, W.: Web-Based Security Protocols. Springer US (2011)
80. Stallings, W.: Network Security Essentials: Applications and Standards (2016)
81. Stallings, W.: Cryptography and Network Security: Principles and Practice (2017)
82. Stinson, D.: Cryptography: Theory and Practice, Second Edition. Chapman & Hall, CRC, London, UK (2002)

La Ciberseguridad en la Adopción de la Industria 4.0

Eduardo Cornejo-Velázquez [1][0000-0002-0653-9459] y Mireya Clavel-Maqueda [2][0000-0002-5487-9888]

[1] Centro de Investigación en Tecnologías de la Información y Sistemas, Universidad Autónoma del Estado de Hidalgo, Hidalgo, México
[2] Instituto de Ciencias Básicas e Ingeniería, Universidad Autónoma del Estado de Hidalgo, México
ecornejo@uaeh.edu.mx

Resumen. La Industria 4.0 representa un desafío para las personas y organizaciones. Aprovechar las tecnologías asociadas a este paradigma permite desarrollar nuevas formas de trabajo y nuevos modelos de negocios que fortalezcan la competitividad organizacional. En este sentido, las estrategias de ciberseguridad representan un aspecto de suma importancia porque garantizan el funcionamiento de los bienes y servicios de la organización, y previenen situaciones que pongan en riesgo los datos u operaciones de las empresas. En este documento se contextualiza el desarrollo de estas actividades prioritarias, se aborda la situación específica en México y se describen los avances en términos de regulaciones y buenas prácticas. Seguir estas recomendaciones, promueve un entorno seguro en el cual los datos puedan circular a lo largo de su ciclo de vida. La ciberseguridad es fundamental no solo para salvaguardar los datos operativos y la confidencialidad de sus procesos, sino también para cumplir con las regulaciones legales, fomentar la competitividad y proteger la propiedad intelectual de una empresa.

Palabras clave: seguridad de datos, riesgos en la infraestructura, vulnerabilidad de usuarios.

1. Introducción.

El término Industria 4.0 surge durante la Feria de Hannover en abril del año 2011; fue presentado como parte de una estrategia de alta tecnología y se convirtió en un punto de referencia internacional, estableciendo el liderazgo de Alemania en el sector de tecnologías innovadoras [1].

En el año 2012, los resultados de la colaboración entre el Grupo Bosch y Kagermann se presentan al gobierno alemán a través de un proyecto en el que se identifican y describen varios aspectos clave para lograr el éxito de la Industria 4.0 [2].

Dentro del conjunto de aspectos clave se incluye la estandarización de la arquitectura de comunicación del hardware para garantizar la eficaz colaboración entre empresas en el proceso de producción; la gestión de sistemas complejos para abordar los desafíos tecnológicos en constante evolución; la necesidad de comunicación integral y de alta velocidad mediante redes de Internet confiables; la seguridad de la información en un entorno de fácil acceso desde todos los procesos de producción; la organización y diseño del trabajo para fomentar un entorno empresarial participativo; y, la educación continua de los empleados.

Además, se incluyen la importancia de la regulación adecuada para adaptarse a esta nueva etapa; el uso eficiente de los recursos; y, la implementación de estrategias de formación apropiadas para mejorar las competencias profesionales de los empleados.

Para promover el desarrollo de la Industria 4.0 y la creación de nuevos modelos de negocio basados en sistemas ciber-físicos, se estableció la *Plattform Industrie 4.0* en 2013, como una asociación digital en Alemania que involucró a Bitkom, la Asociación de la Industria de Ingeniería Mecánica Alemana (VDMA por sus siglas en alemán) y la Industria Eléctrica de Alemania (ZVEI por sus siglas en alemán), entre otros [3].

La Industria 4.0 se considera como una revolución en la producción industrial que implica innovaciones disruptivas y cambios en los procesos, con el objetivo de lograr una productividad significativamente mayor. En la literatura científica también se conoce como la Cuarta Revolución Industrial [4].

De acuerdo con Almada-Lobo [5], la Industria 4.0 se puede describir como un entorno de producción altamente conectado en el que se emplean tecnologías de información e Internet para lograr una operación ágil, veloz y eficiente. En la Industria 4.0, se utiliza la tecnología de identificación automática para orientar el proceso de fabricación y se busca fomentar una comunicación y colaboración ininterrumpida y directa entre individuos, máquinas, equipos y sistemas logísticos.

El objetivo principal de la Industria 4.0 es lograr una producción autónoma altamente eficiente y efectiva, optimizando el procesamiento y la comunicación del sistema integrado [6]. Esto se logra mediante la integración inteligente a lo largo de los procesos de fabricación y logística, creando un ecosistema de producción integrado y eficiente.

El Boston Consulting Group, publicó su estudio *"Sprinting to Value in Industry 4.0"* [7] en el año 2016, en él identificó los siguientes retos para la adopción de la Industria 4.0:

- La definición de una estrategia para la Industria 4.0.
- El replanteamiento de la organización y los procesos para maximizar los resultados.
- Entender el modelo de negocio.
- Realización de proyectos, prototipos y pilotajes exitosos.
- Hacer que la organización se dé cuenta de que se necesita acción.
- La gestión del cambio.
- Cultura de la empresa.
- Una verdadera interconexión entre departamentos.
- Talento humano.

El organismo alemán Plattform Industrie 4.0, sugiere que a los puntos anteriores se incorporaren los siguientes dos retos de corte práctico y tecnológico [8]:

- Excelencia en la gestión de la información.
- Ciberseguridad.

Este conjunto de retos demanda una adaptación directa de los trabajadores y también de las empresas y organizaciones, en función del nivel de colaboración necesario entre sus máquinas y procesos cada vez más sofisticados [9]. Para lograr esta adaptación, será necesario obtener una mayor educación, así como desarrollar habilidades y capacidades humanas que sean difíciles de automatizar, tales como la creatividad y las habilidades emocionales [10].

Sin embargo, es crucial considerar que el aumento de la automatización también puede generar presión en los salarios de los trabajadores con habilidades menos especializadas [11]. Con el propósito de aprovechar los beneficios de la tecnología y lograr un crecimiento inclusivo, es fundamental adoptar una postura proactiva para enfrentar las posibles repercusiones económicas y sociales, tales como el aumento del desempleo y los desafíos relacionados con los sistemas de bienestar [12].

Los modelos de negocio disruptivos están teniendo un impacto significativo en el empleo, lo que resulta en la creación y desplazamiento de puestos de trabajo, así como en un aumento en la brecha de habilidades entre los puestos que ofertan los empleadores y los posibles empleados [13]. Para adaptarse a estas transformaciones, se requerirán nuevos planes y sistemas de formación con el fin de aprovechar las oportunidades que surgen.

Para ello, es crucial comprender las habilidades existentes en diferentes países e industrias, así como los nuevos requisitos, estándares y legislaciones que surgirán y se transformarán como resultado de los cambios disruptivos [14].

Los desequilibrios y las brechas en los sistemas educativos dificultan la redistribución efectiva del talento disponible, lo cual tiene un impacto social y económico considerable, especialmente en un contexto de alto desempleo a nivel global [15]. En consecuencia, los trabajadores deben adaptarse a los sectores e industrias en crecimiento y enfocarse en el desarrollo de habilidades necesarias en los campos emergentes [10].

Para enfrentar este desafío se requiere la implementación de estrategias proactivas de gestión del talento y una colaboración continua entre empresas, gobiernos, proveedores de educación y la sociedad civil [12].

Conforme evolucionan el lugar y la forma de trabajo, surgirán nuevos desafíos en términos de gestión y regulación [16]. Por lo tanto, es esencial prepararse para un mercado laboral en constante cambio.

2. Tecnologías de la Industria 4.0.

De acuerdo con el Boston Consulting Group [17], la Industria 4.0 se refiere a la convergencia y aplicación de nueve tecnologías digitales que constituyen un conjunto de oportunidades y desafíos para las organizaciones con el propósito de transformar e innovar en sus modelos de negocio y procesos. En la Figura 1 se presenta el ecosistema de las tecnologías de la Industria 4.0; a continuación, se presenta una descripción general de cada una de ellas:

1. Robots autónomos. Son utilizados cada vez más en diversos campos como la producción, logística y distribución. Los robots autónomos son flexibles, cooperativos y pueden interactuar de manera segura con los humanos.

Estos robots pueden ser controlados a distancia a través de sistemas ciber- físicos, y se utilizan para abordar tareas complejas, así como para ayudar a los operarios humanos en sus tareas diarias.

2. Manufactura aditiva. Esta tecnología está siendo adoptada por las empresas para crear prototipos y producir componentes individuales.

Se utiliza ampliamente para producir pequeños lotes de productos personalizados con diseños complejos.

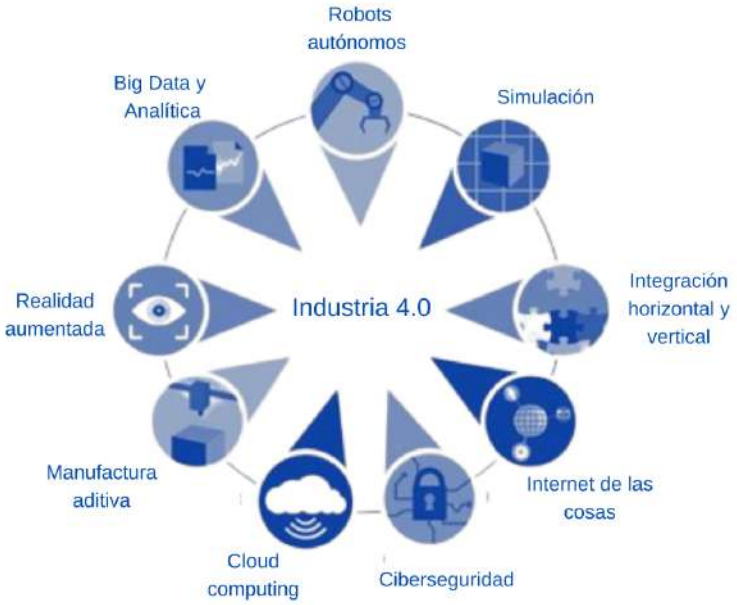

Figura 1. Tecnologías digitales de la Industria 4.0
Fuente: Elaboración propia con base en [17].

3. Realidad aumentada. Esta tecnología proporciona a los trabajadores información en tiempo real a través de dispositivos móviles, mejorando la toma de decisiones y los procedimientos de trabajo.
La realidad aumentada combina gráficos generados por computadora con objetos físicos y permite el control del movimiento mediante sensores.

4. Simulación. Las simulaciones se utilizan cada vez más en las operaciones de planta para aprovechar los datos en tiempo real y crear modelos virtuales que reflejan el mundo físico. Esto permitirá a los operarios probar y optimizar los ajustes de la máquina, reduciendo los tiempos de preparación y mejorando la calidad.
Las herramientas de simulación desempeñan un papel importante en la planificación estratégica y en la investigación dinámica de los sistemas de producción.

5. Integración horizontal y vertical. Con la Industria 4.0, las empresas están mucho más cohesionadas a través de redes de integración de datos universales. La integración horizontal y vertical permite una mayor automatización de las cadenas de valor, donde toda la organización estará interconectada y las empresas estarán conectadas entre sí.
La red de datos industrial recopila grandes bloques de datos, Big Data, y optimiza el rendimiento del sistema, ello permite configurar servicios guiados por datos para los sistemas de producción y logística.

6. Internet de las cosas. Con la Industria 4.0, un mayor número de dispositivos y productos están enriquecidos con la informática integrada, lo que permitirá una comunicación e interacción entre ellos y con controladores centralizados.

El Internet de las Cosas (IoT) habilita la comunicación entre dispositivos, máquinas y sistemas, lo que permite su funcionamiento independiente y la intervención humana cuando sea necesario.
Cada vez más productos están conectados mediante protocolos estándar, descentralizando el análisis y permitiendo respuestas en tiempo real.

7. Cloud Computing. Se requerirá un mayor intercambio de datos entre diferentes sistemas internos y externos a la empresa con tiempos de respuesta extremadamente rápidos. Como efecto a ello, los datos y la funcionalidad de las máquinas se desplegarán cada vez más en la nube, lo que permitirá el desarrollo de servicios basados en datos para los sistemas de producción. Esto ayudará a los servicios de cómputo a automatizar, integrar, gestionar y administrar de manera más eficiente.
La virtualización de recursos y servicios, así como la combinación de sistemas basados en cliente/servidor, son elementos clave en la computación en la nube. La cual incluye un conjunto de recursos informáticos que ofrecen capacidades de almacenamiento y procesamiento en un sistema virtual utilizado por múltiples usuarios. Existen tres modelos de computación en la nube: software como servicio (SaaS, por sus siglas en inglés), plataforma como servicio (PaaS, por sus siglas en inglés) e infraestructura como servicio (IaaS, por sus siglas en inglés).

8. Ciberseguridad. Con el aumento de la conectividad y el uso de protocolos de comunicación estándar en el contexto de la Industria 4.0, se ha vuelto crucial proteger los sistemas industriales críticos y las líneas de producción de las amenazas de ciberseguridad. Para ello, se requieren comunicaciones seguras y confiables, así como una sofisticada gestión de identidad y acceso para máquinas, dispositivos y usuarios.
Se utilizan sistemas avanzados de gestión de identidad y acceso para garantizar comunicaciones seguras y confiables. Es necesario implementar soluciones preventivas y sistemas de defensa contra los efectos perjudiciales de los ataques a los sistemas de información.
Asimismo, es importante salvaguardar la integridad y seguridad de todos los repositorios de información sensible para las organizaciones. Además, construir sistemas de defensa nacionales y capacitar a los empleados en la protección contra ciberataques se vuelve igualmente importante.
Aunque implementar soluciones de ciberseguridad puede implicar un costo para las empresas, el costo total previsto no será alto en comparación con los posibles efectos negativos de los ciberataques.

9. Big Data y Analítica. En el contexto de la Industria 4.0, la recopilación exhaustiva, almacenamiento y la evaluación de datos provenientes de diversas fuentes, como equipos y sistemas de producción, así como sistemas de gestión empresarial y de clientes, se convertirán en una herramienta común para respaldar la toma de decisiones en tiempo real. Esto permitirá optimizar la calidad de la producción, ahorrar energía y mejorar los servicios.

El proceso de análisis de Big Data implica examinar grandes conjuntos de datos para obtener información sobre las preferencias de los clientes, algoritmos de correlación, tendencias y otros conocimientos relevantes.

La analítica de Big Data se aplica en diversas áreas, como la predicción de fallas para reducir la probabilidad de errores y el uso de algoritmos predictivos basados en Big Data para mitigar daños potenciales.

La capacidad de gestionar el Big Data proporciona ventajas competitivas a las empresas, mejorando sus operaciones, impulsando el marketing y mejorando la experiencia del cliente.

2.1 Ecosistema de IoT.

El Internet de las Cosas (IoT) es una red de objetos físicos, dispositivos, vehículos, entre otros elementos conectados a Internet que pueden recopilar y compartir datos. Estos objetos, también conocidos como "*dispositivos inteligentes*" o "*dispositivos conectados*", están equipados con sensores, actuadores y tecnología de comunicación que permiten la interacción con su entorno y con otros dispositivos conectados.

De acuerdo con Muñoz [18], el funcionamiento del IoT se basa en la interconexión de estos dispositivos a través de Internet, lo que permite recopilar datos, comunicarse entre sí y tomar acciones en función de la información recibida. Los elementos funcionales que se incluyen son:

- ***Dispositivos.*** Los objetos físicos, como sensores, cámaras, electrodomésticos, vehículos y muchos más, están equipados con tecnología de conectividad, Ethernet, WIFI, Bluetooth o red celular, que permite su conexión a Internet.
- ***Sensores y actuadores.*** Los dispositivos IoT están equipados con sensores para recopilar datos del entorno, como temperatura, humedad, movimiento, presión y otras variables de interés. Los datos recolectados son procesados internamente o enviados a la nube para su análisis. Además, los dispositivos también pueden tener instalados actuadores, que son componentes que permiten realizar acciones físicas, como encender o apagar luces, abrir o cerrar puertas, controlar el flujo de agua, entre otros.
- ***Comunicación.*** Los dispositivos IoT se comunican entre sí y con sistemas externos a través de protocolos de comunicación estándar, como TCP/IP, MQTT, CoAP, entre otros. Estos protocolos permiten la transmisión de datos de manera segura y eficiente.
- ***Plataforma IoT.*** La información recopilada por los dispositivos IoT se envía a una plataforma IoT, que puede ser una nube o un servidor local. Esta plataforma procesa y almacena los datos, y puede realizar análisis y tomar decisiones en función de la información recibida.
- ***Análisis y toma de decisiones.*** Los datos recopilados por los dispositivos IoT son analizados para extraer información útil y generar conocimientos. Esto puede incluir detección de patrones, identificación de tendencias, correlaciones, entre otros. Con base

en estos análisis, se pueden tomar decisiones automatizadas o proporcionar información relevante a los usuarios para que tomen decisiones informadas.

- ***Acciones y retroalimentación.*** Los dispositivos IoT pueden tomar acciones en relación de la información recibida y las decisiones tomadas. Por ejemplo, un termostato inteligente puede ajustar automáticamente la temperatura en una habitación según la información de los sensores y las preferencias del usuario. Además, los dispositivos IoT pueden proporcionar retroalimentación y enviar informes sobre su estado, funcionamiento y datos recopilados.

En resumen, el IoT se basa en la interconexión de dispositivos físicos a través de Internet, permitiendo la recopilación, comunicación y análisis de datos para tomar acciones automatizadas y brindar información útil.

1.2 IoT en México.

Según la Organización para la Cooperación y el Desarrollo Económicos (OCDE), en México hay un bajo número de dispositivos conectados al Internet de las Cosas (IoT), con poco más de 8 millones de objetos conectados, lo que nos coloca por debajo de países como Corea del Sur y Brasil [19].

Esta situación se debe a varios factores, entre otros las limitaciones en la conectividad y una capacidad insuficiente para almacenar, administrar, analizar y garantizar la seguridad de la gran cantidad de información generada por los dispositivos interconectados [20].

Por otra parte, el IoT Survey [21] en la edición México, reporta que siete de cada diez (72%) organizaciones mexicanas ya han aplicado el IoT en sus proyectos activos o en desarrollo. Menciona que más del 60% de las compañías en México están implementando IoT en iniciativas orientadas a la protección de los empleados y clientes. Asimismo, incluye que cerca del 57% lo está utilizando en operaciones de manufactura, mientras que alrededor del 55% lo emplea en logística.

Además, el mismo reporte señala que la mayoría de las organizaciones tienen previsto utilizar IoT en áreas como mantenimiento predictivo (aproximadamente el 40%), gestión de activos (cerca del 37%) y en el aprovechamiento de las instalaciones y la productividad de los empleados (alrededor del 35%).

Hay un crecimiento sostenido en el uso de IoT, que se confirma con los datos que proporciona el sitio Statista [22]. De acuerdo con lo que se presenta en la Figura 2, en el año 2018, había aproximadamente 81.9 millones de dispositivos de IoT operando en México, y se pronosticó que el número aumentaría a más de 247 millones para el año 2023.

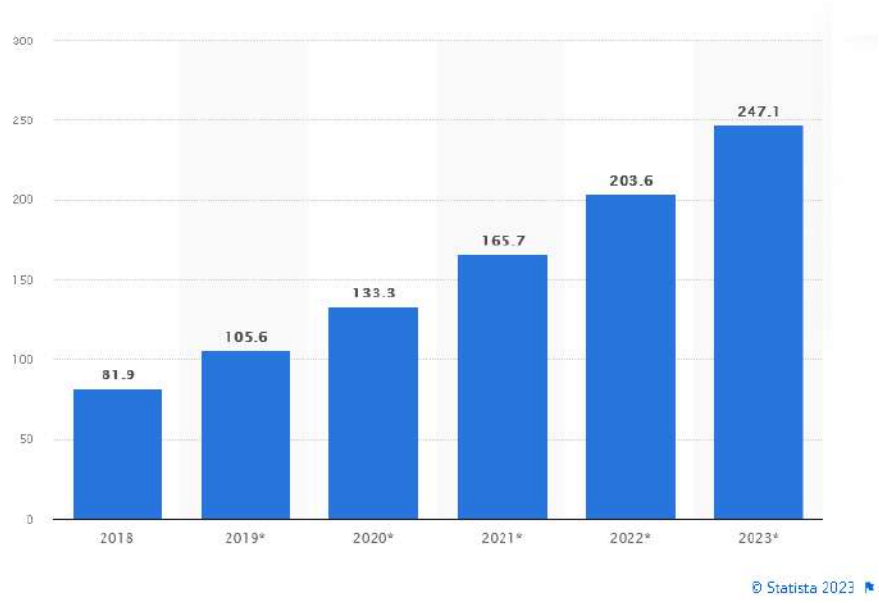

Figura 2. Número de dispositivos de IoT en México de 2018 a 2023.
Fuente: Statista [22].

Ante la situación global y teniendo en cuenta las particularidades del entorno nacional, es imprescindible abordar los factores que permiten el uso de IoT. En México, la Secretaría de Economía (SE) del gobierno federal se encarga de desarrollar e implementar estrategias integrales de innovación, diversificación e inclusión en la producción y el comercio, así como fomentar la inversión tanto a nivel nacional como extranjera [23]. Asimismo, la SE trabaja en el desarrollo de estrategias para potenciar un incremento en el uso y aprovechamiento de la tecnología.

Al interior de la SE, se encuentra en funcionamiento el Organismo Nacional de Normalización y Certificación (NYCE) encargado de atender a diversas industrias; entre ellas, la industria electrónica, telecomunicaciones y tecnologías de información. Dicho organismo nacional se encarga del diseño y formalización de las Normas Oficiales Mexicanas (NOM) [24].

El NYCE ha publicado tres Normas relacionadas con IoT y que están bajo su responsabilidad:

1) NMX-I-320-NYCE-2020 "TELECOMUNICACIONES-TÉRMINOS Y DEFINICIONES PARA EL INTERNET DE LAS COSAS", elaborada, aprobada y publicada como Proyecto de Norma Mexicana [25].

2) NMX-I-321-NYCE-2020, "TELECOMUNICACIONES-DESCRIPCIÓN GENERAL DEL INTERNET DE LAS COSAS", elaborada, aprobada y publicada como Proyecto de Norma Mexicana [26].

3) NMX-I-1362-NYCE-2021, "TELECOMUNICACIONES-PROCEDIMIENTO SIMPLE DE ENCRIPTACIÓN PARA ENTORNOS DE INTERNET DE LAS COSAS (IOT)", tiene concordancia modificada (MOD) con la Norma Internacional *Recommendation X.1362 (2017), Simple encryption procedure for Internet of things (IoT) environments*.

> Esta Norma proporciona un procedimiento de encriptación para la seguridad de los dispositivos destinado para aplicarse a entornos de IoT; especialmente para dispositivos IoT que tienen capacidades obligatorias para comunicación y capacidades opcionales para detección, accionamiento, almacenamiento de datos y procesamiento de datos [27].

Por otra parte, el Instituto Federal de Telecomunicaciones (IFT) es la institución federal encargada de supervisar y promover el uso de las telecomunicaciones y la radiodifusión en México. Su función principal es regular el espectro radioeléctrico, las redes y los servicios de telecomunicaciones y radiodifusión, garantizando el acceso a la infraestructura y otros recursos fundamentales.

El IFT se encarga de garantizar el derecho a la información y el acceso universal a estos servicios, y también es la autoridad competente en temas de competencia económica en los sectores de telecomunicaciones y radiodifusión [28].

En cuanto al tema de IoT, el IFT desarrolla el "*Código de mejores prácticas para la ciberseguridad del IoT*", con el objetivo de establecer pautas y sugerencias que garanticen la seguridad en dispositivos de IoT que emplean el espectro radioeléctrico o se conectan a través de redes de telecomunicaciones.

El código de mejores prácticas pretende abarcar servicios digitales relacionados con estos dispositivos, enfocándose en la gestión de riesgos y la seguridad desde la etapa de diseño. El desarrollo de este código tiene como finalidad disminuir las vulnerabilidades y los ataques cibernéticos, salvaguardando a los usuarios y fomentando la innovación tecnológica para adaptarse a las necesidades en constante evolución del sector [29].

El IFT en su plan estratégico para el período 2021-2025, reconoce la creciente relevancia del sector de las Telecomunicaciones y la Radiodifusión (TyR) en el contexto del ecosistema digital y los desafíos asociados a la era de la transformación digital.

Finalmente, este organismo mexicano tiene como objetivo promover la disponibilidad de espectro radioeléctrico para permitir la provisión de una variedad de servicios y aplicaciones de radiocomunicaciones; realizar un seguimiento y análisis tecnológico constante para identificar de manera anticipada tecnologías y casos de uso emergentes, y evaluar cómo el Instituto puede promover su adopción; informar sobre los beneficios y fomentar la adopción de nuevas tecnologías y casos de uso en la sociedad y en los sectores productivos; facilitar el desarrollo regulatorio, tanto en los sectores productivos como en la sociedad, de casos de uso y modelos de negocio asociados a las nuevas tecnologías que están directamente relacionadas con los sectores de telecomunicaciones y radiodifusión [30].

2. Seguridad de la información.

Los sistemas de información almacenan grandes cantidades de datos y son vulnerables a amenazas de muchos tipos. Debido a que los componentes del sistema se interconectan en distintas ubicaciones a través de redes de comunicaciones, por lo que el potencial de acceso sin autorización, abuso o fraude no se limita a una sola ubicación, sino que puede ocurrir en cualquier punto de acceso.

Las amenazas más comunes en los sistemas de información contemporáneos se pueden derivar de factores técnicos, organizacionales y ambientales integrados de forma errónea por malas decisiones gerenciales [31]. En la Figura 3, se presenta el esquema general de un sistema de información con una arquitectura multinivel y se describen algunas vulnerabilidades que pueden surgir en cada capa y canal de comunicación que los conecta.

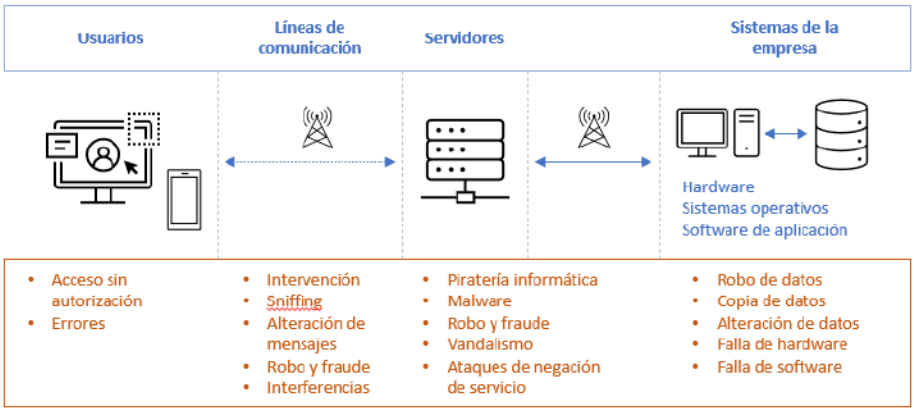

Figura 2. Vulnerabilidades de los sistemas de información.
Fuente: Elaboración propia con base en [31].

En la capa de usuarios se pueden provocar daños a los sistemas de información al introducir errores o lograr ingresar sin autorización. Por otra parte, es posible acceder a los bloques de datos que fluyen a través de las redes de comunicación, robar datos durante la transmisión o alterar mensajes sin autorización.

En la capa de los servidores, los intrusos pueden lanzar ataques para provocar denegación de servicio o utilizar software malicioso para interrumpir las operaciones de los servicios del sistema. Finalmente, en la capa de los sistemas de la empresa, los intrusos pueden penetrar para destruir o alterar los datos almacenados en base de datos y archivos.

En este contexto, la seguridad de la información es el conjunto de estrategias, técnicas y procedimientos utilizados para controlar y resguardar todos los datos que se manejan dentro de las empresas, además de garantizar que los datos no salgan del sistema que ha establecido la organización.

La seguridad de la información es relevante para las empresas, al tratarse de una pieza clave en la ejecución de sus operaciones, tiene el propósito de garantizar que sus datos esenciales y valiosos sean tratados de forma correcta al evitar amenazas y minimizar los riesgos.

Es importante comprender que las empresas y organizaciones, independientemente de su tamaño, cuentan con datos confidenciales de sus procesos internos, clientes, trabajadores, proveedores y otros elementos esenciales en su modelo de negocio. Por ello, es relevante el establecer medidas de seguridad de protección de datos para garantizar la continuidad de operaciones y el resguardo de su información.

2.1. Objetivos de la seguridad de la información.

La estrategia de seguridad de la información cambia en función de las características de cada organización, del sector económico al que se oriente y del contexto en el que se desarrolle. Sin

embargo, es posible definir una serie de objetivos comunes que comparten todas las organizaciones en los ámbitos de la seguridad de la información y protección de datos.

La Norma ISO 27001 establece objetivos comunes a las organizaciones en los ámbitos de la seguridad de la información y protección de datos a través de la implementación de un sistema de gestión de seguridad de la información.

El propósito principal de esta Norma es la protección de los activos de información de la organización, es decir, infraestructura, equipos, usuarios y datos, considerando los siguientes aspectos fundamentales:

- Integridad.
- Confidencialidad.
- Disponibilidad.

A continuación, se describen los aspectos fundamentales considerados en la protección de los activos de información:

Integridad. Los sistemas que gestionan la información de la organización deben garantizar la integridad de los datos, es decir, que se conserven sin alteraciones o manipulaciones que no hayan sido autorizadas de forma específica.
Garantizar la integridad de la información que se procesa y almacena, así como la que se transmite. Se logra con la configuración de entornos seguros utilizando protocolos de seguridad y técnicas para evitar posibles riesgos y amenazas.

Confidencialidad. Los sistemas de seguridad de la información tienen el propósito de garantizar la confidencialidad de los datos de la organización y que no se vea comprometida en ninguna situación o circunstancia.
La confidencialidad asegura que solo las personas o entidades autorizadas tengan acceso a los datos de la organización, además de que no se divulgarán sin autorización.

Disponibilidad. Los sistemas de seguridad de la información deben garantizar que los datos de la organización se encuentren disponibles en todo momento para todas las personas o entidades autorizadas.

La disponibilidad requiere de medidas de soporte y seguridad para acceder a la información, así como evitar que se presenten interrupciones en los servicios de la organización.

2.2. Importancia de la seguridad de la información.

La seguridad de la información es un elemento clave para el funcionamiento eficiente y continuo de las empresas y organizaciones, debido a que todas ellas manejan datos para realizar sus actividades de acuerdo con su modelo de negocios, por lo que necesitan garantizar su protección e integridad.

El desafío para los sistemas de seguridad de la información es gestionar los riesgos existentes y enfrentarlos minimizando los impactos para la organización. Se requiere que sean capaces de fortalecer la resiliencia de las organizaciones y de sus sistemas de seguridad para

prevenir, evitar y solucionar cualquier riesgo, amenaza o ataque que derive del procesamiento de los datos de la empresa.

Generalmente, las empresas y organizaciones implementan soluciones tecnológicas para configurar e implementar la protección de sus activos de información. Además, es necesario conocer en todo momento el estado en el que se encuentran dicha protección y se habilitan herramientas para garantizar la continuidad de las organizaciones y sus actividades en caso de que sufran algún tipo de ataque, intrusión o amenaza.

Existen tres tipos de información con las que trabajan las empresas y organizaciones, independientemente de su modelo de negocio, actividades o sector, y deben ser entendidos y delimitados para implementar estrategias de protección de datos adecuadas.

Información crítica. Son los datos indispensables para el correcto funcionamiento de la organización y sus operaciones. La información crítica está relacionada con el objeto principal del modelo de negocios y que representa en el mediano y largo plazo beneficios para la empresa, puesto que facilita las relaciones con clientes, proveedores y demás actores importantes para el negocio.

Información valiosa. Son los datos que la organización necesita para continuar sus operaciones de forma habitual. Es importante entender que la identificación de la información valiosa de una empresa tiene un componente subjetivo, ya que depende del modelo de negocios, las actividades y del sector en el que se desarrolle. No todos los datos e información tienen el mismo valor para las organizaciones; sin embargo, es necesario que se determine cuáles datos son necesarios para el correcto funcionamiento de las empresas y cuáles no lo son.

Información sensible. Se refiere al conjunto de datos que son accedidos solo por personas autorizadas. Es relevante para las organizaciones mantener privados los datos de sus operaciones y actividades para resguardar la confidencialidad de clientes, proveedores y otros actores integrados en el modelo de negocio de la empresa. Así, los sistemas de seguridad de la información deben garantizar la protección y privacidad de los datos de las organizaciones.

3. Seguridad de la infraestructura de TI.

Desde el punto de vista de las Tecnologías de la Información (TI) la infraestructura de una empresa, la constituyen los activos de hardware y software, dispositivos de usuarios, centros de datos, sistemas de comunicaciones y recursos de Cloud Computing.

La seguridad de la infraestructura de las empresas y organizaciones se refiere a la práctica de proteger los sistemas y activos críticos contra amenazas y riesgos tanto físicos como cibernéticos.

Actualmente, el incremento y mejora de la interconectividad, así como la adopción de nuevas tecnologías como los son servicios de Cloud Computing, arquitecturas de microservicios y componentes de software en plataformas heterogéneas hacen que la tarea de proteger la infraestructura tecnológica sea muy importante a pesar de la complejidad de este desafío.

Una estrategia efectiva en el contexto de TI es la de adoptar arquitecturas con seguridad de confianza cero como una de las formas que tiene la empresa de afrontar el desafío de la seguridad de la infraestructura. El enfoque de confianza cero se orienta en la gestión de accesos

y la validación de identidades que establece que no se confía en ninguna acción del usuario o de las actividades de trabajo de forma predeterminada. La seguridad de confianza cero requiere que todos los usuarios, dispositivos e instancias de las aplicaciones demuestren que son quienes afirman ser y que están autorizados para utilizar los recursos que solicitan

Por otra parte, la formación de los empleados en la operación de la seguridad basada en contraseñas y credenciales juega un papel relevante en la protección de la infraestructura de las empresas. Diferentes autores y organizaciones especializadas en el sector de la seguridad consideran que el factor humano puede ser el eslabón más débil de la estrategia de fortalecimiento de la seguridad de las organizaciones, por lo que la capacitación de los empleados y la formalización de las estrategias de seguridad son sumamente importantes.

En los ambientes empresariales actuales son cada vez mayores los números de intentos de intrusión no autorizada, lo que demanda el funcionamiento eficiente y continuo del perímetro de seguridad de las empresas debido a que una interrupción, aún mínima, en el funcionamiento de la seguridad de la infraestructura puede provocar daños importantes.

Las nuevas amenazas se multiplican cada día, demandando nuevas estrategias de gestión y continuidad de las actividades de las empresas; de igual forma, la amenaza de que se presenten desastres naturales con consecuencias graves no previstas. Para enfrentar a estas amenazas y desafíos, las empresas pueden utilizar la estrategia de copia de seguridad de sus activos de datos de forma frecuente para construir una red de seguridad importante para la continuidad del negocio.

Esta estrategia debe complementarse con soluciones y herramientas que garanticen la disponibilidad constante a través de un proceso de recuperación rápido y sencillo ante las interrupciones, para mantener las operaciones globales uniformes, consistentes y favorecer la movilidad ágil de aplicaciones y datos entre los componentes de los sistemas de información de las empresas.

3.1. Niveles de seguridad de la infraestructura de TI.

Las buenas prácticas de las empresas y organizaciones, así como de las normas y estándares de los sectores relacionados con la seguridad de la infraestructura de TI contemplan cuatro tipos o niveles de seguridad.

Seguridad de datos. La protección de los datos de las organizaciones resulta cada vez más compleja debido a que los volúmenes de generación se incrementan y los espacios de almacenamiento son cada vez más diversos (centros de datos, fragmentación horizontal o vertical de las bases de datos, múltiples nodos en la nube).

Además, el número de dispositivos que se conectan a las redes de comunicación son cada vez mayor debido a las iniciativas de Traiga su Propio Dispositivo (BYOD, por sus siglas en inglés), adopción del IoT entre otras medidas. Ello implica que existen más puntos de acceso a las redes de comunicación de datos de la empresa que necesitan protegerse.

Algunas estrategias de seguridad para el procesamiento de peticiones de las terminales en las empresas incluyen el filtrado de URL, software antivirus, configuración de espacios seguros, protección de los servicios de correo electrónico y el uso de herramientas de detección y respuesta a los múltiples puntos de conexión. Las tecnologías de cifrado o encriptación también contribuyen en la protección de datos al asegurarse que solo los usuarios con la clave de cifrado correcta pueden acceder a ellos.

Seguridad de aplicación. Los sistemas operativos y el software de aplicación desactualizados pueden contener vulnerabilidades que los ciberdelincuentes conocen y pueden aprovechar para lograr acceder a los sistemas de información de las empresas. Por ello, es de suma importancia asegurarse que las actualizaciones de software y firmware en los dispositivos físicos se distribuyen y aplican en todos los componentes de la red de datos y comunicaciones de la empresa.

La instalación de actualizaciones de sistemas operativos, software de aplicación y firmware en dispositivos físicos ayuda a cerrar puertas traseras y agujeros en la seguridad, además de habilitar nuevas funciones, mejora en el rendimiento y corrección de errores en los sistemas de información de la empresa.

Seguridad de red. La primera línea de defensa en la seguridad de una red, por lo general, es la instalación y operación de un software firewall (corta fuegos) que sirve como una barrera entre la red de confianza y segura de la empresa y otras redes desconocidas como las redes WIFI o Internet.

Se recomienda la configuración de un conjunto de reglas para realizar la monitorización del tráfico saliente y entrante de la red para asegurar que solo se permite el tráfico previamente definido en las políticas de seguridad para acceder a los recursos que están disponibles en el sistema de información de la empresa y accesibles a través de la red.

Seguridad física. Las estrategias de seguridad y recuperación de datos incorporan la realización de copias de seguridad externas con ubicaciones geográficas distintas como un mecanismo de protección eficaz para proteger los activos tecnológicos de la sustracción física, el vandalismo o los desastres naturales.

4. Seguridad del IoT.

La seguridad del ecosistema del Internet de las Cosas (IoT) implica proteger los dispositivos conectados a las redes de comunicación de la empresa y al Internet, ya que son vulnerables a las amenazas en línea y las filtraciones de datos. Para lograrlo, se deben identificar, monitorear y abordar múltiples vulnerabilidades de seguridad en los dispositivos encargados de la generación, transmisión, recolección y procesamiento de datos.

Los sistemas IoT integran a casi cualquier dispositivo que tenga un interruptor de encendido y apagado, ya que potencialmente pueden ser conectados a Internet y formar parte del ecosistema. Dentro de la gran cantidad y variedad de '*cosas'* que pueden integrarse, estas interactúan con una gran cantidad de datos críticos, valiosos y sensibles de las empresas. Lo anterior, implica que los datos de los sistemas IoT pueden ser robados, accedidos o modificados por personas externas a la empresa sin autorización; cada dispositivo conectado tiene asociadas diferentes amenazas y riesgos de seguridad.

Las consecuencias de no resolver las brechas de seguridad en los sistemas IoT pueden tener diferentes impactos sobre los datos de las personas y empresas, así como en la continuidad de las operaciones del sistema y en la eficiencia de los servicios. En los hogares inteligentes, las amenazas y riesgos no cubiertos en los dispositivos conectados podrían permitir que personas no autorizadas vigilen los espacios privados de las familias. En el ámbito del cuidado de la salud,

los dispositivos pueden permitir el acceso a datos sensibles de un paciente e incluso comprometer su bienestar.

4.1. Riesgos de seguridad.

Los principales riesgos y amenazas de seguridad en los sistemas IoT se presentan en la Tabla 1, además se indica si el riesgo o amenaza es responsabilidad de los fabricantes, proveedores, integradores, ciberdelincuentes y usuarios al poner en operación un dispositivo IoT, o bien, al integrar un sistema IoT con diferentes dispositivos y servicios.

Tabla 1. Riesgos y amenazas en los sistemas IoT.

	Riesgo o amenaza	Responsables de la brecha de seguridad
1	Falta de pruebas y desarrollo	Fabricantes y proveedores
2	Contraseñas por defecto	Fabricantes, proveedores y usuarios
3	Malware y ransomware	Ciberdelincuentes
4	Privacidad de los datos	Fabricantes, proveedores e integradores
5	Aumento de ciberataques	Ciberdelincuentes
6	Interfaces de comunicación no seguras	Fabricantes, proveedores e integradores
7	Entornos complejos	Fabricantes, proveedores, integradores y usuarios

Fuente: Elaboración propia.

A continuación, se describen los riesgos o amenazas incluidos en la Tabla 1, con el propósito de dar a conocer su origen, características y potenciales impactos dañinos a los sistemas IoT.

Falta de pruebas y desarrollo. Ante la necesidad de ofertar en el mercado nuevos dispositivos y servicios IoT los equipos de desarrollo de las empresas tienen pocas oportunidades para fortalecer la seguridad. En muchos casos, una vez que los productos están en el mercado, los fabricantes ofrecen actualizaciones de seguridad a los usuarios; sin embargo, las brechas de seguridad pueden continuar activas si no se realizan las actualizaciones.

Contraseñas por defecto. Los dispositivos IoT tienen contraseñas por defecto y no son seguras. De igual forma, las credenciales de inicio de sesión por defecto no son seguras, exponen a los dispositivos y sistemas IoT a el robo de contraseñas y habilitan los ataques de fuerza bruta. Los usuarios después de comprar los dispositivos IoT y antes de ponerlos en operación deben cambiar las contraseñas por defecto por seguridad.

Malware y ransomware. Mientras que el malware, es cualquier tipo de software que altera o elimina datos sin el consentimiento explícito del usuario; el ransomware, es un tipo de software malicioso que cifra los archivos de la computadora y los mantiene como rehenes hasta que se realiza un pago para desbloquearlos. Debido al aumento importante en el número de

dispositivos IoT conectados, y que se proyecta continúe en aumento, también crecen los riesgos y las amenazas de ataques de malware y ransonmware.

Privacidad de los datos. Los usuarios al comprar y poner en operación los diferentes dispositivos IoT comúnmente aceptan los términos y condiciones del fabricante o proveedor sin leerlos. Por ello, es común que los usuarios no tengan claras las formas, las personas o las empresas que pueden utilizar sus datos personales. Es una realidad que los dispositivos IoT se encargan de recopilar, transmitir, almacenar y procesar una enorme cantidad de datos del usuario por lo que su privacidad debe ser resguardada.

Aumento de ciberataques. Los dispositivos IoT intervenidos sin autorización o infectados con algún software malicioso pueden ser utilizados para realizar ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés). De esta forma, un sistema IoT puede ser utilizado como base para realizar ataques a otros dispositivos o sistemas, provocar la infección de más dispositivos o esconder las actividades maliciosas.

Interfaces de comunicación no seguras. Muchos de los dispositivos IoT que se integran a los sistemas empresariales y domésticos implementan estrategias de transmisión de datos sin cifrado, con algoritmos frágiles de cifrado o con autenticación insuficiente, lo que genera brechas de seguridad en las interfaces de comunicación entre los dispositivos del sistema IoT.

Entornos complejos. El número y variedad de dispositivos IoT en el mercado sigue en aumento, ello posibilita que los sistemas integrados crezcan en cantidad y diversidad de servicios, tamaños y configuraciones, resultando entornos de trabajo complejos con requerimientos específicos en la configuración de sistemas de defensa para minimizar las amenazas y riesgos de seguridad.

Por otra parte, las diferentes modalidades implementadas con trabajo presencial, remoto e híbrido en las empresas y organizaciones se han ido fortaleciendo con el uso de dispositivos IoT para trabajar desde el lugar que se requiera; las vulnerabilidades de seguridad también se han incrementado debido a que no todas las redes brindan seguridad a las operaciones y actividades laborales.

5. Regulación y modelos de seguridad.

En las siguientes secciones se describen las regulaciones y modelos de seguridad internacionales y nacionales para dar legalidad y formalidad a los sistemas de defensa ante los riesgos y amenazas que enfrentan las personas, la sociedad y las organizaciones frente a los delitos informáticos.

5.1 Convenio de Budapest.

El Convenio de Budapest se firmó el 23 de noviembre de 2001 y entró en vigor el 1° de julio de 2004, en la ciudad de Budapest, República de Hungría [32]. Es el primer tratado internacional

creado con el objetivo de proteger a las personas, la sociedad y a las organizaciones frente a los delitos informáticos y los delitos en Internet.

El Convenio promueve la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional. Se ha empleado como referencia, originalmente, en la Unión Europea, y luego se ha extendido al resto de los países, para la creación de las leyes nacionales de protección contra los ciberdelitos.

El también conocido como *Convenio sobre la Ciberdelincuencia* tiene el propósito de articular una política internacional común, dirigida a la protección de los individuos y la sociedad ante los delitos cibernéticos, mediante la adopción de legislaciones apropiadas y el fomento a la cooperación internacional.

Es un tratado multilateral que brinda las siguientes alternativas ante los delitos informáticos:

- Proporcionar herramientas para que las autoridades investiguen y sancionen adecuadamente la ciberdelincuencia.
- Garantizar la protección de los derechos humanos y las libertades de acuerdo con los documentos internacionales vigentes.
- Brindar mecanismos flexibles para aminorar y evitar conflictos jurisdiccionales a nivel internacional.
- Armonizar las disposiciones penales nacionales sobre delitos informáticos con las de otros países.
- Articular estándares globales más ágiles y efectivos en materia de cooperación internacional sobre ciberdelincuencia.

Por otra parte, establece la tipificación de cuatro categorías de delitos:

a. Delitos cometidos contra la confidencialidad, integridad y disponibilidad de sistemas y datos informáticos.
    - *Acceso ilícito; interceptación ilícita; ataques a la integridad de los datos; ataques a la integridad del sistema; y, abuso de los dispositivos.*
b. Delitos cometidos mediante el uso de las tecnologías de la información y las telecomunicaciones.
    - *Falsificación informática; y, fraude informático.*
c. Delitos por su contenido, como la producción, distribución y posesión de pornografía infantil.
d. Delitos en materia de derechos de autor.

La cooperación internacional en el marco del *Convenio sobre la Ciberdelincuencia* facilita la investigación de infracciones cibernéticas. Lo anterior, es relevante por las características de los delitos informáticos y la posibilidad de que sean cometidos fuera de las fronteras del país, pero con impactos en un territorio determinado.

Algunos países latinoamericanos están vinculados con el Convenio de Budapest y han publicado diversas reformas a su marco normativo con la finalidad de adoptar las políticas de seguridad informática estipuladas en el tratado [33]. Las jurisdicciones de los países han actualizado sus leyes para endurecer las penas contra la ciberdelincuencia.

En el caso de México, dentro del Convenio, sólo actúa como Estado Observador [34]. A pesar de no estar inscrito en el Convenio, el país tiene un marco jurídico propio conformado por el Código Penal Federal y la Ley de Seguridad Nacional [35]. Sin embargo, los actores de la política nacional y el gobierno mantienen un debate interno relacionado con los numerosos informes que revelan que el país ocupa el primer lugar en Latinoamérica en recibir ataques cibernéticos.

En un hecho de relevancia nacional e internacional, el 29 de septiembre de 2022 fue hackeada la Secretaría de la Defensa Nacional de México, situación que aceleró la postulación del primer borrador de la Ley Federal de Ciberseguridad con el propósito de tipificar los ciberdelitos desde una estrategia de seguridad nacional en el marco del Convenio sobre la Ciberdelincuencia.

5.2 Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones.

El *Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM)*, elaborado en el Centro Global de Capacidad en Seguridad Cibernética (GCSCC, por sus siglas en inglés) de la Universidad de Oxford [36] contó con la participación de expertos internacionales de los sectores gubernamental, sociedad civil y academia.

El Modelo CMM ofrece una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país, asignándole una etapa específica que corresponde con el grado de logro en materia de ciberseguridad [37].

Estructura del modelo CMM.

La estructura del Modelo CMM [38], se presenta en la Figura 4, tiene cinco elementos básicos: dimensiones, factores, aspectos, etapas e indicadores. Los elementos del modelo se integran para realizar la evaluación del estado de madurez de los países en sus capacidades de ciberseguridad.

Dimensión. El Modelo CMM se compone de cinco dimensiones que cubren la amplitud de la capacidad de seguridad evaluada. Las dimensiones del modelo se describen en las siguientes secciones.

Cada dimensión está constituida por una serie de factores que relacionan con las capacidades básicas necesarias para cumplir la dimensión. Las dimensiones constituyen los lentes a través de los cuales se puede evidenciar y analizar la capacidad de seguridad.

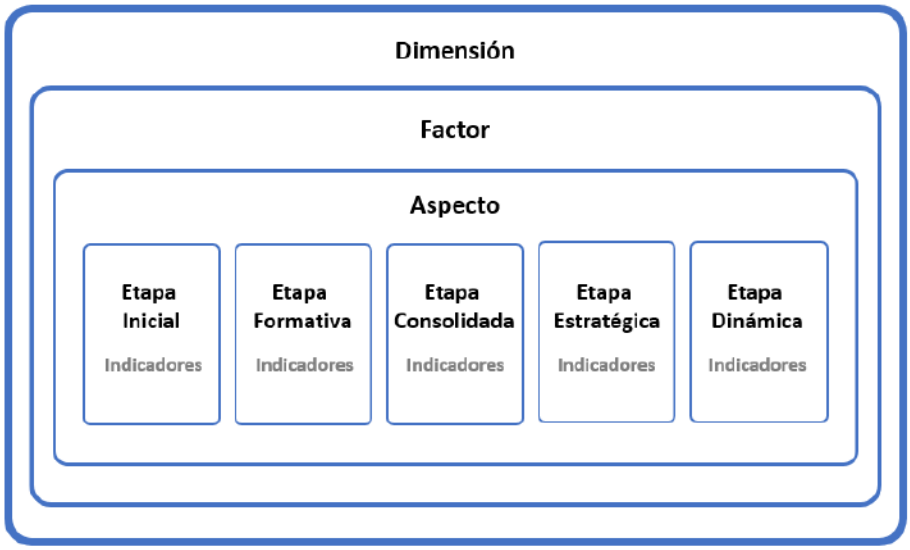

Figura 4. Estructura del Modelo CMM.
Fuente: Elaboración propia con base en [38].

Factor. Dentro de cada una de las dimensiones del Modelo CMM, los factores describen lo que significa poseer capacidades de ciberseguridad. Cada factor se trata de un elemento esencial de la capacidad nacional, que luego se mide para determinar la etapa de madurez.

La lista de factores incorpora de forma holística todas las necesidades de capacidad de ciberseguridad de un país. La mayoría de los factores se compone de una serie de aspectos que estructuran los indicadores del factor que se relacionan directamente con la recopilación y pruebas de medición.

Aspecto. Los aspectos son múltiples componentes de un factor. Son un método de organización para dividir los indicadores en grupos más pequeños que sean más fáciles de comprender. El número de aspectos depende de los temas que integran el contenido del factor y de su complejidad global.

Etapa. Las etapas definen el grado de avance de un país en relación con determinado factor o aspecto de la capacidad de ciberseguridad. El Modelo CMM consta de cinco etapas de madurez, las cuales se describen en las siguientes secciones.

En la evaluación se compara la situación de un país captando la capacidad de ciberseguridad existente con respecto a las etapas, a partir de las cuales un país puede mejorar o empeorar en función de las medidas que adopte.

Indicador. Los indicadores representan la parte más básica del Modelo CMM. Cada indicador describe los pasos, acciones o elementos constitutivos que son indicativos de cada etapa de madurez. Para elevar la madurez de la capacidad de ciberseguridad de un país, deberán cumplirse todos los indicadores de una etapa concreta.

La mayoría de los indicadores son de naturaleza binaria, es decir, se puede demostrar que se han cumplido los criterios del indicador o bien no puede aportar tales pruebas.

Dimensiones del Modelo CMM.

La evaluación de los niveles de madurez se realiza en las cinco dimensiones que se presentan en la Figura 5. Las dimensiones del modelo CMM corresponden a aspectos esenciales y específicos de la ciberseguridad y están orientadas a objetivos específicos [38].

Dimensión 1. Política de ciberseguridad y estrategias. Se relaciona con el diseño de la estrategia nacional de ciberseguridad mediante la respuesta a incidentes relacionados con delitos informáticos; protección de la infraestructura crítica; mecanismos de gestión de crisis; estrategias de defensa cibernética; y mecanismos de redundancia en las comunicaciones.

Dimensión 2. Cultura cibernética y sociedad. Se refiere al fomento de la cultura cibernética responsable en la sociedad a través del fortalecimiento de la confianza y seguridad en Internet; comprensión por parte del usuario de la protección de información personal en servicios en línea; mecanismo de presentación de informes de revisión y evaluación; y, manejo de medios digitales y redes sociales.

Dimensión 3. Conocimientos y habilidades en ciberseguridad. Esta dimensión se refiere al desarrollo del conocimiento de ciberseguridad mediante la sensibilización de las personas y usuarios de los servicios digitales; formalización de modelos y estrategias para la educación; y, definición de lineamientos para formación profesional.

Figura 5. Dimensiones del Modelo CMM.

Fuente: Elaboración propia con base en [38].

Dimensión 4. Marcos legales y regulatorios. Se refiere a la creación de marcos legales y regulatorios efectivos; adecuación de los sistemas de justicia penal; y, definición de marcos de cooperación formal e informal para combatir los delitos cibernéticos.

Dimensión 5. Estándares y tecnologías. Se relaciona con el control de riesgos a través de estándares, organizaciones y tecnologías mediante la adhesión a los estándares; resiliencia de infraestructura de Internet; calidad en el desarrollo de software; controles técnicos de seguridad; controles criptográficos; mercados de ciberseguridad; y, divulgación del responsable.

Etapas de madurez del Modelo CMM.

Las cinco etapas de madurez del modelo CMM se presentan en la Figura 6, cada una describe el grado de avance alcanzado por las organizaciones o países en los indicadores, aspectos y factores de cada dimensión del modelo.

Figura 6. Etapas de madurez de la capacidad de ciberseguridad.
Fuente: Elaboración propia con base en [38].

Etapa Inicial. En esta etapa no existe madurez en ciberseguridad. Puede haber discusiones o propuestas iniciales sobre el desarrollo de capacidades de ciberseguridad, pero no se han tomado medidas concretas.

Etapa Formativa. En esta etapa algunos aspectos relacionados con la ciberseguridad han comenzado a crecer y formularse, pero aún son nuevos, desorganizados o mal definidos.

Etapa Consolidada. En esta etapa los indicadores de ciberseguridad están instalados y funcionando. Sin embargo, no se ha dado mucha consideración a la asignación de recursos y la relevancia que estos tienen con la obtención de resultados.

Etapa Estratégica. En esta etapa se han tomado decisiones sobre qué indicadores de ciberseguridad son importantes y cuáles lo son menos, tanto para las organizaciones o Estado en particular.

Etapa Dinámica. En esta etapa existen mecanismos claros para alterar la estrategia de ciberseguridad en función de las circunstancias que se presentan, tales como sofisticación tecnológica, el entorno de la amenaza, el conflicto global o un cambio significativo en un área de preocupación.

El objetivo del Modelo CMM es alcanzar etapas dinámicas en las organizaciones y países. Ello, representa que han desarrollado métodos para cambiar las estrategias de forma ágil y cuidadosa. Sin embargo, se hace necesaria la rápida toma de decisiones, la reasignación de recursos y la atención constante al entorno cambiante.

En el caso de México, el Observatorio de la Ciberseguridad en América Latina y el Caribe en su Reporte de Ciberseguridad 2022 [39], describe que de acuerdo con el Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM) en el país la Mentalidad de Seguridad Cibernética tanto para los sectores privados, gobierno, así como los usuarios, se encuentra en un grado de madurez en un nivel tres, es decir, refiere que existen indicadores que están implementados y funcionando.

Sin embargo, no se le ha dado mucha consideración a la asignación de recursos y han tomado pocas decisiones estratégicas acerca de los beneficios con respecto a la inversión relativa en torno a la ciberseguridad.

5.3 Norma ISO/IEC 27001

La información es un activo que para las organizaciones tiene valor y requiere de una protección adecuada. La información de las empresas puede adoptar diversas formas: formato impreso o escrito en papel, almacenada en formato electrónico, enviada por correo electrónico, presentada en videos o compartida en conversación.

Así, las empresas y organizaciones deben proteger adecuadamente cualquiera que sea el formato en la que genere, distribuya, comparta o almacene su información; incluidos los medios físicos, electrónicos y digitales que se utilicen para el ciclo de vida de los datos de las organizaciones.

Los riesgos de seguridad de la información representan una amenaza importante para las empresas, se relacionan con la posibilidad de provocar pérdidas financieras, daño a la disponibilidad de los servicios, inaccesibilidad a los servicios esenciales de red, o afectación a la reputación y confianza de los clientes.

Ante esta necesidad, la Norma ISO/IEC 27001 propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas [40].

La gestión de riesgos es uno de los elementos clave en la prevención del fraude cibernético, robo de identidad, daños a los servicios en Internet, pérdida de los datos empresariales y personales, y muchos otros incidentes de seguridad de la información.

La Norma ISO/IEC 27001 es de alcance internacional y está orientada a la *seguridad de la información*, tiene el propósito de ayudar a las organizaciones a implementar y mejorar la gestión de sus riesgos de seguridad de la información.

La Norma propone la creación de un *Sistema de Gestión de Seguridad de la Información (SGSI)* dentro de las organizaciones mediante un enfoque sistémico que incluya a las personas, procesos y sistemas de TI con el propósito de fortalecer y mejorar la gestión de la información confidencial de la empresa para que sea segura.

El diseño y la implementación de un SGSI de acuerdo con la Norma ISO/IEC 27001:2005 brinda confianza a clientes y proveedores de que la seguridad de la información se toma en serio

dentro de la organización, por lo que buscar estar a la vanguardia en la aplicación de estrategias técnicas y de procesos para hacer frente a las amenazas de la información y a los problemas de la seguridad.

Evaluación de riesgos. La implantación del Sistema de Gestión de la Seguridad de la Información (SGSI), de acuerdo con la Norma ISO/IEC 27001, dentro de las empresas, permite a las áreas directivas definir los alcances y ámbitos de aplicación de la norma.

El proceso de implementación debe considerar como eje central la *evaluación de riesgos* para definir las políticas y medidas que serán consideradas en las áreas de la empresa. Además, se debe integrar la metodología de mejora continua en correspondencia a las normas ISO.

La tarea inicial es elegir una metodología de evaluación del riesgo apropiada para los requerimientos de la empresa. La Norma ISO/IEC 27001 sugiere la metodología que se presenta en la Figura 7.

Figura 7. Metodología de evaluación de riesgos.
Fuente: Elaboración propia con base en [40].

Las etapas de la metodología propuesta en la Norma ISO/IEC 27001 son las siguientes:

1. Definición de los *activos de información*. Un activo de información es aquello que tiene valor para la organización, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (ideas, aplicaciones, proyectos) así como las marcas; además, se considera la confianza clientes y proveedores y la reputación de la empresa.

2. Identificación de las *vulnerabilidades*. Se refiere a las debilidades propias de cada activo de información y que lo hacen susceptible de amenazas de seguridad que posibilitan el sufrir ataques o daños.
3. Determinación de las *amenazas*. Una amenaza a los activos de información es una situación, cosas o condición que puede suceder y generar daños. Los desastres naturales, incendios, ataques de virus y espionaje son algunos ejemplos de amenazas.
4. Análisis de los *requisitos legales y contractuales*. Conocer y analizar los requisitos legales y contractuales que la empresa tiene la obligación de cumplir con sus clientes, socios y proveedores.
5. Definición de los *riesgos*. Para cada activo de información se define la probabilidad de que las amenazas o las vulnerabilidades puedan causar un daño total o parcial, en relación con su disponibilidad, confidencialidad e integridad.
6. Realización del *cálculo* de riesgos. Es necesario priorizar los riesgos que deben ser controlados. La ecuación (1) permite efectuar el cálculo del riesgo a partir de la probabilidad de su ocurrencia y el impacto que este tendría sobre la organización.

$$Riesgo = impacto\ x\ probabilidad\ del\ riesgo \quad (1)$$

7. Integración de un *Plan de tratamiento* del riesgo. Con los resultados del análisis y cuantificación de los riesgos es posible definir estrategias de tratamiento y mitigación, así como de políticas específicas desde la dirección de la empresa. El plan de tratamiento de riesgos incluye los controles adecuados orientados a:
    - Asumir el riesgo
    - Reducir el riesgo
    - Eliminar el riesgo
    - Transferir el riesgo

A finales del año 2022, los dos organismos principales de normalización a nivel mundial: ISO, de Ulrika Francke, y el IEC, de Jo Cops, liberaron el nuevo estándar ISO/IEC 27001:2022. Esta nueva versión es la integración actualizada de las mejores prácticas a nivel internacional en materia de resguardo y seguridad de la información, tanto en el mundo físico como en el ámbito digital.

6. La ciberseguridad en México.

De conformidad con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares [41], en el año 2022 en México se reportaron 93.1 millones de personas usuarias de Internet, lo que representó el 78.6% de la población de 6 años o más. Los resultados de la encuesta registraron 93.8 millones de personas usuarias de teléfono celular, la cifra equivale al 79.2% de la población de 6 años o más. Además, el 37.0% de la población de 6 años o más utilizó computadora.

En la Tabla 2 se presentan los porcentajes de usuarios de Internet según su lugar de acceso. En 2022, el 41.3% de las personas usuarias de Internet se conectaron en el trabajo, lo que significó un aumento de 2.7 puntos porcentuales con respecto a 2021. Las personas que se conectaron en la escuela representaron 18.0% del total, con un incremento de 3.9 puntos porcentuales respecto al año 2021. Los usuarios que se conectaron a Internet desde su hogar representan el 95.4%, que representa un aumento de 0.2 puntos porcentuales respecto del año anterior. Mientras que quienes se conectaron en cualquier otro lugar mediante una conexión móvil representaron el 54.9%, lo que significó una disminución de 0.3 puntos porcentuales respecto del año anterior.

Tabla 2. Lugar de acceso de los usuarios de Internet.

	Lugar de acceso	2021	2022	Crecimiento
1	Hogar	95.2	95.4	0.2
2	Trabajo	38.6	41.3	2.7
3	Escuela	14.1	18.0	3.9
4	Otro lugar con conexión móvil	55.2	54.9	-0.3

Fuente: Elaboración propia con datos de [41].

Respecto a los tipos de usos que dan los usuarios al Internet, en la Tabla 3 se presentan las cifras de la encuesta para el año 2022. El uso principal que se le dio al Internet fue para comunicarse (93.8%), siguieron el acceso a redes sociales (90.6%) y el entretenimiento (89.6%). Respecto a los tipos de usos que presentan mayores incrementos del año 2019 a 2022 son la realización de pagos vía internet con un 8.6%, la compra de productos o servicios con 8.5% y las operaciones bancarias en línea en 7.8%. En contraste con lo anterior, leer periódicos, revistas o libros disminuyó 7.2%, descargar software o aplicaciones disminuyó 5.1% y buscar información disminuyó 1.2%, en el mismo periodo.

Tabla 3. Tipos de usos de los usuarios de Internet.

	Lugar de acceso	2019	2022	Crecimiento
1	Comunicarse	90.5	93.8	3.3
2	Acceder a redes sociales	87.7	90.6	2.9
3	Entretenimiento	91.4	89.6	-1.8
4	Acceder a contenidos audiovisuales	80.4	79.5	-0.9
5	Leer periódicos, revistas o libros	47.1	39.9	-7.2
6	Buscar información	90.5	89.3	-1.2
7	Apoya la capacitación o educación	83.5	83.3	-0.2
8	Descargar software o aplicaciones	48.1	43.0	-5.1
9	Interactuar con el gobierno	35.4	39.1	3.7
10	Comprar productos o servicios	22.1	30.6	8.5
11	Pagos vía Internet	18.3	26.9	8.6
12	Operaciones bancarias en línea	16.6	24.4	7.8
13	Utilizar servicio en la nube	19.2	23.0	3.8
14	Ventas por Internet	9.3	11.3	2.0

Fuente: Elaboración propia con datos de [41].

De acuerdo con la Asociación de Bancos de México y la American Chamber [42], las empresas en México fueron víctimas del 66% de los ataques cibernéticos ocurridos en América Latina en el período de 2021-2022, lo que provocó pérdidas de entre 3,000 y 5,000 millones de dólares por año.

El Estudio sobre el Estado Global de la Ciberseguridad en México 2023 [43] de CyberRisk Alliance reporta que el país ocupa el primer puesto de Latinoamérica en recibir más ciberataques. El documento reporta que el 70% de las personas encuestadas confesó que sufrió uno o más ataques de phishing o ransomware en los últimos 12 meses.

Los ataques de phishing o ransomware que implican la manipulación, exposición o bloqueo de datos confidenciales y/o la interrupción de la actividad del sistema. La fuga de datos y el ransomware fueron los ataques más alarmantes para el 51% de las empresas mexicanas incluidas en el estudio.

Por otra parte, el reporte incluye las cifras que están relacionadas con el temor de la posibilidad de las amenazas o riesgos que se pueden presentar en las empresas y organizaciones, se presentan en la Tabla 4. De las mayores amenazas o riesgos se menciona que el 43% de los encuestados considera a los ataques directos a través de servicios en la nube; el 35% a los ataques a través de conexiones de trabajadores remotos; el 27% a amenazas persistentes avanzadas; el 21% a ataques a través de IoT en red; el 18% a amenazas internas; el 10% a ataques a la cadena de suministro o de terceros; y, el 3% a ataques patrocinados por un Estado.

Tabla 4. Riesgos o amenazas para las empresas mexicanas.

	Riesgo o amenaza	Respuestas
1	Ataques directos a través de servicios en la nube	43%
2	Ataques a través de conexiones de trabajadores remotos	35%
3	Amenazas persistentes avanzadas	27%
4	Ataques a través de IoT en red	21%
5	Amenazas internas	18%
6	Ataques a la cadena de suministro o de terceros	10%
7	Ataques patrocinados por un Estado	3%

Fuente: Elaboración propia con datos de [43].

El mismo estudio incluye algunos elementos clave para el mercado mexicano. Destaca que el 65% de los encuestados aceleraron las transformaciones digitales para apoyar a los trabajadores remotos; el 58% agregó recursos a sus redes y bases de datos; y, el 57% aumentó el soporte de los portales de los clientes para la interacción remota.

Por otra parte, el estudio describe que el 79% de las organizaciones tarda hasta 24 horas en investigar una amenaza, y aunque el 69% de las empresas aumentó su presupuesto para seguridad informática, hay un 12% que no modificará este recurso, mientras que un 26% podría incluso reducir el monto.

7. Buenas prácticas de seguridad para IoT

Para definir las estrategias encaminadas a garantizar la seguridad de los dispositivos, la red y los sistemas IoT en las siguientes secciones se incluyen algunas buenas prácticas reportadas en la literatura y por los organismos internacionales del sector de seguridad de la información.

Mantener los dispositivos y software actualizados. Las actualizaciones de firmware y software son una parte importante para fortalecer la seguridad de los sistemas IoT. Es recomendable que siempre que se adquiera un nuevo dispositivo debe asegurarse que los fabricantes o proveedores proporcionen las actualizaciones de firmware o software, según corresponda, y deben instalarse de forma constante cada vez que estén disponibles.

Se debe considerar que los fabricantes o proveedores de los dispositivos IoT pueden enviar actualizaciones automáticas, o quizá se deba ingresar a los sitios web oficiales para consultar si hay nuevas versiones para descargarlas e instalarlas de forma manual.

Cambiar las contraseñas por defecto de los dispositivos IoT. Las asignaciones de contraseñas de acceso y de credenciales de inicio de sesión en los dispositivos IoT es una tarea importante para configurar las estrategias de seguridad del sistema. Es recomendable que las contraseñas y credenciales por defecto sean cambiadas por otras nuevas y únicas para cada dispositivo IoT integrado en el sistema.

Utilizar contraseñas seguras. Las contraseñas asignadas a los dispositivos IoT y los componentes de la red de comunicación deben ser seguras. Es recomendable que las contraseñas sean largas (al menos 12 caracteres), utilizar combinaciones de letras mayúsculas y minúsculas, además de agregar símbolos o números.

Se debe evitar las contraseñas obvias tales como secuencias de letras o números, información personal que alguien conozca o fácil de adivinar, tales como fechas de nacimiento o nombre de lugares o mascotas.

Es importante formalizar el uso de un administrador de contraseñas para ayudar a resguardar y organizar las contraseñas de acceso y credenciales de inicio de sesión.

Cambiar el nombre de los dispositivos IoT y de red. Los componentes del sistema IoT están identificados por un nombre, por ello es importante no conservar el nombre de fábrica de los dispositivos IoT y de componentes de la red. Por tanto, es recomendable asignar un nombre nuevo a cada dispositivo y componente de red integrado en el sistema para incrementar la seguridad; lo anterior, con el propósito de que resulte más difícil para los intrusos la identificación de las marcas, modelo o versiones.

Utilizar un método de cifrado de WIFI seguro. En caso de utilizar redes inalámbricas WIFI es recomendable utilizar un método de cifrado seguro para la configuración de los componentes de la red. Al utilizar WPA2 (Wi-Fi Protected Access 2) o versión posterior contribuye a mantener la red y las comunicaciones seguras. Los métodos WEP (Wired Equivalent Privacy) y WPA (WIFI Protected Access) son vulnerables a ataques de intrusos.

Controlar los ajustes de privacidad. Los valores de los ajustes de privacidad y de seguridad de los dispositivos IoT deben ser revisados y configurados para asegurarse que se utilizan las opciones y funciones en correspondencia a las estrategias de seguridad de la información.

Es recomendable revisar las políticas de privacidad del fabricante o proveedor para conocer y entender cómo se almacenan y utilizan los datos del usuario.

Desactivar funciones que no se utilicen. Se trata de realizar la revisión y seguimiento de las funciones disponibles en los dispositivos IoT para desactivar las que no se utilizan con el propósito de disminuir las posibilidades de riesgos o amenazas. El deshabilitar funciones que no se utilicen no afecta la operación y eficiencia de los dispositivos IoT.

Activar la autenticación de varios factores. La autenticación de varios factores (MFA, por sus siglas en inglés) es un método de autenticación que solicita a los usuarios que proporcionen dos o más métodos de verificación para acceder a un dispositivo o iniciar sesión en el sistema. En lugar de solo solicitar nombre de usuario y contraseña, la autenticación de varios factores solicita más información, tales como una contraseña de uso único que los servicios de autentificación del sistema envían al teléfono móvil o al correo electrónico del usuario.

Estas buenas prácticas pueden servir de base para la configuración, formalización e implementación de soluciones preventivas y sistemas de defensa para hacer frente a los riesgos y amenazas cibernéticas que enfrentan las personas, organizaciones y empresas.

Conclusiones

A través de las tecnologías digitales asociadas a la Industria 4.0 se fortalece la propuesta de lograr sistemas de producción y de gestión autónomos altamente eficientes y efectivos, a través de un ecosistema integrado y comunicado. La convergencia y aplicación de dichas tecnologías configuran un conjunto de oportunidades y desafíos para las empresas, organizaciones y personas en los procesos de creación, transformación e innovación en su modelo de negocios y procesos de trabajo.

Entre las tecnologías que constituyen la Industria 4.0, se encuentra el ecosistema del Internet de las Cosas (IoT) el cual permite la operación de sistemas integrados y conectados por redes de comunicación e intercambio de datos entre objetos físicos, dispositivos, vehículos y sistemas de software que recopilan, comunican, comparten y procesan datos que permiten la interacción con el entorno y con otros sistemas integrados.

En este nuevo contexto, los sistemas de las empresas y organizaciones almacenan y procesan continuamente grandes cantidades de datos que son vulnerables a amenazas y riesgos tanto físicos como cibernéticos. Por ello, es necesario e importante diseñar e implantar estrategias, procedimientos y regulaciones encaminadas a fortalecer la protección de los activos de información e infraestructura de tecnologías de la información en las organizaciones.

Para enfrentar los riesgos de ciberseguridad de los ecosistemas del Internet de las Cosas (IoT), dispositivos físicos, redes de comunicación e intercambio de datos, los organismos

internacionales y nacionales promueven la aplicación de regulaciones y modelos de seguridad dirigidos a la protección de las personas y las empresas ante los delitos cibernéticos.

Del mismo modo, las organizaciones implementan acciones preventivas, refuerzan la seguridad de sus sistemas y establecen planes de respuesta ante incidentes con el fin de proteger su infraestructura, servicios y datos contra posibles ataques, lo cual permite minimizar los efectos en caso de que se produzcan.

Es fundamental que tanto los gestores como los usuarios de datos, mantengan una postura proactiva y sean parte integral de una estrategia de ciberseguridad, lo cual implica que estén informados y capacitados, cumplan las políticas y procedimientos establecidos en sus organizaciones, usen responsablemente los recursos tecnológicos disponibles, identifiquen posibles amenazas y colaboren con los profesionales de seguridad de la información en su entorno.

Finalmente, las buenas prácticas incluidas en este trabajo tienen el propósito de fomentar la seguridad de los datos personales, preservar la integridad de los dispositivos IoT, salvaguardar la privacidad de las redes de comunicación y el intercambio de datos, y garantizar el funcionamiento adecuado y continuo de los sistemas de información que son fundamentales para el correcto desempeño de cualquier empresa u organización en la actualidad.

Referencias

[1]. Kagermann, H., Lukas, D. & Wahlster, W. (april 1, 2011). Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution. *VDI nachrichten.* http://www.wolfgang-wahlster.de/wordpress/wp-content/uploads/Industrie_4_0_Mit_dem_Internet_der_Dinge_auf_dem_Weg_zur_vierten_industriellen_Revolution_2.pdf

[2]. Kagermann, H., Wahlster, W., & Helbig, J. (2013). Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Final report of the Industrie 4.0 Working Group. *Final Report of the Industrie 4.0.* National Academy of Science and Engineering.

[3]. Schroeder, W. (2016). *Germany's Industry 4.0 strategy*. Friedrich Eberto Stifitung. https://www.fes-london.org/fileadmin/user_upload/publications/files/FES-London_Schroeder_Germanys-Industrie-40-Strategy.pdf

[4]. Navarro, M. & Sabalza, X. (2016). Reflexiones sobre la Industria 4.0 desde el caso vasco. *Ekonomiaz: Revista vasca de economía*, (89), 142-173.

[5]. Almada-Lobo, F. (2015). The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES) *Cyber-physical Systems,* 4, 16–21.

[6]. Prieto, M. I. A. (2018). Planeación para la automatización en el proceso de maquinado [Tesis de pregrado, Universidad Tecnológica del Centro de Veracruz]. http://reini.utcv.edu.mx/bitstream/123456789/328/1/IMI_MIGUEL%20DIMAS_FLORES.pdf

[7]. Rose, J., Lukic, V., Milon, T. & Cappuzzo, A. (2016). Sprinting to value in Industry 4.0. *BCG* Perspectives.https://www.bcg.com/publications/2016/lean-manufacturing-technology-digital-sprinting-to-value-industry-40

[8]. Abramovici, M., Gebus, P. & Savarino, P. (2018). Engineering smarter Produkte und Services Plattform Industrie 4.0 studie. *Acatech–Deutsche Akademie der Technikwissenschaften, München*. https://www.acatech.de/wp-content/uploads/2018/04/PI40_Forschungsbeirat_SmartEngineering_web_bf.pdf

[9]. Motyl, B., Baronio, G., Uberti, S., Speranza, D. & Filippi, S. (2017). How will Change the Future Engineers' Skills in the Industry 4.0 Framework? A Questionnaire Survey. *Procedia Manufacturing,* 11(June), 1501–1509. https://doi.org/10.1016/j.promfg.2017.07.282

[10]. Mikhailov, A. N., Rodin, A. B. & Smirnova, M. I. (2018). Humanization of Engineering Education in Conditions of the Process of Industry 4.0 Forming. *2018 4th International Conference on Information Technologies in Engineering Education, Inforino 2018 - Proceedings*, 1–4. https://doi.org/10.1109/INFORINO.2018.8581805
[11]. Coşkun, S., Kayıkcı, Y. & Gençay, E. (2019). Adapting Engineering Education to Industry 4.0 Vision. *Technologies,* 7(1), 10. https://doi.org/10.3390/technologies7010010
[12]. Stachová, K., Papula, J., Stacho, Z. & Kohnová, L. (2019). External partnerships in employee education and development as the key to facing industry 4.0 challenges. *Sustainability (Switzerland),* 11(2). https://doi.org/10.3390/su11020345
[13]. Ciolacu, M. I., Binder, L., Svasta, P., Tache, I. & Stoichescu, D. (2019). *Education 4.0–jump to innovation with IoT in higher education.* 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), 135-141. IEEE.
[14]. Motyl, B., Baronio, G., Uberti, S., Speranza, D. & Filippi, S. (2017). How will Change the Future Engineers' Skills in the Industry 4.0 Framework? A Questionnaire Survey. *Procedia Manufacturing,* 11(June), 1501–1509. https://doi.org/10.1016/j.promfg.2017.07.282
[15]. Piccarozzi, M., Aquilani, B. & Gatti, C. (2018). Industry 4.0 in management studies: A systematic literature review. *Sustainability (Switzerland),* 10(10), 1–24. https://doi.org/10.3390/su10103821
[16]. Rocha, L., Savio, E., Marxer, M. & Ferreira, F. (2018). Education and training in coordinate metrology for industry towards digital manufacturing. *Journal of Physics: Conference Series,* 1044(1). https://doi.org/10.1088/1742-6596/1044/1/012026
[17]. BCG. (2016). Industry 4.0. https://www.bcg.com/capabilities/manufacturing/industry-4.0
[18]. Muñoz, O. Q. (2019). Internet de las cosas (Iot). Ibukku LLC.
[19]. OECD (2018), IoT measurement and applications, *OECD Digital Economy Papers*, No. 271, OECD Publishing, Paris, https://doi.org/10.1787/35209dbf-en.
[20]. Deloitte (2021). *México rezagado en Internet de las Cosas.* https://www2.deloitte.com/mx/es/pages/dnoticias/articles/internet-de-las-cosas-en-mexico.html
[21]. PwC. (2019). *IoT Survey 2019, edición México* [Video]. YouTube. IoT Survey 2019, edición México.
[22]. Statista. (2023, March 31). *Mexico: number of IoT devices 2018-2025.* https://www.statista.com/statistics/1001025/mexico-number-iot-devices/?gclid=Cj0KCQjw1_SkBhDwARIsANbGpFuQtKw7hmVz2btkO5XsAcLfvmoomvDI3g6-tuammSAAynVftNnA3UaAieMEALw_wcB#statisticContainer
[23]. Gobierno de México (2021), *Secretaría de Economía ¿Qué hacemos?* Disponible en: https://www.gob.mx/se/que-hacemos
[24]. NYCE (2021), ¿Quiénes somos? Disponible en: https://www.nyce.org.mx/quienes-somos/
[25]. Diario Oficial de la Federación (2020a), *DECLARATORIA de vigencia de la Norma Mexicana NMX-I-320-NYCE-2020*. Disponible en: https://sidof.segob.gob.mx/notas/5593710
[26]. Diario Oficial de la Federación (2020b), *DECLARATORIA de vigencia de la Norma Mexicana NMX-I-321-NYCE-2020*. Disponible en: https://sidof.segob.gob.mx/notas/5593711
[27]. Diario Oficial de la Federación (2022), *DECLARATORIA de vigencia de la Norma Mexicana NMX-I-1362-NYCE-2021*. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5642167&fecha=08/02/2022#gsc.tab=0
[28]. IFT (2021), Objetivos Institucionales. Disponible en: http://www.ift.org.mx/conocenos/objetivosinstitucionales
[29]. IFT (2021), Programa Anual de Trabajo 2021, Pág. (42). Disponible en: http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/pat2021.pdf
[30]. IFT (2020), Estrategia IFT 2021-2025. Hoja de Ruta. Pág. (4). Disponible en: http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025
[31]. Laudon, K. & Laudon, J. (2016). Sistemas de información gerencial. (Décimo cuarta ed.). Pearson, México.
[32]. Consejo de Europa. (2002). Convenio sobre la Ciberseguridad, Budapest, 23.XI.2001. Serie de Tratados Europeos No. 185.

[33]. Díaz, R. M. (2021). Estado de la ciberseguridad en la logística de América Latina y el Caribe, serie Desarrollo Productivo, N° 228 (LC/TS.2021/108), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL).
[34]. Comisión de Relaciones Exteriores. (2021). Dictamen de la Comisión para la adhesión de México al Convenio de Budapest, México, Senado de la República.
[35]. Covarrubias, L., Zadamig, J. (2020). El estatus de México y el Convenio sobre la Ciberdelincuencia de Budapest (The status of Mexico and the Budapest Convention on Cybercrime). Foro Jurídico.
[36]. BID. (2020). Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe; Banco Interamericano de Desarrollo, Organización de los Estados Americanos. Doi: http://dx.doi.org/10.18235/0002513
[37]. Rea Guaman, A. M. (2020). Madurez en la identificación y evaluación de riesgos en ciberseguridad. Universidad Politécnica de Madrid, Tesis Doctoral.
[38]. GCSCC. (2021). Cybersecurity Capacity Maturity Model for Nations (CMM). Global Cyber Security Capacity Centre, Oxford University.
[39]. BID. (2022). Observatorio de la Ciberseguridad en América Latina y el Caribe en su Reporte de Ciberseguridad 2022. BID. https://observatoriociberseguridad.org
[40]. ISO. (2023). ISO 27001 Seguridad de la Información. Normas ISO. https://www.normas-iso.com/iso-27001/
[41]. ENDUTIH. (2022). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, Instituto Federal de Telecomunicaciones, México. https://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/encuesta-nacional-sobre-disponibilidad-y-uso-de-tecnologias-de-la-informacion-en-los-hogares-endutih-0
[42]. Guerrero, S. (2023). Dientes contra ciberdelincuentes. Forbes. https://www.forbes.com.mx/dientes-contra-ciberdelincuentes/
[43]. CRA. (2023). Estudio de 2023 sobre el estado global de la ciberseguridad en México. CyberRisk Alliance, Infoblox. https://info.infoblox.com/resources-whitepapers-mexico-2023-global-state-of-cybersecurity-study

El proceso de democratización del internet y el surgimiento de la ciberseguridad

Juan Manuel Aguilar Antonio[1] [0000-0002-4686-685X]

[1] Centro de Investigaciones sobre América del Norte (CISAN), Universidad Nacional Autónoma de México (UNAM). Este artículo se realizó con apoyo del Programa de Becas Postdoctorales de la UNAM, el autor está adscrito al CISAN, asesorado por el Dr. Leonardo Curzio.
[2] Pisos 1, 7, 9 y 10, Torre II de Humanidades, C.U., 04510, Ciudad de México, México
alchemistffvii@hotmail.com

Abstract. El presente artículo tiene como objetivo presentar una historia de la evolución de la historia del internet, hasta englobar el surgimiento de la ciberseguridad como un problema de seguridad pública, seguridad nacional y seguridad internacional. En ese sentido, el texto comienza a abordar aspectos como el surgimiento del internet, desde el proyecto ARPANET, del Departamento de Defensa de los Estados Unidos, hasta el desarrollo de la World Wide Web por parte de la Organización Europea para la Investigación Nuclear (CERN). Del mismo modo, se presenta aspectos que permitieron la democratización del internet, como el surgimiento de los PC en la década de los ochenta y la evolución de la historia del telefónico móvil desde los noventa. Posteriormente, se presenta cómo durante la década de los años 2000 la ciberseguridad se transformó en un problema de seguridad pública, con ejemplos representativos como Napster, Pirate Bay, Megaupload y Silk Road, que pusieron de manifiesto la problemática del uso de internet y su regulación. Después, se presenta como la ciberseguridad se convirtió en un problema de seguridad nacional a razón del ciberataque de Estonio, en 2007, lo que transformó la postura de organismos internacionales como la Organización del Tratado del Atlántico Norte (OTAN) y lo cual promovió el desarrollo de políticas nacionales de ciberseguridad por los gobiernos del mundo. Por último, se presenta una pequeña reflexión de cómo tecnologías como la inteligencia artificial (IA), Big Data, Computo Cuántico y redes 5G influirán en el futuro de ciberseguridad.

Keywords: Palabras clave: Internet, Ciberseguridad, Internet de las Cosas, Telefonía Móvil, Ciber Crimen.

1. ARPANET: el origen del internet.

La historia de ARPANET (acrónimo de la Red de la Agencia de Proyectos de Investigación Avanzada), es un testimonio del espíritu innovador y la colaboración entre el gobierno, instituciones académicas y la industria tecnológica. Iniciada como un proyecto de investigación y desarrollo, ARPANET abrió el camino para la creación del internet moderno que define la actualidad.

Del mismo modo, su desarrollo forma parte de la historia de la informática, la computación y ramas de conocimiento que han estado llenas de visionarios que contribuyeron de manera significativa al desarrollo de la tecnología de la información. En ese sentido, el personaje clave en el desarrollo de ARPANET fue Joseph Carl Robnett Licklider, comúnmente conocido como J.C.R. Licklider, quien nació el 11 de marzo de 1915, en San Luis, Misuri, Estados Unidos. Desde temprana edad, Licklider demostró un talento sobresaliente en diversas disciplinas académicas, incluyendo la psicología, la física y las matemáticas. Sus primeros logros académicos lo llevaron a obtener una licenciatura en letras en 1937 y, posteriormente, una licenciatura en psicología en 1938 de la Universidad de Washington en San Luis [1].

Sin embargo, su interés por la psico acústica lo llevó a realizar estudios de posgrado en la Universidad de Rochester, donde obtuvo un doctorado en psico acústica en 1942. Durante este tiempo, Licklider llevó a cabo investigaciones importantes sobre la percepción auditiva y la psico acústica, lo que sentó las bases para su futura carrera en el campo de la tecnología de la información. No obstante, a pesar de su formación en dicha área, el interés de Licklider se desvió hacia la tecnología de la información. En 1950, se unió al Instituto Tecnológico de Massachusetts (MIT) como profesor asociado y desempeñó un papel crucial en el establecimiento del Laboratorio Lincoln del MIT. Durante su tiempo en el MIT, Licklider inició un programa de psicología para estudiantes de ingeniería, marcando su transición de la psico acústica a la informática [2].

En esos años, uno de los logros más destacados de Licklider fue su visión de la interacción hombre-ordenador. En 1960, escribió un influyente artículo titulado *Man-Computer Symbiosis* (Simbiosis Hombre-Computador), donde delineó la necesidad de simplificar la interacción entre los seres humanos y las computadoras [3]. En este artículo, Licklider argumentó que las computadoras deberían convertirse en herramientas accesibles que ampliarían las capacidades humanas en lugar de ser máquinas intimidantes. De esta forma, Licklider previó un futuro en el que las computadoras serían utilizadas como medios de expresión y herramientas para la creatividad. Su visión sentó las bases para el desarrollo de interfaces de usuario amigables, sistemas de tiempo compartido y, en última instancia, la computación personal.

Para 1962, Licklider asumió el cargo de jefe de la Oficina de Técnicas de Procesamiento de la Información (IPTO) en la Agencia de Investigación de Proyectos Avanzados (ARPA) del Departamento de Defensa de los Estados Unidos. Fue en este lugar en el que concibió la idea de una red de computadoras interconectadas a nivel mundial en uno de sus cuadernos de apuntes durante el mes de agosto de ese mismo año. En estas notas, Licklider delineó una visión audaz y ambiciosa de una red global de computadoras que permitiría la comunicación y el intercambio de información entre sistemas informáticos dispersos por todo el mundo, a la que denominó "Red de ordenadores intergaláctica" (o *Intergalactic Computer Network* en inglés) [4].

Su visión no se limitaba simplemente a la transferencia de datos, sino que abarcaba la idea de que las computadoras servirían como herramientas de colaboración y expresión creativa, en lugar de meras máquinas de cálculo, con lo que abrió el camino para una revolución en la forma en que las personas interactúan con la tecnología y comparten conocimientos. Aunque estas notas originales no son de acceso público, su influencia en el desarrollo de ARPANET y, finalmente, en la creación de Internet, es innegable y ha dejado una huella indeleble en la historia de la informática y las redes de computadoras.

Sin embargo, la visión de Licklider no se detuvo en las palabras escritas en sus notas o en la simple idea de la *Intergalactic Computer Network*. En su posición como director de ARPA reconoció la necesidad de asociarse con la academia y empresas tecnológicas innovadoras para hacer realidad su visión. En ese sentido, el Departamento de Defensa se interesó en el proyecto y convocó a destacados investigadores del área de la informática como Ivan Sutherland, Robert Taylor y Paul Baran, quienes desarrollaron ideas clave como la descentralización de la red y la fragmentación de mensajes en paquetes. También, Licklider identificó que la empresa BBN Technologies, originalmente Bolt, Beranek and Newman, Inc., era un actor líder en tecnología de la información y la investigación en computadoras [5].

El origen de BBN Technologies se remontaba a 1948, cuándo Leo Beranek, Richard Bolt y Robert Newman, crearon una firma de consultoría acústica antes de diversificarse hacia la computación y las redes de comunicación. Es precisamente durante sus años de estudios de doctorado en el MIT, y su interés en la psicoacústica, que Licklider conoce el trabajo de la empresa para una consultoría que realizó BNN Technologies para el diseño acústico de la Asamblea de la Organización de Naciones Unidas, en Nueva York, evento que marcó el comienzo de su historia de éxito.

Sin embargo, la necesidad de realizar cálculos complejos llevó a BBN Technologies a adquirir computadoras, incluida la legendaria PDP-1 de *Digital Equipment Corporation* (DEC). La DEC era una empresa que fue fundada en 1957, que tuvo una idea innovadora en su tiempo, transformar las computadoras enormes, costosas y generalmente utilizadas para aplicaciones científicas y militares, en modelos más pequeños y asequibles que pudieran ser utilizadas por la gente común. En ese sentido, a diferencia de las computadoras de gran escala de la época, la PDP-1 era notablemente más pequeña y asequible. Su diseño compacto la hizo accesible para instituciones académicas y empresas que no podían permitirse las costosas computadoras principales entre las cuales estuvieron BNN Technologies, que quedaron fascinados con su funcionamiento y decidieron diversificar su empresa hacia el mundo de la informática [6].

La visión de BBN Technologies por apostar por la tecnología de la información hicieron que ARPA la eligieran para llevar a cabo el ambicioso proyecto de la *Intergalactic Computer Network*. Entre las labores que realizó se encuentran:

- Desarrollar y construir la interfaz de mensajes (IMP): que fue un conmutador de paquetes especializado diseñado para enrutar datos a través de ARPANET. El IMP permitió la conmutación de paquetes de datos, una tecnología esencial para la transmisión eficiente de información a través de una red de computadoras.
- Desarrollo del Protocolo NCP: el cual fue el primer protocolo utilizado en ARPANET para permitir la comunicación entre las computadoras conectadas a la red.

- Configuración de los Primeros Nodos de ARPANET: la empresa instaló los primeros nodos experimentales de ARPANET [7].

El trabajo de BNN Technologies se prolongó por casi siete años, hasta que el 26 de octubre de 1969 se realizó el envío del primer mensaje a través de ARPANET. Sin tener conocimiento de causa, esa jornada el mundo estaba al borde de una revolución que transformó la forma en que la humanidad se comunica y comparte información. El punto de conexión fue entre la Universidad de California en Los Ángeles (UCLA), y el Instituto de Investigaciones de Stanford (Stanford Research Institute, en inglés) a más de 560 kilómetros de distancia.

La conexión comenzó desde la UCLA, en la que el estudiante de posgrado Charley Kline a través de la computadora SDS Sigma 7, ingresó los caracteres del mensaje que daría inició a la era del internet, el cual fue: "LOGIN" Pronto, a 560 kilómetros de distancia, en Stanford, el mensaje llegó con éxito. Con lo cual, ARPANET, la "Red de ordenadores intergalácticas" concebida en un cuaderno de notas en agosto de 1962 por J.C.R. Licklider, y financiada por el proyecto ARPA del Departamento de Defensa de los Estados Unidos, era una realidad [8].

Este primer mensaje marcó el inicio de una revolución en la forma en que las personas se comunican, comparten información y acceden al conocimiento. Hoy en día, vivimos en un mundo en el que la conectividad global es una parte fundamental de la vida cotidiana, y todo comenzó con un atrevido "LOGIN" enviado a través de ARPANET en una fría noche de octubre de 1969.

Uno de los aspectos más destacados de ARPANET fue su enfoque en la conmutación de paquetes, que permitía la transmisión eficiente y resistente a fallos de datos. Inicialmente, ARPANET utilizaba el protocolo NCP (Network Control Program), pero en 1981, se adoptó el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol), que se convirtió en el estándar para las comunicaciones en redes y sigue siendo fundamental para internet en la actualidad [9].

Con el pasar de los años, ARPANET experimentó un crecimiento constante, con 213 computadoras conectadas, en 1971, y más de 500, en 1983. Este crecimiento fue impulsado en gran medida por el correo electrónico y otras aplicaciones de red. Con esto, ARPANET sentó las bases para el desarrollo del internet moderno, con su infraestructura descentralizada, tecnología de conmutación de paquetes y protocolos TCP/IP. Entre los grandes personajes que pasaron a la historia junto a Licklider en el desarrollo de proyecto se encuentran Ray Tomlinson, quien inventó el correo electrónico, Bob Kahn quien fue vital en él desarrolló del protocolo TCP/IP, e Ivan Sutherland que desempeñó un papel importante en la creación de la red.

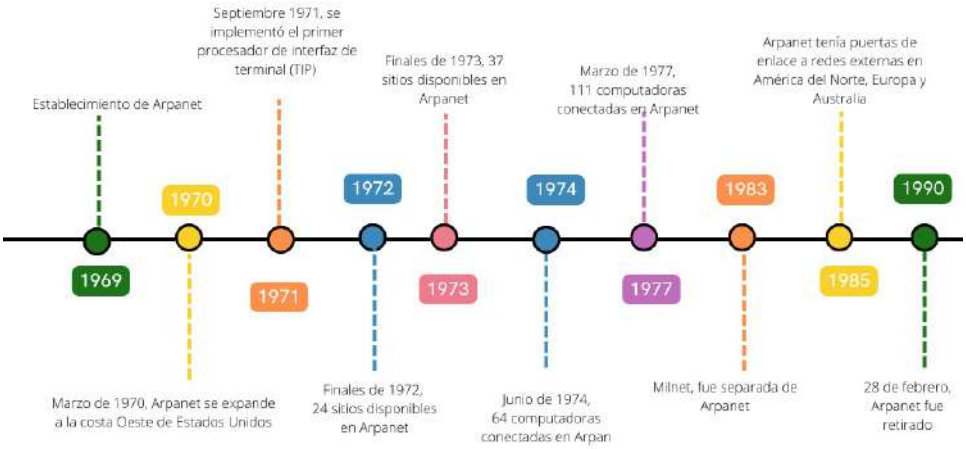

Fig. 1. Evolución de ARPANET desde 1969 hasta 1990 [10].

ARPANET fue un proyecto pionero que transformó la forma en que el mundo se comunica y comparte información. Su impacto perdura en el internet moderno, que se ha convertido en una parte integral de la vida cotidiana en todo el mundo. No obstante, la red fue retirada el 28 de febrero de 1990, para ser sustituida por la World Wide Web o WWW. Para ese punto la red ya realizaba comunicaciones entre redes externas que unían a América del Norte, Europa y Australia. A pesar de su jubilación, el legado de ARPANET nos recuerda la importancia de la investigación, la colaboración y la innovación en el desarrollo de tecnologías que cambian el mundo. Lo cual daría paso al proceso de la democratización del internet.

2. La revolución de los PCs y el surgimiento de la World Wide Web

Si bien ARPANET sentó las bases para el internet moderno, aún existía un importante problema para llevar el internet a todos los rincones y usuarios del mundo: un computador pequeño y a un precio accesible para el ingreso medio de los ciudadanos de los diferentes países del mundo. Cómo ya se mencionó en la sección anterior, la PDP-1 de Digital Equipment Corporation fue un computador pequeño y costo accesible para universidades y empresas durante la década de los años sesenta. Sin embargo, la idea de que una persona perteneciente a la clase media tuviera un computador era impensable, qué decir de una persona en situación de rezago social o pobreza.

En este punto, es cuándo se vuelve trascendental la historia del desarrollo de las computadoras personales (PCs), las cuales representaron una narrativa fascinante de innovación tecnológica, avances en la informática y una revolución en la forma en que interactuamos con el internet y el ciberespacio. Desde los primeros kits de computadoras hasta los dispositivos ultraportátiles y potentes como son hoy en día los IoT (Internet of Things en inglés) que usamos en la actualidad, las PCs han recorrido un largo camino. Con lo cual daremos un breve recorrido histórico desde los inicios de las PCs hasta la era moderna, explorando los hitos clave que han dado forma a la evolución de estas máquinas.

Los inicios de las PCs se remontan al año 1975, cuándo se dio el paso inicial para la revolución de las PCs con el lanzamiento del Altair 8800, un kit de computadora que requería habilidades de ensamblaje. Aunque carecía de una interfaz gráfica de usuario (GUI en sus siglas por inglés) y tenía una capacidad de procesamiento limitada, el Altair 8800 marcó el comienzo de una nueva era. Al año siguiente, en 1976, Steve Jobs y Steve Wozniak fundaron Apple Computer y lanzaron el Apple I, una de las primeras PCs comerciales que incluía una placa de circuito impreso. Esta máquina marcó el camino para el éxito de Apple en el mercado de las PCs y lo perfilaría para ser el gigante de la tecnología que es en la actualidad [11].

Para la década de los ochenta, en concreto en 1981, IBM introdujo la IBM PC, que se convirtió en un estándar en la industria y contribuyó a la popularización de las PCs en entornos empresariales. A mediados de la década, Apple lanzó el Macintosh, el primer ordenador personal en incluir una interfaz gráfica de usuario. Por su parte, una nueva empresa de nombre Microsoft lanzó Windows 1.0 en 1985, sentando las bases para su dominio posterior en el mercado de sistemas operativos [13].

Es precisamente a finales de los ochenta, en el marco de la popularización de los PCs de IBM y Apple, así como de la popularización de Windows, que la idea de la World Wide Web (WWW) se originó. En 1989 el científico británico Tim Berners-Lee quien trabajaba en el CERN (Organización Europea para la Investigación Nuclear) en Ginebra, Suiza, tuvo la inspiración detrás de su creación con el fin de gestionar y compartir información de manera más eficiente en un entorno de investigación científica global.

Lo anterior, se debió a que en el CERN Berners-Lee enfrentó el desafío de manejar vastas cantidades de información y documentación científica dispersa en diferentes sistemas informáticos y dispersos en diferentes países de Europa y el mundo. Su visión era crear un sistema que permitiera a los científicos acceder y compartir fácilmente documentos, resultados de investigaciones y recursos en línea. Para lograr esto, en marzo de 1989, Berners-Lee escribió un memorando en el que propuso un sistema de gestión de la información basado en la hipertextualidad. En este memorando, esbozó la idea de una red de "documentos vinculados" que se podrían acceder a través de hipervínculos [14].

Dicha idea llevó Tim Berners-Lee a crear el primer servidor web, conocido como "httpd" (HTTP daemon) y el primer navegador web llamado "WorldWideWeb" (más tarde renombrado Nexus para evitar confusiones), en 1990. Estos dos componentes iniciales permitieron a los usuarios crear y ver páginas web utilizando un sistema de hipertexto. También, Berners-Lee desarrolló el Protocolo de Transferencia de Hipertexto (HTTP) y el Lenguaje de Marcado de Hipertexto (HTML) como estándares para la Web. Esto es trascendental a razón que HTTP definió cómo se comunicarían los servidores web y los navegadores, mientras que HTML permitió la creación de documentos con formato y enlaces.

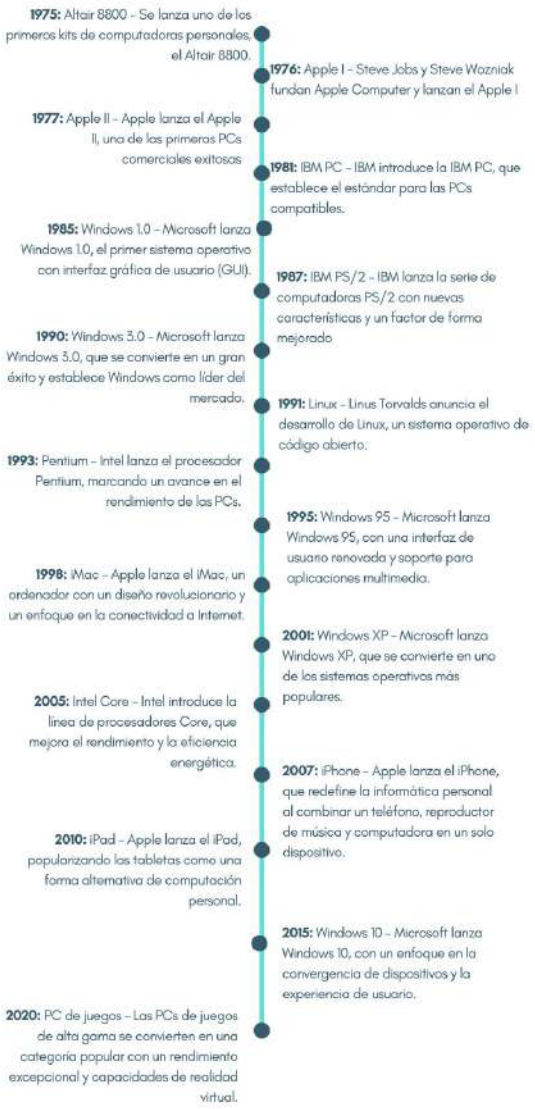

Fig. 2. Línea del tiempo resumida sobre la historia de las PCs [12].

Posteriormente, el primer sitio web sería lanzado el 6 de agosto de 1991 por Berners-Lee, el cual fue el primer portal publicó de la historia, que fue el del CERN. Este portal, presentaba información sobre el propio proyecto de la World Wide Web y cómo usarla. Con esta acción, la idea de la Web se propagó rápidamente, y para 1993, ya había varios navegadores web y servidores en funcionamiento en diferentes partes del mundo [15]. La Web comenzó a crecer exponencialmente y surgieron los primeros motores de búsqueda para ayudar a los usuarios a encontrar información en línea, entre estos se encontraban Wandex, Wencawler, Lycos, AltaVista y Yahoo.

Para garantizar la interoperabilidad y la evolución ordenada de la Web, Berners-Lee fundó el World Wide Web Consortium (W3C) en 1994. El W3C se encargó de desarrollar y mantener estándares abiertos para la Web, como HTML y CSS. La creación de esta institución correspondió al vertiginoso incremento de número de usuarios del internet, tan solo de 1990 el internet había pasado de unos cuántos miles de usuarios, a más de un millón de usuarios en 1993. Sin embargo, el ritmo de crecimiento de usuarios demostró su potencial tan solo un año después, cuándo en 1994 la a WWW continuó su rápido crecimiento y superó los 10 millones. Tan solo en un año el internet presentó una tasa de crecimiento de más del 1000 %, fenómeno inédito en cualquier tecnología de la información o comunicación previa como el correo, el telégrafo o el teléfono.

A medida que el internet se volvió más accesible en la década de los noventa, las PCs se convirtieron en herramientas esenciales para la navegación web, la comunicación por correo electrónico y el acceso a información en línea. Esto impulsó aún más su adopción en hogares y empresas. En 1995, Microsoft lanzó Windows 95, un sistema operativo que incluía la integración de un navegador web llamado Internet Explorer con conectividad a internet, el cual marcó un hito en la adopción generalizada de la web. Este período también vio el surgimiento de los navegadores web, como Netscape y Navigator que intentaron competir con Windows [16].

A pesar de esto, Windows 95 marcó un hito clave debido a la integración de Internet Explorer. Esto facilitó que los usuarios accedieran a la web sin tener que descargar e instalar navegadores por separado. Por lo que Internet Explorer se convirtió en uno de los navegadores más utilizados. El éxito de Windows 95 se debe a que fue lanzado en un momento en que las computadoras personales (PC) se estaban volviendo más asequibles y comunes en los hogares y las empresas. Esto aumentó la base de usuarios potenciales para internet que se sirvieron de este como su primera experiencia en la WWW, entre los principales aportes que realizó este navegador a crear el internet moderno se encuentran:

- Acceso dial-up: gran cantidad de personas comenzaron a utilizar conexiones dial-up para acceder a Internet desde sus hogares. Esto permitió la conexión a la web mediante una línea telefónica y un módem, lo que hizo que Internet fuera más accesible para un público más amplio. El sistema operativo de Windows 95 e Internet Explorer fueron la primera experiencia de los usuarios en el uso del dial-up.
- Correos electrónicos y mensajería instantánea: Además de la navegación web, las funciones de correo electrónico y mensajería instantánea se volvieron populares. Los servicios de correo electrónico como Hotmail y Yahoo! Mail permitieron a las personas comunicarse en línea de manera efectiva, lo que contribuyó a la adopción de internet. Del mismo modo, Windows 95 permitió interfaces directas con estos servicios que lo hicieron popular entre los cada vez más nuevos usuarios de internet [17].

Con esto, Windows 95 desempeñó un papel fundamental en la adopción masiva de internet al facilitar el acceso y la navegación web para una audiencia más amplia. Además, la creciente

disponibilidad de computadoras personales, el acceso dial-up y el correo electrónico contribuyeron a que internet se convirtiera en una parte fundamental de la vida cotidiana de las personas en la década de los noventa.

No obstante, no debemos olvidar que si bien el internet continuaba teniendo un crecimiento exponencial, los PCs vivián un proceso similar, y del mismo modo, pronto aparecían los dispositivos de tecnologías móviles, punto central de la siguiente parte de esta investigación.

3. De la telefonía celular a los dispositivos IoT

Si bien el internet fue concebido para ser utilizado a través de computadoras, en la actualidad es un hecho que el mayor uso de él no lo hacemos a través de un instrumento de esta naturaleza. En la actualidad, el uso del internet, y la generación de datos vinculados al mismo, se da principalmente a través de los Smartphones, que son la antesala de la creación de los dispositivos IoT (Internet de las Cosas) [18].

La historia de las generaciones de los Smartphones se asocia a la historia de la telefonía móvil, comúnmente referidas como las generaciones de "G" (1G, 2G, 3G, 4G, 5G), la cual es una crónica de avances tecnológicos que han transformado la forma en que nos comunicamos y accedemos a la información en dispositivos móviles.

La generación 1G surge durante la década de los ochenta, en este punto, los dispositivos de telefonía móvil eran completamente analógicos y permitían llamadas de voz inalámbricas. Sin embargo, tenían limitaciones significativas en términos de calidad de sonido y seguridad. Esto se debía a que en sus inicios las redes 1G eran incompatibles entre sí, lo que limitaba la capacidad de los usuarios para realizar llamadas en diferentes áreas geográficas. Del mismo modo, es importante mencionar que en la primera generación de telefonía móvil 1G, estos eran bastante diferentes a los dispositivos que conocemos hoy en día. Eran más grandes, pesados y tenían capacidades limitadas en comparación con los teléfonos inteligentes modernos [19].

Entre los primeros modelos de teléfonos móviles utilizados en la era 1G estaban el Motorola DynaTAC 8000X, lanzado en 1983, el cual ganó notoriedad por ser uno de los primeros teléfonos portátiles. Otros de los modelos populares fueron Nokia Mobira Senator, creado en 1982, el Ericsson Dialog 1, de 1984, que fue uno de los primeros teléfonos móviles fabricados por Ericsson. Para el cierre de la década uno de los más populares fue el Motorola MicroTAC, lanzado en 1989, el cual fue uno de los primeros teléfonos móviles que se podían llevar en el bolsillo debido a su diseño más compacto, a pesar de esto, el modelo era muy grande en comparación con los teléfonos modernos.

La generación 2G marcó la transición a sistemas digitales a principios de la década de 1990. En esta época se introdujeron estándares digitales como el GSM (Global System for Mobile Communications) y el CDMA (Code Division Multiple Access). La generación 2G mejoró la calidad de las llamadas y permitió servicios como la mensajería de texto (SMS). También, se establecieron estándares internacionales que permitieron la itinerancia global, a la par que la homologación de las redes mejoró sustancialmente la calidad del audio y la conexión de las llamadas celulares.

La generación 2G abarcó un período de tiempo en el que se lanzaron varios modelos de teléfonos móviles populares. Entre estos estuvo el Nokia 3310, que se transformó en un icono de cultura popular al ser uno de los teléfonos móviles más reconocidos y queridos de todos los tiempos por los usuarios. Este modelo fue conocido por su durabilidad, a tal grado que se indicó era indestructible. También, por incluir el primer juego en un celular, el cual fue Snake. Otros modelos conocidos fueron el Motorola StarTAC, que fue uno de los primeros teléfonos móviles plegables y se convirtió en un símbolo de estatus en su época. Y el Ericsson T28, que fue un teléfono compacto y elegante que ganó popularidad en la era 2G.

La tercera generación o del 3G e implementó a principios de la década de 2000 y permitió una mayor velocidad de transferencia de datos. Esto posibilitó servicios como la navegación por internet móvil, la transmisión de video en tiempo real y el surgimiento de las videollamadas. Con este tipo de avances, la tecnología 3G mejoró significativamente la capacidad de conexión en comparación con el 2G. Con la introducción de la tecnología 3G, aparecieron una variedad de modelos de teléfonos móviles que aprovechaban estas capacidades mejoradas [20].

Entre estos se encuentran el Nokia N95, el iPhone 3G, el Samsung Galaxy S (I9000), el BlackBerry Bold 9000 y el Sony Ericsson K800i estos modelos fueron emblemáticos porque tenían características como una cámara de alta calidad, conectividad 3G para compartir fotos y videos de manera más eficiente y servicio de geolocalización y posicionamiento (Global Positioning System o GPS). La anexión de estas características junto con el surgimiento de los sistemas operativos móviles como iOS y Android marcaron una clara diferencia entre la generación del 3G con su antecesor.

Sin embargo, fue la cuarta generación de tecnología móvil, que comenzó a principios de la década de 2010, la que desencadenó un despliegue gradual de conexiones de internet y generación de datos en todo el mundo. Los primeros despliegues comerciales de 4G generalmente se realizaron alrededor de 2010 y 2011. Es importante destacar que la adopción de las redes 4G fue un proceso gradual y llevó algún tiempo antes de que se convirtiera en la

norma por todo el mundo. Durante este período, los operadores de telecomunicaciones actualizaban sus infraestructuras de red para ofrecer velocidades de datos más rápidas y una mejor calidad de servicio en comparación con las redes 3G anteriores.

Los aspectos más destacados de la era del 4G fueron:

- Mayor velocidad de datos: La principal característica del 4G fue la velocidad de datos significativamente más rápida en comparación con las generaciones móviles anteriores (2G y 3G). Esta mayor velocidad permitió una experiencia de navegación en Internet más rápida, descargas más veloces y una reproducción de contenido multimedia más fluida.
- Redes de banda ancha móvil: El 4G introdujo la idea de redes de banda ancha móvil, lo que significa que la velocidad de datos era lo suficientemente rápida como para competir con las conexiones de banda ancha fija en el hogar. Esto posibilitó el uso de dispositivos móviles para actividades como la transmisión de video en alta definición y el juego en línea.
- Mejora en la latencia: La latencia, o el tiempo que tarda un paquete de datos en viajar desde el dispositivo hasta su destino y regresar, se redujo considerablemente en las redes 4G. Esto fue beneficioso para aplicaciones en tiempo real, como videollamadas y juegos en línea, que requieren una respuesta rápida.
- Expansión de aplicaciones móviles avanzadas: El 4G impulsó la popularidad de aplicaciones y servicios móviles avanzados. La App Store de Apple y Google Play Store se llenaron de aplicaciones que aprovechaban la velocidad y la capacidad de las redes 4G.
- Desarrollo de dispositivos avanzados: Los dispositivos móviles, como teléfonos inteligentes y tabletas, se volvieron más avanzados con procesadores más rápidos, pantallas de mayor resolución y capacidades de captura de video de alta definición. También, se introdujeron dispositivos específicos, como enrutadores 4G, para brindar conectividad de alta velocidad en áreas sin acceso a banda ancha fija.
- Competencia global: El 4G se desplegó en todo el mundo, y varios estándares, como LTE (Long-Term Evolution) y WiMAX, compitieron por la supremacía en términos de implementación tecnológica [21].

Otro aspecto trascendental de esta generación fue el surgimiento del estándar de tecnología LTE (Long-Term Evolution), que se convirtió en el estándar dominante para las redes 4G en todo el mundo que fue adoptado por las empresas líderes en telefonía móvil. Los Smartphones más populares en esta generación fueron el iPhone 5, lanzado en 2012, que fue uno de los primeros teléfonos de Apple en ser compatible con redes 4G LTE. El Samsung Galaxy S4 de 2013, este fue un teléfono Android líder en su época y aprovechó las capacidades 4G LTE para una navegación web y una transmisión de medios más rápidos. También, estuvieron el Sony Xperia Z que era resistente al agua y fue conocido por su diseño resistente y su pantalla de alta resolución. Y el Motorola Moto X que fue un teléfono personalizable que ofrecía una experiencia de usuario optimizada.

Con el tiempo, la compatibilidad de las redes 4G con el surgimiento de cada vez más dispositivos IoT como las tabletas, pulseras, relojes inteligentes y asistentes de voz hicieron que también en la década de 2010 se diera la popularización del IoT. A razón que es en esta década que la proliferación de dispositivos móviles, la disponibilidad de conexiones de alta velocidad

y la adopción generalizada de la tecnología Wi-Fi y Bluetooth aceleraron su crecimiento. Del mismo modo, grandes empresas tecnológicas, como Google, Apple y Amazon, lanzaron plataformas y dispositivos IoT para el consumidor, como el termostato Nest y los asistentes de voz como Amazon Echo.

Por último, desde el año 2020 estamos viviendo la generación del 5G, la cual ha introducido una serie de características y mejoras significativas en comparación con las generaciones anteriores, entre estas se destacan:

- Mayor velocidad de datos: El 5G ofrece velocidades de datos significativamente más rápidas en comparación con las generaciones anteriores. Puede proporcionar velocidades de descarga de varios gigabits por segundo (Gbps), lo que permite una navegación web ultrarápida, descargas de archivos instantáneas y transmisión de medios sin problemas.
- Latencia ultrabaja: Una de las características más destacadas del 5G es su latencia extremadamente baja, que puede ser de milisegundos o incluso menos. Esto es crucial para aplicaciones en tiempo real, como juegos en línea, cirugía remota y vehículos autónomos, donde incluso un ligero retraso puede ser crítico.
- Mayor capacidad de red: El 5G está diseñado para manejar una mayor cantidad de dispositivos conectados simultáneamente en la misma área geográfica. Esto es esencial para admitir la creciente cantidad de dispositivos IoT (Internet de las cosas) y la proliferación de dispositivos inteligentes en hogares y ciudades.
- Cobertura mejorada: Aunque las redes 5G utilizan una variedad de bandas de frecuencia, incluidas las de alta frecuencia (mmWave) y las de baja frecuencia, en general, se espera que ofrezcan una cobertura mejorada en áreas urbanas y rurales. Las señales de 5G pueden penetrar mejor los obstáculos, lo que mejora la cobertura en interiores.
- Eficiencia energética: El 5G está diseñado para ser más eficiente en términos de energía, lo que puede prolongar la duración de la batería de dispositivos móviles y reducir el consumo de energía en las redes de comunicación.
- Mayor ancho de banda: El espectro de frecuencia utilizado por el 5G es más amplio y variado en comparación con las generaciones anteriores. Esto permite un mayor ancho de banda, lo que se traduce en una mayor capacidad para transportar datos y admitir aplicaciones de alta demanda, como realidad virtual y aumentada.
- Conectividad más confiable: El 5G utiliza técnicas avanzadas de corrección de errores y redundancia para garantizar una conectividad más confiable, incluso en situaciones de alta densidad de dispositivos o en áreas con mucha interferencia.
- Apoyo a tecnologías emergentes: El 5G es fundamental para habilitar tecnologías emergentes como vehículos autónomos, ciudades inteligentes, telemedicina de alta definición, IoT industrial y más. Su capacidad para manejar una variedad de casos de uso tecnológicos lo hace versátil y esencial para el futuro de la conectividad [22].

De esta forma, la década de 2020 es aquella en el que el desarrollo de la telefonía móvil se empató con la mayor adopción de dispositivos IoT en áreas como la vida cotidiana como salud, la agricultura, la industria y el transporte.

En ese sentido, la red 5G se han desplegado para proporcionar conectividad de alta velocidad y baja latencia, lo que impulsa más y más el uso de los dispositivos IoT. A pesar de esto, en la actualidad la seguridad y la privacidad en el internet, el ciberespacio, y los dispositivos de tecnología móvil e IoT se han convertido en preocupaciones importantes debido a la cantidad de datos generados y compartidos por estos dispositivos. Hasta este punto del presente texto solo hemos abordado la evolución del internet y los dispositivos a través de los cuales accedemos a él. Ahora hace falta analizar el surgimiento de la ciberseguridad, así como los riesgos que emanan de esta revolución de las tecnologías de información que hemos vivido en los últimos treinta años.

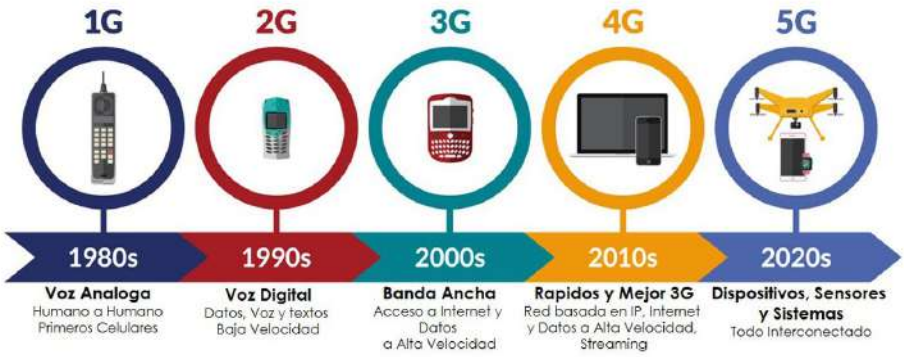

Fig. 3. Evolución de las Redes G de telecomunicaciones [23].

3. **De la securitización del internet a la ciberseguridad: el surgimiento de los delitos cibernéticos**

El desarrollo del internet ha sido uno de los fenómenos más impactantes en la historia de la comunicación y la información. Durante sus primeras décadas, esta tecnología se percibía como un espacio abierto y libre, donde la información y la expresión fluían sin restricciones significativas. Sin embargo, a medida que la red crecía en tamaño y alcance, los Estados y otros actores comenzaron a verla como un espacio que requería regulación y control. Esta evolución en la percepción fue impulsada por varias razones clave.

Por lo cual, a medida que la red global creció, también lo hicieron las estrategias de regulación implementadas por los gobiernos y otros actores. Esto se debe, a que desde la creación del proyecto ARPANET, hasta el proceso de mundialización de la WWW y el surgimiento de los

dispositivos de acceso a internet, esta red de comunicación fue ideada para compartir información de forma ágil y efectiva. Sin embargo, a pesar de esta condición, nunca se consideró que debía ser segura, tanto en el flujo de la información como en las intenciones de los usuarios en el mismo.

Una de las principales motivaciones detrás de este cambio fue la creciente preocupación por la seguridad cibernética y la protección de datos. Con el aumento de las amenazas, los gobiernos consideraron que era necesario tomar medidas para proteger sus sistemas y ciudadanos en línea. Esto condujo a la implementación de estrategias de regulación destinadas a bloquear el acceso a sitios web y contenido malicioso o potencialmente perjudicial.

Esta condición llevó a que, desde inicios de la década de los años 2000, el internet fuera utilizado para la comisión de actividades ilícitas o ilegales. Precisamente porque a través de esta nueva red de información se empezaron a realizar gran cantidad de acciones que podían comprometer la seguridad de las personas, así como lo derecho de individuos, empresas y gobierno. Este proceso fue denominado por John G. Palfrey, profesor de la Harvard Law School, como el proceso de regulación del internet. Precisamente, este autor indica que durante los años de 2000 y 2005 los gobiernos de diversos países del mundo se vieron en la necesidad de bloquear o gestionar diversas actividades y expresiones en línea, a razón de que comprometían la seguridad y los derechos de diversos sectores de la sociedad [24].

Por ejemplo, los gobiernos comenzaron a ver la necesidad de regular ciertas formas de discusión como la incitación al odio, la difusión de material ilegal (como la pornografía) y la promoción de actividades terroristas. En lugar de considerar internet como un espacio de libre expresión, diversos actores de la sociedad indicaron que como medio de comunicación requería supervisión y control. Con lo cual, los Estados empezaron a aplicar diversos métodos de regulación que tuvieron un impacto significativo en la forma en que percibimos y utilizamos internet en la actualidad.

Uno de los enfoques más comunes fue el uso de filtros de Internet, que bloqueaban el acceso a sitios web específicos o categorías de contenido. Estos filtros podían basarse en diversas métricas, como palabras clave, direcciones URL o contenido específico. Esta medida fue tan efectiva que tan sólo para el año 2005 más de 70 gobiernos y 289 proveedores de servicios de internet implementaron filtros de regulación de contenido y discusión en regiones del mundo como América del Norte, Asía, África y Europa Occidental. Los países pioneros en la implementación de estas medidas fueron China y Arabia Saudita, estableciendo regulaciones estrictas para bloquear ciertos sitios web y contenido considerado inapropiado o peligroso. China, en particular, desarrolló uno de los regímenes de filtrado más intrincados del mundo, abarcando múltiples niveles de la red y una amplia gama de temas [25].

Para el caso de regiones como América del Norte y Europa, la regulación de Internet ha tomado una forma diferente en comparación con algunos estados más autoritarios, aun así, se han implementado ciertas medidas de control y regulación. Entre las principales medidas que existen en estas regiones se encuentran:

- Regulación de protección de datos y protección de menores: En América del Norte y Europa, los esfuerzos de regulación de internet han estado más enfocados en la protección del contenido sensible, como la pornografía infantil y el discurso de odio. Se han promulgado leyes y regulaciones para bloquear y eliminar dicho contenido de la web. Por ejemplo, entre las legislaciones más famosas se encuentra la Children's Online Privacy Protection Act (COPPA), que es una ley federal estadounidense que protege la privacidad de los niños menores de 13 años en línea. También, se han implementado medidas para proteger la privacidad de los ciudadanos. Como es la Directiva 2004/38/CE en la Unión Europea, la cual hace alusión a la protección de los datos personales y la libre circulación de estos.
- Derechos de autor: En Europa, se han introducido regulaciones más estrictas en relación con los derechos de autor en internet. Esto se materializó en la creación de la Ley de Derechos de Autor de la Unión Europea (conocida como Directiva sobre Derechos de Autor de la UE) que tiene como objetivo proteger los derechos de autor y garantizar que los creadores reciban una compensación justa por su trabajo en línea.
- Privacidad de datos: Tanto en América del Norte como en Europa, se han implementado regulaciones de privacidad de datos, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Estas regulaciones establecen estándares para la recopilación, el almacenamiento y el procesamiento de datos personales en línea.
- Libertad de Expresión y neutralidad de la red: A diferencia de algunos estados autoritarios, las democracias en América del Norte y Europa tienden a proteger la libertad de expresión en línea. Sin embargo, existen limitaciones legales en cuanto a la incitación al odio y la difusión de contenido ilegal. Del mismo modo, es clave para estos países la neutralidad de la red, tema que ha sido objeto importante de regulación. Se han debatido y aplicado reglas para garantizar que los proveedores de servicios de internet no puedan dar prioridad a ciertos contenidos o bloquear el acceso a otros [26].

La historia del desarrollo del internet está llena de casos en los cuales surgieron formas de interacción en el ciberespacio que surgieron en una era previa a la existencia de regulaciones de actividades que en su momento no eran ilegales, pero sí estaban fuera del marco de la ley. Esto implica que gran cantidad de actividades como el compartir música en MP3, distribuir contenidos de video, o incluso fomentar el consumo de drogas o estupefacientes se promovieron a través del internet sin que existieran medidas de contención, aun en los países más avanzados y modernos del mundo.

Esta reflexión es importante en el marco de la comprensión de cómo las tecnologías evolucionan más rápido que los marcos regulatorios o la acciones que toman los gobiernos para tipificar y combatir los ciberdelitos, o del mismo modo, para promover la ciberseguridad. A continuación,

daremos un breve recorrido a algunos de los casos más controversiales vinculados a este fenómeno, entre los que se encuentran Napster, Silk Road, Pirate Bay y Megaupload. Todos sitios de internet, que se sirvieron de estos vacíos alegales para promover actividades ilícitas, hasta que fueron contenidos por diferentes regulaciones y gobiernos por todo el mundo.

4.1 Napster, el compartir música en la era pre legal

La historia de Napster es un relato fascinante de cómo una idea innovadora y disruptiva cambió para siempre la forma en que el mundo consume música. En su apogeo, a inicios de los años 2000, Napster fue famoso por permitir a los usuarios compartir archivos de música en formato MP3 de manera descentralizada, desencadenando una revolución digital en un momento en que las leyes de derechos de autor aún no se habían adaptado completamente al mundo en línea [27].

Napster nació en 1999, como un proyecto creado por Shawn Fanning y Sean Parker, dos jóvenes visionarios que vieron la oportunidad de revolucionar la industria musical. El concepto detrás de Napster era simple pero poderoso: permitir a los usuarios compartir sus colecciones de música digital en formato MP3 directamente entre ellos, sin la necesidad de intermediarios como discográficas o tiendas de música en línea. En un momento en que la velocidad de conexión a internet estaba mejorando y el almacenamiento digital se volvía más asequible, Napster se convirtió en un fenómeno viral.
En este sentido, es importante mencionar que lo que hizo que Napster fuera tan revolucionario fue su capacidad para reunir a millones de usuarios en una red de intercambio de archivos peer-to-peer. Esto significa que los usuarios podían buscar y descargar canciones de la vasta biblioteca de música compartida por otros usuarios, todo de forma gratuita. Esto creó una experiencia de descubrimiento musical sin precedentes y permitió que artistas menos conocidos ganaran notoriedad a través de la distribución viral de sus canciones.

Del mismo modo, debemos recordar que, con base a lo explicado en la sección anterior, e incluso a lo señalado por John Palfrey, es que en esa época no existían leyes claras que limitaran el intercambio de música en formato MP3 en línea. La industria de la música no estaba preparada para lidiar con esta revolución tecnológica y quedó en una posición desfavorable para proteger sus intereses y derechos de autor [28].

Esto se debió a que la popularidad explosiva de Napster no pasó desapercibida para la industria discográfica. Pronto, sellos discográficos y artistas comenzaron a interponer demandas contra la compañía, alegando que el servicio fomentaba la violación de los derechos de autor al permitir a los usuarios compartir canciones protegidas sin permiso. Por lo cual, gran cantidad de firmas discográficas pronto tomaron medidas legales en contra de Napster.

El caso legal de la compañía se prolongó durante varios años, lo que llevó a un cierre temporal del servicio en 2001. Finalmente, en 2002, Napster llegó a un acuerdo con la industria discográfica para pagar una compensación por los derechos de autor y cambiar su modelo de negocio. Sin embargo, este acuerdo marcó su declive como una plataforma de intercambio de música gratuita. A pesar de su desaparición, Napster dejó un legado duradero en la industria de

la música. Revolucionó la forma en que las personas consumían música y allanó el camino para la transición de la música a la era digital. La lucha legal de Napster también puso de manifiesto la necesidad de revisar y actualizar las leyes de derechos de autor para adaptarse a la era digital en constante evolución [29].

En los años posteriores, surgieron servicios de streaming de música legales, como iTunes, Spotify y Apple Music, que aprovecharon el modelo de distribución digital, pero con un enfoque legal y compensación adecuada para los artistas y la industria de la música. A pesar de eso, Napster fue la empresa pionera del intercambio de música en línea, que emergió en un momento en que las leyes de derechos de autor aún no se habían puesto al día con la tecnología digital. A pesar de su desaparición, su impacto en la industria de la música es innegable. La historia de Napster es un recordatorio de cómo la innovación puede desafiar las normas establecidas y cambiar el panorama de una industria para siempre. Y su legado perdura en la forma en que consumimos y compartimos música en la era digital actual.

4.2 Torrents, Piratería y Privacidad: El Legado Duradero de Pirate Bay en Internet

Pirate Bay es un testimonio de la era dorada y la controversia del intercambio de archivos en línea. Fundado en 2003 por un grupo de entusiastas bajo seudónimos como "TiAMO" y "anakata", Pirate Bay se erigió como un medio para compartir archivos a través de Torrent, desafiando las leyes de derechos de autor y los paradigmas establecidos. Precisamente, Pirate Bay fue un fenómeno que floreció en un momento en que las regulaciones en torno compartir contenido en línea aún no habían evolucionado completamente para abordar la era digital emergente [30].

En este contexto, Pirate Bay nació como una respuesta a la creciente demanda de acceso a contenido digital. Su propósito era proporcionar a los usuarios una plataforma para compartir y descargar archivos torrent que contenían una amplia variedad, desde películas y música hasta programas de televisión y software. En sus primeros días, Pirate Bay se aprovechó de un vacío legal en la regulación para compartir archivos en internet. Del mismo modo, la tecnología torrent permitía a los usuarios compartir fragmentos de archivos entre sí de manera descentralizada, lo que dificultaba la persecución legal de los operadores del sitio. Además, las leyes de derechos de autor no habían evolucionado completamente para abordar la distribución de contenido digital en línea.

Esta falta de claridad legal permitió que Pirate Bay prosperara, atrayendo a una gran comunidad de usuarios que buscaban acceder a contenido de forma gratuita, a menudo infringiendo los derechos de autor en el proceso. A medida que Pirate Bay ganaba notoriedad y popularidad, se convirtió en el objetivo de la industria del entretenimiento y los titulares de los derechos de autor. Esto provocó que se interpusieron demandas legales y presiones gubernamentales en un

intento por cerrar el sitio y responsabilizar a sus operadores por la infracción de derechos de autor masiva. De esta forma, Pirate Bay enfrentó desafíos legales y técnicos, como bloqueos de dominios y arrestos de sus fundadores y operadores. Sin embargo, el sitio continuó operando, a menudo cambiando de dominio y ubicación para evadir las restricciones. Eso inevitablemente convirtió al sitio en un símbolo de la lucha por la libertad en línea y la privacidad, atrayendo el apoyo de grupos y defensores de la neutralidad en la red [31].

4. Megaupload, la caída de un gigante del alojamiento en línea

El lanzamiento de Megaupload en 2005 marcó un hito en el mundo de la tecnología, la plataforma permitía a los usuarios cargar y compartir archivos de manera eficiente, lo que facilitaba la distribución de contenido digital, incluyendo documentos, imágenes, música y videos. Con una interfaz sencilla y opciones tanto gratuitas como de pago, Megaupload atrajo a millones de usuarios de todo el mundo. A medida que ganaba popularidad, también se convertía en el centro de una creciente controversia. Las autoridades de los Estados Unidos y otros países alegaron que el sitio estaba siendo utilizado para compartir ilegalmente una gran cantidad de contenido protegido por derechos de autor, como películas, música y software.

El argumento central era que Megaupload no hacía lo suficiente para prevenir la infracción de derechos de autor en su plataforma. Aunque el sitio tenía medidas para la retirada de contenido infractor, las autoridades argumentaron que estas medidas eran insuficientes y estaba lucrando con la distribución ilegal de material protegido por derechos de autor. Por esta razón, el 19 de enero de 2012 el FBI cerró Megaupload en una operación internacional que involucró el arresto de Kim Dotcom, su fundador, y otros asociados del sitio en Nueva Zelanda. Este dramático cierre dejó a millones de usuarios de Megaupload sorprendidos y llevó a una batalla legal de alto perfil que se prolongaría durante varios años [32].

Kim Dotcom y sus asociados enfrentaron una serie de cargos, incluyendo conspiración para cometer lavado de dinero, conspiración para cometer fraude electrónico y conspiración para cometer infracción de derechos de autor. El caso se centró en gran medida en cuestiones legales y éticas relacionadas con la responsabilidad de los servicios en línea por el contenido compartido por sus usuarios. A pesar de esto, Megaupload dejó un legado complejo en la historia de la tecnología y los derechos de autor en línea. Mientras algunos argumentaron que el sitio era un ejemplo de cómo los servicios en línea podían ser utilizados para compartir contenido ilegal, otros vieron el cierre de Megaupload como un caso emblemático de la lucha entre la innovación tecnológica y la aplicación de la ley [33].

5. Silk Road, un viaje a través de la Dark Web y la revolución del comercio ilícito

La historia de Silk Road es un intrigante capítulo en la evolución de la tecnología y su impacto en la economía subterránea en línea. Fundado en 2011 por el misterioso Ross Ulbricht, bajo el seudónimo “Dread Pirate Roberts", Silk Road emergió en un momento en que las leyes y regulaciones que abordaban el comercio en línea y la utilización de criptomonedas aún no habían alcanzado la madurez necesaria para enfrentar este nuevo y oscuro fenómeno.

En este sentido, el surgimiento de Silk Road fue un hito significativo en la historia de la Dark Web o web oscura, una parte de Internet que opera fuera de los motores de búsqueda convencionales y es inaccesible a través de navegadores estándar. Silk Road funcionaba en la red anónima Tor, que ocultaba las direcciones IP de los usuarios y los servidores, lo que permitía el anonimato tanto para los compradores como para los vendedores [34].

El sitio se presentó como un mercado en línea que facilitaba la compra y venta de una amplia gama de productos, desde drogas ilegales y armas de fuego hasta documentos falsificados y servicios de hacking. Lo que hizo que Silk Road fuera especialmente notorio fue su uso de Bitcoin y otras criptomonedas para procesar las transacciones, lo que dificultaba aún más el rastreo de las operaciones financieras. Silk Road surgió en un momento en que las leyes y regulaciones en torno al comercio en línea y las criptomonedas aún estaban en desarrollo. La naturaleza anónima de la tecnología Tor y el uso de criptomonedas planteaban desafíos significativos para las autoridades y reguladores, que se encontraban luchando por mantenerse al día con los avances tecnológicos.

El sitio prosperó en gran parte debido a este vacío legal. Sus usuarios, tanto compradores como vendedores, operaban bajo un relativo grado de anonimato, lo que dificultaba que las fuerzas del orden rastrearan y persiguieran a los responsables. La historia de Silk Road cambió dramáticamente en 2013, cuando Ross Ulbricht fue arrestado y acusado de ser el cerebro detrás del sitio. Las autoridades alegaron que Ulbricht era "Dread Pirate Roberts", el pseudónimo bajo el cual se había dirigido el sitio.

El arresto de Ulbricht marcó el principio del fin para Silk Road. El sitio fue inmediatamente clausurado por las autoridades, y Ulbricht enfrentó una serie de cargos, incluyendo conspiración para cometer lavado de dinero, tráfico de drogas y otros delitos relacionados con la operación del sitio. En 2015, fue condenado a cadena perpetua sin posibilidad de libertad condicional [35]. La historia de Silk Road destaca la interacción entre la tecnología emergente, las regulaciones legales y la actividad criminal en línea. El sitio surgió en un momento en que las leyes que

regulaban estas actividades aún estaban en desarrollo, lo que permitió su crecimiento y éxito temporal. Sin embargo, también puso de relieve los desafíos que enfrentan las autoridades para mantener el ritmo de la innovación tecnológica y adaptar sus regulaciones para abordar la creciente economía subterránea en internet. La historia de Silk Road sigue siendo un recordatorio de las complejidades y desafíos de la era digital.

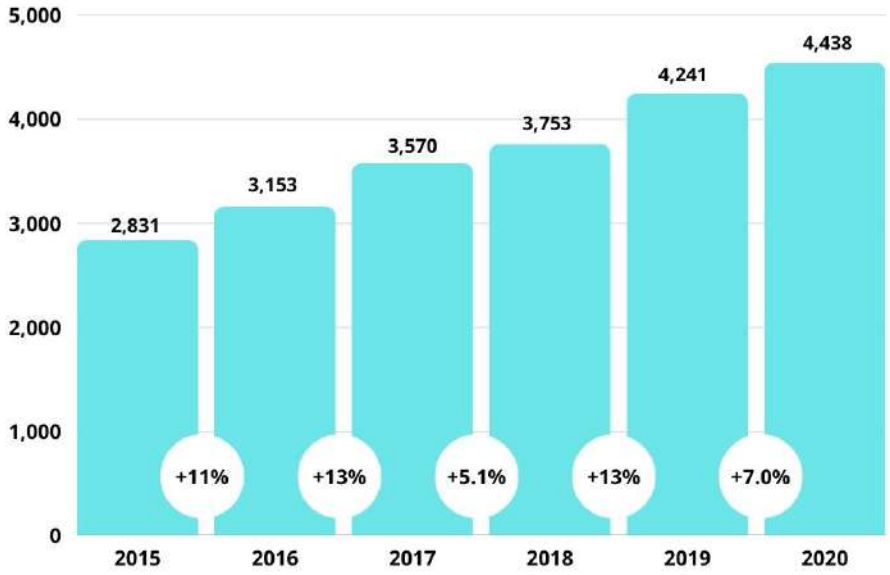

Fig. 4. Crecimiento de usuarios de internet 2015-2020 [36].

Lo anterior, se interrelaciona con el hecho de que los delitos cibernéticos evolucionan constantemente a medida que la tecnología avanza, y en la actualidad, se han diversificado de forma impresionante al nivel del incremento de usuarios de internet. Sobre el crecimiento global de los usuarios, basta tan sólo con echar un vistazo a las tasas de crecimiento de hace menos de una década, en el año 2015. Datos del Banco Mundial nos revelan que en ese año 2,831 millones de personas tenían acceso a la red. Para el año 2020, la cifra se incrementó a un total de 4,538 millones de usuarios, lo que representa aproximadamente 59 % de la población mundial. En los hechos, las tasas de crecimiento de usuarios del internet en promedio superaron el 10 % de crecimiento anual durante la última década.

El contexto anterior nos lleva a comprender que la securitización del internet derivó en el surgimiento de la ciberseguridad. Además, es importante mencionar que los efectos derivados de la crisis global de salud por la pandemia de COVID-19, durante los años 2020-2022, han incrementado exponencialmente el nivel de amenazas cibernéticas a nivel global. Por ejemplo, el informe de la empresa de soluciones de firewall y ciberseguridad Sonic Wall 2021 indicó que durante el bienio 2019-2020, se dio el incremento más alto de ataques de malware o software

malicioso, por todo el mundo, con una tasa de crecimiento del 57.6%, al pasar de 9.9 miles de millones, a una cifra de 15.6.

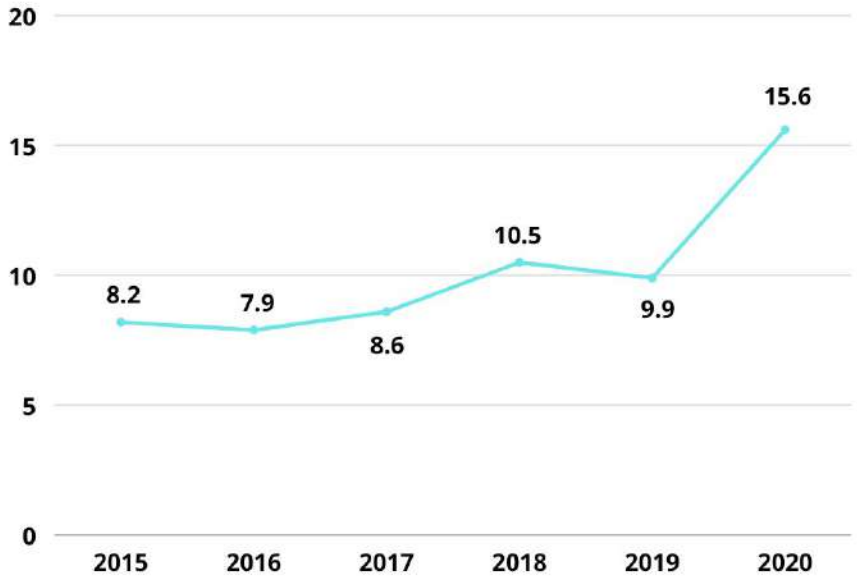

Fig. 5. Número anual de ataques de malware en todo el mundo desde 2015 hasta 2020 (en miles de millones) [37].

En consonancia, con esta información, se encuentra el reporte de Mordor Intelligence 2021, que indica que entre 2020 y 2025, el mercado de la ciberseguridad, y, por lo tanto, los gastos y costos para los gobiernos, se duplicará prácticamente en toda la región de América Latina. Al pasar de los 13.73 miles de millones de dólares (mmd), a los 26.2 mmd. Con lo cual cada año, que pase a partir del 2022, implicará un incremento del 12 al 18 %, de los costos para gobiernos, empresas y usuarios en gastos de ciberseguridad por el alto potencial de vulneración que tienen los cibercriminales para afectar a todo tipo de actores alrededor del mundo.

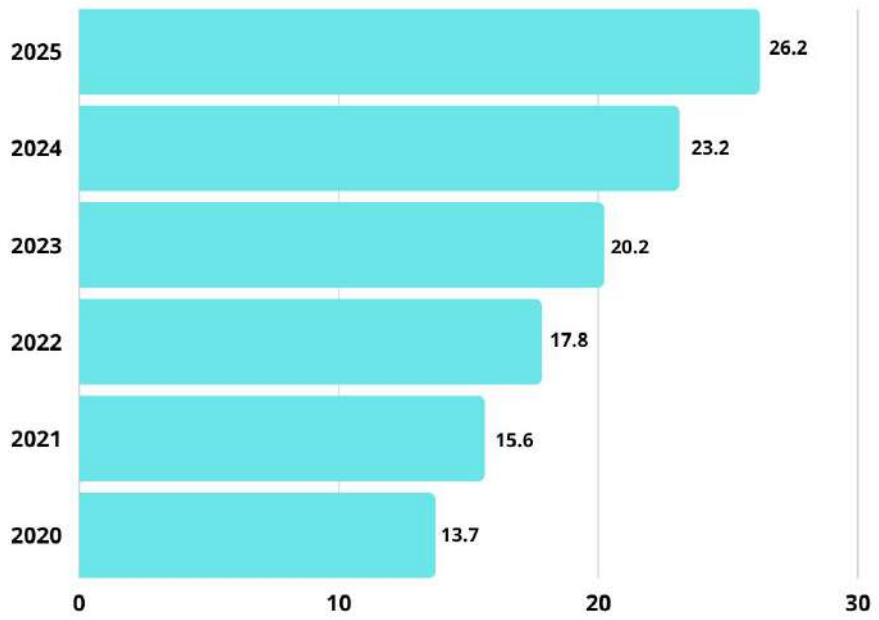

Fig. 5. Valor del mercado de ciberseguridad en América Latina de 2019 a 2025 (en miles de millones de dólares) [38].

En la actualidad, la incidencia de los delitos cibernéticos es una realidad que se ha normalizado, y a pesar de esto, aún existen múltiples naciones que no cuentan con un marco legal adecuado para enfrentar este tipo de actividades delictivas. En los hechos, los ciberdelitos más comunes que se observan en todo el mundo son los siguientes [39]:

- Phishing: Los ataques de phishing involucran el envío de correos electrónicos falsificados que parecen ser de fuentes legítimas con el fin de engañar a las personas para que revelen información personal, como contraseñas, números de tarjeta de crédito o información bancaria.
- Ransomware: Este tipo de ataque cifra los archivos o el sistema de una víctima y exige un rescate a cambio de la clave de descifrado. Los ransomware a menudo causan daños significativos a individuos y organizaciones.
- Estafas en línea: Incluyen una amplia variedad de engaños, desde estafas de inversión hasta ventas falsas en línea. Los estafadores suelen utilizar sitios web y plataformas de redes sociales para atraer a las víctimas.
- Robo de datos personales: Los ciberdelincuentes roban información personal, como números de seguridad social, números de tarjeta de crédito o información de cuentas bancarias, para cometer fraudes financieros.
- Ciberacoso y ciberbullying: Implican el uso de Internet y las redes sociales para acosar, intimidar o difamar a otros, a menudo de manera anónima.

- Intrusiones y ataques a sistemas informáticos: Los hackers pueden buscar vulnerabilidades en sistemas informáticos y redes para acceder a información confidencial, interrumpir servicios o robar datos.
- Ataques de denegación de servicio (DDoS): Los atacantes inundan un sitio web o una red con tráfico falso o solicitudes, lo que hace que el servicio sea inaccesible para los usuarios legítimos.
- Fraude en línea y tarjetas de crédito: Involucra el uso fraudulento de tarjetas de crédito o débito en línea para realizar compras no autorizadas.
- Suplantación de identidad (pharming): Los atacantes redirigen a las víctimas a sitios web falsificados que parecen ser legítimos con el fin de robar información confidencial.
- Pornografía infantil en línea: Este delito implica la distribución y posesión de material pornográfico que involucra a menores de edad, lo que es ilegal en la mayoría de los países.
- Robo de propiedad intelectual: Los ciberdelincuentes roban propiedad intelectual, como software, diseños y secretos comerciales, para su propio beneficio o para venderlos en el mercado negro.
- Ataques a redes sociales: Los hackers pueden comprometer cuentas de redes sociales para difundir información falsa, spam o incluso extorsionar a los propietarios de las cuentas.
- Extorsión en línea: Los delincuentes amenazan con divulgar información comprometedora o sensible a menos que se les pague un rescate.

Estos son solo algunos ejemplos de ciberdelitos comunes a nivel global. La evolución constante de la tecnología y las tácticas de los delincuentes significa que siempre hay nuevos tipos de ciberdelitos en desarrollo, lo que hace que la ciberseguridad sea una preocupación constante para individuos y organizaciones en todo el mundo.

Sin embargo, es importante hacer notar que la historia de la actividad ilegal o ilícita en el internet se debe a grandes vacíos legales que existían en este dominio al momento de materializar este tipo de actividad. Y en los hechos, múltiples países en todo el mundo no cuentan con un marco legal para el combate de los delitos cibernéticos, a razón de que dicha tecnología evolucionó tan rápido que creó dinámicas sociales para las cuales no existían códigos legales o marcos regulatorios.

6. La ciberseguridad como un problema de seguridad nacional e internacional

Nuestra revisión anterior nos revela el panorama en el cual la delincuencia cibernética se convirtió en un problema de seguridad pública que hizo emerger la necesidad de securitizar el internet y crear códigos y marcos legales para combatir actividades ilícitas hechas a través del dominio. Pero, ¿qué pasaría si el internet pudiera comprometer la seguridad de un país completo? E incluso, ¿volverse un problema que compete al mundo entero? El ejemplo que

puede materializar las respuestas a estas preguntas se dio en el conflicto en torno al ciberataque DDoS a Estonia en el año 2007, el cual representa un caso paradigmático que ilustra la convergencia de tensiones étnicas, históricas y políticas en Europa del Este, junto con un componente de ciberseguridad que marcó un punto de inflexión en la percepción de la ciberseguridad a nivel internacional [40].

En ese sentido, es importante mencionar que el 2007 marcó un año significativo en la historia de Estonia, una nación que emergió de la Unión Soviética en 1991. Ese año, el Monumento a los Libertadores o Soldado de Bronce en Tallin, capital de Estonia, se convirtió en el epicentro de un conflicto que involucró tensiones étnicas, historias divergentes y cuestiones de identidad nacional. Y este conflicto se impulsaría desde el ciberespacio para demostrar la vulnerabilidad de las naciones en el mundo digital emergente.

El conflicto se originó en torno al Monumento a los Libertadores en Tallin, un símbolo de las complejas relaciones históricas entre Estonia y la Unión Soviética. Para los rusos étnicos en Estonia, este monumento representaba un recuerdo orgulloso de la victoria soviética sobre el nazismo y la liberación del país. Sin embargo, para los estonios étnicos, era un recordatorio de más de cincuenta años de ocupación soviética, caracterizada por el autoritarismo y la supresión de libertades.

De esta forma, ese año el parlamento del país promulgó una legislación que prohibía la ubicación de tumbas de guerra en lugares públicos, con lo cual el monumento tendría que ser retirado del centro de la ciudad de Tallin, este evento exacerbó las tensiones, dividiendo a la población estonia. Esto llevó a disturbios y protestas, y el gobierno estonio decidió trasladar el monumento a un cementerio militar. La cuestión se volvió aún más compleja cuando, a la par de los disturbios en las calles, el gobierno nacional del país se dio cuenta de que estaban siendo víctimas de un ataque DDoS de magnitudes colosales, el cual paralizó completamente toda la infraestructura digital de Estonia. Los ataques incluyeron ataques DDoS masivos y la saturación de sitios web gubernamentales y medios de comunicación, con lo cual el ciberespacio se convirtió en un campo que amplificó las tensiones en el mundo real.

Frente a este contexto, Estonia solicitó el apoyo de la Organización del Tratado del Atlántico Norte (OTAN) y la Unión Europea, organismos de los que era miembro el país, lo que dio como resultado el reconocimiento de que los ciberataques podrían considerarse una forma de agresión. Frente a esta queja, la OTAN modificó su marco legal como organismo internacional para incluir los ciberataques como una forma de agresión, lo que marcó un cambio importante en la percepción de la ciberseguridad a nivel internacional. También, la OTAN estableció el Centro Cooperativo de Ciber Defensa de Excelencia (CCD COE por sus siglas en inglés) en Tallin, lo que refleja la importancia de la ciberseguridad en el ámbito internacional. Este centro se ha

convertido en un actor fundamental en la promoción de la cooperación y el intercambio de información en materia de ciberseguridad [41].

El conflicto "Estonia 2007" dejó varias lecciones importantes, por ejemplo, destacó la creciente importancia de la ciberseguridad en un mundo interconectado y demostró la necesidad de que los países refuercen sus defensas cibernéticas y colaboren en la lucha contra las amenazas del ciberespacio. De esta forma, representa un punto de partida de cómo el desarrollo de una política de ciberseguridad es una labor que deben atender los países por sí mismos y la comunidad internacional.

De esta forma, el ciberespacio ha emergido como una arena crítica de la política internacional, con el potencial de influir en eventos políticos a nivel global y desafiar la seguridad nacional de los Estados. Bastante tiempo ha pasado desde la creación de ARPANET, en la década de 1960, y de la popularización y democratización de la WWW en lo noventas. En la actualidad, el internet y el ciberespacio han experimentado una evolución vertiginosa y se han convertido en un componente esencial de la vida cotidiana y las dinámicas políticas en todo el mundo. Sin embargo, han trascendido su función inicial como una red de intercambio de información académica y militar para convertirse en un medio de intercambio de información en todas las esferas de la vida cotidiana. Con miles de millones de usuarios en todo el mundo, este espacio digital tiene la capacidad de influir en cuestiones políticas, económicas y sociales, y puede dar forma a la opinión pública y la agenda global.

La creciente importancia del ciberespacio en la política internacional ha llevado a un número significativo de países a desarrollar Estrategias Nacionales de Ciberseguridad. Este enfoque refleja la comprensión de que la ciberseguridad es esencial para salvaguardar la integridad de los Estados-Nación. De esta forma, el internet ha trascendido su papel original como una red de intercambio de información para convertirse en una arena crítica de la política internacional.

Los ciberataques a Estonia en 2007, junto con otros casos significativos que surgen día a día, subrayan la necesidad de abordar los desafíos y oportunidades que presenta este entorno digital en constante evolución. El estudio del ciberespacio y la ciberseguridad se ha convertido en una prioridad para teóricos y formuladores de políticas desde todas las disciplinas académicas. Y la regulación y la seguridad en este espacio son temas de alta trascendencia en el siglo XXI [42].

7. El futuro de la ciberseguridad: la influencia de la IA, el Big Data, el Cómputo Cuántico y las Redes 5G

En la actualidad, el panorama de la ciberseguridad está evolucionando rápidamente, impulsado por avances tecnológicos que incluyen la Inteligencia Artificial (IA), el Big Data, el Cómputo

Cuántico y las Redes 5G. Estas tecnologías, individualmente y en conjunto, están definiendo el futuro de la ciberseguridad, tanto en términos de amenazas como de soluciones.

Daremos cierre a este ensayo analizando la importancia de cada una de estas tecnologías en el futuro de la ciberseguridad:

- La influencia de la Inteligencia Artificial (IA): La IA ha emergido como un habilitador esencial en la ciberseguridad. Su capacidad para analizar grandes volúmenes de datos en tiempo real permite la detección temprana de amenazas y la identificación de patrones anómalos en el tráfico de red. Los sistemas de IA pueden aprender y adaptarse continuamente a nuevas amenazas, lo que los hace más efectivos que las soluciones basadas en firmas estáticas. Por otra parte, la IA también se utiliza en la autenticación biométrica, fortaleciendo la seguridad de los sistemas de acceso. Sin embargo, esta misma tecnología se puede utilizar en ataques cibernéticos más sofisticados, lo que plantea la necesidad de desarrollar contramedidas basadas en IA [43].
- El papel del Big Data: Esta tecnología desempeña un papel crucial en la ciberseguridad al permitir la recopilación y el análisis de grandes conjuntos de datos relacionados con la seguridad. Esto incluye registros de actividad de red, registros de eventos de seguridad y datos de aplicaciones. El análisis de Big Data revela patrones y tendencias que pueden indicar amenazas cibernéticas en desarrollo. Además, es fundamental para la generación de informes forenses después de un incidente de seguridad. La capacidad de rastrear y analizar datos históricos es esencial para comprender la extensión de un ataque y tomar medidas para prevenir futuros incidentes [44].
- El desafío del Cómputo Cuántico: A medida que la tecnología de cómputo cuántico avanza, plantea un desafío significativo para la ciberseguridad. Los algoritmos de cifrado utilizados actualmente, que dependen de la factorización de números primos grandes, pueden ser vulnerables a ataques de cómputo cuántico. Esto significa que la seguridad de la información confidencial puede estar en riesgo en un futuro donde los ordenadores cuánticos sean una realidad. La respuesta a este desafío radica en el desarrollo de algoritmos de cifrado cuánticos resistentes y la implementación de técnicas de seguridad cuántica que aprovechen las propiedades únicas de la física cuántica para garantizar la privacidad y la integridad de la información [45].
- Redes 5G y su impacto en la Ciberseguridad: Las redes 5G están revolucionando la conectividad, ofreciendo velocidades de conexión más rápidas y una mayor capacidad de dispositivos conectados. Esto es beneficioso para la Internet de las cosas (IoT), pero también plantea desafíos en términos de ciberseguridad. La mayor superficie de ataque debido a la mayor cantidad de dispositivos conectados y la velocidad de transmisión de datos pueden exponer a las redes 5G a amenazas como ataques distribuidos de denegación de servicio (DDoS) más potentes. La seguridad en las redes 5G debe ser una prioridad para garantizar la protección de la información y la privacidad del usuario [46].

Conclusiones

El internet es hoy en día una pieza clave de la vida cotidiana y de la esfera social. Muchos cambios se han dado desde el surgimiento del proyecto ARPANET, hasta la democratización de la World Wide Web y la construcción de la ciberseguridad cómo un problema de seguridad pública, nacional e internacional. Hoy, podemos concluir que la ciberseguridad se encuentra en un momento crítico de su evolución, impulsada por nuevas tecnologías que se emparan con ella como las redes 5G o el IoT. Las cuales ofrecen nuevas oportunidades para la detección y prevención de amenazas, pero también plantean desafíos significativos en términos de seguridad.

En el futuro, los expertos en seguridad cibernética deben mantenerse al tanto de estos avances tecnológicos y adaptar sus estrategias para proteger datos y sistemas en este entorno en constante cambio. El futuro de la ciberseguridad dependerá de la capacidad para innovar y desarrollar soluciones que aprovechen estas tecnologías emergentes y mitiguen sus riesgos asociados. En última instancia, la colaboración y la inversión en investigación y desarrollo son esenciales para garantizar un futuro digital, seguro y protegido, en un mundo que cada vez más inmerso en la esfera digital que será crucial en las próximas décadas.

Referencias

[1] Licklider, J. C. R. (2002). Historia de Internet. Boston, Estados Unidos, 1-2.
[2] Trilnick, C. (2011). Nuevos medios, viejos medios. Arkadin, 3.
[3] Licklider, J. C. (1960). W.(1962). On-line Man Computer Interactions.
[4] Gisbert, V. S. APUNTES SOBRE LOS ORÍGENES DE INTERNET. DE LA INFORMÁTICA, 71.
[5] Sandroni, G. (2016). Breve Historia y Origen del Internet. Recuperado de: http://www. academia. edu/download/57128740/internet. pdf.
[6] Trenta, M. (2012). Orígenes del videojuego: conexiones históricas y sociales de un producto cultural. In Presentado en IV Congreso Internacional Lafina de Comunicación, Laguna.
[7] Hardy, I. (1996). The Evolution of ARPAnet Email [On-line]. History Thesis, UC Berkeley [Citado: Septiembre 1999]. Disponible en Internet: http://www. ifla. org/documents/internet/hari1. txt.
[8] Licklider, J. C. R. (2002). Historia de Internet. Boston, Estados Unidos, 1-2.
[9] Becerra, L. R. (2000). El auge de Internet. Revista Páginas.
[10] Licklider, J. C. R. (2002). Historia de Internet. Boston, Estados Unidos, 1-2.
[11] Coello, C. A. C. (2003). Breve historia de la computación y sus pioneros. México: Fondo de cultura económica.
[12] Calero, S. (2018). NP: Una historia de la innovación en PC (Infografía), Fanáticos del Hardware. Recuperado de: https://fanaticosdelhardware.com/una-historia-la-innovacion-pc-infografia/
[13] Cerritos, A. (2002). Los hacedores de la historia, las computadoras. Rev Fac Med UNAM, 45(4).
[14] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (1999). Una breve historia de Internet. Primera y segunda parte), en: http://www. ati. es/DOCS/internet/histint/histint1. html.
[15] Aranda, V. T. (2004). Historia y evolución de Internet. Autores científico-técnicos y académicos, 33(1), 22-32.
[16] Luján-Mora, S. (2013). iDESWEB: Historia de los navegadores web. iDESWEB.
[17] Tabarés Gutiérrez, R. (2012). El inicio de la Web: historia y cronología del hipertexto hasta HTML 4.0 (1990-99). El inicio de la Web: historia y cronología del hipertexto hasta HTML 4.0 (1990-99), 57-82.
[18] Garzón, W. L., & López, J. C. (2019). Tecnología internet of things (IoT) y el big data. Mare Ingenii, 1(1), 73-79.
[19] Joskowicz, J. (2015). Breve historia de las telecomunicaciones. Universidad de la República de Montevideo, Uruguay. Versión, 11.

[20] Peréz Naranjo, T. S. Estudio de las metodologías ITIL Y Lean Six Sigma para ubicación y uso de las Tecnologías 2G, 3G Y 4G en la actualidad en Colombia (Doctoral dissertation, Universidad Santo Tomás).
[21] Naranjo, D., Buenaño, D. C., & Mejía, I. T. (2016). Evolución de la tecnología móvil. Camino a 5G. Revista Contribuciones a las Ciencias Sociales, 1-13.
[22] Colombo, S., López, M. P., & Vera, N. (2021). Emerging technologies, competing powers and disputed regions: Latin America and 5G in the technological contest between China and the United States. Estudos Internacionais, 94-111.
[23] Telecomm. (s2020). 1G, 2G, 3G, and 4G all led to 5G (Everything you Need to Know). Telecomm, Recuperado de: https://telecomm.in/topic/679/1g-2g-3g-and-4g-all-led-to-5g-everything-you-need-to-know
[24] Palfrey, John G. and Palfrey, John G., Four Phases of Internet Regulation. Social Research, Vol. 77, No. 3, Fall 2010 , Berkman Center Research Publication No. 2010-9, Harvard Public Law Working Paper No. 10-42, Available at SSRN: https://ssrn.com/abstract=1658191
[25] Aguilar, J. A. M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO Revista Latinoamericana de Estudios de Seguridad, (25), 24-40.
[26] Barrio, A. M. (2010). Global challenges and threats: European and US approaches. Revista UNISCI, (22), 142-160.
[27] Torres Medina, V. L. (2001). El caso de Napster, Archivos MP3 y similares: Viaje de campo por el Ciberespacio.
[28] Ku, R. S. R. (2002). The creative destruction of copyright: Napster and the new economics of digital technology. The University of Chicago Law Review, 263-324.
[29] Waldfogel, J. (2012). Copyright protection, technological change, and the quality of new products: Evidence from recorded music since Napster. The journal of law and economics, 55(4), 715-740.
[30] Poort, J., Leenheer, J., van der Ham, J., & Dumitru, C. (2014). Baywatch: Two approaches to measure the effects of blocking access to The Pirate Bay. Telecommunications Policy, 38(4), 383-392.
[31] Elert, N., Henrekson, M., & Wernberg, J. (2016). Two sides to the evasion: The Pirate Bay and the interdependencies of evasive entrepreneurship. Journal of Entrepreneurship and Public Policy, 5(2), 176-200.
[32] Moreno Muñoz, M. (2012). Propiedad intelectual, seguridad y control de las comunicaciones en Internet. Impacto sociocultural del fenómeno Megaupload.
[33] Parloff, R. (2012). Megaupload and the Twilight of Copyright. Fortune, 166(2), 130-140.
[34] Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. Criminology & Criminal Justice, 14(3), 351-367.
[35] Weiser, B. (2015). Ross Ulbricht, creator of Silk Road website, is sentenced to life in prison. New York Times.
[36] ITU (2022). Statistics Individuals using the Internet.
[37] Sonic Wall (2021). Threat Report 2021. Disponible: https://www.sonicwall.com/resources/white-papers/2021-sonicwall-cyber-threat-report/

[38] Mordor Intelligence (2021). Latin America Cybersecurity Market - Growth, Trends, Covid-19 Impact, And Forecasts (2022 - 2027). Recuperado de: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market
[39] Jain, A., & Gupta, N. (2020). Cyber crime. National Journal of Cybersecurity Law, 2(2), 152-158.
[40] Buresh, D. L. (2020). A critical evaluation of the estonian cyber incident. Journal of Advanced Forensic Sciences, 1(2), 7.
[41] Aguilar-Antonio, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO Revista Latinoamericana de Estudios de Seguridad, (25), 24-40.
[42] Aguilar- Antonio, J.(2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. Revista de estudios en seguridad internacional, 6(2), 17-43.
[43] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. International Journal of Advanced Research in Computer and Communication Engineering.
[44] Alferidah, D. K., & Jhanjhi, N. Z. (2020, October). Cybersecurity impact over bigdata and iot growth. In 2020 International Conference on Computational Intelligence (ICCI) (pp. 103-108). IEEE.
[45] Kilber, N., Kaestle, D., & Wagner, S. (2021). Cybersecurity for quantum computing. arXiv preprint arXiv:2110.14701.
[46] Mohan, J. P., Sugunaraj, N., & Ranganathan, P. (2022, May). Cyber security threats for 5G networks. In 2022 IEEE international conference on electro information technology (eIT) (pp. 446-454). IEEE.

Ciberseguridad, Regulación y ética,

Imprescindibles en la sociedad actual

Roberto Morales Estrella

1. Todo tipo de información requiere de Ciberseguridad

La ciberseguridad cada vez tiene más relevancia en la nueva economía científico-tecnológica. De todos es sabido que vivimos una sociedad en acelerada transformación, los procesos históricos anteriores, se registraban con mayor lentitud, pero hoy los escalamientos son a mayor velocidad y profundidad, por la intensidad del desarrollo tecnológico, los comportamientos de la sociedad en general, han pasado de ser procesos evolutivos a mutaciones aceleradas.

La ciberseguridad nace con el internet y con las plataformas tecnológico-virtuales, teniendo como antecedente la red ARPANET, construida por la Agencia de Proyectos Avanzados del Pentágono de los EE. UU.; en la medida en que estas plataformas y la multiplicidad de sus aplicaciones, escalan su transformación, también los ciberdelincuentes perfeccionan sus tecnologías, siendo las más frecuentes el ramsomware y el malware y el exploit, como el llamado phishing; a través de las cuales secuestran o sustraen información, la cual venden en el mercado negro, o piden rescate.

Los ciberataques a las actividades industriales se multiplicaron, sobre todo después de la pandemia, por lo que la ciberseguridad, es ya una prioridad en todo tipo de organización, sin que sea la excepción el nivel individual, dada su transversalidad; en sociedades como la nuestra están estructuradas en torno a una *oposición bipolar entre la red del internet y el yo*, como lo precisó Manuel Castells, en su Prólogo la Red y el Yo (Manuel, 2023), por ello la ciberseguridad es fundamental en nuestra vida.

Según el INEGI (, INEGI, 2023, págs. 1-2), por acoso cibernético o ciberacoso se entiende "como un acto intencionado, ya sea por parte de un individuo o un grupo, teniendo como fin el dañar o molestar a una persona, mediante el uso de tecnologías de información y comunicación, en específico el internet".

Las cifras de INEGI identifican a 105 millones de personas de 12 años y más como usuarios de internet en 2022, el 79% de esa población utilizó internet en cualquier tipo de dispositivo móvil

o fijo, correspondiendo el 44% de mujeres; el 20.8% de esa población de 12 años y más a nivel nacional, fueron víctimas de ciberacoso en 2022, por entidad federativa correspondió al Estado de Hidalgo el 23.5% superior a la media nacional. Las medidas de seguridad que se aplicaron por parte de los usuarios son las contraseñas, las claves, las huellas digitales y los patrones de desbloqueo, pero no han sido suficientes.

El acelerado proceso de digitalización tecnológica, ha venido abarcando cada vez más actividades empresariales, gubernamentales y de la sociedad, dando lugar al surgimiento de tres tipos de mercado: uno centrado en el *intercambio de bienes y servicios*, que incluye la educación y la necesaria formación de una masa crítica de expertos en el manejo, comprensión y creación de nuevas herramientas tecnológicas, como extensión de los resultados logrados, en los procesos de I+D+i; el otro mercado *es el de la información*, cuya generación es a ritmo de cada clic, y la transmisión de la información es a la velocidad de la imaginación, en tercer lugar está el *mercado negro de los datos*, cuyos actores son los ciberdelincuentes o hackers, el Dark web (Steve, 2022) mueve recursos por 8 billones de dólares, se estima que puede llegar a los 10 billones de dólares en 2025, que ya está a la vuelta de la esquina, lo que representa un empoderamiento del cibercrimen

Jorge Bravo (Jorge, 2023), visitó el Centro de Transparencia, Protección, Privacidad y Ciberseguridad de la empresa Huawei, donde Kira Peng, funcionaria de Huawei, le explicó que la ciberseguridad es fundamental para su empresa por el grado de complejidad y la multiplicidad de los stakeholders o partes interesadas, por lo que la ciberseguridad debe considerarse como un problema común, pero de responsabilidad compartida, que exige la participación de todo tipo de organización pública y privada, como de la sociedad en general.

Para contrarrestar los ciberataques, se estima que las empresas, han erogado 150 000 millones de dólares; sin embargo, los ciberdelincuentes surgen como hongos; en estaera hiperconectada del 5G y del 6G, los ciberdelincuentes son tan numerosos como ocultos para la mayoría, los más peligrosos nunca son atrapados, o sea que la impunidad es un factor que prevalece, dada la creciente destreza cibertecnológica.

Trascendió en una publicación de AVG.com (J. Regan, e I. Belcic 2022) que entre los hackers más famosos están: Ellion Guton, quien a los 16 años se le sorprendió hackeando a la empresa TalkTalk; otro detectado es Evgeni Milkhailovich Bogachev, quien generó una red de bots (GameOver ZeuS) infectando con ramsomware, a millones de ordenadores en todo el mundo, las autoridades de los EE. UU. y de otras naciones, están ofreciendo 3 millones de dólares como recompensa para localizarlo. Existen otros miles más, que buscan la forma de realizar

ciberataques depredando empresas y organizaciones públicas, y México no ha sido la excepción. Por ejemplo, fue público el ataque del grupo de hackers que se hizo llamar Guacamaya Leacks (, Redaccion BBC News Mundo, 2022) que extrajo de la Secretaría de la Defensa Nacional 6 terabytes (10^{12}) de información confidencial, si bien no tuvo repercusiones serias, si evidenció la vulnerabilidad de los sistemas informáticos, que ya debieron haberse fortalecido su ciberseguridad.

También hay empresas especializadas en ciberseguridad, existen más de 200 en nuestro país (Rufino, 2023). Su función principal es dar soluciones de ciberseguridad, garantizando la integridad de los sistemas de información y la confidencialidad de los datos. Las más conocidas son: ho1a. Innovación; ESET; Akamai; OneseQ; GMV; HornetSecurity y Kaspersky, entre otras tantas.

La ciberseguridad no solo son metodologías y herramientas tecnológicas, que eviten o mitiguen el riesgo de ciberataques, constituye un factor fundamental para la estrategia operativa, tanto de empresas, como de gobiernos, y de los hombres y mujeres a nivel personal, es tal la dimensión de la gravedad que se requiere de tres componentes estratégicos: el legal, el tecnológico y por supuesto el ético, que garanticen el resguardo y cumplimiento de los derechos humanos, como de los objetivos del desarrollo sustentable.

En virtud de que la información es considerada como un mensaje, ya sea verbal, mediante texto o imagen, en sí es todo aquello que puede ser captado por nuestros sentidos, vinculándonos con el entorno físico y social, incluyendo el estímulo a nuestra imaginación; en consecuencia, por *dato* se puede entender la unidad básica de la información, los datos transmiten elementos únicamente descriptivos, que requieren de una interpretación, para lo cual entran a un proceso de ordenamiento, para identificar en ellos algún sentido, o bien modificarlo para intereses particulares de personas o de organizaciones, pudiendo dar por verdad algo que no lo es.

El significado de la información como concepto está necesariamente en función del contexto epistémico en que se utiliza. El término leer no solo es el texto o la palabra escrita, sino también todo aquello que puede representar un mensaje entre dos entidades, el que lo envía y el que lo recibe.

Como ya es sabido, el conocimiento es resultado de un conjunto de elementos como los datos, que se pueden obtener a partir de las vivencias o experiencias, al relacionarnos con el entorno físico y social (Davenport y Prusak, 1999, citado por Paul Iles y Yochana Altman 2002 (Paul &

Yochana, 2002) En la perspectiva de la *teoría de la información*, (Valbuena de la Fuente, 1997:18 (De la Fuente , 1997)) se observa como una rama de la teoría de las matemáticas y hoy de las ciencias de la computación, que estudia la información y todo lo que ello implica, confirmando su creciente importancia socio-transformadora.

En la década de los 60, Manuel Castells planteó la llegada de la era de la información, basada en la alta velocidad de los cambios tecnológicos, dando paso al software, la informática y la telemática, impactando a todas las actividades productivas, educativas y sociales.

Peter Drucker (Peter F, 1993, pág. 57) describió a la sociedad del conocimiento, como una nueva forma de organización social a partir de los procesos de producción y sistematización de la información, considerando que el conocimiento era la nueva fuente de la riqueza. Dado que hemos llegado al punto donde el conocimiento es el eje articulador de todos los procesos económicos, tecnológicos, políticos y sociales (Juan Carlos, 2010), la habilidad cognitiva es la variable decisiva en la estructura social, impulsando o disminuyendo la desigualdad.

El proceso tecno-social transformó a los datos en el combustible de la revolución 4.0, donde la Inteligencia Artificial detonó las fábricas inteligentes, aplicando tanto el conocimiento automático (Aprendizaje automático), como el conocimiento profundo (Deep Learning); en cuanto a activos intangibles, los datos dieron relevancia a la Propiedad Intelectual, sin faltar en estadinámica la generación de bienes y servicios intensivos en conocimiento, resultado del desarrollo científico-tecnológico, en aquellas naciones que incrementaron su inversión en investigación y desarrollo (I+D+i), derivando en el dominio de los mercados globales.

La sociedad informatizada se fundamenta en la Ciencia de los datos, aplicando herramientas tecnológicas para identificar los comportamientos de objetos, tecnologías y personas mediante las llamadas tendencias tecnológicas y de mercado, que se utilizan para la toma de decisiones más precisas, son un gran recurso para la competitividad. La ciencia de los datos puede llegar a convertir lo inesperado en una ventaja y la incertidumbre en una oportunidad, en la ruta por lograr o continuar dominando los mercados.

La ciencia de los datos es un sub-apartado de la Inteligencia Artificial (IA) que aborda las áreas interconectadas de estadísticas, métodos científicos y análisis de datos, para extraer significados y conocimientos aplicándolos en tiempo real.

El aprendizaje automático como parte de la ciencia de los datos y de la IA se fundamenta en técnicas que permiten a las computadoras a identificar comportamientos a partir de los datos; también forma parte de la ciencia de los datos el aprendizaje profundo, dado que permite a los equipos informáticos resolver problemas complejos.

Pero el escalamiento de la Inteligencia Artificial (IA) como la tecnología más poderosa, por su transversalidad, la hace aparecer en casi toda actividad tecnológica. A partir del surgimiento del ChatGPT, un chat con la potencia del GPT que significa un modelo de lenguaje extenso basado en el *Transformador Generativo Preentrenado*, para la construcción del ChatGPT 3 se utilizaron 12 capas y 175 000 millones de parámetros, pero para el ChatGPT 4 estos se incrementaron en 600 veces más, para llegar a 100 billones de parámetros (Xataca [11]). (Javier , 2023)

La Inteligencia Artificial Generativa deriva de la Inteligencia Artificial, desarrollando redes neuronales generativas a partir del Deep Learning (aprendizaje profundo) lo que facilita el aprendizaje de manera automática (Marcelo Granieri (Marcelo, 2023), permitiendo construir una capacidad de captar y analizar grandes volúmenes de datos, identificando patrones al relacionar todos los parámetros de información, en la primera fase se utilizan los llamados datos sintéticos, para su entrenamiento, y después ya captan la información de diversas fuentes, principalmente de usuarios de Internet, desarrollando su gran capacidad de relacionar información, lo que les permite a los Chats, construidos con Inteligencia Artificial Generativa, contestar las preguntas y consultas que les hacen.

Es importante destacar que sus respuestas son resultado de su gran capacidad de relacionar grandes volúmenes de información, como textos, imágenes y videos, pero no son creativas, por lo que no tienen la garantía de la veracidad de sus respuestas que pueden estar equivocadas. El mismo Sam Altman CEO de OPENAI (Vargas, 2023), lo mencionó cuando se presentó en la audiencia del Subcomité Judicial del Senado de los EE. UU. sobre Privacidad, Tecnología y Ley sobre Inteligencia Artificial, el 16 de mayo de este 2023, cuando admitió estar bastante preocupado por el impacto de los modelos de lenguaje extenso, como el ChatGPT, su mayor temor es que lleguen a causar un daño significativo al mundo, como en los procesos democráticos y la generación de información falsa, por lo que propuso se trabaje de manera conjunta industria tecnológica y gobierno.

Estas redes neuronales generativas o Inteligencia Artificial Generativa, mejor conocida como GANS o redes antagónicas generativas, constan de dos partes, un generador de contenido nuevo, y un generador discriminador, cuya función es valorar si el contenido es falso o real, este proceso

le permite a la Inteligencia Artificial Generativa aprender de los grandes volúmenes de información a grandes velocidades. EstaInteligencia Artificial Generativa es una herramienta que se aplica, tanto en actividades industriales, como comerciales y educativas; sin embargo, no está exenta de los ciberataques.

En el tiempo desde que apareció el ChatGPT 3, su aplicación ya cubre actividades como los análisis de imágenes médicas y pronósticos meteorológicos de alta resolución (Michael , 2023) el uso y las inversiones en este tipo de Inteligencia Artificial muestran un escalamiento impresionante, a pesar del riesgo de alta vulnerabilidad ante los ciberataques.

2. Los flujos de Información son el ADN de la sociedad actual

Para Yuval Noah Harari (Harari, 2017, págs. 400-431) "el Dataísmo sostiene que el universo consiste en flujos de datos, y que el valor de cualquier fenómeno o entidad está determinado por su contribución al procesamiento de datos". El riesgo de la información como paradigma, también lo plantea Noah Harari, cuando describe que la humanidad, en el siglo XVIII, pasó de una visión teocéntrica, basada en los algoritmos bioquímicos (imaginación), a una visión homocéntrica, al considerar que el único conocimiento verdadero es el científico, pero en el siglo XXI el Dataísmo podría dejar de lado a los humanos, al pasar de una visión homocéntrica a una visión datacéntrica.

El tránsito de los homínidos al Homo sapiens y de este al Homo videns, es un largo proceso histórico de transformaciones y mutaciones, donde el conocimiento se erige en el factor transformador, cuyo escalamiento va de la capacidad de fabricar y usar instrumentos, a la transformación del entorno físico mediante el trabajo, generando sus satisfactores, dotándolos de valor de uso; el cambio incremental y disruptivo, convergen hoy en el binomio tecnología-ciencia.

La historia de las civilizaciones (Miguel Angel, 2017, págs. 25-29) es la de sus tecnologías y técnicas (habilidad para manejar sus instrumentos) que se han venido aplicando en sus actividades para sobrevivir, a lo largo de la historia misma de la humanidad, incluyendo la guerra y la organización-control de la sociedad.

La génesis de la actual era tecnológica se localiza en los siglos XVIII y XIX con las revoluciones industriales, que han dado paso a una nueva era tecnológica basada en la digitalización-nube-Big Data.

La generación del conocimiento científico-tecnológico fue un factor decisivo en la transformación económica y por ende social, así como del crecimiento económico y del desarrollo en algunos países, pero también trajo consigo la desigualdad y el rezago en grandes masas de la población; la desigualdad, la marginalidad y la pobreza de ese entonces, se siguen reproduciendo.

Nuevas prácticas productivas y sociales a la luz de los desarrollos científico-tecnológicos, han sido contundentes por la ruta marcada por la Investigación, el Desarrollo Tecnológico y la innovación (I+D+i) sin faltar la apropiación del conocimiento creado y generador de valor, o sea la Propiedad Intelectual. Arribamos al siglo XXI con un incremento sustancial de dispositivos electrónicos donde los procesos productivos fueron, incluyendo la digitalización, que se aceleró con la pandemia del covid.

Ha sido descomunal el incremento de la información, según Data Never Sleeps (Domo.com, 2023), en el 2021 se generaron 5.2 billones de bytes, incremento que no muestra signos de desaceleración; en la economía digital-nube-Big Data se considera la inserción de todos los agentes económicos, políticos y sociales, a través de sus equipos de cómputo, generando y consumiendo cada vez más información, los gigas (10^9) se han convertido en la unidad de consumo de conexión a Internet, no tardará que de los gigas pasemos a los terabytes (10^{12}) y a los petabytes (10^{15}) en un tiempo no muy lejano.

El internet-nube también está escalando a nivel satelital, dados los satélites de órbita geosincrónica, dando respuesta a los problemas de ancho de banda. Estamos pasando de las prácticas tradicionales de las TIC, que se basaban en poseer, a la de consumir.

A la par de la construcción de una sociedad de macrodatos-nube se ha generado la cibercriminalidad, por lo que tanto individuos (Garc, Garc, & Garcia, s.f.) (Garcia, Ciberseguridad ¿porque es importante para todos?, 2019) como organizaciones públicas y privadas, necesitan de normas, leyes y reglamentos sobre ciberseguridad, protegiendo la información a nivel local como global.

Los ciberataques son a través de virus informáticos que se autorreplican, además de gusanos, troyanos, botnets, programas espía, el ransomware, los rootkits, y los exploits[3] que ya citamos, así como aquellos nuevos productos informáticos malignos que los cibercriminales están creando.

El Foro Económico de Davos publicó en este enero del 2023 su informe *Global Cybersecurity Outlook 2022* (, World Economic Forum, 2022) donde planteó pasar de la ciberseguridad a la ciber-resiliencia, que implica no solo la formación de capital humano especializado, lo que representa un desafío para las Instituciones de Educación Superior, sino también desarrollar y aplicar nuevas tecnologías, asegurando la protección de la información.

En la medida, en la que todo individuo, familia, organización pública y privada, se digitaliza, participa interactivamente en la dimensión virtual del ciberespacio, que se intensificará, cada vez más, con otros espacios como el metaverso.

Multiplicándose también los ciberdelitos, como el robo de identidad, el espionaje industrial, los cibersecuestros, la pornografía infantil, el ciberbullying, fraudes electrónicos y financieros; todo aquel que navegue en el ciberespacio es objeto probable de un ciberdelito, propiciado por los programas informáticos que se infiltran o implantan en sus equipos de cómputo fijos o móviles.

El Internet abrió la posibilidad de que los cibercriminales tengan acceso a la población global. La información es un bien cada vez más valioso, tanto por su valor de uso como su por su valor de mercado. Protegerla de los ataques cibernéticos es tarea de todos, por lo que es imprescindible hacer de la ciberseguridad una cultura educativa y social.

3. La ciberseguridad es imprescindible en la sociedad actual

La convergencia tecnológica es el fundamento del paradigma científico-tecnológico, es un proceso que se evidencia en la convergencia entre la electrónica del estado sólido, la ciencia de los materiales, la óptica y la ingeniería de telecomunicaciones, que derivó en las Tecnologías de Comunicación y de Información (TIC) las cuales junto al internet y a la Inteligencia Artificial han transformado a toda la humanidad.

[3] Se le denomina así a una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o dispositivo electrónico; es un ataque remoto a los sistemas informáticos [57].

Pero, ¿qué es la Inteligencia Artificial? La Inteligencia Artificial son estadísticas aplicadas utilizando grandes cantidades de información, utilizada como base para que el talento humano crea conocimiento, se distingue por su gran capacidad y velocidad de relacionamiento, *pero no es consciente*, tiene como fundamento a las matemáticas (algoritmos) con base en ellas crea un lenguaje lógico para la resolución de problemas cuantitativos; en su construcción tiene una capa de estadísticas y matemáticas aplicadas para interpretar y predecir resultados basados en datos; cuenta con una fase de Aprendizaje Automático lo que implica aprovechar las estadísticas aplicadas mediante computadoras para automatizar y mejorar el desempeño de las actividades a realizar; finalmente, la Inteligencia Artificial es aprendizaje automático aplicado para realizar tareas complejas y novedosas fundamentalmente *imitando a los humanos* (J. D., Gustav, Minh, & Ng, 2023).

El eje transversal de esta convergencia de la nanotecnología, biotecnología, cognotecnología e infotecnología *es la Inteligencia Artificial*, que ha venido ampliándose y diversificándose, creciendo de manera exponencial, sobre todo del 2011 al 2017, llegando en el 2019 a más de millón y medio de publicaciones y superando las 340 000 solicitudes de patentes, siendo un poco más de 500 empresas las solicitantes, de las cuales 333 son trasnacionales norteamericanas, encabezando la lista IBM y Alphabeth (, OMPI, 2019, págs. 40-45).

Solo para visualizar la dinámica del escalamiento, cabe señalar que la Inteligencia Artificial aplicada en Robótica creció en 265% y en métodos de control 262% (James , 2019). En el informe de Inteligencia Artificial 2023, publicado por el Instituto Stanford para la Inteligencia Artificial centrada en el ser Humano (, Stanford University, Human Centered AI, 2023) ha destacado que los grandes modelos de lenguaje como el ChatGPT han aumentado de forma exponencial, en tal virtud la inversión de las agencias estadounidenses incrementaron en 13.1% en 2022 respecto a 2021, para llegar a 1.7 millones de dólares para investigación y desarrollo (I+D). Por su parte, el Departamento de Defensa de los EE. UU. solicitó para 2023 1.1 mil millones de dólares, también para I+D en este rubro. Estas inversiones evidencian la importancia que representa el seguir investigando sobre Inteligencia Artificial.

De las múltiples aplicaciones de la Inteligencia Artificial, las que alcanzaron un impacto más que sobresaliente son el ChatGPT, sobre todo el 3 y 4, por el número de usuarios que se ha multiplicado en un corto tiempo, el ChatGPT 3 ya ha alcanzado más de 100 millones de usuarios. Sus capacidades están relacionadas con el lenguaje natural, o sea humano, y a su capacidad multimodal.

El concepto de ciberseguridad más aceptado, es el conjunto de procedimientos, políticas, y el diseño, como la aplicación de diversas herramientas tecnológicas, que se crean para proteger sistemas de redes y programas, para proteger a la infraestructura tecnológica de ataques principalmente de Ransomware, Malware y de Phishing, sin faltar el exploit. En últimas fechas surgió en la Dark Web el denominado WormGPT (Daniel , 2023) emulando al ChatGPT, con el cual los ciberdelincuentes, también llamados Black Hat o crackers, la utilizan como herramienta tecnológica para cometer delitos cibernéticos, mediante correos electrónicos de phishing con inteligencia artificial, creando módulos personalizados similares al ChatGPT pero más fáciles de usar, para insertarse en los sistemas informáticos y dañarlos.

Según los datos de ESET Security Report 2023 (, ESET Digital security, 2023), los ataques de Ransomware en su modalidad de RaaS incluyen métodos extorsivos como el print-bombing y el cold-calling, exigiendo el rescate en criptomonedas; si no, se filtra la información al mercado negro. La infección por códigos infecciosos es la mayor preocupación, seguida del robo de información. México ocupa el segundo lugar en cantidad de detecciones con el 17 %, seguido de Perú con el 18% a nivel Latinoamérica. En el 2021 se generaron 22 000 reportes de vulnerabilidades.

La alta complejidad, en materia de ciberseguridad, a la que se enfrenta la sociedad actual, lo constituyen dos grandes desafíos, por un lado, está la sustitución de la realidad por un mundo virtual, puesto que vivimos escenarios que no son reales, lo que impacta en la conciencia humana, poniendo en riesgo su capacidad de pensar y razonar, frente al avance de procesos automatizados, que carecen de pensamiento crítico analítico, que solo describen, pero no explican, ¿esa va a ser la información que alimentará a las nuevas generaciones?. Por otra parte, está el robo de información, incluyendo los robos de identidad de todo ser humano, pudiendo utilizarla por parte de los ciberdelincuentes para cometer todo tipo de delitos.

La inseguridad cibernética vas más allá de las fronteras de los datos numéricos para alcanzar la información no estructurada como son las imágenes, la voz y los patrones de conducta, rutinas y trayectorias cotidianas. Si estamos enfrentando el fin de la realidad, ¿cuál debe ser el papel de la seguridad cibernética?.

4. La Regulación de la Ciberseguridad

En México, a pesar de que se han realizado numerosas mesas de discusión sobre la construcción de una ley de ciberseguridad, no se ha concretado, a la fecha de escribir este trabajo, solo existían tres propuestas, pero ninguna definitiva que se pueda pasar a convertirse en Ley de Ciberseguridad a nivel nacional, el enfrentamiento de los diversos grupos de interés han

polarizado las distintas propuestas, hay quienes defienden intereses empresariales, sobre todo de corporativos trasnacionales y la otra parte está por darle un sentido social, no queda más que esperar como se negocian las diversas posiciones. Cuando México ocupa la posición 34 de un ranking de 76 de las naciones en ciberseguridad (Armenta, 2020), mientras países como Colombia ya están creando una Agencia Nacional de Ciberseguridad (Sharon, 2023)

De hecho, en México hace falta una *estrategia nacional de ciberseguridad*, en virtud de que no existe una capacidad lo suficientemente fuerte para restar la vulnerabilidad de las estructuras institucionales, y empresarias como de la sociedad en general, su información crítica está en permanente riesgo (G., 2016), Adolfo Arreola García (Garcia, cesnav.uninav.edu.mx, 2018) propuso la creación de un sistema de ciberseguridad nacional para México, que consiste en contar con dos elementos clave la ciberseguridad y la ciberdefensa, en el siguiente nivel están los elementos de la sociedad civil, donde se integrarían las certificaciones, en el segundo elemento está la policía federal, que vendría siendo la Guardia Nacional, de donde dependería la *policía cibernética*, y el tercer elemento serían las fuerzas armadas o sea las Secretarías de la Defensa y Marina.

Obvio este sistema no prosperó ni fue tomado en cuenta en las diversas iniciativas de ley que siguen en el debate legislativo; sin embargo, denota la preocupación; cabe mencionar que dadas las constantes transformaciones que se observan con los escalamientos del desarrollo tecnológico, así como la actuación de los grupos de criminales que constantemente están desarrollando herramientas tecnológicas para identificar nuevas vulnerabilidades, derivando en lo que se ha denominado Amenazas Persistentes Avanzadas (APT) (Luis, 2023), cada vez más sofisticadas para eludir su detección.

Por parte de las organizaciones de todo tipo, pero sobre todo la población a nivel general, requieren de protección especializada contra los ataques avanzados y selectivos. Por ello es imprescindible que en la política y sistema de ciberseguridad nacional se contemple a las Instituciones de Educación Superior, para que mediante la Investigación y Desarrollo e Innovación (I+D+i) se dé el soporte del conocimiento y del personal altamente capacitado, para ir un paso adelante de los grupos criminales que sí están permanentemente investigando.

El concepto de *Identidad Digital Reutilizable* (Iñigo, 2023) es un concepto innovador orientado a otorgar a los usuarios un mayor control sobre los datos que comparten con empresas y servicios que requieren autenticación biométrica. Es una herramienta que, si se regula adecuadamente, puede dar seguridad a clientes y empleados, propiciando que las empresas puedan facilitar la interacción en línea, agilizar los procesos de registros y autenticación, facilitando las transacciones con mayor seguridad en las actividades digitales. Es llevar la biometría a niveles de ciberseguridad, para ello se requiere una política pública a nivel nacional y en las entidades federativas.

Sin lugar a dudas que ya han surgido herramientas y estrategias para hacer frente a ciberataques, que desde la perspectiva empresarial es un mercado muy prometedor, dada su característica de escalamiento en el talento tecnológico en sus dimensiones antagónicas, por un lado, el talento depredador de los ciberdelincuentes que tienen a su disposición medios y formas de propagar sus diversas tecnologías dañinas, sobre todo porque un ciberataque no se advierte de inmediato en virtud de que no a todos los niveles y componentes del sistema se les da seguimiento.

Ya algunas empresas aplican lo que se llama la *Gestión de riesgos de TI,* (, LAC BLOG, 2023) que se identifica con los procesos básicos del management de planear, organizar y controlar los recursos tecnológicos, con la posibilidad de reducir los daños y fallas ante un ciberataque, esto incluye la mitigación de problemas y siniestros, prevención de ciberataques y robo de datos, restauración del back-end como de los contenidos estratégicos, sin dejar de lado el mantenimiento de los sistemas y actividades de TI.

También está la formulación de un *Plan de Contingencia* (, ESET, Digital Security Progress. Protected, 2023) para enfrentar los ciberataques, este Plan de Contingencia tiene como objetivo fortalecer la fiabilidad de los procesos dotándolos de capacidades para responder en tiempo y forma, en una situación de emergencia por un ciberataque, contempla todos los sistemas con que cuenta la organización, para dar respuesta a cualquier indicio de violación de los procesos tecnológicos, como de los aspectos legales, dotando de agilidad al personal para desarrollar lo necesario para evitar los daños y fuga de información estratégica, evitando la inmovilidad, permitiendo que los sistemas informáticos continúen operando.

La dimensión de la ciberseguridad es cada vez más amplia, sobre todo cuando observamos que en los conflictos geopolíticos la Inteligencia Artificial ya es considerada como una arma tanto económica como geopolítica, por parte de las naciones tecnológicamente desarrolladas, como China, que ha expresado que la Inteligencia Artificial es la columna vertebral tanto de su industria productiva como militar, de la misma forma están naciones como España, Francia, Alemania, Reino Unido, los Estados Unidos y no se diga Ucrania y Rusia. La Inteligencia Artificial es uno de los componentes que se usan como armas de ataque-defensa.

Para resguardar los sistemas complejos de grandes organizaciones productivas o militares, el cómputo cuántico, promete un poder transformador para gestionar *el riesgo cuántico* (Michele & Vickram , 2023)*,* a través de la generación y aplicación de la *criptografía cuántica* como un mecanismo de protección, a través de la revisión constante de indicadores clave de rendimiento,

lo significa realizar la llamada *transición cuántica* adoptando tres enfoques principales: *primero* introducir soluciones cuánticas paralelas, esto es hacer uso de los algoritmos criptográficos ya disponibles y desarrollar unos propios de la organización, combinando sus capacidades*; aplicar* un enfoque de etapas, lo que debe de entenderse por realizar una migración de grupos de sistemas a la criptografía cuántica, iniciando el *desarrollo y entrenamiento de los algoritmos* necesarios y suficientes, este enfoque se aplica fundamentalmente en las primeras etapas del desarrollo de un proyecto. Como se alcanza a apreciar, esta transición genera mayores capacidades para reducir las vulnerabilidades, pero no se está exento de ciberataques.

Para Javier Romero M (Muñoz, Dilemata Revista , 2017, págs. 45-57) *los derechos digitales* son un *derecho humano*, en virtud de que todas las naciones forman parte de una sociedad hiperconectada a nivel global y la digitalización está presente en la mayoría de las actividades humanas, *las actividades digitalizadas son un bien de primera necesidad*, lo cual encuentra fundamento en lo estipulado por la Organización de las Naciones Unidas en los artículos 3, 9 y 12 de la Declaración Universal de los Derechos Humanos de 1948, los derechos de cuarta generación corresponde los *derechos digitales* son "derecho a la libre expresión, derecho a la privacidad digital, y la ciberseguridad, derecho de acceso al ciberespacio y a la información, derecho a asociarse en comunidades virtuales en Internet, y derecho a los derechos digitales".

5. El papel de la ética en la ciberseguridad

Sebastián Bilbao (Perez , 2022, págs. 103-104) parte de su concepto de riesgo moral, donde el problema "se da cuando los costos atribuibles a los riesgos de una parte son soportables por otro" (Jeffrey, 2020, pág. 104). La ciberseguridad no solo se refiere a objetos y situaciones tecnológicas, sino que tiene un componente eminentemente humano, por lo que los ciberdelitos están orientados no solo a dañar equipos, sino a dañar el patrimonio de las organizaciones y de individuos de manera específica y directa.

"La capacidad de una organización para hacer frente a las amenazas y vulnerabilidades depende en gran medida de los niveles de formación en ciberseguridad de su personal, y en consecuencia en la existencia de un marco de competencias que identifique los contenidos y niveles de formación y concienciación necesarios para cada puesto de trabajo" (Caldentey, Urquijo, & Almazor , 2022, pág. 197).

Desarrollar las capacidades de ciberseguridad es una necesidad a satisfacer de manera inmediata, aunque habrá que destacarse que debe rebasar las fronteras de las organizaciones

productivas e incluso públicas, para ampliarse al sector académico es decir, impulsar una *cultura de la ciberseguridad*, para que toda la población en su actuar cotidiano desarrolle una conducta de prevención, al estar consciente de los riesgos, más allá de las competencias, que sea parte de los patrones de conducta de toda sociedad, lo que implicaría que se incluya como asignatura en los programas de estudio, si bien desde temprana edad se les da la facilidad a los niños para manejar los dispositivos móviles, entonces desde los primeros acercamientos en los procesos educativos se debe considerar un tema a enseñar.

Sobre todo desde una visión contextual, por ejemplo para Davenport y Prusak (1998) (Tomas H & Laurence , 1998) *el conocimiento es una mezcla fluida de experiencia formulada y valores en una información contextual*; el conocimiento en tanto constructo social es un proceso exponencial, de transmisión de información entre los diversos grupos sociales, que facilita la construcción de valores humanos, siempre y cuando no sea sujeto estricto de oferta y demanda, por el valor monetario de intercambio en los mercados, condición que eclipsa la formación de valores morales, lo cual es superable a partir de la formación de un pensamiento crítico-analítico-sistémico, una forma de pensar diferente a la anticultura de la filosofía de los mercados, que privilegia la alta rentabilidad a toda costa.

El divulgar los ataques por parte de ciberdelincuentes es una actividad fundamental, en virtud de que los usuarios de las plataformas vulneradas, tienen derecho de conocer cuáles fueron las vulnerabilidades de las plataformas que usan cotidianamente, en virtud de que esas plataformas manejan datos críticos de los usuarios, además que la ausencia de información limita la capacidad de generar las estrategias adecuadas y oportunas para tomar las decisiones oportunas y confiables, en las actividades que realizarán en el corto como en el mediano y largo plazo.

Una cultura moral proviene necesariamente de las raíces culturales de los diversos grupos humanos desde una perspectiva histórica, ya que sin esa cultura moral la humanidad no hubiera sobrevivido hasta nuestros días, en la presente era tecnológica-digital la moralidad proviene necesariamente de la educación en todos sus niveles, pero también juegan un papel importante los medios de comunicación ya sean impresos o digitales, pero sobre todo de las redes sociales, cuyo uso ha caído en lo estrictamente mercantil, dejando a un lado los valores morales que han sido superados por la violencia de todo tipo y dimensión.

Tan es así que cuando una organización, sobre todo las trasnacionales, han sido víctimas de un ciberataque, lo que más lamentan los directivos empresariales, son los daños financieros y su reputación, antes que los daños a las personas.

Dado que la Inteligencia Artificial es una tecnología transversal, hoy se localiza en la mayoría de las tecnologías, si bien es cierto que imita y amplifica numerosas capacidades del humano, también es cierto que carece de la capacidad humana de consecuencias, que resulta de las interacciones y de los impulsos propios de la naturaleza humana como la ambición, el odio, la envidia, la mega melomanía, la recompensa, el placer, el dolor, etc. Grandeza y vileza son posibles en el ser humano como ente social.

Si bien ya están surgiendo iniciativas de ley para regular a la Inteligencia Artificial, y las demás tecnologías, así como el comportamiento y operación de las empresas hegemónicas como las trasnacionales, no será fácil regular a los reguladores, por ejemplo a los mandatarios y regímenes autoritarios que ven a la tecnología no como la aplicación de talento humano en beneficio de la sociedad, sino como medios para lograr sus ambiciones de poder, para imponer su hegemonía a nivel global, la evidencia son los conflictos geopolíticos donde converge lo tecnológico, lo financiero, y la apropiación y depredación de los recursos naturales, antes que resolver la siempre creciente desigualdad social mundial, aunque la mencionen en sus discursos de justicia social, los cuales se derriten ante la realidad que vivimos día a día. Por ello, *la Inteligencia Artificial debería de regularse como una entidad y no como un software* (Troica, 2023, págs. 1-10), y sería un gran avance para hacer que la ética trascienda del discurso hacia la realidad social, lo que representaría ganarle terreno al mercado y a la ambición política.

La visualización de la creciente discriminación tanto de género como racial, la invasión a la privacidad como una constante con tendencia creciente, la generación de información sesgada intencional o francamente falsa, así como los numerosos ataques a los sistemas informáticos de todo tipo, por parte de los ciberdelincuentes, dio pauta a que la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2021) en su Conferencia General celebrada en París del 9 al 24 noviembre del 2021, con la participación de 195 naciones, emitiera la Recomendación sobre la ética de la Inteligencia Artificial, reconociendo sus impactos en las diversas dimensiones de la sociedad global, como las actividades económicas, financieras, los ecosistemas y en toda actividad humana, fundamentalmente en la mente humana, al influir en las percepciones de la realidad natural ante la realidad virtual y aumentada.

El propósito es que los países integrantes que la aceptaron, apliquen de manera voluntaria las medidas de la recomendación, acorde a sus estructuras jurídicas y de gobierno, pero también considerando el derecho internacional y fundamentalmente los derechos humanos. La recomendación considera a la Inteligencia Artificial como una reflexión normativa sistemática, teniendo como contexto el marco integral global, multicultural y evolutivo de valores, sin faltar

los principios y las acciones interdependientes, para que cada nación enfrente los desafíos que implica la autorización de la generación y aplicación de la inteligencia artificial, con criterios de sustentabilidad e inclusión, en los procesos industriales y comerciales, como en el ámbito educativo, en todos sus niveles, sin faltar las culturas y tradiciones, crear una cultura de uso y aplicación de la Inteligencia Artificial, que mantenga una tendencia en escalamiento exponencial, lo que significa que *la tecnología se retroalimenta creando nuevos nichos que generan nuevas necesidades y deseos de más tecnología* (Moshe, 2023) lo que obliga a crear y aplicar una estrategia de alfabetización social, desde una perspectiva tridimensional: tecnológica, sustentable y de derechos humanos.

La Unión Europea está legislando la Ley de Inteligencia Artificial (Spencer , 2023), cuyo objetivo es el de fortalecer la posición de Europa como líder en Inteligencia Artificial, cubriendo toda la cadena de valor, desde el laboratorio hasta los diversos mercados, si dejar de dar garantía de que se respeten los valores y las reglas de Europa, pero claro potenciar las aplicaciones Industriales de la Inteligencia artificial.

También aborda los temas de ética y los desafíos de implementación en sectores sensibles para la sociedad europea como la salud y la educación, sin dejar de lado al sector financiero y el energético, la calidad de los datos y la transparencia de los flujos de información con la participación humana en procesos de supervisión

Llama la atención la inclusión en esta normativa europea, para regular a la Inteligencia Artificial, la determinación de cuatro niveles de riesgo: inaceptable, alto, limitado y mínimo. Lo más destacable es el *riesgo inaceptable* que contempla la puntuación social y la aplicación de la biometría para la identificación de las personas en tiempo real en espacios públicos. La Inteligencia Artificial de alto riesgo contempla a los vehículos autónomos, la infraestructura crítica y los dispositivos que se aplican en el sector salud.

La Fundación Española para la Ciencia y la Tecnología (FECYT), tomando como contexto la Estrategia Nacional de Inteligencia Artificial (ENIA) (, Ministerio de Asuntos Economicos y Transform Digit, 2020, págs. 1-5) publicada el 9 de diciembre de 2020 por el Ministerio de Asuntos Económicos y Transformación digital, cuyo propósito es que sea el gobierno español el que lideré el desarrollo y la integración de la Inteligencia Artificial en el tejido productivo, la economía y la sociedad.

La Inteligencia Artificial es reconocida globalmente como la tecnología con mayor proyección e impacto, ya que sus aplicaciones son tan diversas, que funge como catalizador en los procesos de investigación, desarrollo e innovación (I+D+i) propiciando que el big data se haya transformado en un sector económico de alto impacto tecnológico y social.

Esta estrategia está estructurada en seis ejes como impulsar la investigación (I+D+i) en materia de Inteligencia Artificial (IA), impulsar el desarrollo de capacidades digitales y atraer talento especializado en IA, transformar el tejido productivo a través de la inserción de la IA en las cadenas de valor, insertar los procesos y aplicaciones de IA en las actividades gubernamentales, pero sobre todo, por el tema que nos ocupa que es el establecimiento de un marco ético normativo, que tenga impacto positivo en la inclusión social, como en los derechos de los individuos y de las comunidades, sobre todo de las más marginadas.

Con base en la ENIA la FECYT impulsó la investigación que dio forma al informe *"IA Spain 2023: informe público de Percepción Social de la Inteligencia Artificial"* (Calderon, 2023, pág. 44). Este informe considera seis implicaciones éticas relacionadas con la Inteligencia Artificial, tales como: *Privacidad y seguridad*, relativa a garantizar a que los datos de los individuos y organizaciones sean utilizados de manera responsable; *Sesgo y discriminación*, dado que es práctica frecuente la manipulación de la información de individuos y organizaciones, lo que hace necesario garantizar la equidad y la justicia ante las diversas formas de propiciar sesgos en la aplicación de la información en detrimento de la sociedad en general, porque da paso a diversas formas de corrupción; *Responsabilidad y transparencia*, lo que obliga a una estricta rendición de cuentas, para transparentar los procesos tanto de toma de decisiones como sus consecuencias; *Desplazamiento laboral y desigualdad*, sin lugar a dudas que es un tema complejo, pero se tiene que visualizar desde la óptica de los gobiernos para que se generen políticas públicas que apoyen a los desplazados laboralmente, por los avances en la automatización de los procesos productivos y comerciales, además de prever la desigualdad entre los que tienen conocimientos y habilidades para manejar herramientas tecnológicas basadas en Inteligencia Artificial, la formación de las nuevas generaciones de profesionistas deben contemplar la inserción de la inteligencia artificial, para que los nuevos profesionistas adquieran y desarrollen las capacidades necesarias y suficientes para que se inserten en el paradigma tecnológico, en este rubro cobra importancia la Alfabetización tecnológica y sustentable como de inclusión social; *Uso mal intencionado de la Inteligencia Artificial*, como el mal uso de las aplicaciones de la IA, para dañar a personas, organizaciones públicas y privadas, lo que hace necesario establecer, salvaguardas éticas y legales; *Impacto en la Dignidad humana*, esta implicación tiene como propósito prever lo que puede afectar las relaciones interpersonales en al ámbito social y laboral.

En sentido estricto no hay una ética-moral con una aceptación en todas las culturas de los diversos grupos humanos que habitan los diversos países, existe una pluralidad de valores éticos-morales con fuerte sustento en filosofías religiosas y otras corrientes de pensamiento, identificándose el kantismo, el utilitarismo, eudemonismo, hedonismo, cuya característica principal, es que ninguna de ellas es ni moral ni ética.

En los siglos XII y XIII la llamada *virtus* fue motivo de grandes disputas y debates entre los pesadores de la era medieval en torno a la construcción de la ciencia de la moral, los más destacados fueron Alberto Magno y Tomás de Aquino (Fernando G, 2022), cuyas aportaciones evidencian un constructo teórico sobre naturaleza-virtud desde el enfoque de la condición humana en torno a las 4 virtudes cardinales, que se conocen como la *prudencia o templanza*, poco común en las personas jóvenes*; la justicia*, darle a cada quien lo que le corresponde; *la fortaleza*, nunca darse por derrotado, base de la resiliencia, y la *magnanimidad*, no abusar del débil, ni discriminar; estas virtudes cardinales pueden ser un referente de un actuar ético. El ser humano, como especie en la línea del tiempo de su historia, siempre ha tratado de encontrarle sentido a su vida a través de su conducta (Picasso & Cosme, 2010). El asunto no es trivial, sino que es una cuestión de cómo deberíamos vivir en colectividad (Mark , 1988).

En fechas más recientes se localizan las teorías de justicia social como la de John Rawls (John, 1971) y de Jürgen Habermas (Jurgen, 2008) con un enfoque orientado hacia la construcción de un principio de universalidad, pudiendo derivar en darle validez los principios y enunciados morales en una sociedad plural y diversa (Muñoz, Dilemata.net, 2017) como lo es la sociedad global que hoy vivimos.

Esta universalidad de la ética da pauta para dilucidar sobre las éticas aplicadas, a partir de un diálogo intersubjetivo para alcanzar el consenso, esto es aplicar el principio básico de la razón práctica, como hoja de ruta para identificar a la ética aplicada en un universo conformado de sociedades pluralistas en esta era tecnológica y de alta conectividad, y por ende digitalizada, planteándose como punto de partida la razón práctica (Muñoz, Dilemata.net, 2017, págs. 49-59) orientada la acción humana o a la forma de actuar en el mundo, pudiéndose considerar en tres tipos de razones: *la razón práctica de uso pragmático*, es decir razón instrumental orientada a fines, también está *la razón práctica de uso ético* y *la razón práctica de uso moral* basada en la intersubjetividad, esta taxonomía deriva en las éticas aplicadas, constituyéndose en nuevos elementos para una filosofía práctica en las sociedades pluralistas de hoy; de las éticas aplicadas sobresale la Bioética, también la ecoética, identificándose a otras como la ética profesional y la ética empresarial.

En este contexto surge la *Cibernética aplicada*, que si bien le falta precisión y desarrollo, se ha venido complementado en proporción directa con el desarrollo tecnológico, incluso proyectándose a futuro ante las nuevas formas de las aplicaciones de la Inteligencia Artificial en áreas como la cuántica, la fotónica y la neuromórfica (Daniel, 2023), *la Inteligencia Artificial cuántica* se basa en una lógica, una física y de tecnología, que le permite más velocidad y eficiencia, sobre todo en el consumo energético, que es una de las principales debilidades del cómputo convencional, sobre todo el blockchain, la Inteligencia Artificial cuántica tendría la capacidad de convertir información analógica-digital a los procesos cuánticos.

La inteligencia Artificial Fotónica es la convergencia de sistemas fotónicos e internet de las cosas (IoT) y algoritmos, lo que permitirá, entre otras cosas, predecir potenciales defectos de manufactura, generando información para evaluarla y tomar decisiones oportunas y estratégicas. *La Inteligencia Artificial neuromorfica* pretende entender cómo funciona el cerebro humano para imitarlo, lo que implicaría generar una Inteligencia *Artificial Sintiente*, a través de sensores, para percibir el entorno, imitando los 5 sentidos del ser humano, las preguntas obligadas es ¿estamos arribando al post-humanismo?, ¿estas tecnologías superarán a la especie humana?, ¿y la regulación?, ¿y la ética?. Es por ello que la *cibernética* es fundamental tanto en el corto, como el mediano y el largo plazo.

La *ciberética* tiene como propósitos fundamentales ampliar los valores morales como las cuatro virtudes cardinales que se mencionaron anteriormente, sobre todo si consideramos la gran complejidad, de las tecnologías en general y fundamentalmente las tecnologías informáticas, y la hiperconectividad de las sociedades a nivel global, los siguientes principios básicos (J. Romero Muñoz, 54-56): *Autonomía y libertad del usuario del internet* y en el acceso de herramientas tecnológicas, esto significaría privilegiar al código abierto e impulsar la creación de *Organizaciones Autónomas Descentralizadas* (DAO) como las que ya existen en el mundo de los contratos inteligentes de los sistemas de blockchain; la búsqueda de beneficios como propósito esencial, es decir buscar el bien de todos promoviendo legítimos intereses y suprimiendo prejuicios; lo que está relacionado con evitar actos que ocasionen daños de todo tipo a otras personas o usuarios, independientemente si se conocen o no; esto tiene relación directa con un comportamiento basado en la justicia, darle a cada quien lo que les corresponda, respetando, por ejemplo el código fuente y la propiedad intelectual, respetar la creatividad a quien la materializo en prototipos o cualquier otro tipo de resultado de investigación.

Sin lugar a dudas que hoy ha tomado una gran relevancia la sustentabilidad y la inclusión social, sobre todo porque la informática actual como el blockchain, requiere cantidades enormes de energía, generando calentamiento del medio ambiente, la segregación de los grupos de bajos ingresos, por los precios cada vez más altos de los dispositivos, como de los mecanismos de

acceso a las diversas áreas del ciberespacio y del costo de las numerosas herramientas tecnológicas que se están generando, y son necesarias para participar como usuarios de la red y de todo tipo de ciberespacio.

De forma paralela evitar hacer daño de manera intencional, para ello está la generación y aplicación de medidas de ciberseguridad y protección ante los riesgos que representan ciertas tecnologías presentes y futuras, como las armas autónomas el WarmGpt, y la Inteligencia Artificial neuromórfica; parte importante de la ciberseguridad es el fomento y la divulgación de los mecanismos de privacidad, los datos reflejan lo que son las organizaciones públicas y privadas y de todos los usuarios individuales de las tecnologías, los datos son parte esencial de todo ente económico y personal, por lo que *la privacidad es un valor no negociable*, no debe ser una mercancía; finalmente *los derechos digitales son derechos humanos* y como tales hay que hacerlos valer en cualquier espacio, país o tipo de gobierno, violarlos y no respetarlos debe ser considerado como un delito universal.

Matthew Ball (Matthew , 2022, pág. 300), cita a Chris Dixon un inversor de riesgo centrado en las criptomonedas, quien sostiene que si el *ethos* dominante en la web 2.0 era "no seas malvado", entonces una web 3.0, basada en blockchain, sería *"no puedes ser malvado"*.

La Ciberética es un constructo social, porque son todos los habitantes del planeta que navegan en el ciberespacio, que ya es parte de la vida de todos, por lo tanto, es responsabilidad de todos y cada uno de los habitantes del planeta, contribuir en su construcción conceptual y en su aplicación social, nadie debe sustraerse porque es una condición humana para contribuir a la sobrevivencia de la especie, en un mundo donde la tecnología se está empoderando más allá del sentido humano.

6. Reflexión

El mundo está en una etapa de policrisis, en lo económico, lo político y lo social por la persistencia de la desigualdad, dado que en la lucha global por la hegemonía política y tecnológica, se está convirtiendo en una calamidad humana, que va a acentuar y agravar las otras calamidades que históricamente se han padecido, como son *el hambre, la guerra, las enfermedades, y hoy el cambio climático*, la tecnología fomentada por el mercado más que por el sentido humano para construir una vida más armoniosa y justa, está poniendo en riesgo la existencia de la humanidad, ¿cómo serán los humanos al final del siglo XXI?, ¿cómo serán los humanos de los inicios del siglo XXII? Cada inicio de siglo está marcado por cambios

tecnológicos más profundos, que han venido transformando a la especie humana y todo el entorno biológico y no biológico natural, la *Ciberética aplicada* puede ser el fiel de la balanza para construir un mundo más habitable, que nos lleve a superar las calamidades de siempre y las nuevas, la Ciberética puede ser la hoja de ruta de una vida más humana, más justa y más armoniosa con el medio ambiente, porque sin él no habrá ninguna forma de vida biológica, acaso solo las máquinas sobrevivirían, sin vida biológica ni humana no habría ni máquinas.

La humanidad está ante la disyuntiva de permitir que sean las fuerzas del mercado las determinen la dinámica económica y social, lo que significaría poner a la humanidad en la ruta de la distopía con todos los costos sociales inherentes; o bien que pugnemos por una cultura más humana donde la *ciberseguridad llevada al nivel ciberética* sea un parte fundamental en los valores sociales de toda la sociedad global; fácil no será, tampoco rápido, pero por largo que sea el camino, se inicia siempre con el primer paso, sin dejar de buscar el escalamiento hacia un mundo donde haya menos mercado, pero con más humanidad.

Referencias

[1] M. C. «academia.edu,» 27 junio 2023. [En línea]. Available: https://d1wqtxts1xzle7.cloudfront.net/64023041/castellsm-libre.pdf?1595776833=&response-content-disposition=inline%3B+filename%3DCastellsm.pdf&Expires=1687926887&Signature=TQ9Zbfq~J4Yb4YQPASTADvGVt2OTu4j-wmeC1kUSxroGTphxlilmXvlmRmTJ0gO1NTnzPRYDINxsDmAaq~n.

[2] , INEGI, «INEGI», 13 julio 2023. [En línea]. Available: https://www.inegi.org.mx/contenidos/programas/mociba/2022/doc/mociba2022_resultados.pdf.

[3] S. M. «Cybercrime Magazine,» 10 diciembre 2022. [En línea]. Available: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/.

[4] J. B. 25 junio 2023. [En línea]. Available: https://dplnews.com/ciberseguridad-problema-comun-responsabilidad-compartida-huawei/.

[5] Redacción BBC News Mundo, «bbc.com», 6 octubre 2022. [En línea]. Available: https://www.bbc.com/mundo/noticias-america-latina-63167331.

[6] R. C. «Computing» 7 febrero 2023. [En línea]. Available: https://www.computing.es/seguridad/empresas-de-ciberseguridad-cuales-son-las-mejores-y-sus-desafios/.

[7] P. I. y Y. A., «La Gestión del Conocimiento: en busca de una agenda transcultural», Psicología del trabajo y de las organizaciones, vol. 18, n.º 2-3, pp. 233-246, 2002.

[8] F. V. De la Fuente, Teoría general de la información, Madrid: Noesis, 1997.

[9] P. F. D. Post Capitalist Society, San Francisco: Butterworth, Heinermann, 1993.

[10] J. C. T. Educar en la Sociedad del Conocimiento, México: Fondo de Cultura Económica, 2010.

[11] J. M. «XATACA», 16 mayo 2023. [En línea]. Available: https://www.xataka.com/nuevo/gpt-4-que-cuando-sale-como-funciona-toda-informacion#:~:text=De%20acuerdo%20a%20la%20documentaci%C3%B3n,y%20175.000%20millones%20de%20par%C3%A1metros.

[12] M. G. «bsbusiness.school», 5 marzo 2023. [En línea]. Available: https://www.obsbusiness.school/blog/que-es-la-inteligencia-artificial-generativa.

[13] S. R. Vargas, «Voz de América», 16 mayo 2023. [En línea]. Available: https://www.vozdeamerica.com/a/miedo-ejecutivo-chatgpt-inteligencia-artificial-congreso/7096013.html.

[14] M. C. «McKinsey & Company,» 19 enero 2023. [En línea]. Available: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai.

[15] Y. N. Harari, Homo Deus: Breve Historia del mañana, México: Debate, 2017.

[16] M. A. Q. Tecnología:un enfoque filosófico y otros ensayos de Filosofía de la tecnología, México: Fondo de Cultura Económica , 2017.

[17] D. «Domo.com,» 25 junio 2023. [En línea]. Available: https://www.domo.com/data-never-sleeps.

[18] Garc, Garc y A. A. García. [En línea].

[19] A. A. García, Ciberseguridad, ¿por qué es importante para todos?, México: Siglo XXI, 2019.

[20] World Economic Forum, «Global Cibersecurity Outlook 2022», World Economic Forum, Génova, 2022.

[21] J. D. G. F. M. P. y C. M. Ng, «GP.Bullhound», 15 julio 2023. [En línea]. Available: https://insights.gpbullhound.com/report/ai-investing-during-a-technological-revolution/1-introduction.

[22] OMPI, Informe Mundial sobre la Propiedad Intelectual 2019: La geografía de la Innovación, núcleos locales, redes mundiales, Suiza: OMPI, 2019.

[23] J. N. «IPWatchdog/,» noviembre 2019. [En línea]. Available: https://ipwatchdog.com/author/james-nurton/?view-all=1.

[24] Stanford University, Human Centered AI, «Artificial Intelligence Index Report 2023», HAI Stanford University, Human-Centered Artificial Intelligence, EE. UU., 2023.

[25] D. K. «SLASHNEXT», 13 julio 2023. [En línea]. Available: https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/?utm_source=ai-news.talent-academy.com&utm_medium=newsletter&utm_campaign=wormgpt-la-ia-al-servicio-del-mal.

[26] , ESET Digital security, «Cibersecurity Trends 2023, Securing our hybrid lives,» ESET, México, 2023.

[27] M. H. Armenta, «Forbes.com,» 5 marzo 2020. [En línea]. Available: https://www.forbes.com.mx/radiografia-cuales-son-los-paises-mas-ciberseguros-del-mundo/.

[28] S. D. «dplnews,» 21 julio 2023. [En línea]. Available: https://dplnews.com/colombia-presenta-los-primeros-puntos-de-su-estrategia-de-seguridad-digital/.

[29] G. M. «Contralinea», 18 septiembre 2016. [En línea]. Available: http://www.contralinea.com.mx/archivo-revista/index.php/2016/09/18/mexico-indefenso-ante-ciberataques/.

[30] A. A. García, «cesnav.uninav.edu.mx», 5 septiembre 2018. [En línea]. Available: https://cesnav.uninav.edu.mx/cesnav/ININVESTAM/docs/docs_analisis/da_48-18.pdf.

[31] L. C. «Venturebeat,» 16 febrero 2023. [En línea]. Available: https://venturebeat.com/security/ransomware-attackers-finding-new-ways-to-weaponize-old-

vulnerabilities/?mkt_tok=NjczLVBISy05NDgAAAGKDopDT8TXBE2wk741ITjCOFIajpOWx728KY9l-Y18nOyRpts1pZTx86FOwm3t8de-mKFq6gWsUzws4rWwaY6VO7nB_yA2MgX4dVZEhdg.

[32] I. C. «News America Digital,» 14 julio 2023. [En línea]. Available: https://news.america-digital.com/identidad-digital-en-la-era-de-la-disrupcion-como-las-industrias-se-adaptan-al-cambio/.

[33] LAC BLOG, «LAC BLOG», 24 enero 2023. [En línea]. Available: https://blog-es.lac.tdsynnex.com/cual-es-la-importancia-de-la-gestion-de-riesgos-de-ti?utm_id=abril-2023&utm_campaign=newsletter&utm_medium=email&_hsmi=254808047&_hsenc=p2anqtz--hw0pirbo3szhjkloc2x6xe3qouqdrhoh9j3tczm0u5xk30vrmp8vzvtmierc19hykhwlfdpbm715f.

[34] , ESET, Digital Security Progress. Protected, «eset-la,» 15 julio 2023. [En línea]. Available: https://www.eset-la.com/Public_files/ESET_contingency_plan_Handbook_master_2022-ESP.pdf?utm_campaign=latam-es-online-contingencyplan_smb-b2b&utm_medium=email&utm_source=Eloqua&elqTrackId=303a626a4e524d19be76df31a4700e1d&elq=c0037cfc44204160a3aa31d7f5b4a4d.

[35] M. M. y V. S. , «weforum.org,» 14 abril 2023. [En línea]. Available: https://www.weforum.org/agenda/2023/04/the-quantum-security-era-is-coming-here-s-how-leaders-can-reap-its-benefits/?utm_source=sfmc&utm_medium=email&utm_campaign=2800864_WeeklyAgenda21April2023&utm_term=&emailType=Agenda%20Weekly.

[36] J. R. Muñoz, «Dilemata Revista,» 3 mayo 2017. [En línea]. Available: https://www.dilemata.net/revista/index.php/dilemata/article/view/412000100/490.

[37] S. B. Pérez , «Situaciones de riesgo moral e incentivos desalineados en ciberseguridad», Revista Chilena de Derecho y Tecnología, pp. 103-120, 2022.

[38] J. V. «Cibersecurity and Moral Hazard», Stanford Technology Law review, pp. 71-113, 2020.

[39] J. M. Caldentey, B. S. Urquijo y M. G. Almazor, «Formación y Conciliación en Ciberseguridad basada en competencias: una revisión sistemática de literatura», PIXEL-BIT, pp. 197-225, 2022.

[40] T. H. D. y L. P. , Working Knowledge: How organisations manage what they know, Boston: Harvard University Press , 1998.

[41] T. «Medium», 5 julio 2023. [En línea]. Available: https://medium.com/predict/llms-do-mass-shootings-necessitate-ai-regulation-36065bb0bd9f.

[42] U. «UNESDOC Biblioteca Digital», 23 noviembre 2021. [En línea]. Available: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa.

[43] M. S. «medium.com,» 6 julio 2023. [En línea]. Available: https://medium.com/predict/biologic-or-by-ole-logic-cc4e0deb7ea7.

[44] S. F. «Weforum Agenda,» 30 junio 2023. [En línea]. Available: https://www.weforum.org/agenda/2023/06/european-union-ai-act-explained/?utm_source=sfmc&utm_medium=email&utm_campaign=2798611_WeeklyAgenda31March2023&utm_term=&emailType=Agenda%20Weekly.

[45] , Ministerio de Asuntos Económicos y Transform Digit, «Portal Mineco», 9 noviembre 2020. [En línea]. Available: https://portal.mineco.gob.es/es-es/ministerio/areas-prioritarias/Paginas/inteligencia-artificial.aspx.

[46] C. A. Calderón, «ocausal.es», 5 mayo 2023. [En línea]. Available: https://www.ocausal.es/wp-content/uploads/2023/07/Informe_IA_Spain_2023.pdf.

[47] F. G. M. d. B. «Estudios Filosóficos», 19 agosto 2022. [En línea]. Available: https://estudiosfilosoficos.dominicos.org/ojs/article/view/1212.

[48] E. E. Picasso y A. L. E. Cosme, «www.medigraphic.org.mx,» mayo-junio 2010. [En línea]. Available: https://www.scielo.org.mx/pdf/bmim/v67n3/v67n3a3.pdf.

[49] M. P. La ética a través de su historia, México: Instituto de Investigaciones Filosóficas, UNAM , 1988.

[50] J. R. A Theory of Justice, Cambridge: Harvard University Press , 1971.

[51] J. H. Conciencia Moral y Acción Comunicativa, Madrid: Trotta, 2008.

[52] J. R. Muñoz, «Dilemata.net,» 3 mayo 2017. [En línea]. Available: https://www.dilemata.net/revista/index.php/dilemata/article/view/412000100/490.

[53] J. R. Muñoz, «Dilemata.net,» 3 mayo 2017. [En línea]. Available: https://www.dilemata.net/revista/index.php/dilemata/article/view/412000100/490.

[54] D. G. «madri+d / Fundación Bankinter,» 7 julio 2023. [En línea]. Available: https://www.madrimasd.org/notiweb/noticias/futuro-inteligencia-artificial-cuantica-fotonica-neuromorfica?utm_campaign=notiweb-19072023&utm_medium=email&utm_source=mail-marketing#utm_source=notiweb_newsletter&utm_medium=email&utm_campaign=noti3_19jul23.

[55] M. B. El Metaverso y como revolucionará todo, Barcelona: Paidos, 2022.

[56] , ESET, «Security Report Latinoamérica 2022,» ESET Progress Protected, 2022.

[57] P. a. W. b. «Pandasecurity,» 15 julio 2023. [En línea]. Available: https://www.pandasecurity.com/es/security-info/exploit/.

La ciberseguridad
en el mundo contemporáneo,
se diseñó en formato electrónico en la
Imprenta Universitaria de la Universidad Autónoma
del Estado de Hidalgo, en el mes de agosto de 2024.
Cuidado editorial: Joselito Medina Marín.