Universidad Michoacana de San Nicolás de Hidalgo

Instituto de Investigaciones Económicas y Empresariales

Doctorado en Políticas Públicas

T E S I S

Principales factores determinantes de la ciberseguridad en el estado de Michoacán en el año 2023.

QUE PARA OBTENER EL GRADO DE DOCTORA EN POLÍTICAS PÚBLICAS, PRESENTA:

M.S.I. Cecilia Patricia Navarrete Soriano

DIRECTOR DE TESIS

Dr. Mario Gómez Aguirre

Morelia, Michoacán a mayo del 2024.

UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO
INSTITUTO DE INVESTIGACIONES ECONÓMICAS Y EMPRESARIALES
DOCTORADO EN POLÍTICAS PÚBLICAS

ACTA DE REVISIÓN DE TESIS

En la ciudad de Morelia, Michoacán, el día 19 de abril del 2024, los miembros de la mesa de sinodales designada por el H. Consejo Técnico del Instituto de Investigaciones Económicas y Empresariales de la Universidad Michoacana de San Nicolás de Hidalgo, aprobaron para presentar en examen de grado la tesis titulada:

Principales factores determinantes de la ciberseguridad en el estado de Michoacán en el año 2023.

Presentada por la alumna:

Cecilia Patricia Navarrete Soriano

Aspirante al grado de **Doctora en Políticas Públicas.** Después de haber efectuado las revisiones necesarias, los miembros de la mesa de sinodales manifestaron SU APROBACIÓN DE LA TESIS en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

MESA DE SINODALES

Director de la tesis

Dr. Mario Gómez Aguirre

Secretario

Dr. Jerjes Izcoatl Aguirre Ochoa

Primer vocal

Dr. José César Lenin Navarro Chávez

Segundo vocal

Dra. Odette Virginia Delfín Ortega

Tercer vocal

Dr. Felix Chamú Nicanor

UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO
INSTITUTO DE INVESTIGACIONES ECONÓMICAS Y EMPRESARIALES
DOCTORADO EN POLÍTICAS PÚBLICAS

CARTA DE CESIÓN DE DERECHOS

En la ciudad de Morelia, Michoacán, el 17 de abril de 2024, la que suscribe, Cecilia Patricia Navarrete Soriano alumna del programa de Doctorado en Políticas Públicas del Instituto de Investigaciones Económicas y Empresariales de la Universidad Michoacana de San Nicolás de Hidalgo, manifiesto ser la autora intelectual del presente trabajo de tesis desarrollado bajo la dirección del Dr. Mario Gómez Aguirre y cedo los derechos del trabajo titulado: Principales factores determinantes de la ciberseguridad en el estado de Michoacán en el año 2023, a la Universidad Michoacana de San Nicolás de Hidalgo para su difusión con fines estrictamente académicos.

No está permitida la reproducción total o parcial de este trabajo de tesis, ni su tratamiento o transmisión por cualquier medio sin la autorización escrita de la autora y/o del director del mismo. Cualquier uso académico que se haga de este trabajo deberá realizarse conforme las prácticas legales establecidas para este fin.

Cecilia Patricia Navarrete Soriano

DEDICATORIA

A mi familia

Quiero dirigir unas palabras especiales a mi hija Zury; aunque aún eres pequeña, has sido mi mayor motivación y fuerza durante este camino. Este logro es para ti, para que siempre estés orgullosa de tu mamá y para que sepas que con dedicación y esfuerzo, puedes alcanzar grandes metas. Tu amor y presencia han sido mi inspiración y estoy agradecida por ser testigo de tu crecimiento. Te amo profundamente y espero que este logro te inspire a ser un gran ser humano y logres tus metas. A ti madre por tu amor incondicional, paciencia y apoyo inquebrantable que fueron mi mayor fortaleza a lo largo de este viaje académico.

A mi amigo

Un agradecimiento especial al Mtro. Josué Tonathiú López Díaz, quien ha sido mi compañero y amigo desde el inicio de esta aventura académica. Su apoyo, enseñanza y paciencia han sido invaluables a lo largo de este recorrido. Su amistad y colaboración han enriquecido mi experiencia doctoral y estoy profundamente agradecida por su constante apoyo y motivación.

A mis compañeros

Por compartir tiempo y experiencias académicas con ustedes, lo cual ha sido enriquecedor y fundamental para mi crecimiento. El apoyo mutuo, intercambio de ideas y colaboración han contribuido significativamente a mi desarrollo académico y personal.

AGRADECIMIENTOS

Agradezco sinceramente a mi Director de tesis el Dr. Mario Gómez Aguirre, por su inestimable orientación, apoyo y dedicación durante el desarrollo de esta tesis doctoral. Su sabiduría y asesoramiento han sido fundamentales para alcanzar este logro académico.

A mis sinodales, Dr. Jerjes Izcoatl Aguirre Ochoa, Dr. José César Lenin Navarro Chávez, Dra. Odette Virginia Delfín Ortega y Dr. Felix Chamú Nicanor, por su valioso tiempo, conocimientos y contribuciones críticas que enriquecieron mi investigación académica.

Mi agradecimiento al Consejo Nacional de Ciencia y Tecnología (Conacyt) por brindarme la invaluable oportunidad de cursar un doctorado de alta calidad y por el apoyo continúo a través de la beca que hizo posible mi desarrollo académico y profesional. Su compromiso con la formación de investigadores ha sido fundamental en mi trayectoria.

Quiero expresar mi profundo agradecimiento a la Universidad Michoacana de San Nicolás de Hidalgo por brindarme la oportunidad de cursar este doctorado de alta calidad. Estoy muy orgullosa de formar parte de esta gran comunidad académica. Las puertas que se me abrieron y el apoyo recibido por parte del Instituto de Investigaciones Económicas y Empresariales han sido fundamentales para mi crecimiento académico y personal. Estoy agradecida por la excelencia educativa que he experimentado en este Instituto y por el impacto positivo que ha tenido en mi vida: ¡Soy ININEE!

ÍNDICE GENERAL

RELACIÓN DE TABLAS

RELACIÓN DE GRÁFICOS DE CONTENIDO

RELACIÓN DE ILUSTRACIONES

RELACIÓN DE MAPAS MENTALES

RELACIÓN DE LÍNEAS DE TIEMPO

RELACIÓN DE ANEXOS

Acrónimos y abreviaturas

Abreviatura	Significado
ARPANET:	Advanced Research Projects Agency Network.
BANXICO:	Banco de México
BID:	Banco Interamericano de Desarrollo
CERT:	Equipos de Respuesta a Emergencias Informáticas
CIDGE:	Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico
CMM:	Modelo de Madurez de Capacidad de Seguridad Cibernética
CNPP:	Código Nacional de Procedimientos Penales
CONDUSEF:	Comisión Nacional para la protección y defensa de los Usuarios de Servicios Financieros
CPEM:	Código Penal del Estado de Michoacán
CPEUM:	Constitución Política de los Estados Unidos Mexicanos
DUDH:	Declaración Universal de Derechos Humanos
HTML:	Lenguaje de Marcas de Hipertexto
I + D + I:	Investigación, desarrollo e innovación
IA	Inteligencia artificial
JAVA:	Lenguaje de programación orientado a objetos
LFTR:	Ley Federal de Telecomunicaciones y Radiodifusión
LGPDPPP:	Ley Federal de Protección de Datos Personales en Posesión de los particulares.
LGPDPPSO:	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
LGSNSP:	Ley General del Sistema Nacional de Seguridad Pública
MAGERIT:	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
NIST:	Instituto Nacional de Estándares y Tecnología
OEA:	Organización de los Estados Americanos
OTAN:	Organización del Tratado del Atlántico Norte
P2P:	Peer to peer
PC:	Policía Cibernética
PLADIEM:	Plan de Desarrollo Integral del Estado de Michoacán
SGSI	Sistema de Gestión de Seguridad de la Información
SI:	Seguridad de la información
SMS:	Mensaje corto de texto
SPEI:	Sistema de pagos electrónicos interbancarios
SSL:	Secure socket layer
TIC´S:	Tecnologías de la información y comunicaciones
UNIVAC:	Universal Automatic Computer.
WEB:	World Wide Web
XSS:	Cross site scripting

Glosario de términos

Accidente: Es un evento indeseado o inesperado que ocurre rápidamente causando daños a la propiedad, a las personas, infraestructura y/o al medio ambiente (Gobierno de España, 2012).

Actividad: Conjunto de operaciones afines y coordinadas que se necesitan realizar para ejecutar los procesos administrativos (Ramírez, 2010).

Activo: Conjunto de bienes y derechos propiedades de los usuarios (Ecomipedia, 2021).

Activo de información: Toda aquella información, así como, el medio que la contiene, que por su importancia y el valor que representa para la Orgaización, deben ser protegidos para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue (Gobierno de España, 2012).

Alerta: Estado o situación de vigilancia sobre la posibilidad de ocurrencia de un evento cualquiera. Acciones específicas de respuesta frente a una emergencia (Definición.DE, 2021).

Amenaza: Cuando existe la posibilidad de que ocurra un evento físico, ya sea de origen natural, socio-natural o no intencionado por el ser humano, que podría causar daño a la población, sus bienes, la infraestructura, el medio ambiente y tanto la economía pública como la privada. (Gobierno de España, 2012).

Análisis de riesgos: Método sistemático que evalúa los riesgos, las posibles causas y factores de la amenaza, el estudio del impacto y sus consecuencias, a través de la determinación, recopilación, clasificación, evaluación, medición, calificación, priorización, control y atención, descritas e integradas en un documento que permita la toma de decisiones de manera institucional (Gobierno de España, 2012).

Anonimato: Carácter o condición de anónimo, permanecer desconocido o no identificado (Diccionario de la lengua española, 2019).

Antivirus: Son programas cuyo objetivo es detectar y eliminar virus informáticos. Con el transcurso del tiempo, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos (Incibe.es, 2020).

Antispyware: Es un tipo de software diseñado para detectar y eliminar programas maliciosos o amenazantes en un ordenador. Estos programas se llaman spyware como alusión a su tendencia a obtener y enviar información personal de un individuo a un tercero sin su consentimiento (Incibe.es, 2020).

Aplicativos: Cualquier programa de tipo informático que haga una función específica para un usuario. Por ejemplo, mensajerías instantáneas, banca en línea, juegos, entre otros (Pacheco, 2012).

Aptitud: Afinidad de las capacidades de una persona con aquellas que se requieren para el adecuado desempeño de un puesto (Ramírez, 2010).

Bit: Es la unidad mínima de información empleada en informática (Cabrera, 2010).

Bitácora de seguridad: El registro continúo de eventos e incidentes de seguridad, que ocurren a los activos de información o infraestructura tecnológica (Gobierno de España, 2012).

Buscador: Es una página web, generalmente de acceso gratuito, en la que se ofrece la obtención de información relacionada con el tema consultado. Esta información se puede consultar por, temas, categorías, imágenes, etc. (Vergara y Huidobro, 2016).

Canal de comunicación: Es el medio físico a través del cual se transmite y recibe diversa información, videos, correos electrónicos, imágenes, música, etc. (Vergara y Huidobro, 2016).

Cibercrimen: Conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la información y comunicaciones, como fin o como medio en la comisión de un delito (Callanan y Tropina, 2015).

Ciberespacio: Conjunto de dispositivos conectados a través de diferentes protocolos de comunicación de forma virtual, donde coexisten extensas cantidades de información (Callanan y Tropina, 2015).

Ciberseguridad: Conjunto de procedimientos y técnicas que permiten salvaguardar los sistemas y la información que fluye por los distintos canales de comunicación de cualquier riesgo, amenaza o ataque existente en el ciberespacio (IBM, 2021).

Ciclo de comunicaciones: Es el proceso de transmisión de una información o un hecho, en el que un determinado mensaje originado en el punto A llegue a otro punto determinado B, distante del anterior en el espacio y tiempo (Vergara y Huidobro, 2016).

Comportamiento: Acciones, actos, conductas y/o movimientos observables y/o registrables realizados por una persona (Definición.DE, 2021).

Comunidad digital: Es un conjunto de individuos que comparten elementos en común, tales como un idioma, costumbres, visión del mundo, edad, ubicación geográfica, estatus social y roles (Pierre, 2007).

Comunidades virtuales: Grupo de personas que interactúan entre sí a través de diferentes medios digitales para formar redes de relaciones personales en el ciberespacio (Pierre, 2007).

Conocimiento: Información que una persona sabe, entiende, aplica, analiza, sintetiza y/o evalúa sobre un tema, área del saber, disciplina o actividad (Definición.DE, 2021).

Confidencialidad: La cualidad por la cual la información solamente debe ser compartida con personas y procesos autorizados (ISO, 2014).

Correo electrónico: Servicio de intercambio de mensajes entre usuarios, que puede incluir texto y elementos multimedia (Vergara y Huidobro, 2016).

Criminogénesis: explica el origen del delito a través de los factores y las causas criminógenas que han dado origen a una conducta delictiva (Di Tullio 1966).

Criminodinámica; explica los pasos que se llevaron a cabo para cometer conductas delictivas (Di Tullio 1966).

Cultura de ciberseguridad: Conjunto de conocimientos, actitudes, normas y valores de las personas en relación con la ciberseguridad y cómo se manifiestan en el comportamiento de las personas con las tecnologías de la información (Pierre, 2007).

Dato: Es un valor que reciben las computadoras por diferentes medios (Cabrera, 2010).

Datos abiertos: A los datos digitales de carácter público, accesibles, reutilizables, liberados sin exigir permisos específicos (Cabrera, 2010).

Defacement: Ataque a un sitio web que se refiere a cambiar la apariencia visual de una página web, (Jara y Pacheco, 2012).

Desinformación: Acción y efecto de desinformar (Diccionario de la lengua española, 2019).

Disponibilidad: La cualidad de la información de estar disponible de forma inmediata para aquellas personas o procesos autorizados (Gobierno de España, 2012).

Ecommerce: Se refiere a la compra y venta de bienes y servicios a través del internet por medio de diferentes aplicaciones tecnológicas, principalmente por plataformas de Ecommerce, dichas plataformas permiten a empresas y consumidores interactuar y realizar transacciones en la WEB. (ARIMETRICS, 2021).

Ecosistema digital: creación del entorno digital más favorable para el desarrollo de un proyecto en Internet (Pierre, 2007).

Evento: Los eventos pueden presentarse como acciones llevadas a cabo por el usuario, como hacer clic en un botón o pulsar una tecla, o como situaciones que ocurren dentro del sistema, que permiten el registro de incidentes (Arimetrics, Agencia Digital, 2020).

Facebook: Es un sitio web formado por un conglomerado de redes sociales .La gente utiliza utilza está plataforma para mantenerse al día con sus amigos o compañeros compartiendo fotos, enlaces, vídeos, entre otros (Arimetrics, Agencia Digital, 2020)

Fake news: Son noticias, historias, artículos, engañosas, creadas para desinformar deliberadamente o engañar a los lectores (ARIMETRICS, 2021).

Firewall: Se refiere a la parte de un sistema informático o de una red que tiene la función de impedir el acceso no autorizado, permitiendo comunicaciones seguras. (Gobierno de México, 2021).

Google: Motor de búsquedas en internet (Rodríguez, 2016).

Habilidad: Destreza para realizar eficazmente una tarea o actividad física, mental y/o social (Diccionario de la lengua española, 2019).

Hardware: Componentes tangibles que trabajan o interactúan con las computadoras, permitiendo de una u otra manera su funcionamiento (Cabrera, 2010).

Hashtag: Es una etiqueta de Twitter para especificar el tipo de publicación o mensajes por temas específicos (León, 2004).

Hater: Alusión a la persona que se dedicada, a través de las redes sociales o comunidades en línea, a discriminar, denigrar u ofender a una organización, persona o producto (León, 2004).

Incidente: El evento que aunque no sea considerado anormal ni haya sido causado por fenómenos perturbadores graves, puede generar condiciones que anticipan la ocurrencia de accidentes, desastres o situaciones de emergencia (Gobierno de España, 2012).

Infraestructura: Conjunto de elementos, dotaciones o servicios necesarios para el buen funcionamiento de un país, de una ciudad o de una organización cualquiera (Diccionario de la lengua española, 2019).

Infraestructura crítica: Aquella infraestructura esencial para la prestación de bienes y servicios públicos, cuya destrucción o inutilización representa una amenaza para la seguridad nacional y puede provocar afectaciones a la población, su entorno y sus bienes (Ley General de Protección Civil, 2012).

Información: Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada (Diccionario de la lengua española, 2019).

Informática: Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automatizado de la información por medio de computadoras (Diccionario de la lengua española, 2019).

Ingeniería social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal (Hadnagy, 2011).

Inteligencia artificial: combinación de tecnologías, modelos, técnicas y algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano (decide, 2022).

IoT: Es una agrupación e interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet, la red de redes), dónde todos ellos podrían ser visibles e interaccionar (León, 2004).

Instagram: Aplicación de intercambio de fotos en línea que permite a los usuarios editar y subir fotos y vídeos cortos a través de una aplicación para dispositivos móviles (León, 2004).

Institución: Cada una de las organizaciones fundamentales de un estado, nación o sociedad (Diccionario de la lengua española, 2019).

Interacción: Proceso en el cual dos o más entidades, ya sean personas u objetos se relacionan entre si y se da una influencia mutua (Diccionario de la lengua española, 2019).

Internet: Red mundial de computadoras, cuya comunicación se realiza a través del protocolo TCP/IP (León, 2004).

Internauta: Persona que navega por internet para acceder a diferentes servicios en línea(León, 2004).

Interoperabilidad: Capacidad de sistemas, dispositivos o entidades para intercambiar y utilizar información entre si (ACUERDO por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal., 2001).

Inyección de código SQL: Ataque contra un sitio o aplicación web en el que se añade código de lenguaje de consulta estructurado (SQL) a un campo de entrada de un formulario web con el objetivo de acceder a una cuenta o modificar los datos (Incibe.es, 2020).

Like: Es una característica incorporada en redes sociales y otras plataformas online que permite al usuario dar un feedback positivo a cualquier tipo de contenido, y de esta forma conectar con aquello que les interesa (ARIMETRICS, 2021).

Lineamiento: Instrumento por el que se determinan términos, límites y características que deben observarse para actividades o procesos del sector público (Instituto Nacional de Antropología e Historia, 2015).

Malware: Software malintencionado o cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario (Incibe.es, 2020).

Messenger: Aplicación de mensajería instantánea que permite establecer comunicaciones con amigos de la red social de Facebook (ARIMETRICS, 2021).

Metodología: Conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal (Diccionario de la lengua española, 2019).

Mitigación: Es toda acción destinada a reducir, prevenir o minimizar el impacto de un riesgo o amenaza. (Gobierno de España, 2012).

Norma: Regla de conducta obligatoria que dirige la conducta o la correcta realización de una actividad (Diccionario de la lengua española, 2019).

Plan de recuperación de desastres: abarca los procesos de restauración de los datos, el hardware y el software crítico de la organización ante un desastre. Es decir, se centra en el restablecimiento de los sistemas y la infraestructura de la tecnología de la información que soportan los procesos críticos después de haber ocurrido un incidente grave (Incibe.es, 2020).

Plan de respuesta a incidentes cibernéticos: Guía para aplicar una serie de medidas en caso de una violación o una brecha de seguridad. Este plan tiene como objetivo el minimizar la cantidad y gravedad de los incidentes de ciberseguridad (Incibe.es, 2020).

Plataforma digital: sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet (Definición.DE, 2021).

Plataforma tecnológica: Es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible. Dicho sistema está definido por un estándar alrededor del cual se determina una arquitectura de hardware y una plataforma de software (Tecno Accesible, 2021).

Post: Texto escrito que se publica en Internet, en espacios como foros, blogs o redes sociales (LEXICO, 2021).

Prevención: Conjunto de acciones preventivas diseñadas para prevenir y mitigar el impacto de eventos disruptivos (Reglamento de la Ley General de Protección Civil, 2015).

Preservación: Proceso de proteger y mantener intactos todos los elementos probatorios relacionados con un incidente. (Reglamento de la Ley General de Protección Civil, 2015).

Proceso: Conjunto de actividades que transforman o convierten uno o más insumos en productos o resultados, que proporcionan un valor a quien los usa, aplica o demanda (Definición.DE, 2021).

Proteger: Es la acción de resguardar en un lugar a las personas y sus bienes con guardias, barreras físicas y electrónicas, a fin de prevenir, disuadir y reaccionar, para reducir su vulnerabilidad ante los riesgos a los que están expuestos probatorios (Reglamento de la Ley General de Protección Civil, 2015).

Política: Directriz general o principio rector para la conducción de la gestión administrativa en direcciones específicas, que implica el proceso de toma de decisiones y la ejecución de objetivos específicos a nivel institucional (INAH, 2015).

Proyecto: Conjunto de actividades que conforman una unidad de propósitos para el logro de un objetivo que no pueden plantearse de forma aislada (Luna, 2014).

Ransomware: Secuestro de datos, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción (Incibe.es, 2020).

Reacción: Forma en que alguien o algo se comporta ante un determinado estímulo (Definición.DE, 2021).

Recolección: Acción de levantar los indicios o elementos materiales probatorios, mediante métodos y técnicas que garanticen su integridad (ACUERDO A/009/15 , 2015).

Redes Sociales: Sitio de Internet que favorece la creación de comunidades virtuales. Estos sitios web son servicios que permiten desarrollar redes según los intereses de los usuarios, compartiendo fotografías, videos e información en general (Desmurget, 2020).

Reducción de Riesgos: Intervención preventiva de individuos, instituciones y comunidades que nos permite eliminar o reducir, mediante acciones de preparación y mitigación, el impacto adverso de los desastres (ACUERDO A/009/15 , 2015).

Resiliencia: Es la capacidad de un sistema, comunidad o sociedad potencialmente expuesta a un peligro para resistir, asimilar, adaptarse y recuperarse de sus efectos en un corto plazo y de manera eficiente, a través de la preservación y restauración de sus estructuras básicas y funcionales, logrando una mejor protección futura y mejorando las medidas de reducción de riesgos (Resiliencia Sísmica, 2021).

Retos sociales: Objetivo es realizar diversas actividades que se difundes a través de redes sociales, algunos con el objetivo de promover comportamientos dañinos (Desmurget, 2020).

Responsabilidad: Asignación de una tarea a una persona o Unidad Administrativa que debe realizar (ACUERDO A/009/15 , 2015).

Riesgo: Probabilidad de que se presente un acontecimiento o escenario que pueda tener un impacto negativo en personas o activos (Reglamento de la Ley General de Protección Civil, 2015).

Salas de Chat: Servicio que permite mantener conversaciones mediante mensajería instantánea (Desmurget, 2020).

Seguridad: Es el conjunto de elementos humanos, técnicos y normativos, desplegados de acuerdo con un plan operativo de prevención, disuasión y reacción ante actos y condiciones que puedan generar daño en las personas y sus bienes; proporciona tranquilidad y confianza. Acciones encaminadas a mantener los riesgos en un nivel aceptable (Reglamento de la Ley General de Protección Civil, 2015).

Seguridad de la información: Capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y el no repudio de la misma (Ellis y Mohan, 2019).

Sexting: Es un anglicismo de nuevo cuño (contracción de los términos ingleses "sex" y "texting") que se refiere al envío de contenidos eróticos o pornográficos por medio de teléfonos móviles. Comenzó haciendo referencia al envío de SMS de naturaleza sexual. Es una práctica común entre jóvenes, y cada vez más entre adolescentes (e-legales, 2016).

Sextorsión: Es la amenaza de enviar o publicar imágenes o videos con contenido sexual de una persona. Esto puede hacerse a través de teléfonos celulares o Internet (e-legales, 2016).

Sistema Operativo: Es el conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes (Beekman, 2005).

Software: Soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware (Beekman, 2005).

Snapchat: Aplicación móvil que permite a los usuarios enviar y recibir fotos y vídeos efímeros, que desaparecen poco después de haber sido publicados (ARIMETRICS, 2021).

Spyware: También denominado spybot, es un programa malicioso espía. Se trata de un malware, un tipo de software utilizado para recopilar información de un ordenador o dispositivo informático y transmitir la información a una entidad externa sin el permiso del dueño del ordenador (Incibe.es, 2020).

Suplantación de identidad: Expresión informática que se emplea para referirnos a los abusos informáticos cometidos por delincuentes para estafar, obtener información personal, contraseñas, etc (Incibe.es, 2020).

Telegram: Plataforma de mensajería y VOIP, enfocada en la mensajería instantánea, el envío de varios archivos y la comunicación en masa (ARIMETRICS, 2021).

TIC´s: Tecnologías de la información y comunicaciones; conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Beekman, 2005).

TikTok: Aplicación para compartir vídeos de corta duración muy famosa entre adolescentes de todo el mundo (ARIMETRICS, 2021).

Twitter: Es una red de información de tiempo real que permite conectarse y buscar información de interés como: frases, noticias, vínculos en Internet y en general la vida de las personas (ARIMETRICS, 2021).

Variable latente: Son conocidas como variables no manifiestas, también conocidos como constructos, so variables que se deducen a partir de observaciones y no se pueden medir de forma inmediata (Hair, et al., 2017).

Variable observada: Son las variables que se pueden medir de forma explícita, también conocida como variables como variables indicativas (Hair, et al., 2017).

Videoconferencia: Encuentro a través de una red de telecomunicaciones, frecuentemente convocado con anterioridad, que permite a varios interlocutores verse, oírse y compartir información (Definición.DE, 2021).

Videojuegos: Dispositivo electrónico que permite, mediante mandos apropiados, simular juegos en las pantallas de un televisor, una computadora u otro dispositivo electrónico (Definición.DE, 2021).

Virtual: Ubicado o tiene lugar en línea, generalmente a través de internet (Definición.DE, 2021).

Virus: Es un software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo (Beekman, 2005).

Vulnerabilidad: Debilidad de un sistema, persona o entidad frente a las amenazas, daños y riesgos presentes (Gobierno de España, 2012).

Web: Sistema de organización de la información de Internet a través de enlaces de hipertexto. En sentido estricto es el conjunto de servidores que emplean el protocolo HTTP (Beekman, 2005).

Web Spoofing: consiste en la suplantación de una página web real por otra falsa con el fin de realizar una acción fraudulenta. La web falsa adopta el diseño de la web que se pretende suplantar e incluso una URL similar. Un tipo de ataque más sofisticado consiste en crear una "copia sombra" de toda la World Wide Web para conseguir que el tráfico de la víctima pase por el atacante, de esta manera se obtiene toda la información sensible de la víctima (Incibe.es, 2020).

WhatsApp: Aplicación o software de mensajería instantánea para teléfonos inteligentes (Smartphone).Además del envío de texto, permite la transmisión de imágenes, video y audio (Incibe.es, 2020).

YouTube: Sitio web en el cual los usuarios pueden subir y compartir vídeos. Es muy popular gracias a la posibilidad de alojar vídeos personales de manera sencilla. Aloja una variedad de clips de películas, programas de televisión y vídeos musicales, así como contenidos amateur como video blogs (Incibe.es, 2020).

RESUMEN

El aumento en el uso de las tecnologías de la información y las comunicaciones (TIC´s) hace que la ciberseguridad sea un factor crítico y determinante para garantizar la confidencialidad, integridad y disponibilidad de las ingentes cantidades de información que circula en los diferentes canales de comunicación, así como proteger la privacidad, seguridad y protección del patrimonio de los usuarios. Internet se ha convertido en el epicentro de una amplia gama de actividades vitales y rutinarias. Su enlace global y accesibilidad ha permitido que actividades esenciales y cotidianas se realicen a través de este medio. Entre ellas, se encuentran la gestión de servicios gubernamentales, la comunicación vía correo electrónico, las transacciones financieras, el comercio electrónico y las dinámicas interacciones en las diferentes plataformas sociales. La presente investigación tiene el objetivo de diagnosticar de qué manera las Tecnologías de la información y comunicaciones; Aspectos legales; Cibercultura; Cibercrimen; Infraestructuras críticas; y Seguridad de la información, explican la Ciberseguridad en el Estado de Michoacán. Lo anterior se comprueba a partir de un modelo de ecuaciones estructurales de mínimos cuadrados parciales (SEM-PLS), cuyos resultados permiten proponer las directrices de la Política Pública de Ciberseguridad en el estado A partir de los resultados de la modelización se concluye que las variables cibercrimen y seguridad de la información son de gran relevancia para comprender y explicar la situación de ciberseguridad que guarda el estado. Por lo cual, la inclusión del combate al cibercrimen y la promoción de la seguridad de la información en una política pública de ciberseguridad contribuirán a prevenir los delitos cibernéticos, proteger datos confidenciales y robustecer la seguridad, dicha política fortalecerá la resiliencia del estado frente a amenazas cibernéticas y promoverá la confianza en las actividades en línea, respaldando el desarrollo económico y la innovación tecnológica en Michoacán.

Palabras clave: Ciberseguridad, tecnologías de la información y comunicaciones, aspectos legales, cibercultura, cibercrimen, infraestructuras críticas y seguridad de la información.

ABSTRACT

The increase in the use of information and communications technologies (ICTs) makes cybersecurity a critical and determining factor to guarantee the confidentiality, integrity and availability of the enormous amounts of information that circulates in the different communication channels. communication, as well as protecting the privacy, security and protection of users' assets. The Internet has become the epicenter of a wide range of vital and routine activities. Its global link and accessibility has allowed essential and daily activities to be carried out through this medium. Among them are the management of government services, communication via email, financial transactions, electronic commerce and dynamic interactions on different social platforms. This research has the objective of diagnosing how information and communications technologies; Legal aspects; Cyberculture; Cybercrime; Critical infrastructures; and Information Security, explain Cybersecurity in the State of Michoacán. The above is verified from a structural equation model of partial least squares (SEM-PLS), whose results allow us to propose the guidelines of the Public Cybersecurity Policy in the state. From the results of the modeling it is concluded that the variables Cybercrime and information security are of great relevance to understand and explain the state's cybersecurity situation. Therefore, the inclusion of the fight against cybercrime and the promotion of information security in a public cybersecurity policy will contribute to preventing cybercrimes, protecting confidential data and strengthening security. This policy will strengthen the resilience of the state against threats. cyber and will promote confidence in online activities, supporting economic development and technological innovation in Michoacán.

Keywords: Cybersecurity, information and communication technologies, legal aspects, cyberculture, cybercrime, critical infrastructures and information security.

INTRODUCCIÓN

¿Te has imaginado despertar un día solo para descubrir que el suministro eléctrico ha sido interrumpido no por una falla común, sino por un ciberataque devastador? En un mundo donde la tecnología nos conecta en tiempo real, un escenario así parece sacado de una película de ciencia ficción. Sin embargo, en esta nueva era digital, los ataques cibernéticos se han convertido en amenazas tangibles que pueden paralizar sistemas críticos en un instante. Imagina estar en ese momento, con la batería de tu celular agotándose y las noticias anunciando que un ciberataque ha dejado al estado de Michoacán sin suministro eléctrico. Esta no es solo una ficción, sino una posibilidad real. ¿Y si no hubiera un equipo capacitado para enfrentar tal ataque?

La interconexión global nos ha traído avances impresionantes, pero también nos ha dejado vulnerables. La ciberseguridad ya no es solo una opción, es una necesidad urgente (Deutsch, 2022). En esta investigación, se exploran las complejas intersecciones entre desafíos y soluciones en el campo de la ciberseguridad. Desde el surgimiento de las tecnologías de la información y las comunicaciones, nuestras vidas han experimentado una transformación sin precedentes, pero esta revolución digital también ha dado paso a un nuevo tipo de riesgos y amenazas. El objetivo es desentrañar cómo estas tecnologías enriquecen la vida de los usuarios, pueden también convertirse en instrumentos de caos cuando no se implementan las medidas de seguridad adecuadas.

La conectividad que permite el internet y de la cual dependen muchas de las actividades cotidianas, como pueden ser; comunicación, consulta de información, redes sociales, entretenimiento, aprendizaje y educación, banca en línea, noticas, salud, comercio electrónico, entre otras actividades que de realizarlas sin las medidas de seguridad adecuadas pueden convertirse en un riesgo que podría desencadenar en accidentes de seguridad con consecuencias perjudiciales para el patrimonio de los usuarios. Estas amenazas incluyen la posibilidad de fraudes, estafas, suplantación de identidad, ataques a la intimidad, robo de información, phishing, acoso en línea, compras fraudulentas promovidas por publicidad engañosa por lo cual resulta indispensable identificar los riesgos asociados al uso de las tecnologías de la información y la comunicación (TIC´s) en esta nueva era digital. El desconocimiento acerca de estas amenazas ha permitido que se generan diversas conductas de peligro que han dado origen a una forma nueva de criminalidad en el ciberespacio (Steinberg, 2019).

Durante la década de los 90´s y con el surgimiento de las TIC´s, marco un punto de inflexión significativo que estableció las bases para una evolución acelerada. La necesidad de comunicación, en un inicio comenzó con el uso del telégrafo en el año 1830 como medio de comunicación a larga distancia, ya que permitía enviar mensajes de texto en cuestión de minutos, se utilizaba el código

morse para interpretar los mensajes. En 1969 los Estados Unidos de América crearon la Agencia de Proyectos de Investigación Avanzada (ARPA), con el objetivo inicial de desarrollar comunicaciones seguras e intercambio de información entre ordenadores en caso de ataques nucleares. Aunque esta iniciativa no se utilizó para tal fin, está red llego a contar, para el año de 1971, ya contaba con 23 puntos interconectados para facilitar el intercambio de información, Esta necesidad de comunicaciones seguras sentó las bases para el surgimiento de internet en la década de 1970. En los primero años de la década de 1980, el crecimiento exponencial de las computadoras y su disponibilidad masiva han convertido al internet en una herramienta indispensable en la vida cotidiana de la humanidad (De Leeuw y Bergstra, 2007).

En el contexto anterior, la evolución y el crecimiento exponencial de las computadoras en la década de 1980 han dado lugar a la generación de diversos proyectos indispensables en las actividades humanas. Sin embargo, no se pensó en la seguridad de las grandes cantidades de información que ahora coexisten en el ciberespacio y que están circulando por diferentes enlaces de comunicación a nivel mundial, ya que originalmente se centraba en la conectividad y el intercambio de información, sin considerar completamente los riesgos de seguridad asociados.

Considerando este escenario escuchamos actualmente conceptos como; redes sociales, internet, fake news, fanpage, ciberespacio, cloud computing, big data, dark web, virus, troyanos, grooming, sexting, ataques de denegación de servicios, inyección de código SQL, rootkit, internet de las cosas, inteligencia artificial, blockchain, transferencias no autorizadas de activos, robo de datos entre otros (Sanz y Fernandez, 2021). Muchos de estos conceptos son desconocidos por la sociedad, sin saber que existen y que algunos de ellos son amenazas constantes a la seguridad, en el uso de las tecnologías de información y comunicación en el ciberespacio, por lo tanto esto es un problema no solo de las empresas, del Gobierno o de los usuarios, es un problema a nivel mundial. ¿Cuántas veces hemos escuchado a alguien decir que su información ha sido robada? ¡Que dio clic en un enlace! y ¡cuando se percata su cuenta bancaria ha sido afectada en detrimento de su patrimonio económico! Asimismo, los ataques por virus a equipos de cómputo, servidores, la suplantación o el robo de identidad, bases de datos sustraídas, comprometiendo con esto la privacidad y la información de millones de personas, por mencionar algunos casos.

Derivado de lo anterior es importante destacar que con la aparición de las primeras redes de computadoras los ataques fueron apareciendo y con el paso del tiempo se han ido sofisticando y muchos de estos enfocados en vulnerar sistemas específicos o infraestructuras críticas, algunos sin dejar rastro debido a su especialización y la falta de legislación que no permiten su sanción, facilitando con ello la comisión de delitos a través de las tecnologías de la información (Schneier,

2019). El estado de Michoacán debe reconocer la importancia de la ciberseguridad, con el fin de garantizar y salvaguardar la integridad, derechos de la sociedad, la protección a sus infraestructuras críticas y los servicios públicos, como lo hace a través de las leyes generales que regulan la conducta humana, de lo contrario, seguirá siendo blanco vulnerable que afectan no solo a una parte de la población, sino como ya se dijo ponen en riesgo la seguridad del estado (La Voz de Michoacán, 2021).

Aunado a lo anterior el estado busca a través de las leyes la regulación de las conductas humanas y de convivencia social en un determinado territorio que se encuentra delimitado geográficamente y esto hace mucho más fácil que el comportamiento individual y las relaciones sociales sean armónicas en cuanto espacio y tiempo. Pero al ser una sociedad que ha ido evolucionando tecnológicamente, las nuevas formas de interacción no se hacen esperar, lo que da como resultado una mayor complejidad para la regulación de un espacio que no se encuentra definido geográficamente y que es un mundo completamente desconocido y en donde no se puede establecer un inicio ni un fin, mucho menos comprender en dónde termina la jurisdicción mexicana y en dónde inicia la norteamericana o de cualquier otro país del mundo, lo que hace que las leyes no tengan cabida dentro de este espacio virtual conocido como ciberespacio a donde se han expandido conductas que se inician en determinado país, sin importar la distancia, afectan a países que ni siquiera son vecinos geográficamente, mucho menos se ven regulados por normas que den seguridad a la navegación de la sociedad Michoacana y que rijan el ciberespacio en donde la territorialidad no se hace presente (Gutiérrez, 2021).

El nacimiento del ciberespacio dio origen a un conjunto de ecosistemas digitales que envuelven a la sociedad y a los usos que se encuentran en este espacio inmersivo. En este contexto, el número de usuarios a nivel mundial sigue en constante aumento. Sin embargo, la seguridad brindada por sistemas informáticos a nivel empresarial o nacional se ve desafiada por los riesgos inherentes a su uso, así como el establecimiento de crear una cultura digital que nos permita interaccionar en el ciberespacio, buscando ser más empáticos en la capacidad de establecer relaciones y comunicaciones. Estas interacciones han comenzado a manifestarse en cambios de conducta que afectan nuestra forma de interrelacionarnos, modificando nuestra identidad cultural como sociedad.

En este inmenso espacio surge la necesidad de establecer acuerdos, para garantizar la seguridad de los usuarios de esta red mundial a través de la firma de tratados internacionales que permitan fortalecer la capacidad de enfrentar amenazas cibernéticas, así como la armonización la legislación que sea de competencia mundial, que puedan frenar los ataques que se avecinan de lo que podría considerarse la próxima guerra a través de instrumentos tecnológicos poniendo en peligro incluso a naciones enteras (Steinberg, 2019).

El uso desmedido y sin control de las tecnologías de la información es cada vez más preocupante, asimismo la falta de una cultura de la ciberseguridad hace que las interacciones en el ciberespacio sean hostiles, originando con esto conductas de riesgo que trascienden las fronteras digitales a lo físico y que afectan a los individuos en su plano existencial, por lo cual resulta necesario establecer mecanismos que identifiquen, analicen las conductas de riesgo, con el fin de promover, fomentar y concientizar la importancia de una cultura ética digital a través del fortalecimiento de la educación en valores en las interacciones en el ciberespacio (Goodman, 2016).

La evolución que han tenido las tecnologías de la información ha sido significativa y con apego a la sociedad, por lo cual ha modificado su forma de vivir, de todas aquellas que están inmersas e incluso de las que no lo están, modificando espacios de interacción social, espacios de convivencia a través de foros que buscan cubrir todo tipo de "necesidades", hasta desalojar la verdadera interacción social por la "interacción social virtual", lo que trae como consecuencia múltiples problemas como lo pueden ser; adicción, aislamiento, trastornos de conducta, bajo rendimiento que afectan la calidad de vida de la sociedad. De lo anterior se desprende la necesidad de crear programas que promuevan el uso responsable de las TIC's (Echeburúa y Requesens, 2012).

Actualmente en el Estado de Michoacán no existe una política pública de ciberseguridad que sirva como un instrumento de investigación y concientización para la sociedad a partir del reconocimiento de la importancia de las tecnologías de la información como factor determinante en la vida social, que se encargue de regular las conductas y sancionar los delitos que se cometen en el ciberespacio.

Aunado a lo anterior existe un gran desconocimiento sobre el tema para crear e implementar políticas que ayuden a enfrentar este tipo de amenazas, por lo que la mayoría de ellos se quedan sin resolver y la impunidad día a día crece, teniendo cada vez ataques más coordinados, sofisticados y complejos, sin la posibilidad de ser detectados, debido a la falta de mecanismos tecnológicos, políticas y legislación que permitan al Gobierno de Michoacán actuar de manera eficiente ante esta problemática. Tomando como experiencia que en agosto del año 2022, se produjo un incidente de seguridad en el ayuntamiento de Morelia, donde se llevó a cabo la explotación de una vulnerabilidad que encriptó todos los datos almacenados en sus servidores informáticos. Como consecuencia de esto, se exigió un rescate en forma de Bitcoins. Los servidores y sistemas fueron infectados con el ransomware K2, lo que hizo inaccesible el acceso a la información. Esto destaca la urgente necesidad de fortalecer la ciberseguridad de las infraestructuras del estado contra las amenazas cibernéticas (El sol de Morelia, 2022).

El presente trabajo de investigación está dividido en siete capítulos en los cuales se ha desarrollado la problemática a explicar, así como los resultados del trabajo de campo realizado en el año 2023, por lo cual se describe de manera breve lo que se abordará en cada capítulo:

Capítulo 1. Se exponen los fundamentos de la investigación tanto teóricos como metódicos, que permiten explicar los beneficios que las tecnologías de la información y comunicaciones han traído a la sociedad a partir de su uso generalizado, no obstante como objeto de esta investigación se abordan aquellos aspectos negativos en el uso de las TIC´s tal es el caso como afecciones económicas a la organizaciones de cualquier índole, riesgos a la salud de las personas, riesgos a grupos vulnerables como son; niños, niñas y adolescentes y riesgos a las infraestructuras tecnológicas con las que se sustenta la vida política, social, económica en el Estado de Michoacán. A partir de las preguntas de investigación se plantea la necesidad de investigar si las variables definidas tienen un impacto significativo en la ciberseguridad. Estas variables, identificadas a través una revisión exhaustiva de la literatura y una comprensión profunda del tema, serán clave en el establecimiento de las directrices que debe seguir la propuesta de política pública de ciberseguridad.

Capítulo 2. Marco referencial y conceptual en él se abordan los principales conceptos que giran en torno a la ciberseguridad y de aquellas determinantes que la fortalecen o la vulneran y que son susceptibles de ser tratados como instrumento de política pública. Comenzando por la TIC´s las cuales permiten el intercambio de grandes volúmenes de información en el ciberespacio, pero así como la tecnología avanza de manera exponencial el marco jurídico debe hacerlo de la misma manera, por lo que se abordan aquellos aspectos de las TIC´s que deben ser incluidos en los marcos normativos tanto estatal como nacional ya que la ausencia de estos permite la existencia de personas que aprovechan el vacío legal y el anonimato que ofrecen las TIC´s para la comisión de delitos.

Por otra parte se resalta la importancia de la cibercultura en la interacción de los usuarios en el ciberespacio, A su vez se aborda el cibercrimen para comprender su génesis y entender porque surge, de igual manera en este apartado se plantean los aspectos teóricos sobre las infraestructuras que se consideran críticas y que son susceptibles de amenazas y que por lo tanto deben ser consideradas dentro de la política pública de ciberseguridad, adicional a esto se presenta un conjunto de conocimientos específicos en seguridad de la información que guíen y orienten el estado de la ciberseguridad y que afecta o tiene relación directa con los otros aspectos anteriormente señalados.

Capítulo 3. Hablaremos del concepto de políticas públicas y la importancia de está en la resolución de problemas sociales, la importancia de brindar al estado de Michoacán un marco de actuación que guíe y oriente las acciones que ha de tomar el Gobierno y su población para gestionar la seguridad de

la información en el uso de las tecnologías de la información y comunicaciones, así como la creación de una cultura ética digital y un entorno de navegación seguro.

Capítulo 4. Se describe el proceso metodológico utilizado para comprobar la hipótesis planteada, al ser la ciberseguridad un tema poco explorado y estudiado desde la óptica de la política pública, se definirán distintas particularidades y las variables que atienden el estudio de la ciberseguridad desde un punto de vista descriptivo, así como la causalidad entre cada una de las variables para demostrar la fortaleza de sus relaciones. Por otra parte el universo de estudio está limitado a la población del estado de Michoacán dado el incremento de delitos que se cometen por el uso de las TIC´s, es así que a través de la aplicación de un instrumento de medición a setenta y seis expertos en ciberseguridad a nivel nacional, los cuales forman parte de las diferentes Policías Cibernéticas en el territorio nacional, que dada su experiencia y contacto en la atención a la sociedad, permite obtener una visión más clara de la realidad que guarda la ciberseguridad.

Capítulo 5. Se muestran los resultados de la aplicación de la técnica de segunda generación PLS-SEM (Partial Least Squares Structural Equation Modeling) utilizada para estudios exploratorios, la cual es una herramienta estadística que permite analizar las relaciones entre variables latentes y observables en un modelo teórico. La ciberseguridad abarca múltiples dimensiones y constructos abstractos que no pueden ser medidos directamente. PLS-SEM permite modelar constructos latentes y evaluar sus relaciones con variables observables, lo que facilita el análisis de los constructos que se definieron como determinantes para la ciberseguridad, con la finalidad de generar conocimiento nuevo en este campo, al permitir un análisis flexible y comprensivo de las relaciones entre variables propuestas así, como la elaboración de conclusiones de la modelación teórica propuesta.

Capítulo 6. Finalmente se muestra la propuesta de política pública de ciberseguridad que le permitirá contar al estado de Michoacán con un instrumento que oriente los esfuerzos realizados para el diseño e implementación de acciones, leyes, programas, servicios y ejecución de recursos en materia de ciberseguridad a partir del reconocimiento de la importancia de las tecnologías de la información y comunicación como factor determinante en la vida social.

Por lo que está investigación pretende diagnosticar de qué manera las Tecnologías de la información y comunicaciones, Aspectos legales, Cibercultura, Cibercrimen, Infraestructuras críticas y Seguridad de la información explican la Ciberseguridad en el Estado de Michoacán, en el año 2023, así mismo comprobar la influencia de las variables dependientes sobre la independiente que conforman las hipótesis de esta investigación.

CAPÍTULO 1. FUNDAMENTOS DE LA INVESTIGACIÓN

Este capítulo se inicia con la exposición de la problemática central, donde se desglosan los fundamentos tanto teóricos como metodológicos de la investigación. Estos fundamentos proporcionan una mejor visión sobre los impactos beneficiosos de las tecnologías de la información y comunicación en la sociedad debido a su amplio uso. Sin embargo, el enfoque de esta investigación radica en analizar las implicaciones negativas del uso de estas tecnologías. Esto impulsa la formulación de las preguntas de investigación y la definición de objetivos específicos. Las hipótesis a comprobar se presentan junto con las variables de estudio que enmarcarán los límites de esta investigación.

La justificación que acompaña a este enfoque explica la relevancia y la imperiosa necesidad de emprender este estudio. Finalmente, se detalla el enfoque metodológico que se aplicará para asegurar la validez y confiabilidad de los hallazgos obtenidos en el transcurso de esta investigación.

1.1. Planteamiento del problema

En su conjunto el Internet ha propiciado que muchos sectores de la economía y gobiernos basen su operación en esta red. El cual millones de personas lo utilizan como parte de su modo de vida actual para la comunicación, consulta de información e incluso para realizar compra venta de artículos y operaciones financieras. La evolución de tecnologías como el Internet, ha contribuido al desarrollo de las sociedades que han sabido incorporarlas y aprovecharlas en sus actividades cotidianas; empresas, gobiernos y países enteros poseen cantidades exorbitantes de información por lo que actualmente garantizar; la integridad, disponibilidad y confidencialidad de la información se vuelve un tema fundamental en lo económico y político de las naciones (Puig, 2017).

Así mismo, con el desarrollo de las tecnologías de información y comunicación y el aumento del uso de Internet en los sectores económico, cultural, académico, recreativo y social, se generan circunstancias propicias para aquellos que buscan un beneficio personal en detrimento de otros. Las afectaciones derivadas comparten un origen y una serie de características comunes de la actividad delictiva como el bajo grado de riesgo para el delincuente y el alto grado de efectividad y gran impacto, así como la facilidad de ejecución y el anonimato (Puig, 2017).

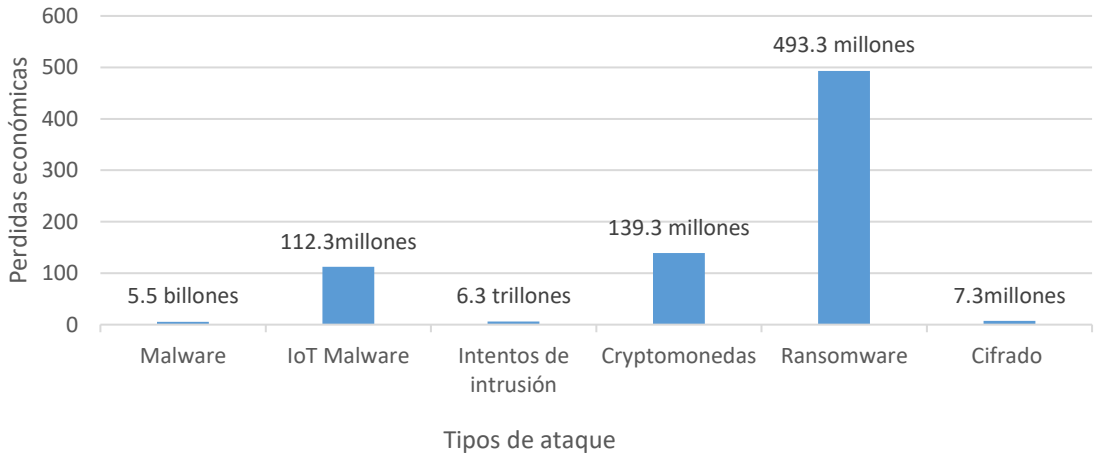
Las nuevas tecnologías y la creciente demanda del internet, resultan un campo fértil para la delincuencia, que ha encontrado nuevas formas para consumar delitos a través de medios electrónicos y tecnológicos, los cuales son aprovechados para afectar a la ciudadanía, las empresas y el gobierno. Actividades como el comercio electrónico, el periodismo digital, la publicidad y las opiniones,

mensajes o elementos vertidos en redes sociales pueden derivar en menoscabos del patrimonio, la reputación, el honor o la actividad profesional de alguien. Acciones como el acoso, el contacto en redes sociales con fines de trata de personas, los fraudes, la suplantación de identidad, la violencia digital a la intimidad sexual, entre otros son conductas nocivas que se están presentes cada vez más con mayor frecuencia. El incremento de los incidentes va en estricta relación con el incremento del número de usuarios de internet, redes sociales y medios informáticos (Callanan y Tropina, 2015).

Tecnologías de la información y de las comunicaciones

El informe de SonicWall (2022), firma estadounidense líder en ciberseguridad, destaca las tendencias de los ataques en el mundo digital. Según el informe, ha habido un aumento del 2% en los ataques de malware (5,5 billones), mientras que los ataques de malware de Internet de las cosas han advertido un aumento del 87% (112.3 millones). Por otro lado, los intentos de intrusión han incrementado en un 19% (6.3 trillones), y los ataques de criptomonedas en un 43% (139.3 millones), el ransomware presenta una tendencia a la baja en un 21% (493.3 millones), y las amenazas de cifrado en un 28% (7.3 millones), como se puede apreciar en la gráfica 1. Además, según una publicación del portal y su plataforma de monitoreo en tiempo real, Security Center, México experimentó un número récord de ataques en un solo día el 01/10/2020, con 6.14 millones de ataques maliciosos, lo que se reflejará en el próximo informe semestral (SonicWall, 2022).

Gráfica 1. Ataques maliciosos a nivel mundial, primer semestre 2022.



Fuente: Elaboración propia con base en SONICWALL (2022).

El crecimiento exponencial de las tecnologías de la información y comunicaciones ha revolucionado las formas en las que las personas interactúan y se relacionan en el ciberespacio, las cuales forman parte de la vida integral y se utilizan para una variedad de actividades cotidianas de los seres humanos, al iniciar nuestras actividades despertamos con la alarma del dispositivo móvil, revisamos mensajerías

instantáneas, nos duchamos escuchando música, mientras desayunamos revisamos el correo o el periódico digital, camino al trabajo o a otras actividades conectados por una gran infraestructura tecnológica que se desconoce que existe (estaciones base de telefonía, repetidores, routers, satélites, concesionarias de servicios de internet, entre otros) esta arquitectura en su conjunto, ofrece el acceso a internet a los usuarios en el ciberespacio y con esto que sean informados en: llamadas, mensaje de texto, correos electrónicos, notificaciones push y aplicaciones de mensajería instantánea, así, los usuarios continúan su actividad rutinaria con la dependencia de las diferentes TIC´s, revisando la banca, posteando o compartiendo información en las diferentes plataformas digitales a las que están inscritos, terminan el día abordando sus tareas pendientes. Así es como transcurre la vida diaria, impulsada por la convergencia tecnológica de está era digital. Todo esto impensable años atrás, los canales de comunicación eran más rudimentarios, así como los métodos asociados a su utilización, como lo menciona el autor Pérez (2016) el envío de cartas o pergaminos como los primeros canales de comunicación en la antigüedad y ahora lo digital, a través del correo electrónico. Continuando con los avances científicos a lo largo de los años y dada la globalización cultural y económica, la evolución de las tecnologías de la información y comunicaciones ha revolucionado a nuestra sociedad.

Derivada de la pandemia por el virus SARS-CoV-2 (COVID-19). La secretaría de Gobernación emitió el acuerdo 24/03/2020, que obligo a nivel mundial al confinamiento y distanciamiento de la sociedad, para reducir la propagación del virus (2020). Durante dicho lapso las tecnologías de la información y comunicaciones desempeñaron un papel primordial para la continuidad de las actividades cotidianas de la sociedad; el teletrabajo, enseñanza a distancia, actividades financieras, compras en línea con entregas a domicilio, consultas médicas en línea, servicios gubernamentales, entre otros. Sin embargo, junto con estos beneficios, también se incrementaron los riesgos, vulnerabilidades y desafíos relaciones con la conectividad, así como la utilización de una manera imprescindible, impulsiva y necesaria, algunos sin conocimiento de buenas prácticas, falta de concientización, desconocimiento de las tecnologías y las amenazas cibernéticas.

Derivado de lo anterior, la dependencia de la conectividad y el uso de las TIC´s, se volvió algo imperativo y necesario, La sociedad adopto su uso, sin las medidas de seguridad necesarias, quedando en un estado de vulnerabilidad, indefensión y exposición a riesgos, la cual no pasó desapercibida para los delincuentes cibernéticos quienes aprovecharon esta situación. Como resultado, hemos observado un aumento en los delitos y riesgos cibernéticos preexistentes, como el spam, la suplantación de sitios web, el robo de identidad, la ingeniería social, el fraude, llamadas de extorsión, los ataques de denegación de servicios, el malware, el ransomware, el phishing, el grooming, violencia digital a la

intimidad sexual, la pornografía infantil, la trata de personas, uso de redes inalámbricas inseguras (WIFI) entre otros (Franco, 2018).

Adicional a lo mencionado. El fácil acceso a la tecnología y la posibilidad de estar constantemente conectado han generado nuevas posibilidades para la distracción y la diversión en la interacción con el ciberespacio, fomentado con esto; descarga de videojuegos, visualización de pornografía, salas de chat, redes de búsqueda de pareja, contenido violento, retos peligrosos, generación y exposición a contenidos falsos o desinformación (fake news), falta de privacidad y seguridad en línea por mencionar algunas (Franco, 2018).

A medida que las personas pasan más tiempo en línea, surgieron una serie de problemas relacionados con la salud y el bienestar. Uno de los desafíos más notorios ha sido el aumento de las adicciones a la tecnología y las redes sociales. Muchos usuarios encontraron consuelo y distracción en línea, lo que llevó a un consumo excesivo y a la dificultad para desconectarse. Esto tuvo un impacto negativo en la calidad del sueño, salud mental, contribuyendo a problemas como la ansiedad, irritabilidad, depresión entre otros, con el riesgo de desarrollar patrones de comportamiento inusuales en menoscabo de su salud física y emocional, aislamiento de su núcleo social, adicciones, bajo rendimiento, perdida de la privacidad, adicción tecnológica, dependencia emocional de las redes sociales, entre otros problemas (Franco, 2018).

En contexto con lo anterior resulta fundamental generar mecanismos que ayuden a tomar conciencia sobre los riesgos, creando políticas y regulaciones adecuadas, procedimientos, guías de buenas prácticas y difusión, con el fin de reducir la brecha digital y lograr una sociedad más informada, conocedora y robusta en el uso del ciberespacio.

Podemos enfatizar que las TIC´s son una herramienta angular que ofrecen múltiples beneficios y oportunidades de desarrollo en las actividades diarias a la sociedad Michoacana, sin embargo existe una tecnología asociada capaz de provocar fallas, denegaciones de servicio, interrupciones en la continuidad de las operaciones, impedir el desarrollo y afectar los servicios tecnológicos anteriormente citados lo que en caso de suceder afectaría al Estado de Michoacán, poniendo en riesgo el desempeño de las actividades esenciales: actividades económicas, financieras, servicios públicos, entre otros.

Aspectos legales de la ciberseguridad

En este momento y por lo comentado en el párrafo anterior cobra relevancia la necesidad de incorporar un marco normativo que garantice el uso responsable y seguro de las TIC´s que regule la interacción de los usuarios en el ciberespacio y con esto responder a los desafíos de la digitalización,

combatir amenazas como los ciberdelitos, los ataques informáticos, el robo de datos y las actividades cotidianas de la sociedad.

Es así que entendemos por Derecho; al conjunto de normas jurídicas que regulan la conducta del individuo en sociedad, en está era digital es imprescindible contemplar aquellas conductas antijurídicas que afectan la integridad jurídica y material de los seres humanos, con el fin de garantizar los derechos de los usuarios brindando ambientes confiables y seguros en su interacción en el ciberespacio (Reyes, 2012).

En el contexto penal de la legislación mexicana, se identifican dos tipos de delitos relacionados con los equipos de cómputo. Esta situación surge debido a la versatilidad de estos dispositivos, los cuales pueden ser utilizados para facilitar la comisión de diversas actividades delictivas; los que se utilizan como instrumento o medio en la comisión del delito; modificación de datos, falsificación de documentos, fraudes en línea, hackeos, malware y donde se utilizan como el fin, cuyo objetivo es comprometer los sistemas informáticos; alterar el funcionamiento o acciones destructivas en el equipo, involucrando el uso de: virus, malware, ransomware, ataques de ingeniería social, ambos con el objetivo de causar una afectación a los usuarios de las TIC´s (Téllez, 2008).

México ha avanzado en temas de regulación en el uso de medios electrónicos, en el año 2000 las reformas realizadas al código de comercio y al código civil, fueron necesarias para impulsar la competitividad y eficiencia ante la convergencia tecnológica y la creación de nuevos modelos de negocio en la era digital, donde el objetivo es dar certeza, seguridad y confianza a los usuarios que realizan operaciones en el internet, es así que se reconoció la validez legal de la firma electrónica como un medio de autenticación y se crean reglas específicas para las transacciones comerciales, brindando un marco jurídico sólido para el comercio electrónico (Gutiérrez, 2003).

Los Estados y la Federación han legislado de manera independiente sobre estos temas, los delitos están repartidos en diferentes códigos (Estatales y el Federal), por citar un ejemplo; la revelación de secretos y la intervención de comunicaciones, su regulación es de manera distinta no se crea un capítulo especial para éste rubro cibernético, se trata de adaptar a los códigos ya existentes, así como su redacción en cada código muestra lagunas que no permiten identificar la conducta que se busca regular, creando vacíos legales esto debido a lo sofisticado de los ataques, lo complicado que es la rastreabilidad y al anonimato que ofrecen las diferentes plataformas tecnológicas, con relación a las conductas delictivas que se comenten en el ciberespacio.

En lo que respecta a legislación internacional se encuentra el convenio sobre la ciberdelincuencia conocido como el convenio de Budapest elaborado por el consejo de Europa en el año 2001, cuyo objetivo es enfrentar al cibercrimen y mejorar la colaboración internacional en la lucha contra los delitos informáticos. Esto se logra mediante la armonización de las leyes, la promoción de la cooperación entre naciones y la implementación de medidas preventivas y de seguridad en el entorno digital. México al día de hoy no forma parte de dicho convenio, solo participa como observador, siendo importante su adhesión, para contar con asistencia mutua en la investigación, persecución y sanción de estos delitos, aplicación de leyes uniformes, simplificando con esto la cooperación entre los países en la lucha contra el cibercrimen (Sala de Comisiones de la Cámara de Senadores , 2021).

En el delito informático no hay una uniformidad mundial en su conceptualización, tiene muchas aristas, la informática puede ser el medio o el instrumento y no el fin, son complejos dada la propia tecnología, no hay un punto de acuerdo entre los responsables de legislar respecto a la definición de una conducta de riesgo o delito informático, una conducta de riesgo para considerarse delito, tiene que estar tipificado, debe ser punible o culpable, se tienen que dar ciertas situaciones que en la práctica no se ha logrado consensuar sobre este tema. Las conductas delictivas que se cometen a través de los medios cibernéticos son cada vez más artificiales y confusas. Escuchamos en las noticias hablar de redes de pornografía infantil, tráfico de órganos, trata de personas, grooming, phishing, fraude en línea, suplantación de identidad, ataques de denegación de servicio, ataque de hombre al medio, entre otros.

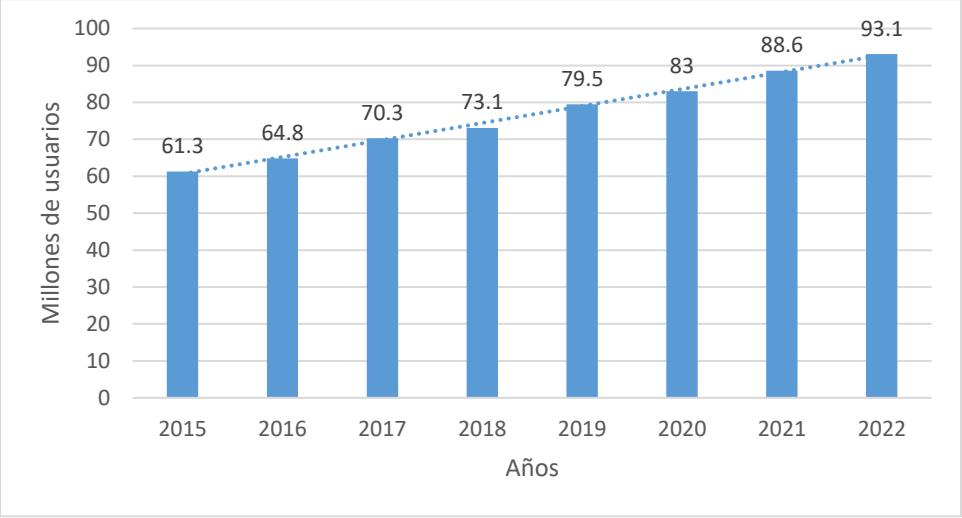
Por otra parte con la crisis sanitaria que se atravesó a nivel internacional y que obligo al confinamiento de la sociedad, medidas que fueron impuestas por el Gobierno Federal, con el fin de garantizar la integridad de las familias, el Estado de Michoacán no fue la excepción, con fecha 30 de marzo del 2020 el Gobernador del Estado emitió el acuerdo administrativo número 78 en el que se establecen diversas acciones ante la pandemia de COVID-19 (2020), entre ellas la suspensión de clases, actividades laborales no esenciales. Las TIC´s se convirtieron en un pilar fundamental que permitió mantener las actividades en las dependencias públicas, centros académicos y oficinas. Por lo antes mencionado se ha observado un incremento de los incidentes cibernéticos a través de fraudes en línea, clonación de tarjetas, ingeniería social, extorsiones telefónicas, ataques a la propia imagen, a la intimidad, violencia digital a la intimidad sexual, por mencionar algunos, por consiguiente las afectaciones económicas en detrimento del patrimonio de la sociedad michoacana, las cuales se han visto afectadas de manera significativa por lo cual es imperante la adecuación al marco normativo que tenga en cuenta las características únicas de los delitos cibernéticos, siendo vital para garantizar los derechos de los usuarios en el internet.

Adicional a lo anterior es fundamental que las Instituciones encargadas de la prevención y persecución de este tipo de conductas sean más eficientes en sus protocolos de actuación, contar con conocimientos técnicos, equipo tecnológico especializado para rastrear, recabar pruebas, investigar y sancionar estás conductas a los responsables de la comisión de este tipo de delitos. Por lo cual resulta fundamental que así como la innovación tecnológica avanza en beneficio de la sociedad, el marco legal lo haga en el mismo sentido, de manera oportuna en la prevención y persecución de los nuevos tipos delictivos, reglamentos y leyes que regulen la conducta, con el fin de que en el Estado de Michoacán se cuente con un andamiaje legal más certero en materia de ciberseguridad.

Cibercultura

Según la Encuesta Nacional sobre Disponibilidad y uso de Tecnologías de la Información en los hogares (ENDUTIH) en coordinación con el Instituto Nacional de Estadística y Geografía (INEGI) y el Instituto Federal de Telecomunicaciones (IFT) (2023), que recopila datos del año 2022 sobre la disponibilidad y el uso de las tecnologías de la información y la comunicación en los hogares de la República Mexicana, mostrando que al finalizar el año, se contabilizo un total de 93,1 millones de usuarios conectados a internet, lo que constituye el 78.6% de la población de seis años en el país. Lo que significa un aumento del 4.5% respecto al año anterior ubicándose en 88.6 millones de internautas, el aumento en la disponibilidad y acceso a las tecnologías han generado una mayor exposición a riesgos en las interacciones en el ciberespacio.

Gráfica 2. Usuarios de internet en México.



Fuente: Elaboración propia con base en ENDUTIH, IFT e INEGI (2023).

En congruencia con el párrafo anterior y como es del conocimiento, las sociedades desde sus inicios han utilizado la comunicación para interrelacionarse, expresar sentimientos, compartir ideas, como

parte de su convivencia y supervivencia, así como para la transmisión y preservación de su cultura de generación en generación. En este sentido entendemos por cultura; el conjunto de conocimientos que caracterizan a una sociedad y que se transmite de generación en generación (Molano, 2007). En este contexto existen elementos culturales e históricos que influyen en la forma que se comportan las personas de una determinada época. En esta era digital la sociedad ha cambiado su estructura en términos de comunicación e interacción en el ciberespacio. El desarrollo de las tecnologías de la información y comunicaciones ha generado cambios significativos en la forma en que las personas se comunican, comparten información y se relacionan entre sí en el entorno virtual.

Con el surgimiento de las TIC´s las estructuras de las sociedades han cambiado y experimentado grandes cambios significativos en la forma en la que las personas se relacionan, esto debido a la creación de las comunidades digitales o en línea, las cuales traspasan fronteras y son más numerosas que las tradicionales, que cuentan con límites o barreras geopolíticas. El ciberespacio ha proporcionado un espacio a través del cual los usuarios ejercen su autonomía y con ello una forma de comunicarse libremente, de expresar ideas o sentimientos en las diversas redes sociales (Facebook, Instagram, Twitter, WhatsApp, Messenger, Google, YouTube, Telegram, Snapchat, TikTok entre otros), foros en línea, plataformas de juego, blogs y microblogs, comunidades académicas, por mencionar algunas, ofreciendo con esto oportunidades de colaboración, aprendizaje, socialización e intercambiar conocimientos. Las TIC's han facilitado el acceso a la información, facilitando el progreso y elevando la calidad de vida de las sociedades, pero su uso no siempre ha sido el apropiado, pues el cúmulo de interacciones, como ya se ha mencionado anteriormente, implica ciertos riesgos para los usuarios (Fernández, 2010).

Antes los medios de comunicación tradicionales como; la televisión, la radio y los diarios, tenían un papel preponderante en la difusión de la información a la sociedad, ahora en la actualidad, los usuarios de las TIC´s, solo con disponer de una conexión a internet y un dispositivo móvil tienen la capacidad de comunicarse y compartir información, expresar ideas, opiniones, estados de ánimo los cuales cuando no son manifestados de manera responsable afectan a otros usuarios, desinformando a la sociedad, ya que difunden imágenes, videos, retos para los jóvenes, comparten información sensible, ubicaciones, rutinas, conversaciones y noticias falsas que tienen un impacto negativo tanto en la percepción de la realidad como en el comportamiento individual. Por lo anterior es Jnecesario establecer mecanismos que instruyan a las personas a discernir el tipo de información que consumen, evaluar la veracidad de las fuentes y como esta puede afectar la interpretación de la realidad para fomentar un consumo responsable del contenido en línea (Fernández, 2010).

Las plataformas digitales son administradas por diferentes concesionarios de servicios de internet y proveedores de contenido en línea, quienes ofertan diversos productos y servicios a los usuarios (descarga de software, juegos, aplicativos, redes sociales, mensajería instantánea, libros, música, videos, etc.) a cambio de algo: los datos de los usuarios, información personal que suelen llenar en los formularios que son necesarios para la alta en sitios web, al suscribirse a diferentes plataformas sociales, descarga de diversos aplicativos y servicios en línea (datos generales, número de teléfono, dirección de correo electrónico, datos bancarios, preferencias personales, información laboral) mismos que son almacenados en grades repositorios. Lo que representa un problema ya que la información es comercializada, no existe una protección de los datos por parte de los diferentes proveedores de servicios, lo que implica un riesgo de que caiga en manos de personas que puedan utilizar para temas de extorsión, robo de identidad, secuestro, suplantación de identidad, fraude, entre otros, de igual manera influir en la toma de decisiones de los usuarios a través de la recolección de dichos datos (Véliz, 2021). De lo anterior es necesario crear estrategias eficaces que aseguren la correcta manipulación y uso de los datos que se proporcionan a las diversas plataformas digitales, resultando ineludible crear una cultura de la protección y no divulgación de información personal de los usuarios.

Las plataformas digitales actúan como medios de expresión en un mundo virtual y que tienen un impacto en el físico, estos espacios del mundo digital han permitido que la sociedad se manifieste, discuta y en muchas ocasiones levante la voz para manifestar su inconformidad ante ciertos hechos, por otra parte, existen usuarios que las utilizan como una manera de criticar, atacar y ofender (hater), posteando y publicando información falsa en muchas ocasiones, sin argumentos válidos, sus actitudes negativas suelen estar motivadas por la envidia, discurso de odio, la búsqueda de atención, frustración personal, el anonimato o simplemente por diferencias de opinión, provocando que esto se haga viral y transgrediendo así, las reglas morales (Laniel, 2021).

En el ciberespacio, adoptamos un comportamiento diferente al que desempeñamos de manera presencial, el anonimato que ofrece las redes sociales permite la creación de nuevas identidades, jugar a ser otra persona, ya que al ocultar su identidad real, se sienten menos limitados por las expectativas sociales y pueden explotar diferentes aspectos de su personalidad, tales como; imponer retos buscando popularidad, al sentirse más libres de hacer comentarios ofensivos, engañar, mentir, así como el desarrollo de varias personalidades o personajes virtuales. En este contexto se han generado conductas de riesgos, tales como: Ciberacoso, discriminación en línea, cyberbullyng, sexting, sextorsión, ingeniería social, retos sociales, grooming (Molina y Vecina, 2015).

Estas conductas de riesgo en el ciberespacio han tenido grave consecuencias en el tejido social, los retos han acabado con la vida de personas, solo por buscar la aceptación de una minoría, las reacciones que alguien postea ante nuestras publicaciones influyen en los estados de ánimo, la adicción por estar en constante comunicación han generado un aislamiento en los propios núcleos familiares, mientras que la desinformación en las redes ha resultado en linchamientos públicos que han terminado con la vida de personas, como el caso ocurrido en la comunidad de Acatlán Puebla, a través de la difusión de mensajes WhatsApp, alertaron a la población sobre la presencia de supuestos secuestradores. Estos mensajes incitaron al pueblo a tomar justicia por su propia mano, la información no se confirmó, lo que resulto trágicamente en la vida de dos personas (Martínez, 2018). La desinformación puede tener consecuencias devastadoras, como se ha mencionado anteriormente. Es fundamental fomentar una cultura de responsabilidad en el uso de las redes sociales, subrayando la importancia de no compartir información sin antes verificar su veracidad.

La opinión colectiva y manipulación de información a través de las redes sociales influyen en el comportamiento de los individuos, manipulando su conducta, pasando del plano digital a las agresiones físicas, violencia, odio, insultos y hostigamientos. Por lo cual es inexcusable crear una cultura digital que fomente el uso del ciberespacio de una manera más responsable, siendo empáticos, reflexivos y generando principios éticos y morales que guíen el comportamiento de los usuarios al interactuar en el ciberespacio.

Cibercrimen

Como resultado de esta interacción en el ciberespacio los delitos se manifiestan en dos modalidades: como el medio y/o como el fin en la comisión de delitos cibernéticos (Téllez, 2008). En este sentido el delito es una acción ilegal, particular y contraria a la ley, que es castigada por una pena (Granadillo, 2019) y en el contexto del medio cibernético la palabra ciber es una palabra que proviene del término cibernética y se utiliza para referirse a la relación con el mundo digital o el ciberespacio.

Podemos definir al cibercrimen como aquella conducta ilícita en la cual están involucrados los equipos tecnológicos y medios electrónicos, donde estos pueden ser el medio o el fin para la comisión de un delito. En el primer caso, los delincuentes utilizan los equipos y las redes informáticas como instrumentos para llevar a cabo actos delictivos (Barrio, 2017). Un ciberdelincuente puede aprovechar un equipo para ingresar de forma ilegal a sistemas informáticos, sustraer información delicada, cometer estafas en línea, distribuir un virus o compartir contenido ilícito. Los dispositivos se emplean como herramientas para facilitar y ejecutar estas acciones delictivas.

Por otra parte cuando los equipos y las redes son utilizados como el objetivo principal del delito, se convierten en el blanco de la actividad delictiva. Los criminales pueden atacar sistemas informáticos con la finalidad de causar daños, interrupciones en servicios, apropiarse de información valiosa o realizar actos de sabotaje. Entre estos delitos se encuentran el hackeo de redes, ataques de denegación de servicio, robo de dispositivos, secuestro de datos, la manipulación de sistemas informáticos, ataques de fuerza bruta, ransomware, ataques man in the middle, entre otros.

En este escenario, la problemática que presenta el Estado de Michoacán es el incremento de las conductas delictivas cometidas a través de los medios cibernéticos, Este aumento se atribuye a la creciente dependencia en el uso de las tecnologías de la información y comunicaciones, la globalización de la conectividad, así como la falta de concientización sobre los riesgos, los avances tecnológicos, entre otros factores. Por lo que con información brindada por el Estado de Michoacán a través del portal de transparencia, se obtuvieron los siguientes datos, con los cuáles se puede apreciar el incremento en la incidencia delictiva.

Tabla 1. Estadísticas de colaboraciones Policía Cibernética.

Año	Colaboraciones Policía Cibernética	Variación porcentual	Incremento con respecto al año base
2016	373	------	----
2017	413	10.72%	110.72%
2018	630	52.54%	168.90%
2019	1,238	96.50%	331.90%
2020	1,749	41.27%	468.90%
2021	1,920	9.80%	514.74%
2022	2,931	52.65%	785.79%
TOTAL. .	**9,254**		

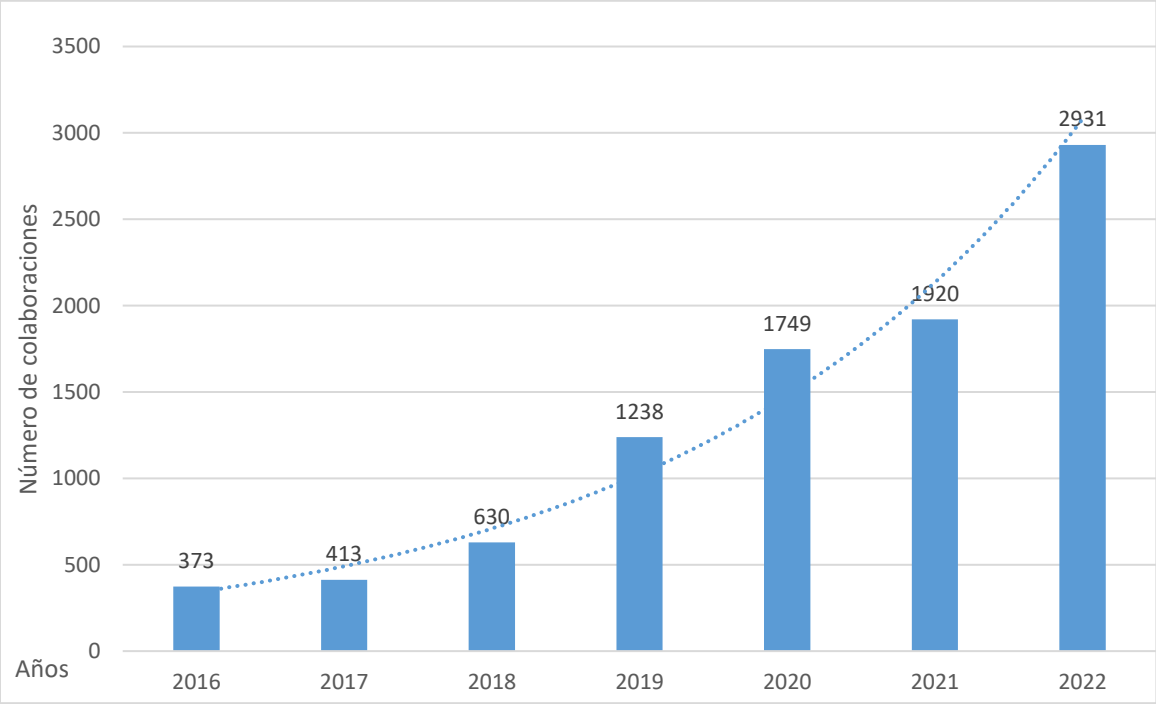
Fuente: Elaboración propia con base en el Portal de Transparencia del Estado de Michoacán (2022).

En la siguiente gráfica se observa la tendencia de las investigaciones realizadas por la Policía Cibernética[1], que muestra el aumento en este tipo de delitos en el Estado por año, se aprecia la siguiente información: año 2017 se tuvo un crecimiento del 10.72% en relación al año 2016, en el año 2018 un aumento del 52.54% en relación al ejercicio 2017, en el año 2019 el aumento se vio en un 96.5% respecto al año 2018, en el año 2020 el incremento reflejo un 41.27% en correspondencia

[1] Las investigaciones realizadas por la Policía Cibernética pueden no corresponder con el número de delitos cibernéticos iniciadas en el Estado, ya que por cada delito iniciado en la Unidad de Investigación y Persecución de delitos cometidos a través de medios cibernéticos y las Fiscalías Regionales al interior del Estado pueden requerirse uno o más solicitudes de investigación.

con el año 2019, en el año 2021 se observa un aumento del 9.8% en proporción al año 2020 y finalmente en el año 2022 un incremento del 52.65% en relación al ejercicio 2021. Estas cifras únicamente representan las colaboraciones iniciadas mediante la denuncia formal por parte de la ciudadanía, sin contar todas aquellas que no se denuncian; con lo que podemos observar que el aumento es evidente, continuo y significativo durante los últimos siete años, reflejando con ello la problemática de ciberseguridad que tiene el Estado relacionado con la dependencia tecnológica, la falta de concientización por parte de los usuarios en la navegación y la sofisticación de los ataques cibernéticos.

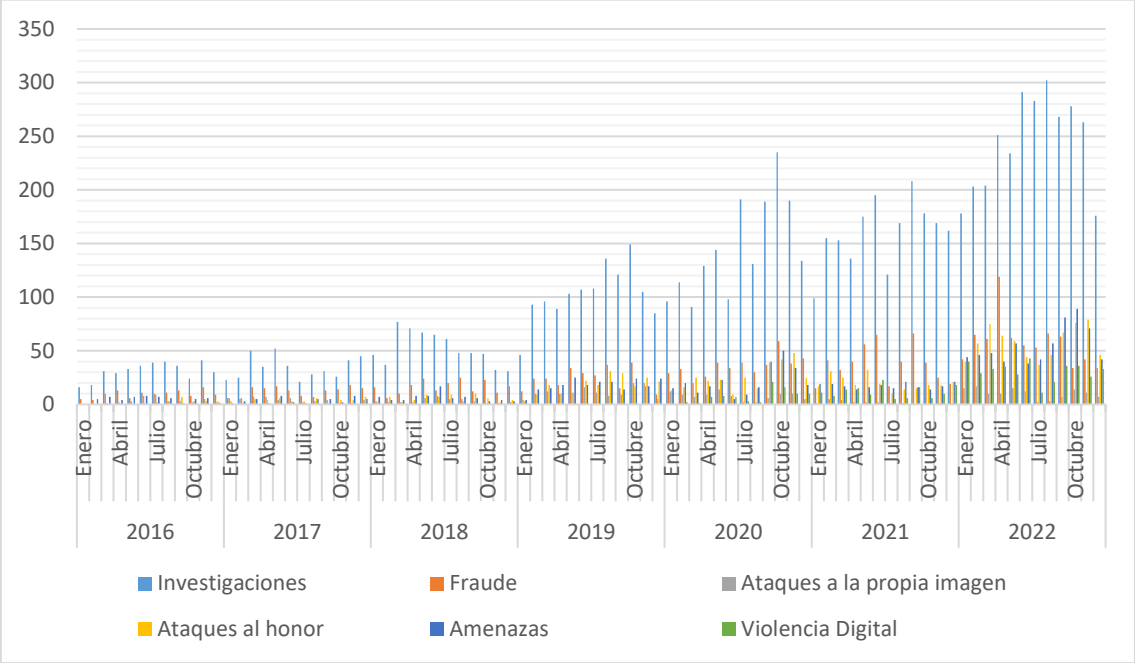
Gráfica 3. Incremento en las investigaciones realizadas por la Policía Cibernética.



Fuente: Elaboración propia con base en el Portal de Transparencia del Estado de Michoacán (2021).

La gráfica presenta información detallada sobre la incidencia de delitos que impactan a la sociedad Michoacana en el periodo comprendido entre los años 2016 al 2022. Destaca la evolución de los delitos cibernéticos por bimestre, resaltando el total de colaboraciones atendidas por la Policía Cibernética, mediante una barra azul. Además, identifica los delitos más frecuentes mediante colores específicos, evidenciando una tendencia ascendente hasta el año 2022. Este análisis subraya la importancia de implementar medidas efectivas para abordar esta problemática.

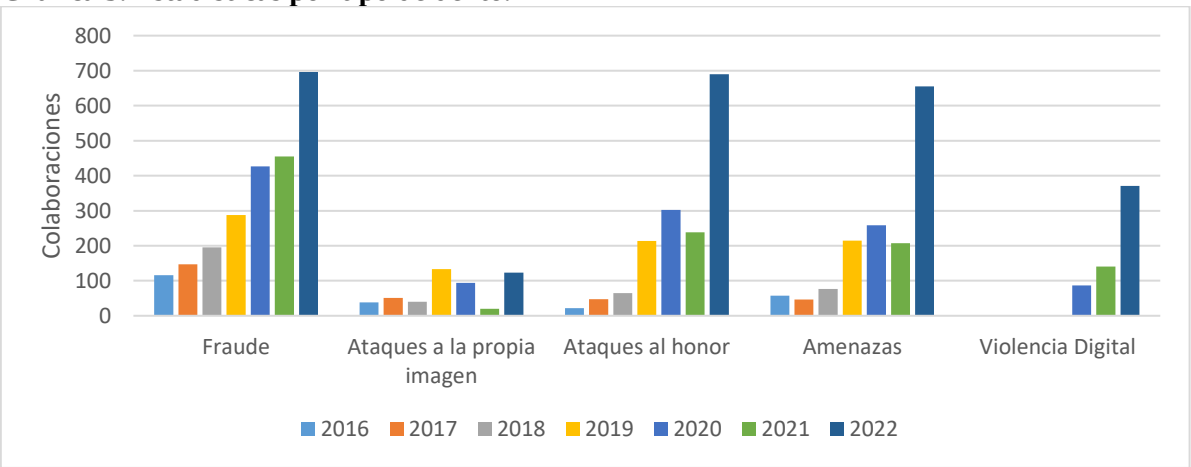
Gráfica 4. Tendencia en las investigaciones realizadas por la Policía Cibernética.



Fuente: Elaboración propia con base en el Portal de transparencia del Estado (2021).

En el Código Penal para el Estado de Michoacán (2022) se encuentran tipificados los siguientes delitos; 1) Ataques al honor, 2) Ataques a la propia imagen, 3) Ataques a la intimidad, 4) Fraude, 5) Amenazas, 6) Falsificación, 7) Pornografía de personas menores de edad, 8) Acoso sexual, 9) Instigación o ayuda al suicidio, 10) Hostigamiento sexual, 11) Extorsión, 12) Violación de correspondencia, 13) Usurpación de identidad, 14) Violencia digital a la intimidad sexual; de los cuales la suma de colaboraciones realizadas por la Policía Cibernética del año 2016 al 2022 es de 9,254 colaboraciones, lo que representa un 70.46% con 6,515 carpetas de investigación.

Gráfica 5. Estadísticas por tipo de delito.



Fuente: Elaboración propia con base en el Portal de transparencia del Estado (2021).

Las instancias gubernamentales están prestando cada vez más atención a los delitos cibernéticos, esto se debe a diversos factores: el incremento de las amenazas en el ciberespacio abarca desde simples robos de datos hasta ataques altamente sofisticados y complejos dirigidos a infraestructuras críticas. Esta creciente realidad subraya la urgente necesidad de salvaguardar los intereses tanto de los ciudadanos como del Gobierno en el ciberespacio. Actualmente los delitos se analizan, se investigan y son encuadrados en tipos penales obsoletos o insuficientes para abordar de manera efectiva la problemática, lo que puede derivar en menoscabos del patrimonio, la reputación, el honor o la actividad profesional de la sociedad Michoacana, y aún más preocupante, es cuando los sistemas de procuración de justicia no logran cumplir con su objetivo en este ámbito.

En otro sentido existen conductas que afectan el patrimonio, los derechos, la integridad, la reputación, y honorabilidad de los individuos, tales como; el robo de información personal o financiera, grooming, sexting, cyberbullyng, la suplantación de identidad, ciberacoso, sextorsión, daño a los sistemas, entre otros, que en muchos casos no pueden ser sancionadas debido a que no existe un marco normativo adecuado, la ausencia de leyes específicas o su insuficiente actualización para abordar este tipo de conductas, lo que limita la capacidad de las autoridades para investigar, perseguir y sancionar dichas conductas.

En virtud de lo anterior, cobra relevancia el diagnóstico general que guarda el marco normativo y operacional del Estado de Michoacán, a fin de detectar las áreas de oportunidad y líneas estratégicas, maximizando su eficiencia en la prevención, combate, persecución y procuración de justicia en delitos cometidos a través del ciberespacio.

Infraestructuras críticas

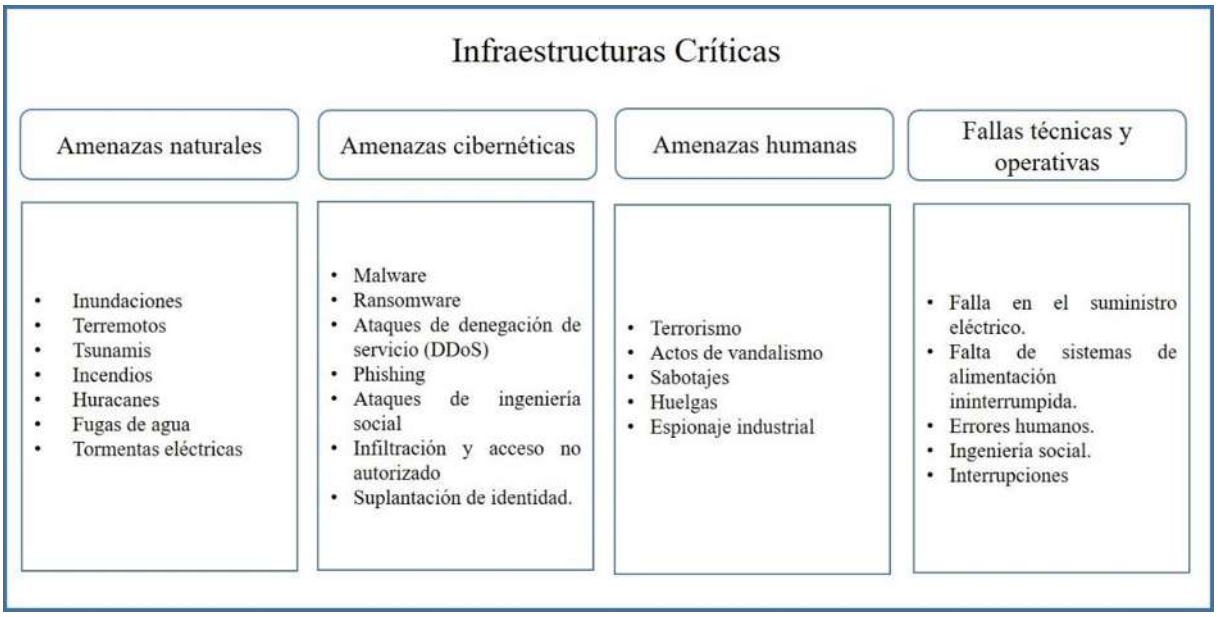
En relación con el párrafo anterior sobre el crecimiento de los delitos cibernéticos y debido al grado de sofisticación y complejidad de las amenazas, se debe tomar en consideración que estas no solo afectan a los usuarios. Las empresas y dependencias del Gobierno también se encuentran en riesgo debido a que soportan sus servicios, procesos y aplicaciones sobre diversas infraestructuras tecnológicas, lo que implica amenazas y riesgos que no se han contemplado, por lo cual es necesario identificar las infraestructuras críticas y los activos estratégicos para salvaguardar su protección, con el fin de mantener su alta disponibilidad en la prestación de servicios esenciales para la sociedad.

En contexto con las líneas descritas entendemos por infraestructura crítica; el conjunto de activos, procesos y servicios que son esenciales para que una sociedad funcione de manera adecuada y para los cuales no existen sustitutos (Mattioli y Levy, 2014). Las infraestructuras críticas se encuentran en

el sector público y privado, conformadas por; las instalaciones, sistemas, equipos físicos, redes de comunicaciones, bases de datos, aplicativos y tecnologías de la información que soportan los activos y servicios de una sociedad, su importancia radica que a través de ellas se brindan servicios precisos en las actividades diarias de la sociedad; tales como; agua, energía, servicios financieros, salud, educación, transporte, tecnología satelital, servicios administrativos, telefonía, espacio aéreo, servicios de emergencia, entre otros.

Como se mencionó anteriormente las actividades esenciales de una sociedad dependen de las infraestructuras tecnológicas, las cuales involucran diversos riesgos en su operación, tales como; amenazas naturales, físicas y lógicas todas ellas con un grado de complejidad diversa que de materializarse pueden producir un impacto negativo que deje inhabilitado un servicio esencial que afectaría la salud, seguridad, economía o las actividades de la población en general, en la siguiente ilustración se categorizan las amenazas que pueden afectar a dichas infraestructuras.

Ilustración 1 Clasificación de amenazas a las infraestructuras críticas.



Fuente: Elaboración propia con base en LISA Institute (2019).

La expansión de aplicaciones en línea, programas, plataformas digitales y equipos electrónicos en las actividades económicas y en la prestación de servicios del Gobierno y empresas, han permitido la automatización de las actividades, agilizando sus procesos productivos en las actividades esenciales. Si bien todo esto representa un uso eficiente de las tecnologías de la información y comunicaciones para optimizar la efectividad y calidad en la prestación de servicios, como se ha comentado anteriormente trae consigo vulnerabilidades inherentes a su uso, por lo que resulta esencial garantizar su seguridad, equipamiento en sistemas redundantes, planes de recuperación, contar con equipos de

respuesta a incidentes que en caso de un riesgo potencial, garanticen la continuidad de los servicios anteriormente mencionados, que como ya se comentó no hay equivalentes, por lo cual se muestra un contexto histórico de los países que han sufrido ataques y que han tenido impacto en sus infraestructuras críticas.

República de Estonia

Lenoir (2017) en el confidencial, informa que el Gobierno de Estonia sufrió el 27 de Abril del año 2007 el primer ciberataque a raíz de que el Gobierno decidió remover del centro de Tallin el monumento del soldado de bronce. Este evento ha generado descontento tanto en la población con origen Ruso como entre los funcionarios del Gobierno Ruso. Se presume que como resultado de lo anterior, se desencadenó un ataque distribuido de denegación de servicios (DDoS) contra la República de Estonia: las páginas gubernamentales experimentaron caídas, y para la segunda semana, los medios de comunicación quedaron desconectados, lo que imposibilito informar al mundo sobre la situación en el país. Siete días después los atacantes desconectaron el sistema bancario, la sociedad impedida a disponer de efectivo, lo que genero un mayor caos. En mayo 19, los ataques se detuvieron; Estonia acusó al Gobierno de Rusia de estar detrás de los ataques, pero nada pudo ser probado. Este incidente en Estonia centro la atención por parte de la OTAN (Organización del Tratado del Atlántico Norte, que es una alianza militar y política, cuyo objetivo es la defensa de sus miembros ante cualquier ataque armado) de tal manera que colocó a la ciberseguridad dentro de sus políticas de defensa. Así mismo otros países comienzan a ver la necesidad en cuanto a proteger su territorio y sus infraestructuras de este tipo de ataques.

Estados Unidos de Norte América

Gorman et al., (2009) en The Wall Street Journal, anuncia que en Estados Unidos hackers accedieron y copiaron información de alta confidencialidad del proyecto; Joint Strike fighter o F-35 Lighting Fighter, el proyecto más costoso para el Pentágono. Los ataques parece que se originaron en China; pero hasta ahora no se ha logrado identificar a los culpables y la embajada china en el país del norte se ha declarado contraria a todo tipo de cibercrímenes.

Popper y Conger (2020) según Infobae, informaron que el 20 de julio del año 2020 se produjo un incidente de seguridad en la plataforma de la red social Twitter. Esta eventualidad involucro un hackeo masivo en el cual los atacantes, utilizando herramientas sofisticadas, lograron comprometer el acceso y obtener privilegios de administrador, lo cual les permitió controlar casi cualquier cuenta en dicha plataforma, incluyendo la del expresidente Barack Obama, el ex vicepresidente Joe Biden, Elon Musk y otras celebridades, con la finalidad de llevar acabo estafas por medio de

criptomonedas, en la primera hora del ataque recaudaron cerca de 100,000 dólares. A pesar de la atención mundial que atrajo la intrusión, lo alarmante es el impacto de esta plataforma en sus publicaciones y lo viral que se hacen en cuestión de minutos. En este ataque fueron utilizadas para un fraude ¿Qué habría sucedido si esos comentarios se hubieran hecho con otros propósitos, como desestabilizar el mercado bursátil o hacer declaraciones políticas?, hasta el momento, los detalles básicos de quiénes fueron los responsables y cómo lo hicieron, este caso resalta la importancia de la seguridad en las redes sociales, plataformas y la importancia de que las empresas generen medidas proactivas para proteger la integridad de las cuentas de los usuarios y prevenir conductas de riesgo.

República de Ucrania

Pérez (2016) en El Confidencial, informa el ataque a la red eléctrica en la República de Ucrania mediante el uso del virus troyano identificado como BlackEnergy, en donde 80,000 mil personas quedaron en la oscuridad hasta seis horas después de que los atacantes informáticos se infiltraran en tres compañías de energía y manipularon remotamente los sistemas para provocar un apagón eléctrico. Se sospechó que el Gobierno Ruso estaba detrás de este ataque, pero no se confirmó, dejando en claro el daño que un virus puede tener en las infraestructuras criticas de un país.

México

Banco de México (BANXICO) (2018) informa, que el 27 de abril del año 2018 se produjo un ciberataque en el cual las plataformas de desarrollo de los bancos participantes, así como la infraestructura tecnológica utilizada para la conexión al Sistema de Pagos Electrónicos Interbancarios (SPEI), fueron comprometidas. Este ataque se llevó a cabo mediante códigos informáticos y virus troyanos que permitieron la manipulación de datos en el Sistema, con la finalidad de afectar su funcionamiento y redirigir transferencias a diversas cuentas. Se estima que el monto afectado fue de aproximadamente $400,000,000 (cuatrocientos millones de pesos 00/100 M.N.). El Gobernador del Banco de México declaró que el sistema central del SPEI administrado por Banxico no fue comprometido, sino que el ataque se produjo a través de los proveedores de servicios de los bancos privados que realizan la conexión mediante software hacia el sistema central.

González (2019) por el Excélsior, comunica que el 10 de noviembre del año 2019, un incidente de ciberseguridad afecto la infraestructura tecnología de Petróleos Mexicanos (PEMEX) mediante un ataque de ransomware conocido como 'Doppel Paymer'. Este ataque implicó el secuestro de información a través de cifrado y por la cual se pedía un rescate de 565 bitcoins, equivalente a 4.9 millones de dólares a cambio de descifrar la información afectada. Este incidente afecto al menos el 5% de los equipos de cómputo personales. A pesar de la magnitud del ataque, tanto PEMEX como el

Gobierno de la República minimizaron la gravedad de lo sucedido, declarando que no se pagaría el rescate solicitado.

Chávez (2020) el 07 de julio del año 2020, informo de un ataque cibernético de "Defacement" dirigido a las páginas web de la Comisión Nacional para la protección y defensa de los Usuarios de Servicios Financieros (CONDUSEF) y el Banco de México (Banxico). Este ataque implicó la alteración o modificación de los sitios WEB, aunque este tipo de ataques no representa una amenaza directa a la integridad de los datos, en muchos casos los atacantes buscan llamar la atención o demostrar sus habilidades para vulnerar la seguridad, lo que pone de manifiesto una falta de controles de seguridad robustos en la infraestructura del gobierno.

09 de julio del año 2020: La página del SAT es comprometida por un ataque cibernético que provocó una intermitencia de tres horas. Este incidente indicón que los ciberdelincuentes intentaron sobrecargar el sistema con solicitudes, con el fin de colapsarlo y hacerlo no disponible para los usuarios. Se informó que la información de los contribuyentes no se vio afectada, ya que los sistemas de alerta activaron los mecanismos de protección de la información tributaria. Con este ataque suman 3 en una sola semana que se suscitaron en México. (Expansión, 2020).

Michoacán

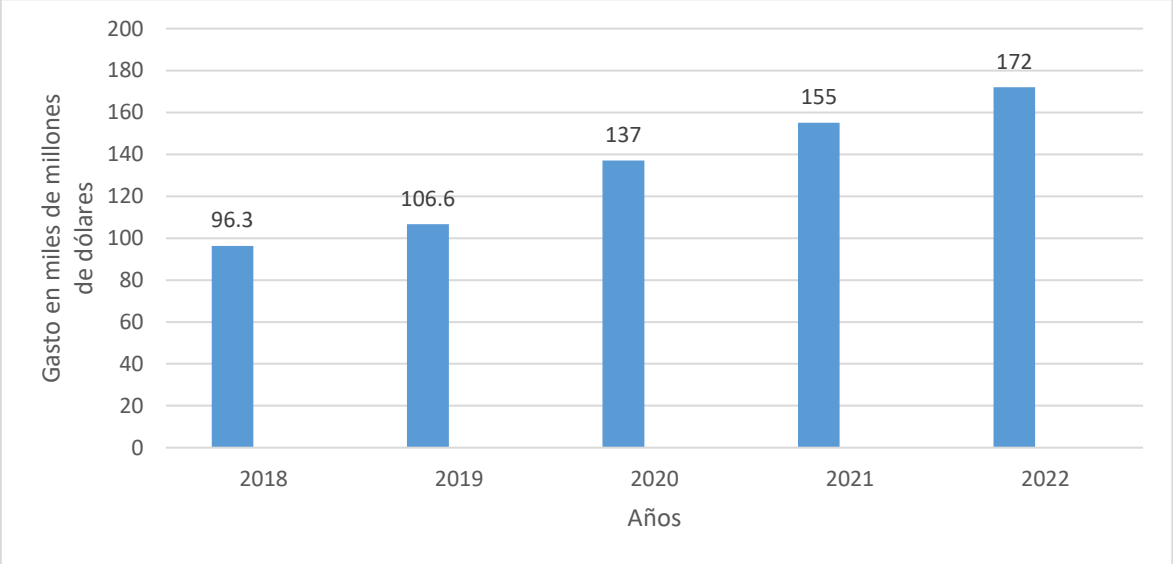
27 de julio del año 2017, la empresa de contenedores APM Terminals, ubicada en el Puerto de Lázaro Cárdenas, Michoacán, se vio afectada en sus operaciones logísticas debido a un ataque cibernético en su sistema informático. Este ataque, realizado con el virus informático "Golden Eye", ingreso al sistema a través del correo electrónico y encriptó archivos. Los atacantes exigieron un rescate en bitcoins equivalente a 360 millones de dólares. Este ataque género importantes pérdidas monetarias para la empresa, ya que se vieron obligados a realizar operaciones manuales, resultando en pérdidas económicas significativas por hora en los movimientos de embarque y desembarque. APM Terminals reconoció que el ataque afecto a diecisiete terminales de carga en diferentes puertos del mundo (Segundo , 2017).

El contexto histórico revela la evolución constante de las amenazas cibernéticas, subrayando así la importancia crítica de comprender a fondo los riesgos y las posibles consecuencias. Aprender de las experiencias pasadas se vuelve imperativo para desarrollar estrategias en materia de ciberseguridad para salvaguardas las infraestructuras críticas del estado de Michoacán. Estos incidentes destacan la necesidad de una colaboración continua entre los sectores público y privado para fortalecer las defensas cibernéticas y poder así responder de manera efectiva a las amenazas.

Seguridad de la información

El artículo de Gartner (2022), empresa de investigación y asesoramiento tecnológico con sede en los Estados Unidos, informo que las empresas están más interesadas en invertir para proteger sus infraestructuras tecnológicas, procesos y servicios de cualquier incidente que pueda llegar a presentarse y que pueda poner en riesgo sus operaciones. Como muestra la gráfica 8, en el año 2018 la inversión fue de 96.3 mil millones de dólares, en al año 2019 de 106.6 mil millones de dólares, en el año 2020 una inversión de 137 mil millones de dólares, para el ejercicio 2021 se invirtieron 155 mil millones de dólares y lo pronosticado para el año 2023 es de 172 mil millones de dólares, lo que representa un incremento del 10.69%, 28.51%, 13.13%, y 10.96% para los mismos años, además derivado de la pandemia los procesos de seguridad tuvieron una adopción del 12% en la implementación de seguridad basadas en la nube, donde se desprende que la inversión en estos cinco años en ciberseguridad ha sido de un 78.60% respecto al año base.

Gráfica 6. Gasto mundial en Ciberseguridad.

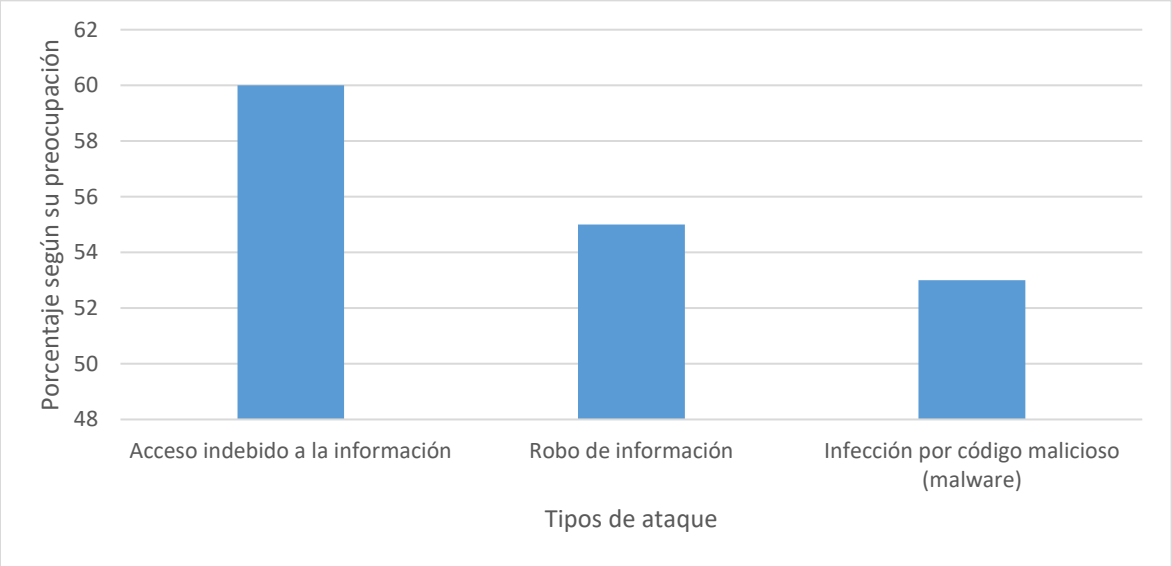


Fuente: Elaboración propia con base en Gartner (2020).

Eset (2020) compañía especializada en ciberseguridad, presenta en el reporte de seguridad cómo está cambiando el enfoque de las organizaciones frente a las tecnologías de la información y comunicación, a través de una encuesta a más de 4,000 empresas de diferentes magnitudes en Latinoamérica, se recopila la opinión sobre cómo gestionan su ciberseguridad, reportando la siguiente información: un 60% de los expertos se dicen preocupados por un ataque de acceso indebido a la información, un 55% de ellos por el robo de información y el 53% de sufrir alguna infección por un código malicioso (malware), como lo muestra la gráfica 9. Por otra parte las organizaciones han encontrado grandes retos de seguridad dentro de la emergencia sanitaria, ya que un 45% de ellos sufrieron intentos de phishing y el 50% no estaban preparados para implementar medidas de seguridad

adecuadas en la nueva modalidad de trabajo conocido como: Home office. Adicional a lo comentado, en el año 2019 se conoció la filtración de más 2,200 millones de contraseñas y direcciones IP, exponiendo con ello la vulnerabilidad de las empresas y el grande reto que al día de hoy existe para crear políticas que sirvan para la protección de los datos, así como la capacitación constante del personal que maneja las infraestructuras tecnológicas, servicios y procesos los cuales deben contar con una capacitación continua, con el fin de hacer frente a los nuevos incidentes cibernéticos que cada vez son más sofisticados debido al constante avance de la tecnología, interconectividad global, el anonimato existente en el ciberespacio que permite vectores de ataques más sofisticados, lo que se vuelve un campo fértil para los ciberdelincuentes.

Gráfica 7. Principales preocupaciones de los encuestados



Fuente: Elaboración propia con base en Eset (2020).

En congruencia con el párrafo anterior y dada la relevancia de proteger a las personas, la información y las infraestructuras que interactúan en el ciberespacio se vuelve indispensable garantizar; la integridad, disponibilidad y confidencialidad de la información, este aspecto se convirtió en un asunto fundamental en lo económico y político de las naciones. La norma ISO 27001 (2014) define a la seguridad de la información como el conjunto de medidas preventivas y reactivas orientadas a la preservación de la confidencialidad, integridad y disponibilidad de la información.

Por otro lado la ciberseguridad, en un sentido más amplio que la seguridad de la información, garantiza la seguridad y protección de las personas por lo que ambas son complementarias y necesarias para mantener la paz y la seguridad de los ciudadanos en su patrimonio, en su persona, bienes y derechos.

La seguridad de la información no la garantiza la infraestructura tecnológica (Hardware y Software) que se implementa en torno a un sistema informático, equipos personales, plataformas digitales, celulares, tablet´s, enlaces de comunicación, entre otros, ya que los datos que coexisten en el ciberespacio y que están circulando por diferentes enlaces de comunicación a nivel mundial no se protegen contra los riesgos, amenazas, vulnerabilidades, ataques e incidentes informáticos.

Aunado a lo anterior la falta de: concientización, entrenamiento y la creación de una cultura de seguridad de la información ha permitido que se vulnere la seguridad del sector público, privado y la sociedad en general. Así mismo existe un gran desconocimiento sobre temas de seguridad de la información y su alcance. Hoy en día la mayor cantidad de ataques provienen del interior de las empresas. Un estudio realizado por IBM X-Force Threat Intelligence Index (2018), empresa dedicada a proporcionar información y análisis sobre las tendencias y amenazas en materia de ciberseguridad, observaron a lo largo de los años 2015, 2016, 2017 y 2018 las causas de diversos incidentes, demostrando que el 95% de dichos incidentes en ciberseguridad se deben a errores humanos.

Otro ejemplo a nivel mundial de la importancia de la información, es el que origino el ransomware Wannacry. Entre el pasado día 12 y 16 de mayo del año 2017, se llevó a cabo un ciberataque que afectó a más de 360,000 dispositivos electrónicos en más de 180 países, bloqueándolos e impidiendo su utilización, el incidente consistió en un tipo de código malicioso que explota una serie de vulnerabilidades en sistemas operativos Windows y en varios protocolos de red, bloqueando y encriptando documentos almacenados en los ordenadores de sus víctimas con el objetivo de solicitar al usuario el pago de una suma de dinero en la moneda electrónica bitcoin para permitirles volver acceder nuevamente, el costo estimado de este ataque se evalúo en 4 mil millones de dólares. (Frieiro et al., 2017).

Derivado de lo anterior, la ciberseguridad debe permear en todos los sectores de la sociedad, alineada a un marco legal que le permita al Estado comprender los riesgos, administrarlos y proteger a las personas y las redes al mismo tiempo que se genera una estrategia que lleve a Michoacán a ser punta de lanza en materia de ciberseguridad a nivel nacional al mejorar las capacidades de prevención y respuesta ante los incidentes que puedan comprometer la provisión de servicios y las actividades cotidianas de los usuarios.

Derivado de lo anterior es ineludible garantizar la seguridad de las Infraestructuras críticas y de información ya que su importancia se debe principalmente al papel que representan dentro de los procesos de provisión de servicios básicos, económicos, sociales, políticos y de seguridad del Estado de Michoacán.

Como resultado de lo anteriormente expuesto, surge la presente investigación con el propósito de realizar un diagnóstico en materia de ciberseguridad. Esta evaluación se plantea como un instrumento para el Estado de Michoacán, con el objetivo de establecer un marco que garantice la seguridad de los usuarios en el ciberespacio, partiendo de las siguientes preguntas de investigación.

1.1.1. Preguntas de la investigación

Pregunta General

¿De qué manera las tecnologías de la información y comunicaciones, aspectos legales, cibercultura, cibercrimen, infraestructuras críticas y seguridad de la información explican a la ciberseguridad en el Estado de Michoacán, en el año 2023?

Preguntas específicas

1. ¿De qué manera las tecnologías de la información y comunicaciones afectan la ciberseguridad en el Estado de Michoacán en el año 2023?
2. ¿En qué grado los aspectos legales afectan la ciberseguridad en el Estado de Michoacán en el año 2023?
3. ¿En qué medida la cibercultura impacta en la ciberseguridad en el Estado de Michoacán, en el año 2023?
4. ¿De qué manera incide el cibercrimen en la ciberseguridad en el Estado de Michoacán, en el año 2023?
5. ¿Cuál es la importancia de las infraestructuras críticas en la ciberseguridad en el Estado de Michoacán, en el año 2023?
6. ¿Cuál es el desempeño de la seguridad de la información en la ciberseguridad en el Estado de Michoacán, en el año 2023?

1.2. Objetivos de la Investigación

Como resultado de las preguntas anteriores a continuación se plantean los objetivos a los que se pretende llegar con la elaboración de la presente investigación.

Objetivo general

Diagnosticar de qué manera las tecnologías de la información y comunicaciones, aspectos legales, cibercultura, cibercrimen, infraestructuras críticas y seguridad de la información explican la ciberseguridad en el Estado de Michoacán, en el año 2023.

Objetivos específicos

1. Investigar de qué manera las tecnologías de la información y comunicaciones afectan la ciberseguridad en el Estado de Michoacán, en el año 2023.
2. Analizar en qué grado los aspectos legales afectan la ciberseguridad en el Estado de Michoacán en el año 2023.
3. Evaluar en qué medida la cibercultura impacta en la ciberseguridad en el Estado de Michoacán, en el año 2023.

4. Diagnosticar de qué manera incide el cibercrimen en la ciberseguridad en el Estado de Michoacán, en el año 2023.
5. Analizar la importancia de las infraestructuras críticas en la ciberseguridad en el Estado de Michoacán, en el año 2023.
6. Identificar cual es el desempeño de la seguridad de la información en la ciberseguridad en el Estado de Michoacán, en el año 2023.

1.3. Hipótesis

Existen elementos que deben ser incluidos en la generación de la política pública de ciberseguridad en el Estado de Michoacán.

Hipótesis general

Las tecnologías de la información y comunicaciones, los aspectos legales, la cibercultura el cibercrimen, las infraestructuras críticas y la seguridad de la información, son factores determinantes que deben ser incluidos en la política pública de ciberseguridad en el Estado de Michoacán en el año 2023.

Hipótesis específicas

1. Las tecnologías de la información y comunicaciones inciden de manera negativa en la ciberseguridad en el Estado de Michoacán, en el año 2023.
2. El perfeccionamiento de los aspectos legales puede impactar de manera positiva la ciberseguridad en el Estado de Michoacán, en el año 2023.
3. La cibercultura trasciende de manera positiva sobre la ciberseguridad en el Estado de Michoacán, en el año 2023.
4. El cibercrimen incide de manera negativa en la ciberseguridad en el Estado de Michoacán, en el año 2023.
5. Las infraestructuras críticas deben ser consideradas para el establecimiento de la política de ciberseguridad en el Estado de Michoacán, en el año 2023.
6. La seguridad de la información impacta de manera positiva a la ciberseguridad en el Estado de Michoacán, en el año 2023.

1.4. Justificación

En su conjunto las tecnologías de la información y comunicaciones han propiciado que muchos sectores de la economía y gobiernos basen su operación en el ciberespacio, el cual millones de personas lo utilizan como parte de su modo de vida actual para la comunicación, consulta de información, transacción en línea, operaciones financieras, educación, salud, entre otros.

Trascendencia.

Una Política Publica en ciberseguridad para el Estado de Michoacán, permitirá contar con un instrumento que guíe los esfuerzos realizados para el diseño e implementación de acciones, leyes,

programas, servicios y ejecución de recursos en materia de ciberseguridad a partir del reconocimiento de la importancia de las tecnologías de la información como factor determinante en la vida social, esto derivado del incremento de usuarios conectados y la utilización de estas herramientas para el desarrollo de sus actividades cotidianas; así como disminuir los riesgos asociados, los delitos cibernéticos y la creación de una cultura de ciberseguridad.

Conveniencia

El aumento no planeado en el uso de las tecnologías de la información y comunicaciones, así como el desconocimiento de los riesgos asociados a ellas, han traído como consecuencia; conductas que afectan la integridad personal, material o en los derechos de los usuarios, por lo cual resulta indispensable el contar con un instrumento que garantice su seguridad al navegar en el ciberespacio.

Relevancia Social

Está política pública permitirá a la sociedad michoacana disponer de una herramienta que les permita conocer las ventajas en el uso de las tecnologías de la información y comunicaciones, así como los riesgos asociados a su uso, convirtiéndose en un apoyo a padres de familia y jóvenes, con el fin de garantizar una inclusión libre de violencia en el manejo del ciberespacio.

Implicaciones prácticas

Una Política pública de ciberseguridad, que le permita hacer frente a las amenazas existentes en el ciberespacio, mitigando los riesgos asociados en el uso de las tecnologías de información, así como identificar las brechas en materia legislativa para regular y sancionar este tipo de conductas que se cometen en el ciberespacio.

Valor teórico

Con la presente investigación se fortalecerá el conocimiento teórico de las tecnologías de la información, brechas legislativas y el cibercrimen para la generación de una política pública de ciberseguridad en el Estado de Michoacán, con el fin de gestionar los riesgos asociados al uso del ciberespacio.

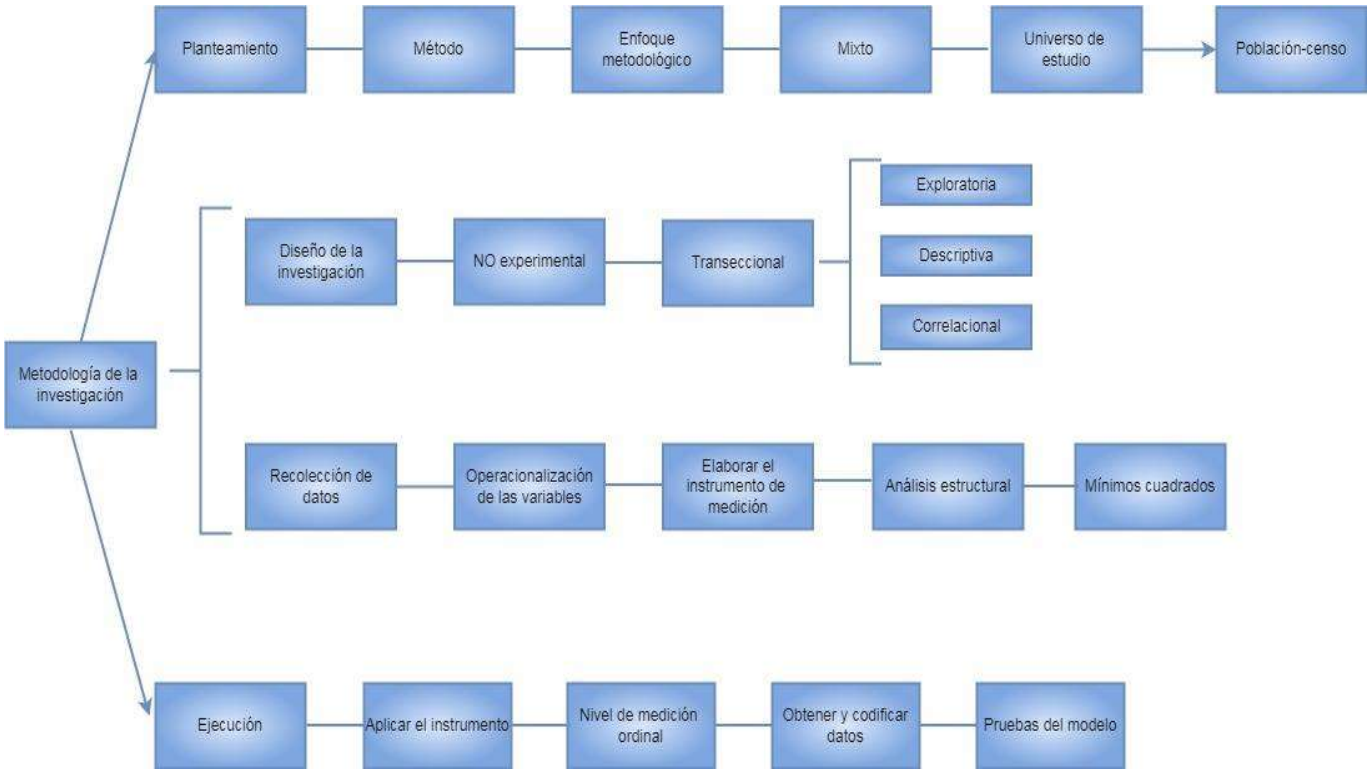
Utilidad Metodológica

La presente investigación permitirá proporcionar un enfoque estructurado para investigar, analizar y abordar los desafíos y riesgos relacionados con la ciberseguridad.

1.5. Método

Para el desarrollo de la presente investigación se emplea el método científico, a fin de garantizar la confiabilidad y veracidad de los resultados obtenidos, a partir de la recolección de datos cualitativos los cuales mediante un tratamiento matemático, permitirán poner a prueba las hipótesis planteadas en la presente investigación y cuyos resultados permitirán realizar una aproximación causal del fenómeno estudiado. La siguiente ilustración presenta la metodología a seguir en esta investigación.

Ilustración 2. Metodología de la investigación.



Fuente: Elaboración propia con base en Hernández et al. (2014).

El estudio actual se fundamenta en el empleo del método científico como base de la presente investigación. Tamayo y Tamayo (2004) lo define como un conjunto de pasos lógicos y procedimientos que se utilizan en la obtención de conocimiento verídico y comprobable del fenómeno objeto de estudio. Mientras que Bunge (2013) afirma que solo puede existir dentro del contexto de la ciencia, ya que el método científico es una parte integral de la actividad científica, en la adquisición de conocimiento por medio de técnicas especializadas para explicar la realidad.

De lo comentado en líneas anteriores se puede entender al método científico como una secuencia estructurada y organizada de etapas, que mediante la aplicación de principios, reglas y normas, buscan alcanzar el objetivo de la investigación y la validación de la hipótesis objeto de estudio.

Tipo de investigación

El enfoque de la investigación es mixto, ya que se combinaran los enfoques cualitativo y cuantitativo para la generación del conocimiento, ya que esto permite obtener una comprensión más amplia y profunda del fenómeno de estudio. En Hernández et al. (2010) Comprendido como una serie de etapas que se vale de la selección de datos de una muestra de la población para su posterior análisis, a través de un tratamiento matemático en la comprobación del hecho estudiado, mientras que en Tamayo y Tamayo (2004) nos refiere que es el contrapunto que un investigador puede realizar entre las diversas teorías actuales, tienen estrecha relación con las hipótesis que derivan de estas, ya que nos arrojan información importante para la realización de un muestreo al azar, pero siempre con el enfoque de aquella población o fenómeno social, en todo momento la investigación de tipo cualitativo y por tanto el investigador se vale para la obtención de información de distintos medios para el estudio del fenómeno a describir.

En tal sentido, mediante la recolección de datos se probarán las hipótesis planteadas utilizando mediciones numéricas y análisis estadísticos, lo que proporcionará un enfoque cuantitativo. Asi mismo, estos datos se contrastarán y complementarán mediante la recolección de información cualitativa que describa el fenómeno estudiado.

Diseño de la investigación

Por consiguiente el tipo de investigación es de tipo no experimental. Hernández et al. (2010) Explica que en este tipo de investigación no existe manipulación alguna sobre las variables de estudio, si no que se observa el fenómeno a explicar en su ambiente natural para un posterior estudio, a partir de hechos ya existentes, que permitan explicar las variables y su incidencia sin la manipulación del investigador. El diseño es de corte transeccional debido a que la recolección de datos será en un único momento, este diseño de divide en tres tipos:

Exploratorios: existen fenómenos limitados en cuanto a exploración, por lo que el investigador tiene que sumergirse y ser parte de todo el contexto relacionado con los mismos, para con ello cumplir con el fin deseado de recolectar todo lo conducente para su investigación, partiendo de una problemática y generando a través de todo un proceso un nuevo conocimiento

Descriptivos: Los fenómenos que derivan de esta investigación tienen que ser detallados y definidos a través del análisis, para con ello tener un fácil manejo y adecuada comprensión de las variables.

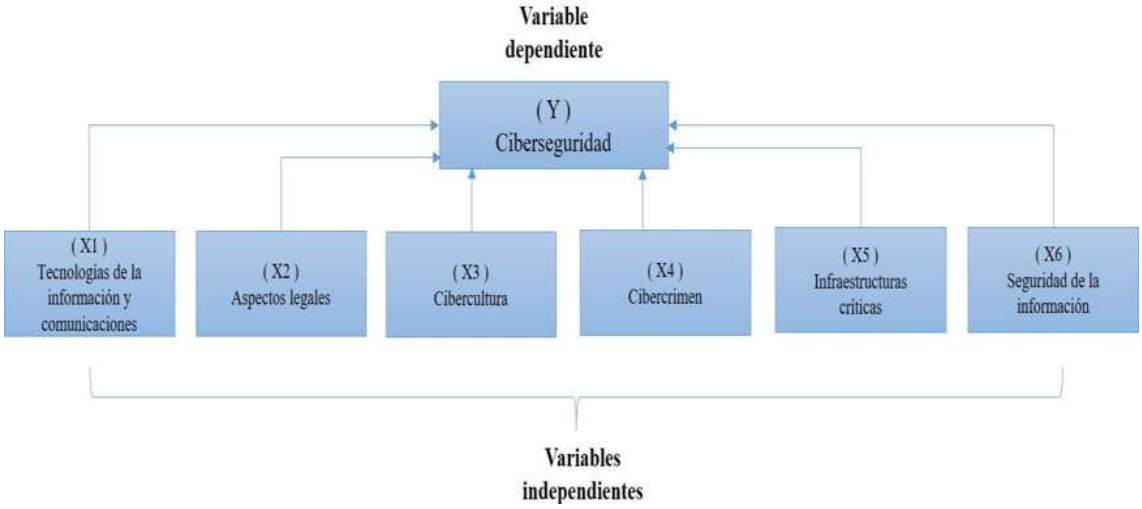
Correlacionales: El investigador tiene la capacidad de relacionar sus variables, lo que impacta directamente en la comprensión del fenómeno objeto de estudio. Esto proporciona mayor claridad y practicidad y puede revelar la dependencia entre causa y efecto.

Por lo cual el tipo de alcance en esta investigación será de tipo exploratorio ya que se intentará explicar un fenómeno poco explorado como lo es la Ciberseguridad, para lo cual se detallarán las distintas características que conformarán la política pública de ciberseguridad, por otra parte de tipo descriptivo ya que definirá las propiedades y variables que conforman el estudio observado para facilitar la construcción del nuevo conocimiento y de manera correlacional cuyo principal objetivo es describir y analizar la correlación entre las tecnologías de la información y comunicaciones, los aspectos legales, la cibercultura, el cibercrimen, las infraestructuras críticas y la seguridad de la información en la generación de dicha política.

1.6. Identificación de variables

La identificación de variables adquiere una importancia crucial en cualquier investigación, ya que focaliza la atención en los aspectos específicos a investigar y contribuye a la construcción de dimensiones e indicadores que facilitan la descripción de los fenómenos bajo análisis y la realización de análisis de correlación de sus componentes diversos. En el contexto de este estudio, se ha decidido seleccionar las variables Tecnologías de la información y comunicaciones, Aspectos legales, Cibercultura, Cibercrimen, Infraestructuras críticas y Seguridad de la información. La elección de estas variables se fundamenta en la literatura consultada. En la ilustración siguiente, se presenta una representación visual de dichas variables.

Ilustración 3. Identificación de variables.



Fuente: Elaboración propia con base en la literatura revisada, 2023.

CAPÍTULO 2. MARCO REFERENCIAL Y CONCEPTUAL DE LA CIBERSEGURIDAD

En esta sección, se explora el marco de referencia y el enfoque conceptual, que engloba los conceptos primordiales relacionados con la ciberseguridad y los factores que la refuerzan o debilitan. Además, se identifican aquellos elementos que pueden ser tratados como herramientas de política pública en este ámbito.

2.1. Ciberseguridad

La ciberseguridad al igual que otros conceptos teóricos de reciente creación ha sido definida de diferentes formas por diferentes autores, por ejemplo para Estrada (2017) esta es la encargada de salvaguardar los activos de información que se procesan, almacenan y que viajan por la infraestructura tecnológica debido a la interconexión en el ciberespacio, la cual está expuesta a riesgos y amenazas. Por otro lado, la Unión Internacional de Telecomunicaciones (2010) la define como un conjunto de instrumentos, políticas, controles de seguridad, procedimientos de gestión de riesgos, capacitación, buenas prácticas y tecnologías que permitirán resguardar los activos de información y a la vez brindar un entorno de navegación seguro a los usuarios. Igualmente Santos (2019) nos presenta el concepto como las medidas de protección de la información a través de prevenir, detectar y ser proactivos a las amenazas y finalmente McKinsey y Company (2018) la describe como el total de acciones encaminadas a reducir los riesgos en el ciberespacio y con ello disminuir los ataques, para lo cual dispone de una infraestructura tecnológica y mejores prácticas de seguridad de la información.

De esta manera sintetizando los principales elementos que pudiesen ser compatibles entre sí, los autores destacan la importancia de salvaguardar los activos de información, a través de diferentes prácticas, mecanismos, políticas, guías de buenas prácticas para brindar un entorno de navegación seguro a los usuarios en el ciberespacio.

2.1.1. Política púbica

Para Aguilar (2010) quien define a la política como la traducción de las prioridades y principios políticos del gobierno a través de programas, con el objetivo primordial de satisfacer las necesidades de la sociedad, para lo cual es necesario conocer dichas necesidades a través de la participación de los ciudadanos, para con ello dar acomodo jerárquico y real a cada conflicto social, auxiliándose de diversas teorías y modelos, así como de métodos que intentaran definir de manera adecuada un problema que previamente se incorporó a la agenda de gobierno y que es de interés público y por

tanto se busca la creación, rediseño posterior implementación de políticas públicas, buscando erradicarlo o tener un control sobre este.

Según Laswell (2017), son planes destinados a dar respuesta a problemas sociales, tomando como base el trabajo interdisciplinario y dinámico, el cual resulta fundamental para el éxito de las políticas, ya que los múltiples actores interdisciplinarios abordaran desde su perspectiva aquellas demandas sociales, en la resolución de problemas a través del análisis de estos y elaborando políticas públicas idóneas para atacar el problema.

Para Velásquez (2009) "la política pública es un proceso integrador de decisiones, acciones, inacciones, acuerdos e instrumentos, adelantado por autoridades públicas con la participación eventual de los particulares, y encaminado a solucionar o prevenir una situación definida como problemática. La política pública hace parte de un ambiente determinado del cual se nutre y al cual pretende modificar o mantener".

Es así que se define a la Política Pública como aquellos planes de acción específicos implementados a través de proyectos o actividades, que conjunta el actuar del gobierno con la ciudadanía, buscando definir y dar solución por medio de un estudio minucioso así como de una serie de pasos definidos para resolver un problema público.

2.1.2. Ciberseguridad y Política pública.

El mundo actual se caracteriza por su creciente interconectividad, que permite el acceso a una amplia gama de información. Sin embargo, esta interconexión también trae consigo riesgos en el ciberespacio que pueden trascender del ámbito virtual al real. Desde la simple sustracción de datos hasta fraudes, suplantación de identidad, extorsiones, ataques de denegación de servicios, ataques de ingeniería social, entre otros, estos riesgos han motivado a diferentes naciones a adentrarse en el ámbito cibernético. Este quinto espacio requiere una consolidación de capacidades técnicas y tecnológicas en cada país, con el objetivo de salvaguardar al Estado de las amenazas cibernéticas. En este contexto, es imperativo analizar los avances logrados por las principales potencias que reconocen la vital importancia de asegurar la ciberseguridad. Estas naciones han diseñado y aplicado políticas y estrategias de ciberseguridad para abordar esta problemática de manera efectiva.

2.1.2.1. Principales países que han implementado políticas de ciberseguridad.

2.1.3.1.1 República de Estonia

En el año 2007 los ciberataques de denegación de servicios paralizaron las actividades en la República de Estonia durante los meses de abril y mayo, debido a la recubicación de un monumento sovietico

al centro del Tallin, la capital de la República de Estonia. Estos ataques afectaron a varias Instituciones gubernamentales, infraestructura digital del sistema financiero, medios de comunicación y sitios web, a consecuencia de esto, se experimentaron interrupciones en los servicios de comunicación y conectividad lo que le impidio al Gobierno de Estonia difundir información y comunicarle al mundo lo sucedido. Estos ataques fueron vistos como los primeros en los que se vieron afectadas las tecnologias de la información y comunicaciones de dicho país, de forma simultanea páginas gubenamentales, aplicativos del sistema financiero y de medios de comunicación, considerados infraestructuras criticas de una nación. Desde entonces los ataques cibernéticos son una amenazas constante a nivel mundial, resaltando con esto la importancia de la ciberseguridad y lo que ha obligado a muchos países al fortalecimiento de sus capacidades.

Por lo antes comentado, la República de Estonia ha fortalecido la seguridad en el ciberespacio, a partir de reconocer el carácter interdisciplinario de la ciberseguridad y la involucran en su seguridad nacional, lo que dio paso a crear la primera ciberestrategia a nivel mundial en el año 2008. En su última versión, La Estrategia de Ciberseguridad 2019-2023 (2020), refleja la visión en materia de ciberseguridad, a través de objetivos, metas y prioridades, involucrando a los actores y áreas estratégicas del gobierno de manera legal e imperativa, no solo protegiendo el desarrollo tecnológico, si no a la sociedad civil, dado que desempeñan un papel esencial en la ciberseguridad, como una responsabilidad compartida entre todos, con el objetivo de asegurar el logro de resultados exitosos.

Como consecuencia de los ataques ocurridos en el año 2007, Estonia ha fortalecido su defensa nacional, reconociendo el liderazgo del país en defensa cibernética, con el establecimiento del Centro de Excelencia de Defensa Cibernética de la OTAN en Tallin, colocando a la República de Estonia a nivel mundial como el país líder en ciberseguridad. Pessino (2017) menciona que La República de Estonia incursiono en el mundo tecnológico desde la década de los años 60´s, siendo un país en el que su economía está basada en la digitalización, debido a la interconexión y compatibilidad de sus sistemas e información, siendo el primer país digital del mundo. De lo anterior se advierte que la ciberseguridad se convirtió en un aspecto integral de su seguridad.

El siguiente mapa mental modela la Estrategia de La República de Estonia, la cual a través de cuatro objetivos garantiza la defensa de su ciberespacio ante diversas amenazas externas.

Mapa mental 1. Estrategia de ciberseguridad de Estonia.

Estrategia de Ciberseguridad Estonia

Principios:

- ✓ La protección y promoción de los derechos y libertades fundamentales es tan importante en el ciberespacio como en el entorno físico.
- ✓ La ciberseguridad es un facilitador y amplificador del rápido desarrollo digital de Estonia, que es la base del crecimiento socioeconómico de Estonia.
- ✓ Las soluciones criptográficas son de gran importancia para Estonia, ya que garantizan la seguridad y son la base de su ecosistema digital.
- ✓ La transparencia y la confianza ciudadana son fundamentales para la sociedad digital, basada en el principio de comunicación abierta.

Fortalezas de Estonia en ciberseguridad.

- ✓ Arquitectura básica segura para la sociedad digital de Estonia.
- ✓ Un nivel de madurez probado.
- ✓ Eficiencia y flexibilidad típicas de un país más pequeño.
- ✓ Influencia internacional.
- ✓ Gran confianza entre los usuarios finales.

Amenazas que afectan la ciberseguridad.

- ✓ Incremento del uso de las TIC´s, creciente dependencia digital y aparición de nuevas tecnologías.
- ✓ Ciberdelincuencia creciente, variable y basada en servicios.
- ✓ Situación de seguridad complicada.
- ✓ Autonomía tecnológica limitada.
- ✓ Globalización y debate sobre ciberseguridad.
- ✓ Entorno legal cada vez más completo para los participantes del mercado.
- ✓ Desafíos que plantea la libertad en Internet.

Coordinación nacional de ciberseguridad y organización de la gestión.

- ✓ Ministerio de Economía y Comunicaciones.
- ✓ Ministerio de Educación e Investigación.
- ✓ Ministerio de Justicia.
- ✓ Ministerio de Defensa.
- ✓ Junta de Policía y Guardia de Fronteras y Servicio de Seguridad Interna.
- ✓ Centro de Desarrollo y Tecnología de la Información del Ministerio Interior.
- ✓ Ministerio de Relaciones Exteriores.
- ✓ Ministerio de Finanzas.
- ✓ Banco de Estonia.
- ✓ Oficina de Gobierno.
- ✓ Centro de Excelencia de Ciberdefensa cooperativa de la OTAN.
- ✓ Universidades, Instituciones de investigación y el sector privado.

Objetivos estratégicos y áreas de actividad

Sociedad digital sostenible.

1. Resiliencia tecnológica.
2. Gestionar y estar preparado para crisis, ataques e incidentes.
3. Liderazgo integral sobre el terreno y una comunidad cohesionada.

Industria, investigación y desarrollo de la ciberseguridad.

1. Apoyar y promover la I + D en ciberseguridad y la empresa basada en la investigación.
2. Aprovechar la cooperación productiva entre el sector privado, estado y academia.
3. Preparación de un plan de I + D en ciberseguridad a nivel nacional que defina áreas de enfoque prioritario para el estado.
4. Apoyo a la generación de innovación y potencial exportador.
5. Garantizar un entorno propicio para el inicio y desarrollo de start-ups.

Principal contribuyente internacional

1. Hacer más eficaz la cooperación con los socios estratégicos extranjeros.
2. Promoción internacional de la capacidad cibernética sostenible.

Sociedad ciber-alfabetizada.

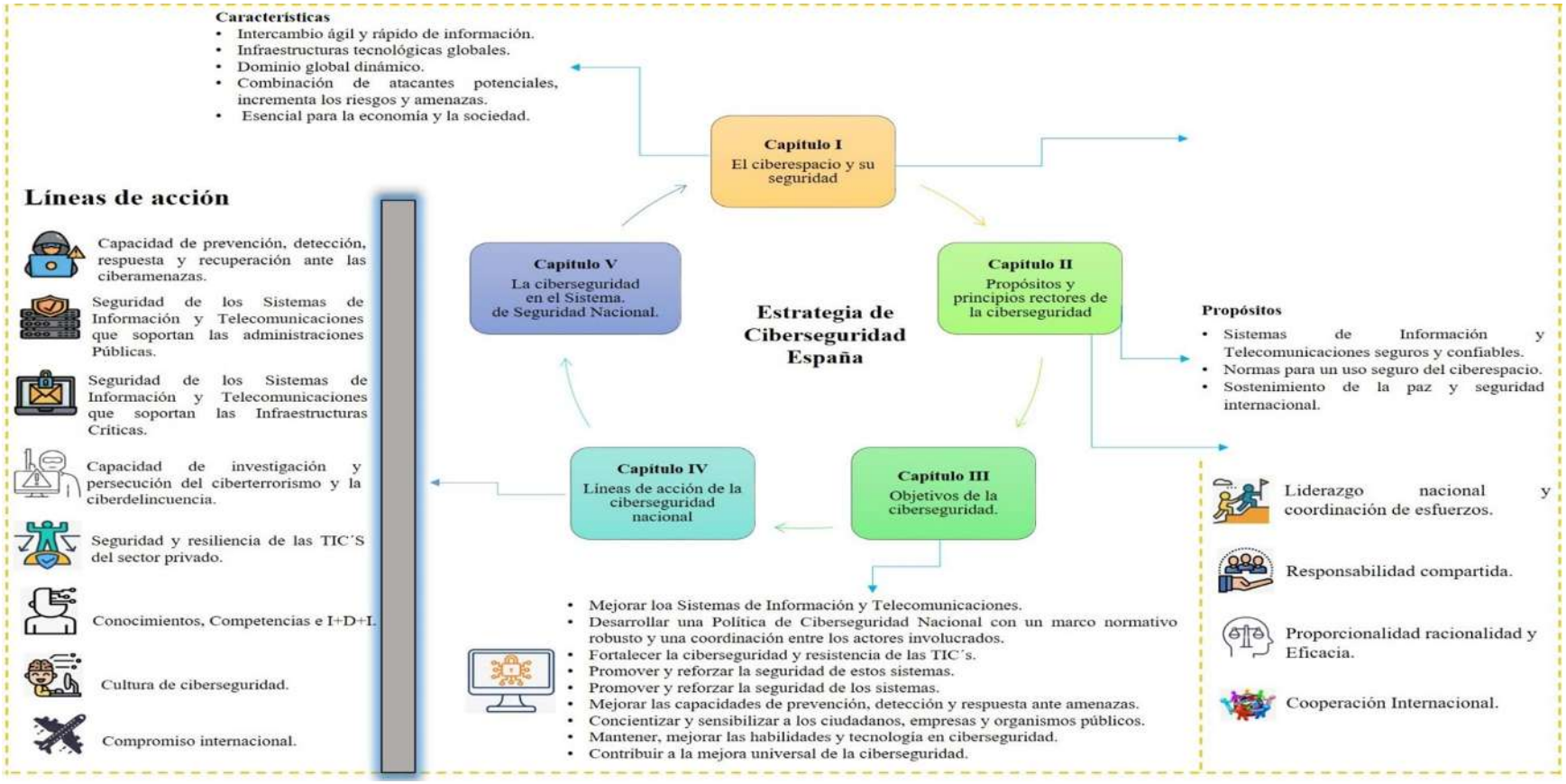
1. Sensibilizar a la ciudadanía, el estado y el sector privado.
2. Desarrollar el talento correspondiente a la demanda estatal y del sector privado.

Fuente: Elaboración propia con base en la Estrategia de Ciberseguridad de la República de Estonia (2020).

2.1.3.1.2 España

En el año 2019, el gobierno de España publica la segunda versión de su Estrategia de Seguridad Nacional (2019) en el marco de la Política de Seguridad Nacional, fijando su posición para hacer frente a las ciberamenazas y a las cambiantes condiciones en el ciberespacio, con el fin de poner en práctica de manera ordenada mecanismos de protección, detección, localización, respuesta oportuna y eficiente a las actividades que son soportadas y desarrolladas en el entorno digital. En el siguiente mapa mental, se plasma la Estrategia, estableciendo cinco capítulos de actuación.

Mapa mental 2. Estrategia de Ciberseguridad España.

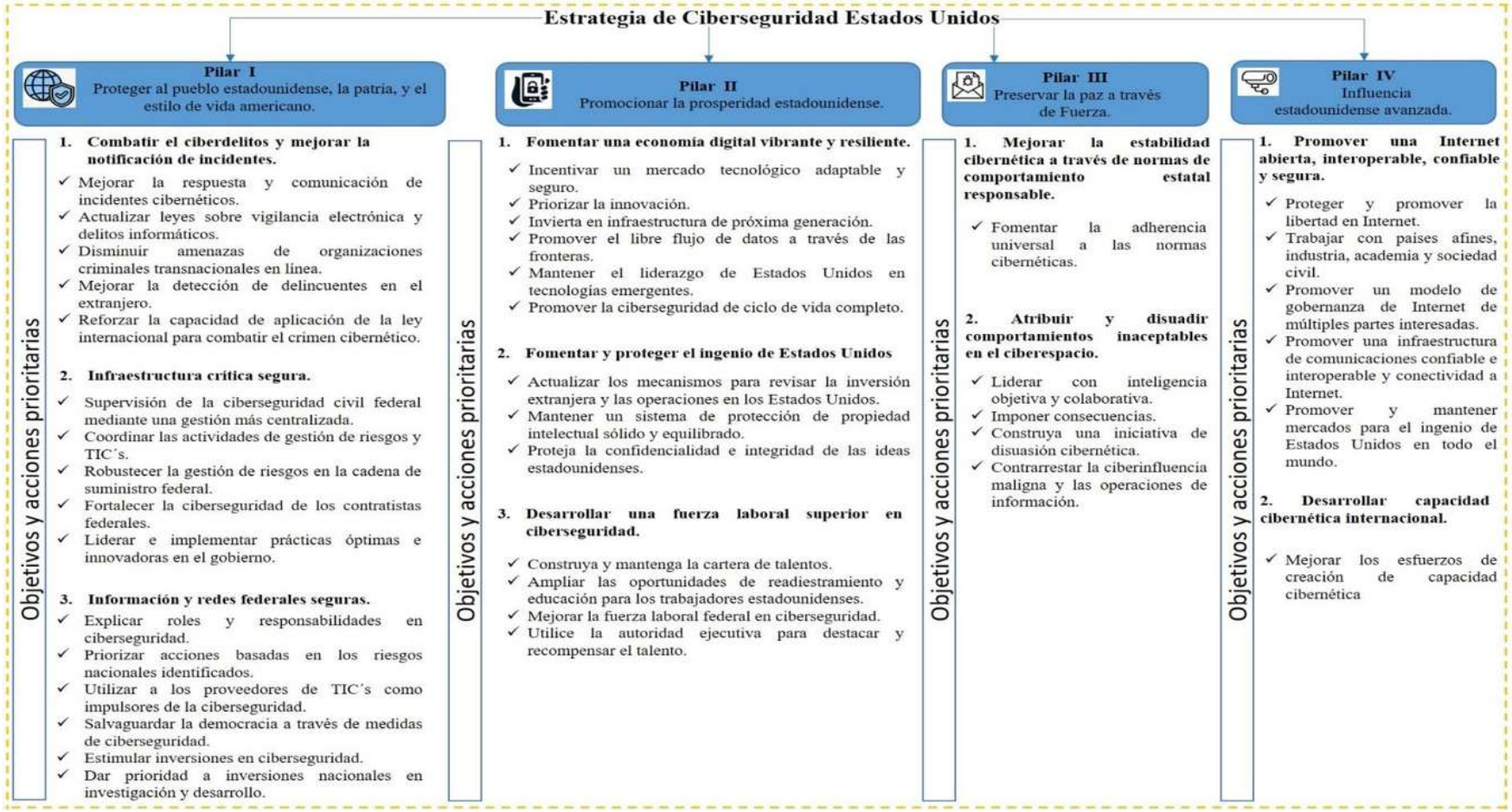


Fuente: Elaboración propia con base en la Estrategia de Ciberseguridad del Gobierno de España (2019).

2.1.3.1.3 Estados Unidos de América.

En el año 2018, el Gobierno de Estados Unidos de América presenta su Estrategia Cibernética Nacional (2018) para facilitar y robustecer las capacidades en materia de ciberseguridad, defensa de riesgos y amenazas cibernéticas. El siguiente mapa mental 3 muestra la estructura integrada por cuatro pilares para hacer frente a los ataques cibernéticos.

Mapa mental 3. Estrategia de Ciberseguridad Estados Unidos.

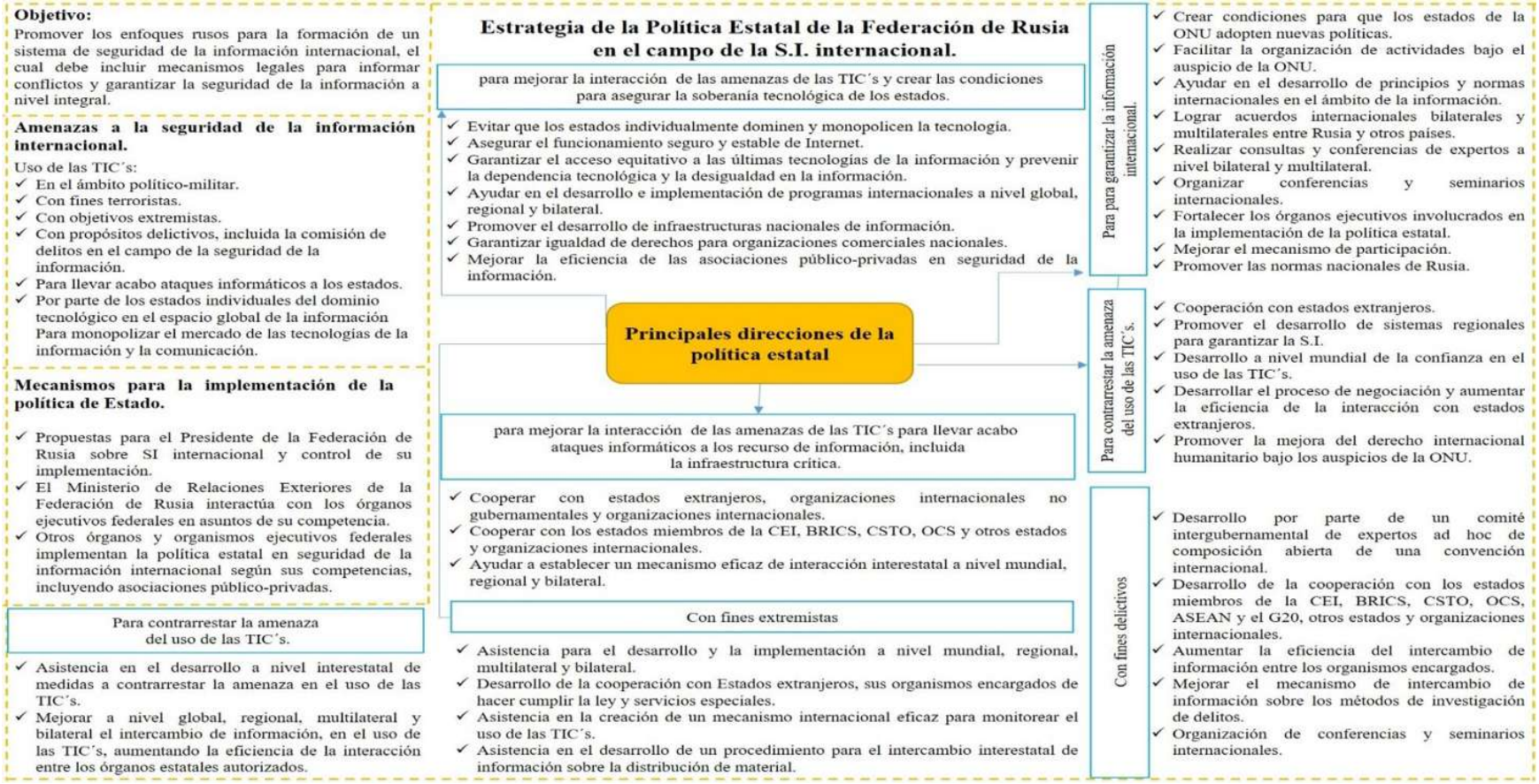


Fuente: Elaboración propia con base en la Estrategia de Ciberseguridad del Gobierno de Estados Unidos de América (2018).

2.1.3.1.4 Rusia

Su estrategia denominada Política estatal de la Federación de Rusia en el campo de la seguridad de la información internacional, tiene como objetivo promover un conjunto de directrices basadas en los intereses nacionales del Gobierno, para asegurar la seguridad de la información a nivel internacional y prevenir riesgos, amenazas y ataques en el ciberespacio. (2021). Las principales direcciones de esta política estatal están basados en seis ejes los cuales se modelan en el siguiente mapa mental:

Mapa mental 4. Política Estatal de la federación Rusia en el campo de la seguridad de la información internacional.



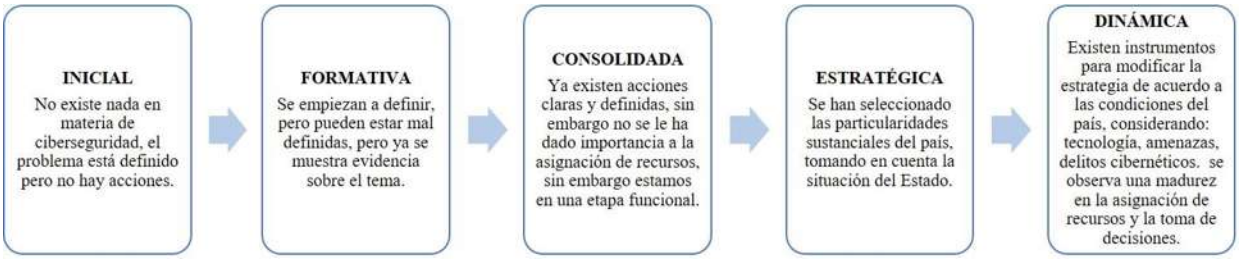
Fuente: Elaboración propia con base en la Política Estatal de la Federación Rusa (2021).

2.1.3.2 Concepto de política pública de ciberseguridad en América Latina

América Latina ha creado el Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM), desarrollado conjuntamente por la Organización de los Estados Americanos (OEA), el Banco Interamericano de Desarrollo (BID) y la Universidad de Oxford en el año 2013, instrumento que evalúa las capacidades en materia de Ciberseguridad en cada país, actualmente 32 países forman parte de esta estrategia, con el objetivo de crear un enfoque a nivel internacional y armonizado sobre una visión estratégica de ciberseguridad, en una actividad de aprendizaje de las mejores prácticas y experiencias de los diferentes países miembros, siendo un documento dinámico, vivo y cambiante, perfectible en cada revisión (Lewis, 2016)**.**

El modelo define cinco niveles, para conocer el estado de desarrollo, los cuales se identifican en: inicial, formativo, establecido, estratégico y dinámico, en la siguiente ilustración de describen de manera más detallada:

Ilustración 4. Niveles de Madurez de las capacidades de Ciberseguridad.



Fuente: Elaboración propia con base en el Banco Interamericano de Desarrollo 2020.

A su vez dichos niveles de madurez, se analizan en cinco dimensiones las cuales proporcionan un panorama sobre las categorías específicas que se evalúan para determinar las capacidades en materia de ciberseguridad de los países participantes, de acuerdo a los siguientes indicadores:

Tabla 2. Dimensiones de los niveles de ciberseguridad.

Dimensión 1 Política y estrategia de ciberseguridad.	Dimensión 2 Cultura cibernética y sociedad.	Dimensión 3 Formación, capacitación y habilidades de seguridad cibernética.	Dimensión 4 Marcos legales regulatorios.	Dimensión 5 ndares, organizaciones y tecnologías.
D1.1 Estrategia nacional de ciberseguridad.	D2.1 Mentalidad de ciberseguridad.	D3.1 Sensibilización.	D4.1 Marcos legales.	D5.1 Adhesión a los estándares.
D1.2 Respuesta a incidentes.	D2.2 Confianza y Seguridad en Internet.	D3.2 Marco para la educación.	D4.2 Sistema de Justicia Penal.	D5.2 Resiliencia de infraestructura de internet.
D1.3 Protección de infraestructura critica.	D2.3 Comprensión del usuario de la protección de información personal en línea.	D3.3 Marco para la formación profesional.	D4.3 Marcos de cooperación formal e informal para combatir el delito cibernético.	D5.3 Calidad del software.
D1.4 Gestión de crisis.	D2.4 Mecanismos de presentación de informes.			D5.4 Controles técnicos de seguridad.
D1.5 Defensa cibernética.	D2.5 Medios y redes sociales.			D5.5 Controles criptográficos.
D1.6 Redundancia de comunicaciones.	D1.6 Redundancia de comunicaciones.			D5.6 Mercado de ciberseguridad.
				D5.7 Divulgación responsable.

Fuente: Elaboración propia con base en el Banco Interamericano de Desarrollo 2020.

Por otra parte el Banco Interamericano de Desarrollo (2020) establece que cada dimensión a su vez se subdivide en factores que representan la capacidad en ciberseguridad de manera que se trata de incluir todos los componentes en su conjunto para mejorar la calidad y precisión del modelo, siendo perfectibles en cada revisión, con esto se fortalece el modelo ya que es un instrumento dinámico que permite la mejora continua, de igual manera estos factores se transforman en indicadores y a su vez en acciones a implementar que permitirán identificar el progreso obtenido en cada etapa, reflejando el estado mundial de la Ciberseguridad.

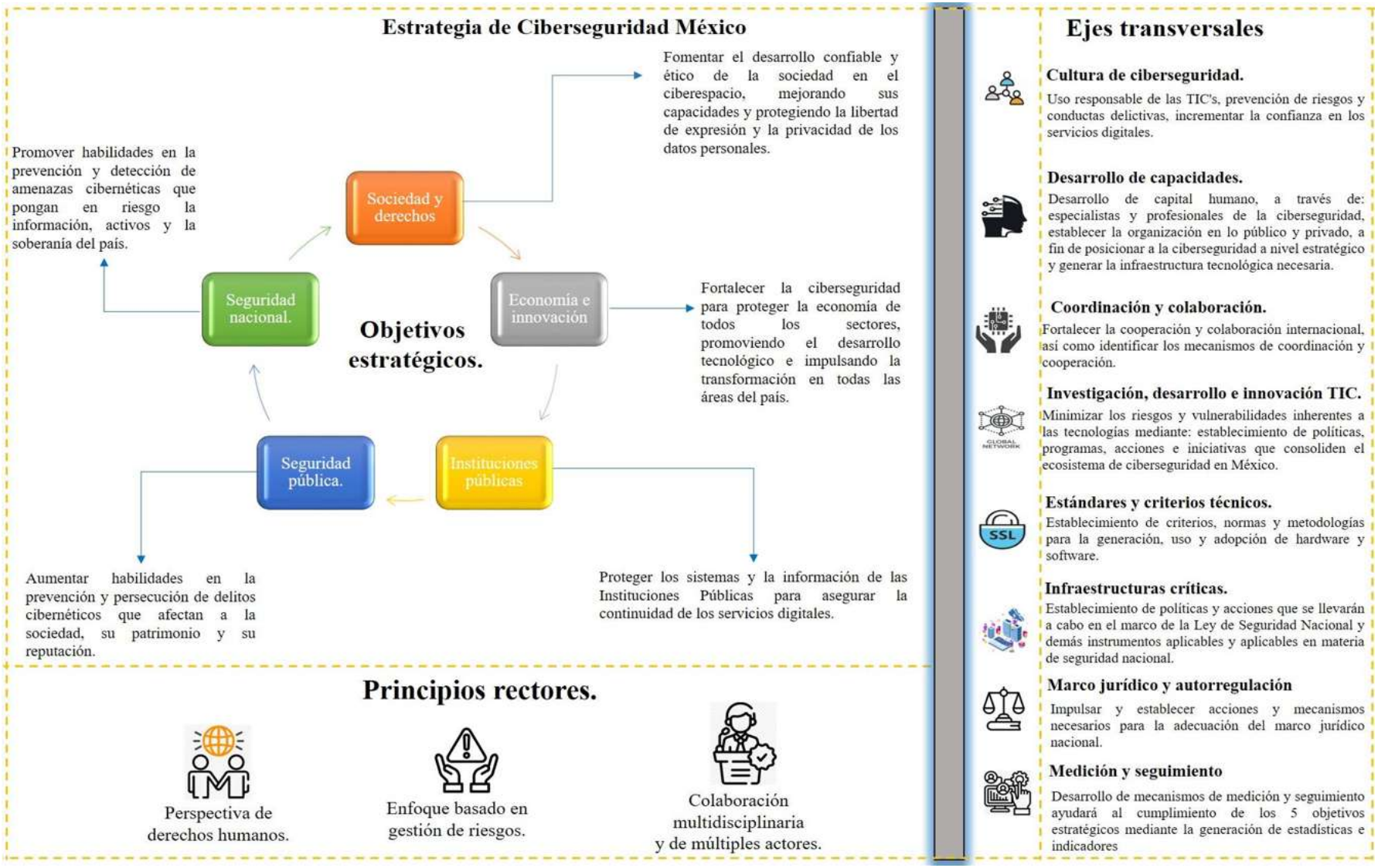
Es así que en esta investigación se toma como referencia el Modelo de Madurez de Capacidad de Seguridad Cibernética, con el fin de evaluar las capacidades de las Tecnologías de la información y comunicaciones, Aspectos legales, Cibercultura, Cibercrimen, Infraestructuras críticas y Seguridad de la información, proporcionando una evaluación estructurada y un marco para el desarrollo continuo en materia de ciberseguridad.

2.1.3.3 Estrategia Nacional de ciberseguridad en México

En el año 2017 y durante la administración del expresidente Enrique Peña Nieto, se realizó un esfuerzo por generar una estrategia nacional de ciberseguridad. Este escrito que refleja la perspectiva del Gobierno Mexicano para afrontar los retos tecnológicos en materia de ciberseguridad, a partir del surgimiento de las TIC´s como vehículo para el desarrollo político, económico, social y cultural de la nación. Este esfuerzo se vio impulsado por el incremento de internautas y su interconectividad en el ciberespacio, reconociendo los riesgos existentes asociados a su utilización en la navegación. La estrategia también subraya las importancia de contar con una cultura de ciberseguridad que permita al Gobierno, ciudadanos y sector privado enfrentar las amenazas actuales y futuras, de igual manera se planteó la necesidad de fomentar la colaboración y el intercambio de información para fortalecer la ciberseguridad a nivel global (Gobierno de la República, 2017).

El siguiente mapa mental refleja la visión del Estado mexicano en la problemática presentada a través de cinco objetivos, ejes transversales y principios rectores, con la finalidad de hacer frente a esta era digital y los restos tecnológicos que implica esta hiperconectividad en el ciberespacio.

Mapa mental 5. Estrategia de Ciberseguridad México.



Fuente: Elaboración propia con base en la Estrategia de Ciberseguridad de México (2017).

Por otra parte el informe de Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe desarrollado por la OEA y el BID, califico a México en un nivel de madurez de dos (nivel formativo) en el aspecto de: Cultura cibernética y sociedad; y en el de Formación, capacitación y habilidades de seguridad cibernética donde refleja que el Estado debe enfocarse en la creación de una estrategia en la formación de los ciudadanos dada la mayor inmersión en el uso de las TIC´s, así como la conformación de una cultura digital. Por otra parte menciona que la formación y especialización en el campo educativo y capacitación en ciberseguridad (hábitos seguros, capacitación, y habilidades), permitirá la navegación en el internet de forma segura, confiable y la preparación de la ciudadanía ante los riesgos cibernéticos (Banco Interamericano de Desarrollo, 2020).

En este sentido la valoración del BID (2020) calificó a México en un nivel tres de madurez (consolidado) en la dimensión Marcos legales regulatorios. Este avance refleja el avance de México en esta área, con la legislación tanto a nivel federal como estatal. Un ejemplo destacado es; la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y la Ley General de Protección de Datos Personales en Posesión de Particulares (LGPDPPP), Reformas legislativas orientadas a reconocer la violencia digital, utilizando a los dispositivos como medios para la comisión de diversos delitos, donde se hace esencial y primordial trabajar en la homogenización de un código penal único para las treinta y dos entidades federativas.

En lo que respecta a la dimensión Política y estrategia de ciberseguridad, el BID (2020) informa que México ha avanzado de un nivel formativo a uno consolidado (valor de madurez de dos a tres), en la creación de una Estrategia de ciberseguridad, haciendo referencia que en el primer reporte del BID 2016, México no contaba con una estrategia, sino hasta finales del año 2017 cuando se publica, pero se observa que no se ve reflejado en los demás indicadores, los cuales debería de mostrar un avance significativo de la estrategia, situación que no se ve reflejada ya que al ser un documento dinámico, a la fecha no cuenta con actualizaciones y , no se le ha dado el impulso necesario, solo ha quedado en papel sin que se traduzca en una política de estado con el reconocimiento del Gobierno, sector empresarial y sociedad en general, por lo que en la actualidad en México no se cuenta con una Política pública en materia de ciberseguridad.

La cámara de Senadores (2021), a través del boletín número-1244, exhorto al poder Ejecutivo a informar sobre los avances de la estrategia de ciberseguridad a través de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE). Esta solicitud se realizó en respuesta al incremento de los delitos cibernéticos, remarcando la necesidad de mantener al país actualizado y protegido frente a las amenazas digitales.

Por consiguiente se observa que la ciberseguridad se ha convertido en una prioridad a nivel mundial, dada la interconectividad y a las grandes cantidades de información que fluyen en el ciberespacio por diferentes canales de comunicación, las redes informáticas, los sistemas y las infraestructuras críticas, las cuales son necesarias para las actividades cotidianas de las sociedades, motivo por el cual se debe realizar una gestión adecuada para protegerse de las amenazas en el ciberespacio.

En tal sentido y dados los principales ataques informáticos, como pueden ser desde un simple robo de datos, suplantación de identidad, redes comprometidas, fugas de información; y aceptando que, las acciones de los ciberatacantes tienen mayores consecuencias en el mundo real, convirtiéndose la ciberseguridad como una prioridad para los diferentes Gobiernos, empresas privadas y sociedad civil, lo que se ve reflejado en la creación de estrategias o Políticas que muestran la visión estratégica, a través de enfoques y principios para gestionar los riesgos de acuerdo a las prioridades de cada nación, desde la privacidad de los datos, protección a la infraestructura critica o la seguridad de la información.

Dado el planteamiento del problema y el presente marco teórico y conceptual de las Políticas de Ciberseguridad, la presente investigación retomara aquellos elementos que sean más congruentes con el contexto político, económico, social, cultural y tecnológico del Estado de Michoacán, los cuales se abordarán en los siguientes apartados.

2.2 Tecnologías de la información y comunicaciones

Vergara y Huidobro (2016) mencionan que a finales del siglo XIX y principios del siglo XX surgieron una serie de invenciones e innovaciones que han modificado radicalmente las formas de relacionarse y de vida. Estas transformaciones incluyeron el desarrollo de conceptos como la informática, las computadoras, las pantallas, las comunicaciones móviles, espaciales, internet y redes sociales, por lo cual mostraremos a través de una línea de tiempo los avances más significativos que anteceden a la conceptualización del termino TIC´s.

La siguiente línea de tiempo muestra a través de una evolución tecnológica las necesidades que el hombre ha tenido siempre a lo largo de su historia, buscando la simplificación de sus actividades y hacerlas más rápidas y eficientes, incluso aquellas que eran repetitivas. Es así que en el año 300–500 A.C. nace el ábaco como el primer instrumento de conteo, posteriormente vemos en Barceló (2008) que en el año 1822 se crea la primera máquina analítica con Charles Babbage la cual trabajaba con tarjetas perforadas que calculaban secuencias de números. Posteriormente, Vergara y Huidobro (2016), manifiestan que en el año 1854 se realiza la primera transmisión entre dos puntos con el telégrafo como el primer dispositivo, el cual a través de impulsos eléctricos enviaban señales para transmisiones de información a distancia y años más

tarde se crea la televisión en el año 1925 con la transmisión de imágenes y voz a través del espectro electromagnético, podemos observar que en estos años ya se utilizaban los conceptos: comunicación, imágenes e informática.

Con el paso del tiempo los avances tecnológicos fueron avanzando, siendo más optimizados y perfeccionados, describe Villar (2006) las cinco generaciones de computadoras, que muestran los adelantos en materia de informática, comunicaciones y software; la primera generación (1940-1952) trabajaban con bulbos al vacío y tarjetas perforadas, una de las más importantes era la Universal Automatic Computer I (UNIVAC I), la cual fue utilizada en las elecciones de los Estados Unidos de América en el año 1952, eran grandes, lentas en su funcionamiento y costosas por su tamaño. La segunda generación (1952-1964) se caracterizó por la sustitución de los bulbos al vacío por los transistores, reduciendo su tamaño y aumentar su velocidad de desempeño. Durante este periodo se desarrollaron capacidades de almacenamiento y surgieron conceptos clave como el software, los lenguajes de programación y las aplicaciones.

Por otra parte en la tercera generación (1964-1971) los transistores fueron sustituidos por circuitos integrados que combinaban diversos componentes electrónicos, como transistores y condensadores. Esto resulto en una mayor efectividad en el procesamiento, una velocidad superior, reducción en el tamaño de los dispositivos y el uso de chips para el almacenamiento. Aquí nace la multiprogramación, surgen empresas dedicadas al desarrollo de software. Al mismo tiempo podemos observar diferentes innovaciones. De acuerdo con Barceló (2008) quien explica que en el año de 1969 se crea ARPANET (Advanced Research Projects Agency Network) como un proyecto de investigación del Gobierno para fines militares, con la finalidad de fortalecer las comunicaciones en diferentes bases militares, posteriormente permitió la conexión de universidades situadas en diferentes puntos geográficos, de este proyecto surge Internet que permitió la interconexión de diferentes equipos de cómputo a través del protocoló de comunicación TCP/IP.

Además, la cuarta generación (1971-1981) se identifica por el reemplazó de los circuitos integrados por los microprocesadores reduciendo a escala los componentes tecnológicos, micro miniaturización de los circuitos electrónicos, se producen las memorias, las primeras computadoras personales y súper computadoras. Por otra parte Vergara (2016) destaca que en el año 1971 con el surgimiento del servidor de correo, desarrollo informático que permitió él envió, gestión y recepción de mensajes por medio de redes de comunicación, con el fin de mantener enlazados a los usuarios en distinto puntos. En lo que concierne a canales de comunicación Ibarra y Serrano (1999) mencionan que el primer enlace telefónico

por fibra óptica se dio en el año 1977, tecnología que emplea haces de luz para él envió de información con velocidades de transmisión muy altas y eficientes.

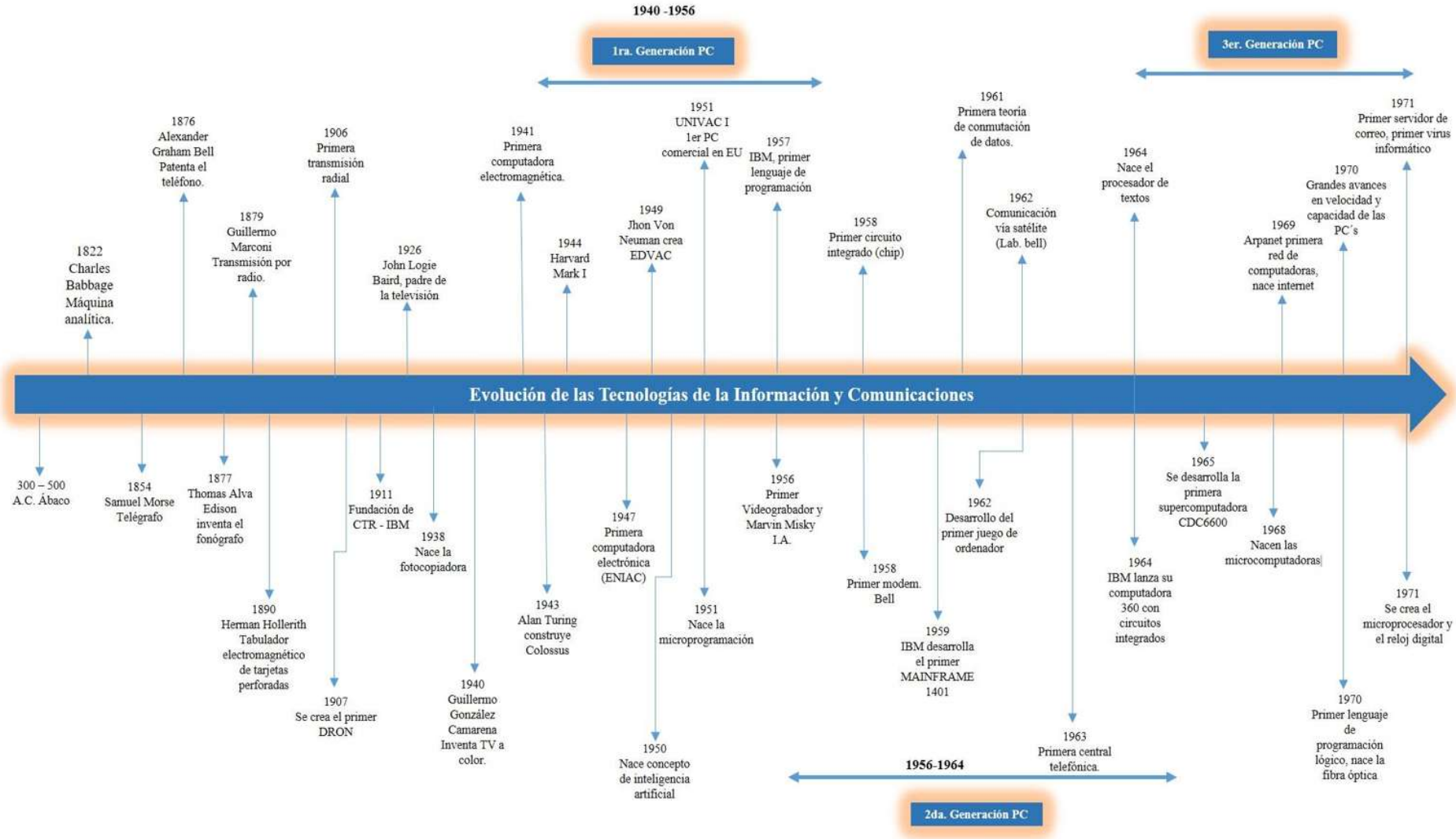
En la quinta generación (1982 a 1989) nacen los equipos portátiles, con mejores características en tamaño, debido a la reducción de sus componentes, dado que la unión de estos componentes dio paso a los microprocesadores, múltiples procesadores lo que permitió manejar velocidades de procesamiento muy significativas, en cuanto a comunicaciones que permitían la posibilidad de poder comunicarse con cualquier tipo de red, incremento en los puertos de comunicación, así como el poder contar con dispositivos de almacenamiento externo (nace el disco disquete o disco flexible) para resguardar la información generada por los equipos de cómputo, se crea el primer sistema operativo Microsoft Windows en el año 1985 al mismo tiempo que el Sistema de Apple.

Por otra parte en la sexta generación (1990 a la actualidad) se aprecian nuevas características de las computadoras; arquitecturas paralelas/vectoriales, microprocesadores para realizar actividades multitareas, por otra parte un crecimiento exponencial de las redes de área amplia (WAN) lo que ha permitido mayor interconexión en distintos ámbitos geográficos, los avances fueron muy significativos en el campo de la inteligencia artificial a nivel de lenguaje de máquina, se crea el CD-ROM como medio de almacenamiento, pero a partir de este periodo se ven diversos avances tecnológicos.

En 1998 surge el motor de búsqueda de google que permite la consulta de información en grandes repositorios de datos. Cabrera (2010) explica en el año 2004 la creación de Facebook como una red social que permitía vincular diferentes usuarios, chatear, envió de mensajes, subir fotos, videos, en el año 2006 surge Twitter, como una red social de microblogging, que trabaja con una comunicación bidireccional que permite el envío de mensajes cortos, compartir contenidos en tiempo real, actualmente son las redes más populares utilizadas por los internautas a nivel mundial.

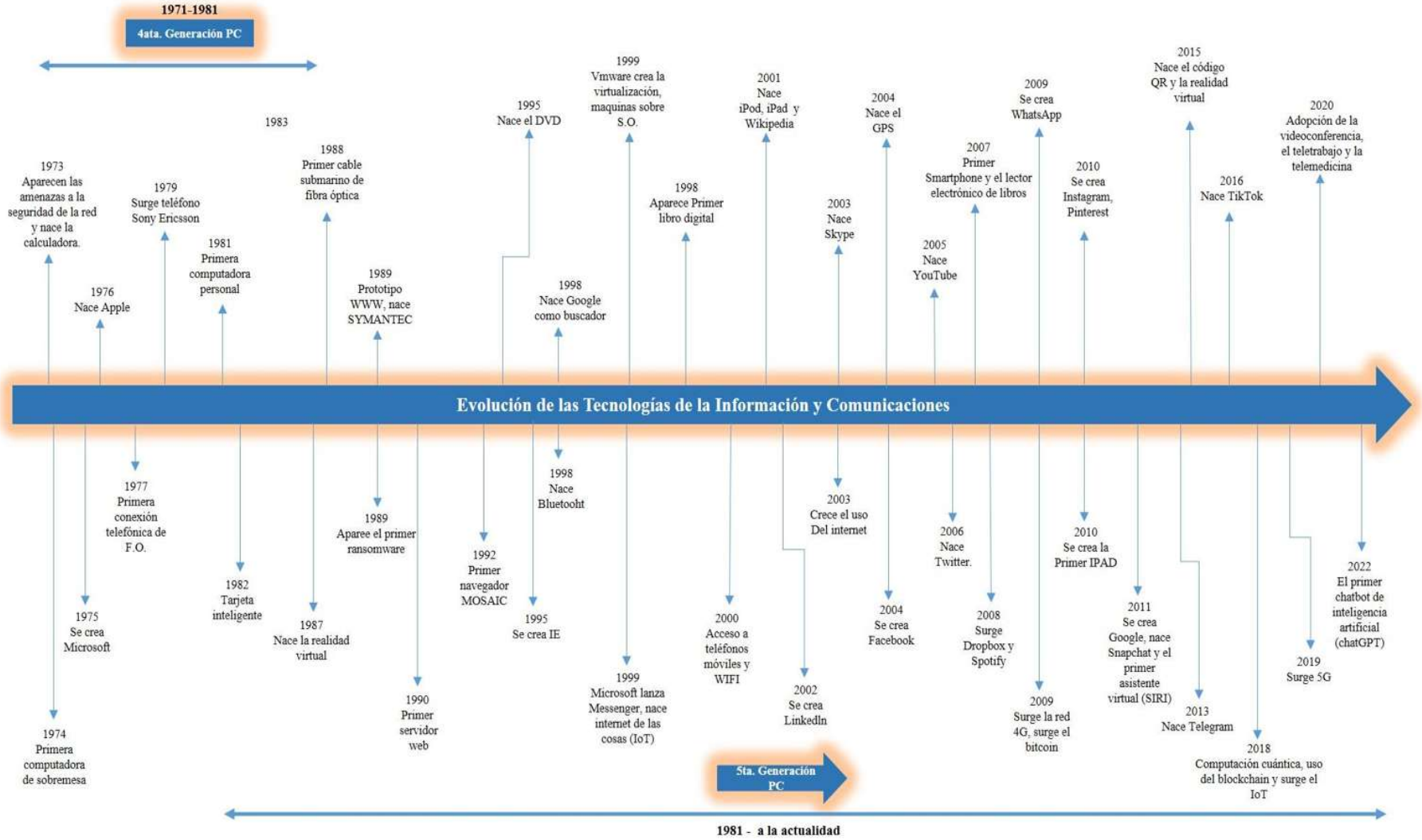
Por último en el año 2005 nace YouTube, como una plataforma para compartir videos en línea, posteriormente en el año 2009, nace WhatsApp como un servicio de mensajería instantánea que permite enviar y recibir una variedad de contenido a través de teléfonos inteligentes. Cabrera (2010), expone la creación de Telegram, plataforma de mensajería instantánea con características muy similares a la anterior descrita, en el año 2016 surge Tiktok red social para crear, editar y compartir videos cortos, estas plataformas digitales son las más utilizadas en el ciberespacio hoy en día y finalmente para el año 2019 Huidrobo (2020) comenta que en el área de las telecomunicaciones nace la tecnología 5G como un estándar de las redes inalámbricas, lo que permitir la conexión de varios dispositivos inteligentes con mayor velocidad en la transferencia de datos, así como una mejor cobertura en la comunicación, la aparición de la inteligencia artificial integrada en dispositivos de uso cotidiano.

Línea de tiempo 1. Evolución de las tecnologías de la información y comunicaciones.



Fuente: Elaboración propia con base en Vergara et al. (2010).

Línea de tiempo 2. Evolución de las tecnologías de la información y comunicaciones (continuación).



Fuente: Elaboración propia con base en Vergara et al. (2010).

Finalmente podemos observar a lo largo de esta línea del tiempo que el termino TIC´s se crea de la convergencia de las comunicaciones, telefonía, los avances tecnológicos en materia computacional y herramientas que permiten el procesamiento, almacenamiento y transmisión de información por diferentes canales de comunicación, se mencionaron las que han generado grandes cambios e impacto en las formas de interaccionar, comunicación y que en la actualidad nos llevan a este campo de estudio, comenzaremos por describir el concepto de TIC´s.

Para Suárez (2007) quien describe a las tecnologías de la información y comunicación como el conjunto de técnicas y procesos que permiten la automatización de los datos, dándoles un sentido y valor, por medio del almacenamiento, procesamiento y transmisión mediante los canales de comunicación establecidos.

Valle (1986) conceptualiza a las tecnologías de la información y comunicación como aquellas cuyo objetivo es el tratamiento automatizado de los datos, representados por medio de cadenas de bits, conjunto de datos agrupados y procesados, los cuales viajan por diferentes medios físicos de comunicación, de igual manera implican procedimientos, técnicas y metodologías que favorecen la obtención, transmisión y transformación de los datos, representación o conocimientos.

Pacheco (2012) por su parte define a las tecnologías de la información y comunicación como el conjunto de principios y teorías que facilitan la interacción de datos entre usuarios y dispositivos conectados en distintos puntos geográficos y esto es posible a la automatización de los datos, para aplicarles un valor el cual posteriormente es almacenado, procesado y difundido a través de señales electromagnéticas por distintos medios de comunicación.

Basándonos en lo mencionado anteriormente, podemos conceptualizar a las Tecnologías de la información y comunicación, como el conjunto de herramientas tecnológicas que permiten la transmisión, procesamiento y almacenamiento de información, presentada en diversos formatos. Estas tecnologías abarcan dos campos principales de aplicación:

1. Tecnologías de la información: se centra en la manipulación y gestión de la información, desde su transmisión hasta su procesamiento y almacenamiento
2. Tecnologías de la comunicación; se enfoca en la infraestructura tecnológica que posibilita la transmisión, procesamiento, almacenamiento y presentación de la información.

La ilustración 2, muestra el esquema de clasificación de las TIC´s de acuerdo a los servicios que ofrecen, los cuales se describen de forma breve para una mejor comprensión:

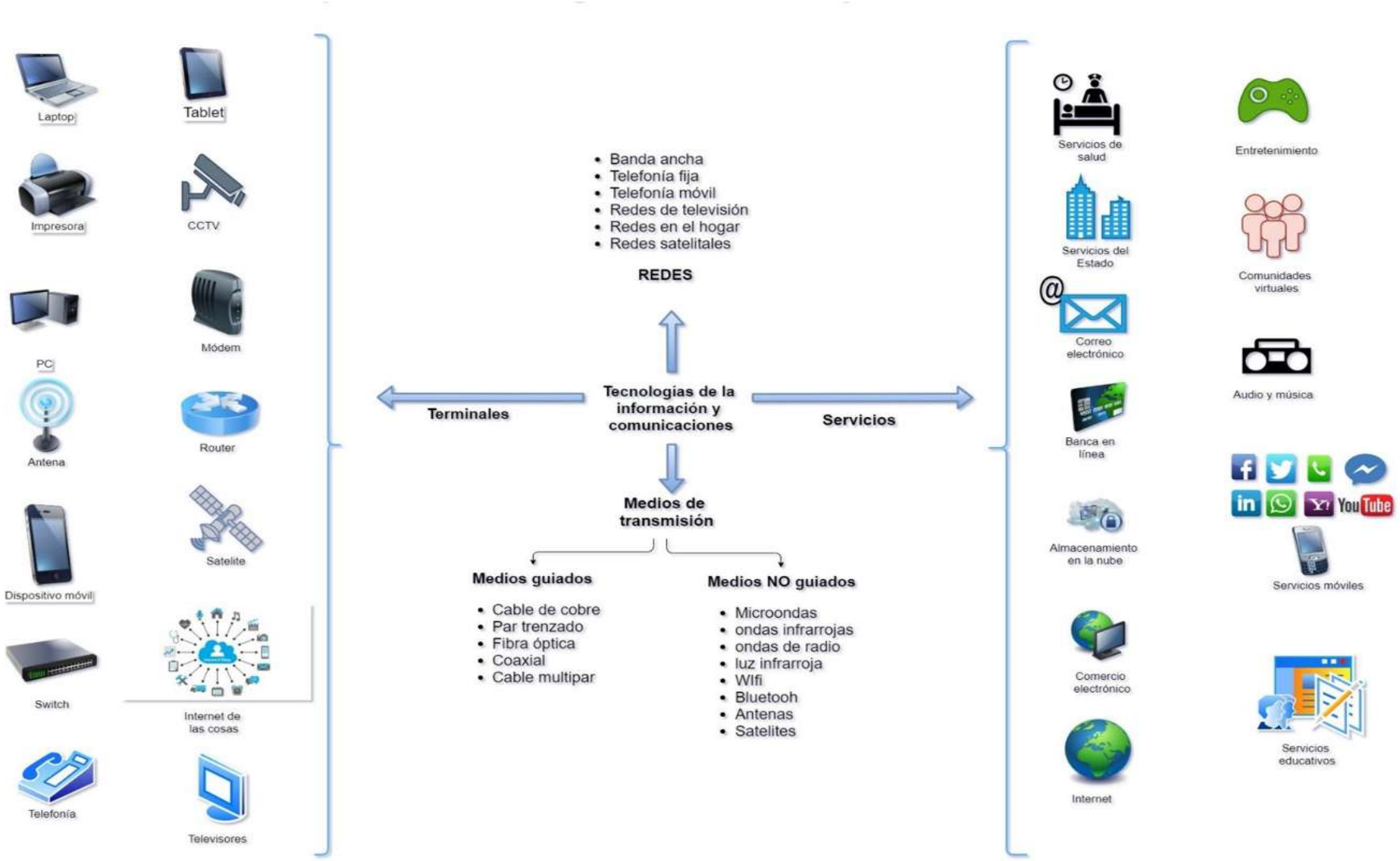
Suárez (2007) describe los medios de transmisión, como el soporte físico que permite la trasferencia de señales y datos entre los diferentes dispositivos y medios de comunicación (cableado estructurado, conectores, fibra óptica, cable coaxial, antenas, medios inalámbricos, torres y postes de transmisión, entre otros), mediante el empleo de ondas electromagnéticas, las cuales pueden ser por medios guiados y no guiados, en los primeros la forma de transmisión es por cables que conducen la señal de un extremo a otro, mientras que en el segundo modo la transmisión de las señales es a través del espectro electromagnético, el vació o el aire para la transmisión de señales por medio de antenas, para ambos casos estos medios permiten la comunicación entre emisor y receptor.

Suárez (2007) define a las redes como el medio para transportar, conducir, enviar la información y compartir diversos recursos: desde una impresora, correo electrónico, mensajería instantánea o el acceso a internet apoyado de diferentes protocolos de comunicación, los cuales son reglas y estándares que establecen como los datos y la información se transmite entre los diferentes dispositivos, con el fin de intercambiar e interconectar distintos puntos geográficos para el intercambio de información, las redes se clasifican según su uso; pudiendo ser desde telefónica básica, banda ancha, redes de televisión, redes satelitales, las rede P2P, redes de área metropolitana (MAN) y Redes de área amplia (WAN), entre otras.

En el ámbito de las comunicaciones, las terminales, tal como las define Suárez (2007), son dispositivos electromagnéticos (hardware) que sirven como puntos de conexión entre los soportes físicos y los canales de comunicación para el transporte de señales y datos. Estos dispositivos pueden variar desde instrumentos análogos hasta equipos digitales, desempeñando un papel fundamental en la interacción entre los usuarios y los sistemas de información.

Finalmente Suárez (2007) describe a los servicios como las aplicaciones (software) de las cuales disponen los usuarios finales de las TIC´s para sus actividades cotidianas, como pueden ser; correo electrónico, buscadores de información, comercio electrónico, videojuegos, redes sociales, servicios públicos gubernamentales, servicios de educación, foros de chat, Teletrabajo y soluciones de home office, video conferencias y comunicaciones en tiempo real, audio y música, streaming por video, plataforma de E-learning, almacenamiento en la nube y demás servicios que son soportados por alguna de las TIC´s.

Ilustración 5. Clasificación de las tecnologías de la información y la comunicación.



Fuente: Elaboración propia con base en Suárez, (2007).

Las TIC's citadas anteriormente, hoy en día están en riesgo de verse afectadas en su funcionamiento, operación y servicios que brindan a cientos de usuarios en el Estado Michoacán, a las dependencias públicas y empresas que utilizan e interactúan con ellas en sus actividades habituales.

Derivado de lo anterior, se mencionan los riesgos y amenazas tecnológicas que afectan a las TIC's, las cuales se categorizan en amenazas físicas o naturales y lógicas. Esa taxonomía está basada en la naturaleza de la amenaza y su origen, por lo cual se describen en las siguientes líneas:

2.2.1. Amenazas físicas

Fallos físicos; fallos en los dispositivos, catástrofes naturales, terremotos, incendios, inundaciones, entre otras. Para contrarrestar estas amenazas se debe aplicar la seguridad física, la cual consiste en la aplicación de barreras físicas, procedimientos y controles de acceso que permitan salvaguardar la infraestructura tecnológica y la información almacenada. Cada sistema tiene un nivel de criticidad único, por tanto los controles a implementar dependerán de lo que se quiera proteger.

Las amenazas físicas a la ciberseguridad son aquellas que implican la manipulación, daño o acceso no autorizado a los componentes físicos de un sistema o infraestructura tecnológica. Algunas de las amenazas físicas más comunes que pueden comprometer la ciberseguridad incluyen:

Acceso no autorizado a instalaciones: Esto puede incluir la entrada no autorizada a los centros de datos, salas de servidores, armarios de telecomunicaciones o cualquier otra ubicación donde se encuentren los componentes físicos de una red. Los intrusos pueden robar, dañar o manipular equipos o infraestructuras de red, lo que puede comprometer la seguridad y la confiabilidad del sistema.

Robo o pérdida de dispositivos: La pérdida o el robo de dispositivos como portátiles, tabletas, teléfonos inteligentes, unidades de almacenamiento externo, o cualquier otro dispositivo que contenga información sensible, puede poner en riesgo la seguridad de los datos almacenados en dichos dispositivos. Esto puede incluir el acceso no autorizado a la información guardada, la exposición de datos personales o confidenciales, o el robo de propiedad intelectual.

Los daños físicos a la infraestructura de red representan una amenaza constante que de materializarse pueden ocasionar grandes daños graves a los usuarios, empresas y organizaciones. Estos daños pueden traducirse en la perdida de datos, impactos económicos significativos y daños a la reputación. Los factores que pueden causar estos daños son diversos tanto intencionales como accidentales, incluyen desde cortes de cables de red, inundaciones, daños en equipos, incendios, entre otros.

2.2.2 Amenazas lógicas

Software o código elaborado, creados de forma intencionada o por errores humanos, con la finalidad de afectar la integridad de los sistemas informáticos y causar daños a la información.

Derivado de lo anterior se describen las principales amenaza a las que están expuestas las tecnologías de la información y comunicaciones.

- Virus: Programa diseñado para que al ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos. A diferencia de otro tipo de malware, como los gusanos, se necesita acción humana para que un virus se propague entre máquinas y sistemas (Incibe.es, 2020).
- Caballos de Troya: Se trata de un tipo de malware o software malicioso que se caracteriza por carecer de capacidad de autoreplicación. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación. Una de las características de los troyanos es que al ejecutarse no se evidencian señales de un mal funcionamiento (Incibe.es, 2020).
- Gusano: Es un programa malicioso (o malware) que tiene como característica principal su alto grado de dispersabilidad, es decir, se propaga rápidamente (Incibe.es, 2020).
- Botnet: conjunto de ordenadores (denominados bots) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDoS (Incibe.es, 2020).
- Spyware: es un malware que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos como adware, falsos antivirus o troyanos (Incibe.es, 2020)
- Adware: Es cualquier programa que automáticamente va mostrando publicidad al usuario durante su instalación o durante su uso y con ello genera beneficios a sus creadores (Incibe.es, 2020).
- Malware: tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información (Incibe.es, 2020).
- Ransomware: El atacante, toma control del equipo infectado y secuestra la información del usuario cifrándola, de tal forma que permanece ilegible. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos. (Incibe.es, 2020).
- Vulnerabilidades en el software (exploit): Secuencia de comandos utilizados que aprovechándose de un fallo o vulnerabilidad en un sistema, provocan un comportamiento no deseado o imprevisto (CN-CERT, 2007).

- Vulnerabilidades en las aplicaciones, son debilidades en el software que pueden ser explotadas por atacantes, con el fin de obtener acceso al sistema o a la infraestructura de la red para el robo de datos o tomar el control de los equipos, dentro de las vulnerabilidades más comunes son; desbordamiento de memoria, fallos en la programación, falta de actualizaciones, entradas de datos no válidos, entre otros.
- DDoS (Distributed Denial of Service): Se entiende como denegación de servicio, en términos de seguridad informática, al conjunto de técnicas que tienen por objetivo saturar un servidor, sistema o red con una gran cantidad de datos y sobrecargar los recursos disponibles y dejarlo inaccesible a los usuarios (Incibe.es, 2020).
- Ataque Man-in-the-Middle: ataque de hombre en el medio, el atacante intercepta y manipula la comunicación entre dos partes, el objetivo es leer, modificar o intervenir la información, cuto objetivo es obtener información confidencial, contraseñas, número de tarjetas bancarios, entro otros. (CN-CERT, 2007).
- Ataques de autentificación: el atacante introduce deliberadamente datos erróneos con el fin de confundir a la aplicación (CN-CERT, 2007).
- Evil twin: consiste en crear un punto de acceso falso, haciéndolos parecer real a los usuarios, con la intención de robar la sesión de su red y espiar su comunicación inalámbrica (Alberto et al., 2018).
- Pharming: ataque para redirigir el tráfico de un sitio Web a una copia de un sitio que aparenta ser real, con la intención de capturar el usuario y contraseña para el robo de información, robo de identidad o incluso la instalación de malware en el dispositivo (Kalaharshaa y Mehtr, 2021).
- Inyección SQL: Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso (Incibe.es, 2020).
- Ingeniería Social: técnicas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima (Hadnagy, 2011).
- Robo de credenciales: a través de técnicas de hacking intentan obtener usuarios y contraseñas para obtener acceso información sensible, con el fin de obtener un beneficios económico o personal (Incibe, 2019).
- Redes P2P (peer tu peer): software para el uso de redes de intercambio de archivos digitales (música, películas, software), donde se comparten diversas carpetas en las que guardan los archivos descargados y son de acceso a los miembros de dicha red, permitiendo con esto la

distribución de código malicioso, virus que aprovechan el uso de buscadores populares donde ingresan diversos usuarios para descarga de contenido digital y con esto obtener acceso a páginas o información con datos sensibles (Álvarez y Pérez, 2004)

- Web defacement: vulnerabilidad que es explotada en el servidor WEB, con la finalidad de alterar y cambiar la apariencia del sitio original de manera maliciosa y con esto obtener acceso, muchas veces por razones de hacktivismo, distribución de malware, modificación o mostrar su propio contenido (Jara y Pacheco, 2012).
- XSS (Cross site scripting): es una vulnerabilidad de seguridad en aplicaciones WEB que facilita que los ciberdelincuentes inyectan scripts maliciosos en los sitios WEB que son visitados por los usuarios, a través de diferentes lenguajes de programación, como; JAVA, HTML, VBScript o cualquier tecnología que soporte el navegador del cliente, con el propósito de realizar phishing, robo de cookies, denegación de servicio (Jara y Pacheco, 2012).

A continuación se describen las tecnologías existentes que permiten neutralizar y proteger los activos informáticos:

- Parches de seguridad: conocidas como actualizaciones que se aplican a un software para corregir vulnerabilidades (Incibe, 2019).
- Antivirus: Programa utilizado para detectar, bloquear, eliminar código malicioso (Incibe, 2019).
- Firewall: sistema de protección (hardware y software) que filtra el flujo de tráfico en ambos sentidos, con el fin de asegurar las comunicaciones entre la red interna y el internet. (Incibe, 2019).
- IDS (sistema de detección de intrusos): sistema que analiza el tráfico de red, con el fin de evitar accesos no autorizados a la red o aun equipo, no lo detiene de manera automatizada. (Incibe, 2019).
- IPS (sistema de prevención de intrusos): sistema que analiza el tráfico y neutraliza las actividades maliciosas detectadas (Incibe, 2019).
- Snnifer: programa que captura el tráfico de la red, con la finalidad de conocer la información que circula en la red y las comunicaciones de los usuarios (Incibe, 2019).
- Auditoria Informática: como el conjunto de técnicas y procedimientos para analizar, recolectar e identificar si un sistema cumple con las funciones para las cuales fue diseñado (Gerardo y Emilio, 2001).
- Controles criptográficos: utilización de algoritmos y métodos criptográficos, con la finalidad de garantizar los canales de comunicación, cifrado de información, integridad y autenticación (Álvarez y Pérez, 2004).

- Actualizaciones de seguridad: las amenazas de seguridad y vulnerabilidades requiere que los sistemas operativos y aplicativos estén actualizados con los parches de seguridad, con la finalidad de evitar riegos a la información (Álvarez y Pérez, 2004).
- Biometría: Es una tecnología que permite la identificación en base a ciertas características biológicas que son únicas e intransferibles de los seres humanos, tales como: reconocimiento facial, voz, iris, geometría de la mano y huellas dactilares a través de los cuales se puede autenticar mediante algo que posee (kaspersky.com, 2021).
- Tarjetas de proximidad o RFID: tarjeta con banda magnética o radiofrecuencia que permite el almacenamiento de datos y su transmisión sin contacto, son utilizadas para autenticación en sistemas de control de acceso (Hidglobal.mx, 2021).

A lo largo de la investigación, se han discutido las amenazas relacionadas con las TIC´S. Sin embargo es importante explicar que estas se realizan en una de las capas conocidas por los cibernautas en el ciberespacio, denominada la internet superficial o visible, donde coexisten millones de registros y con los cuales se interactúa de manera habitual, pero esta interacción, intercambio de información, compras, solo representa el 5% de la información de contenido accesible y público mediante los motores de búsqueda conocidos (Google, Yahoo, Bing, Mozilla Firefox, Opera, Safari, entro otros) en el Internet, por lo que es importante hablar de manera breve sobre el otro 95% de esa información. A continuación se realiza una descripción de manera breve para conocer cuáles son los riesgos de esta parte profunda de la red que casi no es conocida por los usuarios.

Akhgar et al. (2021) describen a la Deep Web como una red encriptada que fue creada a mediados del año 1990 como un proyectó del Gobierno de Estados Unidos de América, con el fin de asegurar las comunicaciones y la privacidad en línea de las agencias de inteligencia; actualmente es sufragada por el Gobierno, organizaciones y por grupos de defensa de la libertad de expresión, lo cual les permite a millones de personas navegar de manera anónima y privada en el ciberespacio a través de navegadores específicos: The Onion Router (TOR) es el navegador más utilizado quien toma los datos que ingresan y salen de las conexiones a internet y que circulan por diversos servidores, la estructura de la red utilizada por TOR consiste en varias capas de cifrado que protege la información que se transmite y se dificulta la trazabilidad de la comunicación.

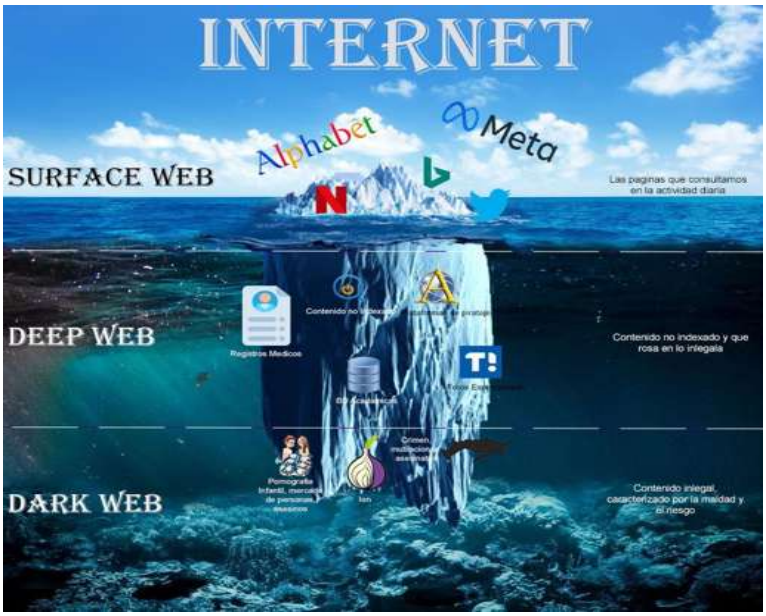
Por tal sentido es importante que comprendamos como está estructurado y como se realiza la conexión en el ciberespacio, en una navegación normal en la Web se realiza una petición a una página Web y cuando la colocamos en un navegador, nos redirige a una dirección IP donde un servidor nos devuelve la consulta solicitada, con TOR la navegación está basada a través de diversos identificadores y protocolos especiales de comunicación distribuidos por medio de redes P2P en distintos puntos de comunicación cifrados y cada

usuario tiene códigos para su acceso, mientras, que en la primera se accede a través de una URL como www.google.com en TOR es un identificador como por ejemplo; X28Z443P.onion no es una URL como las que conocemos y se conecta a un sistema dentro está red para iniciar la navegación en la Web profunda.

Pero lo que en un inicio se creó como un proyecto de seguridad para crear comunicaciones anónimas, en la protección de información de alta secrecía, actualmente se volvió un campo fértil para generar nuevas formas de interacción; comunicación entre grupos criminales, pornografía, espionaje, distribución de artículos ilegales, venta de narcóticos, venta de información, tráfico de órganos, un medio de evitar la censura y la vigilancia.

Por lo tanto puntualizaremos en la clasificación que hace Calderón (2017) del Internet, la siguiente ilustración vista como un iceberg modela las capas que describen dicha clasificación, las cuales se describen para un mejor entendimiento;

Ilustración 6. Las tres capas de Internet.



Fuente: Elaboración propia con base en Calderón (2017).

Surface Web: se define como la punta del iceberg, donde se encuentra el contenido público y de acceso a través de los buscadores de Internet, navegar en esta capa hace rastreable nuestra ubicación por el direccionamiento IP asignado.

Deep Web: contenidos no indexados a través de los motores de búsqueda, se refiere a los archivos que no se puede acceder de manera pública.

Dark Web: es una parte conocida como la red obscura o profunda, para su acceso se requiere de conexiones y protocolos especiales de comunicación que hacen que dicha conectividad sea anónima e irrastreable, donde se tiene acceso ha contenido ilegal.

2.3 Aspectos legales

Antecedentes de la Legislación Mexicana

La vida del ser humano se encuentra en evolución constante, el hombre es un ser social por naturaleza y esa misma naturaleza es la que lo ha llevado a reunirse con otros individuos para su desarrollo, crecimiento, evolución cognitiva que va adquiriendo gracias a su aprendizaje dentro de los grupos sociales. En Serra (2016) quien define a la Sociedad como un grupo humano que se organiza de forma coherente, que actúa de manera unitaria y general, a través de la cooperación para el logro de objetivos comunes, como su propio mantenimiento y preservación. Esta agrupación social trasciende el tiempo, predomina y causa arraigo entre sus miembros, los cuales difieren en sexo, edad y condición económica, es así como la sociedad es una fuente de creación de las formas políticas y sociales que hoy conocemos como Instituciones Públicas, las cuales dan respuesta a las demandas de los individuos.

Por otra parte dentro de la sociedad se da el origen de la cultura, entendida como el conjunto de conocimientos, actitudes, normas y valores de las personas, que han adquirido un grupo humano a lo largo de su historia y que con el paso del tiempo modifican, transforman su medio ambiente y con ellos sus necesidades primordiales y sociales de igual manera. A partir de ella la sociedad crea el derecho y con ello las instituciones jurídicas políticas que a su vez sostienen el Estado y más aún, se crean conceptos como la autoridad.

Como resultado de esta interacción transformadora y creadora de la sociedad, encontramos en la costumbre la primera fuente del Derecho, la cual dictó las primeras formas de regulación de la vida social. En un principio el derecho fue un fenómeno derivado de la experiencia misma acumulada por los grupos, más que una actividad razonada por los hombres, formando parte de la cultura que a su vez dio origen al derecho consuetudinario y luego al escrito (Serra, 2016).

En tal sentido Kelsen (2020) define al derecho, como el conjunto de normas jurídicas que regulan la conducta de los individuos en sociedad y en caso de su incumplimiento se aplicará una sanción. De aquí la importancia de que las Instituciones encargadas de regular, normar y sancionar la conducta de los individuos, con el único fin de garantizar el bienestar de la sociedad y mantener el orden público.

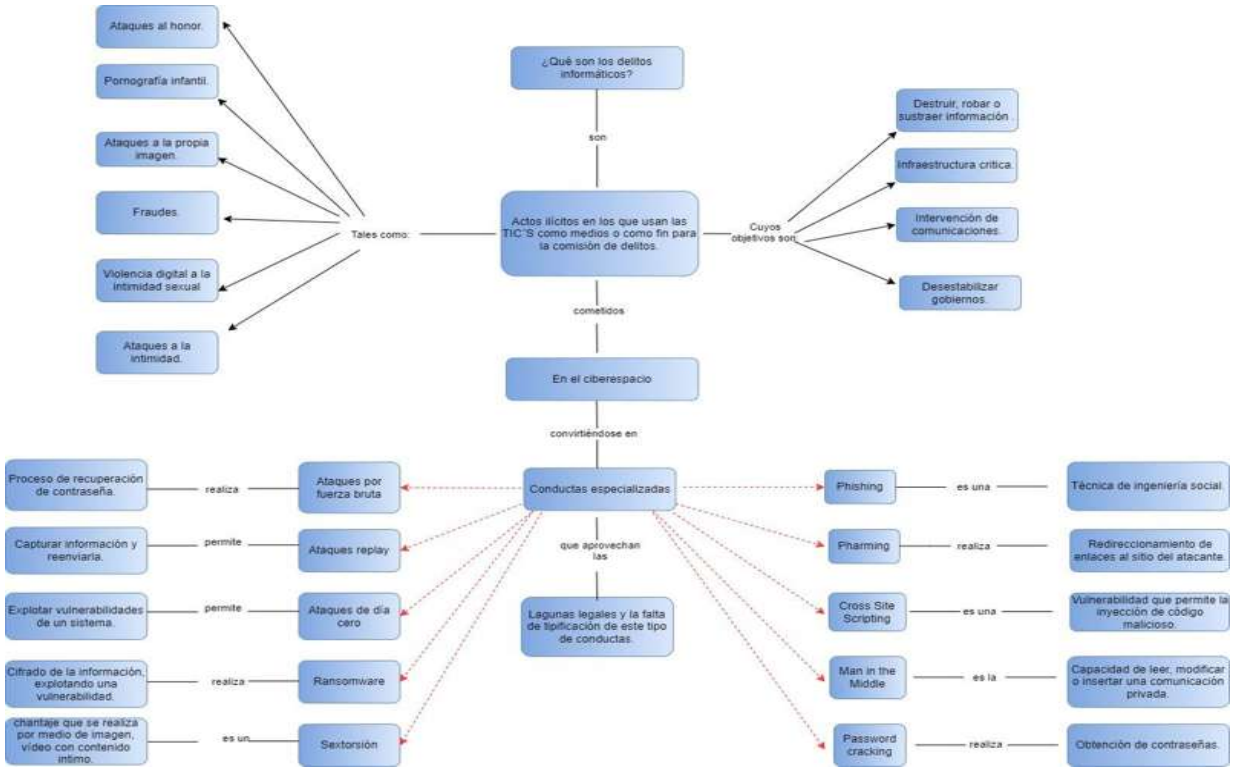
Si bien, en un principio todas esas normas regían la conducta de una acción, hoy en día también la omisión y las nuevas modalidades que han surgido en la comisión de los delitos, son temas que deben de ser de interés del Estado. El paralelismo entre una sociedad “real” que habita este planeta tierra y una sociedad “virtual” que es exactamente la misma, pero en el ciberespacio, creado para revolucionar y avanzar las

formas de aprender, de comunicarnos, de desarrollo económico, social y de romper fronteras nos ha sumergido dentro de lo que hoy conocemos la nueva era tecnológica o digital.

El nacimiento del ciberespacio engloba todo un conjunto de esferas que envuelven a la sociedad y a los usos que se encuentran en este inmerso espacio de nadie, en donde cada vez los usuarios van en aumento a nivel mundial, pero la seguridad que puede brindar un sistema o aquellos sistemas informáticos que permiten la seguridad a una determinada empresa o país no lo es todo, al no existir territorialidad en este inmenso espacio urge la necesidad de llegar a acuerdos, de regular a través de los tratados internacionales legislaciones que sean de competencia mundial y que la próxima era tecnológica pueda frenar los ataques que se avecinan de lo que podría considerarse la próxima guerra a través de los ataques tecnológicos y poniendo en peligro incluso a naciones enteras.

En la siguiente ilustración de manera gráfica se plasma como operan los delincuentes en el ciberespacio, aprovechando la falta de legislación y donde crece la impunidad cada día, con nuevas conductas de riesgo especializadas, complejas y sofisticadas que aprovechan los vacíos legales y el anonimato que brindan las redes sociales para actuar de manera deliberada sin ser castigados.

Ilustración 7. Los delitos y las conductas especializadas en el ciberespacio.



Fuente: Elaboración propia con base en los diversos estudios y experiencia.

2.3.1 Corte Interamericana de los Derechos Humanos (Cuarta Generación)

El desarrollo tecnológico ha ido en aumento en las últimas décadas, ayudando con ello la mejora del entorno social y el desenvolvimiento económico, como nueva fuente de ingresos al encontrarnos inmersos en un mundo de opciones y posibilidades dentro de la tecno ciencia. Altamirano Dimas (2017) considera que "Los derechos humanos de 2ª, 3ª y 4ª generación se incorporan a partir de pensamiento humanista y socialista; son de naturaleza económica y social, e inciden sobre la expresión de igualdad de los individuos".

La cuarta generación de los derechos humanos tiene estrecha relación con "las nuevas tecnologías de la información y de la comunicación", buscando principalmente el reconocimiento y amparo de los derechos que ahora se encuentran inmersos en la nueva era digital, siendo necesario que el sistema jurídico los incorpore dentro de las legislaciones del Estado.

Dentro del proceso penal deben existir garantías que velen por los derechos humanos del hombre, con la finalidad de protegerle de arbitrariedades, motivo por el cual las leyes han ido cambiando o modificando las formas de llevar a cabo el proceso dentro de los sistemas de justicia penal. En la actualidad el uso de evidencias digitales como medios de prueba, han ayudado en la solución de casos, pero también los medios tecnológicos son empleados para la comisión de delitos tradicionales como lo son: fraude, extorsión, trata de personas, pornografía infantil, ataques al honor, ataques a la propia imagen, entre otros), pero a la vez han surgido nuevas conductas delictivas. Haciendo alusión a esta nueva tipología de delitos comenta Ferreyra (2018) que los delitos que se cometen en el ciberespacio y a través de las redes de comunicación tienen un alcance internacional, ya que estos se cometen en diferentes puntos geográficos, la víctima puede estar en otro país y el ciberdelincuente operar desde otro, adicional a esto los servidores utilizados para dicho fin pueden estar en otro distinto, lo que representa una barrera legal al momento de querer imputar un delito, lo que ha dado orígenes a diversas regulaciones por Organismos Internacionales, con el fin de buscar homogenizar los delitos a nivel internacional y buscar la cooperación.

En México es hasta el año 1999, que se incorpora en el Código Penal, un capítulo que contempla el delito de acceso ilícito a equipos y sistema informáticos donde se intenta empezar a normar este tipo de conductas realizadas con el uso de las tecnologías de la información y comunicaciones. Por otra parte se ha recibido la invitación para unirse al convenio de Budapest, instrumento legal vinculante en materia penal. México no se ha integrado debido a la falta de esfuerzo para cumplir con los requisitos y únicamente funge como observador, en Latinoamérica a excepción de Brasil, todos los demás países ya se han adherido al convenio (Gob.mx, 2019).

2.3.2 ¿Qué es el convenio de Budapest?

Es un convenio sobre ciberdelincuencia, firmado en Budapest Hungría el 23 de noviembre de 2001 y entrando en vigor el 01 de julio de 2004, es el primer tratado internacional que busca abordar los delitos informáticos y de Internet para armonizar las leyes nacionales, mejorar las técnicas de investigación y aumentar la cooperación entre las naciones. Es decir, es el primer instrumento multilateral jurídicamente vinculante para regular el ciberdelito, en el mismo sentido posteriormente surgió el Protocolo Adicional al Convenio sobre ciberdelincuencia, tipificado como delito la difusión de material racista y xenófobo a través de sistemas informáticos. (Council of Europe, 2001).

El convenio de Budapest entre sus lineamientos jurídicos que lo regulan y dan sustento requiere que sean implementados puntos que favorezcan la procuración de la justicia y sean regulados a través de actos que faculten y preparen las legislaciones a través de la unificación, para lo cual es importante no solo tipificar, sino reorganizar entre los delitos existentes y criminalizar conductas que se encuentran establecidas en los lineamentos de dicho convenio, como lo son entre otros los delitos de orden nacional, también es necesario que las autoridades encargadas de la procuración de justicia en el ámbito penal se encuentren debidamente facultadas y cuenten con las herramientas necesarias para la investigación de la comisión de los delitos estipulados dentro de este convenio. Asimismo las áreas de inteligencia tienen que ampliar sus capacidades y alcances deseados e implementar funciones de vigilancia, cateo e incautación de bienes; monitoreo de contenido en línea; retención y transferencia de datos e intervención de comunicaciones privadas, tomando en cuenta que la preparación en el actuar nos facilitara el éxito (Council of Europe, 2001).

Se enlistan algunas de las causas que se analizan y que de acuerdo a nuestra legislación, son necesarias para que México se adhiera al convenio de Budapest.

1. La tipificación del artículo 15 del convenio de Budapest, habla de establecer un equilibrio existente entre la acción penal y los derechos humanos, buscando en todo momento la preservación de los derechos inherentes al individuo y a sus libertades (Council of Europe, 2001).

2. La Constitución Política de los Estados Unidos Mexicanos y los tratados internacionales de los que el Estado mexicano sea parte se encuentran en igualdad jerárquica, buscando siempre la igualdad y la protección de los derechos humanos de todos los individuos. La diversidad de tratados internacionales existentes ha obligado a que los Estados que forman parte de ellos modifiquen sus legislaciones ya que los ordenamientos jurídicos lo solicitan para una efectiva implementación y por tanto aplicación. Dentro del artículo 1° constitucional, manifiesta la igualdad jerárquica, así como la compatibilidad de

dichos tratados con nuestra carta magna (Constitución Política de los Estados Unidos Mexicanos, 2020).

3. La Costitución Mexicana de los Estados Unidos se rige bajo el principio de legalidad y de retroactividad de la ley, tipificando en sus artículos 14 y 16 constitucionales, la sanción penal deberá ser mediante orden del juez a través de un juicio cumpliendo con las formalidades del procedimiento, con relación a los juicios la analogía no será suficiente para decretar y aplicar una pena o sanción, el delito tendrá que ser cuadrado al tipo penal para sus efectos. Todo requerimiento y sanción penal debe ser a través de un juicio y llevado a través de los principios de legalidad (Constitución Política de los Estados Unidos Mexicanos, 2020).

4. El principio de proporcionalidad en el derecho penal mexicano tipifica la imposición de la pena, esta tiene que estar prevista dentro de la ley para que esta sea aplicable, siendo proporcional la pena establecida en cuanto al delito y al bien jurídico en tutela. Por otra parte, para exista una sanción tiene que existir la culpabilidad. Está tipificado en el artículo 22. Constitucional (Constitución Política de los Estados Unidos Mexicanos, 2020).

Por lo tanto ha sido cuestionada la postura del Estado mexicano así como el compromiso de éste, por el motivo de que se ha rehusado a realizar las reformas necesarias dentro de su legislación siendo estas necesarias para cumplir con lo estipulado en este tratado internacional, ya que para formar parte de estos no solo es necesario promover y celebrara su adopción, sino cumplir con lo estipulado en cuanto a implementación de medidas jurídicas y procedimentales que logren una efectiva aplicación y cumplimiento (LLamas, 2020).

Actualmente en el ciberespacio, se generan diversas conductas especializadas de riesgo, las cuales no están siendo vistas como riesgos y o amenazas a la integridad, a la privacidad, patrimonio, la vida y la seguridad de los ciudadanos, la descontextualización penal que se vive actualmente hace que muchos de estos delitos no sean sancionados o que sean incluidos en tipos penales obsoletos, lo que provoca que los delincuentes sigan operando al amparo de los vacíos legales y que la incidencia delictiva crezca a niveles no pensados en el ciberespacio.

Se analizaron los treinta y dos códigos penales, con el fin de conocer su legislación en materia de delitos cibernéticos y las sanciones penales que se aplican en cada caso, la siguiente tabla muestra los delitos que involucran el uso de las tecnologías de información y comunicaciones. Para una mayor referencia de la legislación, en el Anexo 1, se encuentra una compilación de las principales leyes en las que se soporta esta investigación.

Tabla 3. Cuadro comparativo de los delitos cibernéticos.

DELITO	Ultima Reforma	Ataques al Honor	Fraude	Ataques a la imagen	Ataques a la intimidad	Pornografía y Pornografía de Personas Menores de Edad	Trata de personas	Amenazas	Instigación o Ayuda al Suicidio	Ciberacoso Sexual	Acoso Sexual	Violencia a la intimidad sexual	Hostigamiento Sexual	Extorsión	Violación de Correspondencia	Corrupción de Personas Menores de Edad	Usurpación de Identidad	Acceso Informático Indebido	Calumnia	Intimidación	Discrimimación	Turismo Sexual	Incitación a la Violencia
ESTADO	Fecha	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo	Artículo
Aguascalientes	18/11/2021		147			117		139	100				114	149	180	116	181 (A)	181			192		
Baja California	14/09/2021		218	175 (S)	175 (S)	262	264	171	131				184	224	257	261 (bis)	175 Quinq	175 (bis)	D	306	160 (ter)	262	170
Baja California Sur	31/07/2021		239		183	173		218	147-148	183 (bis)	182		182	245	353	169	363				205		205
Campeche	07/10/2021	244	206-207	244	244	260	379	171	152		167 (bis)		167	209	235	250	242	388	249	293			
Coahuila de Zaragoza	01/06/2021	272	291	272	272			265	193-194		236 (FI)		236 (FII)	332	270	237	268	273			239		239
Colima	02/05/2020	222-224	199-200			170-171		218	143			152 (3er)	152	204	252	144	224 (bis)	200 (FVII)	222	242	223	144	
Chiapas	04/11/2020		302			333	301 (FVI)	227	176		238 (bis)		237	300-301	386	327		439-443		427	324		378 (bis)
Chihuahua	23/10/2021		223			D	D	204	141		176	180(bis)	176	204 (bis)	326		206 (ter)	327		263	197		170
Ciudad de Mexico	29/07/2020	D	230-231	D	181	187	188	209	142		179			236	334	183	211 (bis)		D	289	206	186	206
Durango	04/07/2021		210	171	172	276		174	151		182		182	D		279	175 (bis)	256		321	306		306 (III)
Estado de México	27/08/2021		305			206	268 (bis)		246		269		269	266	197		264			343	211		170
Guanajuato	22/12/2020	D	201		187-e	236	179	176	164		187a		187 b	213	231	236	214 (A)	235	D	264 bis			
Guerrero	20/11/2020		237-238			173		218	151		185		183	243	341	171				280	204 (bis)	174	204
Hidalgo	22/11/2021	D	213		183 bis	267		172	153					216	260	267	370		D	309 (bis)	202 (bis)		202 (bis)
Jalisco	20/04/2020	D	250			D		188	224		176 (bis)		176 (bis)	189		142 (A)	143 Quater*		D		202 (bis)		170
Michoacán de Ocampo	02/07/2021	192	217	196	194	158	162	187	138		169 (bis)	195	169	224	294	156	301 (bis)			249	179	159	
Morelos	28/07/2021		188			212	D	147	112	158 (bis)	158		158	146	241	211	189 (bis)	148 quarter	D	275	212 Quater	162 (bis)	212
Nayarit	09/01/2020		400		297 (bis)			316	364		296	297 bis	296	328	202	230	326	412		244			
Nuevo León	25/08/2021		385		271 (bis)	201 bis		291	322		271 (bis II)	271 (bis)	271	395	178	196	444	225 Bis 1	235	214 bis	353 (bis)		
Oaxaca	15/04/2018		380			195	348 (bis F)	264	294		241		241	383 (bis)	174	194	232 (bis)		D	216	412 (bis)		412
Puebla	08/11/2021		402		225	217		290	333	278 Nonies	278 (ter)	225	278 (bis)	292 (bis)	195	217		475-478	D	420 (bis)	357		357
Querétaro	11/10/2019		193			D	D	155	135		167 (bis)		167 (bis)	198	187	D		151 Quarter	D	265	170	D	170
Quintana Roo	21/10/2021		152		194 (ter)	192 (bis)		123	91	130 Quin	130 (bis)	130	130 (ter)	156	187	191	195 (Sexties)		D	259	132		132
San Luis Potosí	25/06/2020		222	187			Leyes Generales	168	147		181	187	180	230	361	183	187			343 Quat	186		186
Sinaloa	22/07/2019		214		177	273	D	173	151		185 (bis)		185	231	265	273	177 (bis)	217		302	189	274 Bis E	189
Sonora	15/06/2021		318		167 (bis)	169 (bis)	D	238	264		212		212 (bis)	293	152	168	241		284	189	175 (bis)	D	
Tabasco	18/07/2020		190		163	334 bis	D	161	129			163	159 (bis)	196	315	329	161 Quater	326 bis		239	161		161
Tamaulipas	09/11/2021		417		276 septies	194 (bis)		305	348	390 (Ter)	276 (3er)		276 (bis)	426	175	192	263 bis		D	224	309 (bis)		
Tlaxcala	19/05/2016		338			355		279	244				294	268	392	355	282	316		147	375		375
Veracruz de Ignacio de la	07/05/2020		216		177	190		172	148		190		190 (bis)	220	273	190 (sexies)	283 bis	181	D	326	196		196
Yucatán	30/10/2021	295	323	243 (bis 2)	243 (bis 3)	211		233	374	243 bis 12	308 (bis)		308	327	174	208		243 bis 5	299	258 (bis)	243 (Ter)		243 (FI)
Zacatecas	01/08/2021		339		232 (ter)	183		257	305		233		233 (3er)	261	155	181	227		274	206 (bis)	182 (bis)		

Fuente: Elaboración propia con base en los diversos códigos penales revisados.

Del análisis a la legislación penal se agrupo por tipo de delito, obteniéndose lo siguiente:

Tabla 4. Delitos tipificados por Estado.

Delito	Estados	Estados que han tipificado el delito
Fraude	32	100%
Instigación o ayuda al Suicidio	32	100%
Amenazas	31	97%
Extorsión	31	97%
Violación de Correspondencia	30	94%
Hostigamiento Sexual	30	94%
Discriminación	29	91%
Intimidación	28	88%
Corrupción de personas menores de edad	28	88%
Usurpación de identidad	27	84%
Acoso Sexual	26	81%
Pornografía y Pornografía de Personas Menores de Edad	26	81%
Ataques a la intimidad	20	63%
Incitación a la Violencia	22	69%
Acceso informático indebido	19	59%
Violencia a la intimidad sexual	9	28%
Trata de personas	8	25%
Ataques a la Imagen	7	22%
Calumnia	6	19%
Turismo Sexual	6	19%
Ciberacoso Sexual	6	19%
Ataques al honor	5	16%

Fuente: Elaboración propia con base en los diversos códigos penales revisados.

Como se observa las entidades federativas han realizado grandes esfuerzos por incorporar algunos de los delitos cibernéticos dentro de sus legislaciones, con el fin de reducir la impunidad, quien para Oliva y Escobedo (2013) lo define como algo que no es sancionada debido a la ausencia de legislación que permita aplicar la sanción correspondiente, mientras que para Carbonell y Vázquez (2003) la impunidad la conceptualiza debido a la existencia de un marco jurídico eficiente que permite a los delincuentes aprovechar estos vacíos y delinquir. Por lo que podemos expresar que la ausencia de legislación y la falta de revisión en la actualización a los tipos penales actuales, permite que los delincuentes actúen al amparo de esta impunidad, ya que aprovechan los vacíos legales existentes en el ciberespacio.

En tal sentido y por otra parte en las legislaciones locales son pocas las entidades que contemplan dentro de sus códigos penales a los delitos informáticos, tales como; violencia a la intimidad sexual, ataques al honor, trata de personas, ataques a la imagen, Ciberacoso, entre otros, sin embargo la interpretación es

ambigua ya que muchos de ellos no contemplan la divulgación del contenido, cuando este se realiza a través de las diversas plataformas digitales de manera masiva, por mensajería instantánea, así como la complejidad para la imputación del hecho dado el anonimato que brinda la red.

Por otra parte diversos juristas han manifestado la necesidad de la creación de un código penal único. De la misma forma Carbonell (2014) comenta que debido a la existencia de diversas normas, leyes, reglamento, disposiciones y acuerdo para atender los delitos, complica que todas sean de conocimiento de todas las personas, lo que complica su interpretación, aplicabilidad y con esto obstaculizando la impartición de justicia, es por eso que esta propuesta permitiría contar con un código penal único de los delitos que se comenten a nivel nacional, con el fin de hacer más eficiente, y que se establezcan bases claras y únicas para sancionar las conductas delictivas en México.

Asimismo Sánchez (2020) en IT Masters Mag comenta que no existe una regulación específica en los delitos cibernéticos, tomando en consideración que los elementos que conforman estos delitos, son diferentes de los elementos que integran los tipos penales, por otra parte es importante que se hagan reformas adecuadas al Sistema de Justicia Penal para darles un tratamiento diferente a los delitos que se cometen a través del uso de las tecnologías de la información y comunicaciones, ya que muchas veces se complica la aplicación de la ley, debido a la falta de abogados especialistas en derecho informático, a que los jueves no están actualizados en este tipo de delitos, por otra parte la interpretación que cada caso requiere, ya que como se comentó en líneas anteriores son conductas especializadas, con ataques más sofisticados, los cuales en muchas ocasiones dificulta su trazabilidad y aunado el anonimato que brinda el ciberespacio, hace más complejo la persecución de los delitos, su tratamientos y con esto la aplicación de la ley.

Por su parte la Comisión permanente del H. Congreso de la Unión (2017) externaron que es importante que México atienda los requerimientos que son necesarios para formar parte del convenido de Budapest, para contar con la cooperación internacional en el intercambio de información y así contar con un marco jurídico homogéneo en relación a los delitos informáticos y que permita a México avanzar en materia de Ciberseguridad.

2.4 Cibercultura

La ciberseguridad comprende el término, por lo cual empezaremos por definir la raíz de la palabra cultura:

Para Marvin Harris (1989), la cultura es el conjunto de prácticas y formas socialmente aprendidas de la vida, que se construye en las sociedades de acuerdo a sus vivencias diarias, las cuales incluyen una mezcla de sentimientos, pensamientos, conducta y el desenvolvimiento de los integrantes de una sociedad.

Por su parte la UNESCO (2012) refiere a la cultura como el conjunto de características inconfundibles, espirituales y materiales, intelectuales y afectivas que determinan a una sociedad o un grupo social. Ello incluye igualmente las artes, las letras, la forma de vida, derechos, la estructura de valores, costumbres y creencias del ser humano.

Derivado de las definiciones anteriores comprendemos que la cultura es dinámica, cambia con el transcurso del tiempo, facilitando con esto su adaptación a los nuevos cambios y a esto lo llamamos aculturamiento. Este término se utiliza a finales del siglo XIX en el campo de la antropología social en Norteamérica. Para García y otros (2004) La aculturación es el proceso de una sociedad cuando se realizan cambios profundos por el contacto con otras sociedades, por periodos amplios de tiempo, en relación a sus costumbres, tradiciones, los cambios no solo son culturales, si no también psicológicos ya que estos impactan en el comportamiento de los individuos provocando cambios de conducta, estilo de vida, identidad, entre otros.

De aquí que, según Páez et al. (2000) la aculturación es un proceso de adaptación en la adquisición de una segunda cultura, donde la nueva se integra a la original, pero esta permanece en un nivel superior, conservando su identidad original en el proceso de interrelación lo que le permite integrarse en un nuevo grupo social que incorpora a otros grupos sociales.

De manera que si entendemos la historia de la humanidad, podemos observar los diferentes procesos de cambio cultural que la humanidad ha experimentado hasta nuestros días. Por su parte Díez (2005) define al proceso de cambio como la socialización de las diferentes culturas que han dado origen a diversas prácticas de manera individual o colectiva, a través de la interpretación, comunicación, dialogo y su adaptación a estas nuevas culturas.

En consecuencia este proceso de cambio cultural da origen a la diversidad cultural en la que nos encontramos actualmente, como parte de un largo proceso que va en diversas direcciones, donde hemos visto revoluciones, transformaciones sociales, políticas, culturales, así como la desaparición y aparición de culturas, teniendo como eje principal la migración y el intercambio desde el origen de la humanidad. En este sentido Ortiz (2012) la define como la variedad de culturas que se interrelacionan y que coexisten en un mismo territorio geográfico, compartido por un gran número de personas, capaces de identificarse y de esta interacción se crean nuevas expresiones culturales que se comparten con los miembros de la sociedad.

En consecuencia, la diversidad cultural es vista como un proceso histórico que muestra las civilizaciones alrededor del mundo y hoy en día nos da un panorama a lo largo de la historia de los cambios y

transformaciones de la sociedad, dando con ello paso a la modernidad que tiene sus orígenes en Europa desde el Renacimiento como un cambio de pensamiento e ideas que lleva a nuevas transformaciones culturales, políticas, culturales, sociales y económicos.

Por consiguiente para Echeverría (2013) la modernidad es la evolución que ha tenido lugar desde hace ya varios años y que se logra determinar gracias a aquellos comportamientos de la vida en sociedad, es decir, de los seres humanos en general y de todas sus variabilidades en cuanto a conducta y pensamiento; y es precisamente el comportamiento de estos y aquellas necesidades que necesitan ser cubiertas lo que favorece la transformación, por no llamar evolución social y básica para ir solventando las necesidades actuales y aquellas que van surgiendo día a día.

En tal sentido la modernidad vista como el resultado de diversas culturas da paso a la globalización entendida como un proceso de expansión y crecimiento de las sociedades. Por consiguiente Mittelman (2002), define el concepto de globalización como un acontecimiento mundial, una combinación de procesos y arquitecturas domésticas, que posibilitan que la política, la cultura, la tecnología y la ideología de una nación mantengan interacción con otra.

La tecnología es un factor determinante del crecimiento, con su aparición a fines de la década de los 70´s, las sociedades han cambiado las formas de interactuar y de relacionarse a través del ciberespacio por medio de toda una infraestructura tecnológica, creando con esto nuevas formas culturales de interacción en línea, dando con esto paso a un nuevo fenómeno mundial de comunicación e interacción.

Derivado del contexto anterior, surge la palabra cibercultura compuesta por el prefijo ciber que “indica relación con redes informáticas” (Diccionario de la lengua española, 2019), tomado de la palabra cibernética la cual hace alusión a una serie de conceptos tecnológicos como lo son las computadoras, internet, redes, comunicación, hipertexto, interactividad, entre otros y la palabra cultura como el conjunto de valores y hábitos de una sociedad.

En este orden de ideas podemos ver a la cibercultura como una cultura que se basa en la utilización de las tecnologías de la información y comunicaciones como una nueva forma de comunicación en las sociedades, con cambios culturales importantes debido a esta nueva interacción en línea, con impactos en la educación, salud, ciencia, política entre otros, todos como una nueva forma de construcción social del conocimiento basado en la hipertextualidad y la conectividad en el ciberespacio.

Para Levy (2007) la cibercultura es el movimiento social que parte de la adopción generalizada equipos tecnológicos, ordenadores o equipos de cómputo, sistemas informáticos, infraestructura tecnológica y en

comunicaciones, así como la conjunción de los mismos para generar un entorno virtual, digital o el ciberespacio, en el cual los individuos y sociedades interactúan, se relacionan, intercambian información, costumbres, tradiciones, generando un inteligencia colectiva y la creación de comunidades virtuales, las cuales modifican al comportamiento social en un ciclo al parecer interminable de condicionamiento entre la tecnología y la misma sociedad, las cuales se reconstruyen constantemente como resultado del impacto de una sobre la otra.

Según Galindo (2006), la cibercultura tiene una doble connotación, por un lado, hace alusión a todo aquello relacionado con el ciberespacio, es decir, aquellos términos y lenguaje que están implícitos dentro del mismo ciberespacio, por otro lado, entendemos por cibercultura toda aquella sociedad que se encuentra inmersa dentro del mismo y que ha ido evolucionando principalmente para tener un considerable avance de la sociedad misma, en cuanto a economía, política todas y cada una de las ciencias humanas, sociales y tecnológicas que giran en torno a la vida humana.

De acuerdo con la Estrategia Nacional de Ciberseguridad (2017) se define como el conjunto de valores, principios y acciones en materia de concientización, educación y formación, que se llevan a cabo por la sociedad, academia, sector privado e instituciones públicas, que inciden en la forma de interactuar en el ciberespacio de forma armónica, confiable y como factor de desarrollo sostenible.

En contexto con los conceptos anteriores podemos entender como una nueva forma de comunicación donde se centra como elemento principal los equipos tecnológicos a través del uso de las Plataformas digitales para generar interacciones en el ciberespacio donde el ser humano manifiesta ideas, expresa sentimientos, estados de ánimo, a través de entornos digitales: videos, canales de comunicación, mensajerías instantáneas, redes sociales, hipertextos, imágenes, salas de chat, foros, entre otros, en un mundo virtual, dando paso a la creación de una nueva cultura que nace del ciberespacio partir de esa interacción ya descrita.

Siendo importante resaltar los beneficios de las tecnologías de la información y las comunicaciones en las relaciones humanas, de manera breve se mostrará su alcance en diversas áreas del conocimiento:

2.4.1 Beneficios de las TIC´s en la conducta humana

Nuevas formas de Comunicación.

La comunicación es una aptitud nata del ser humano, para Serrano (2007), no es propia del ser humano, la comunicación y la necesidad de comunicación se da entre especies, pero la misma evolución de nuestra especie humana la ha moldeado con un sentido evolutivo. Uno de los principales cambios que se han dado en esta nueva era tecnológica es la forma de las comunicaciones, pues anteriormente el que un individuo

se comunicara a distancia con otro era a través del telégrafo y del correo, implicaba que los mensajes se tardaran días en llegar, pero con el uso de las nuevas tecnologías de la información solo basta un par de minutos o segundos para estar comunicados, sin importar el lugar en donde los individuos se encuentren, pues a través de los diversos dispositivos, hoy por hoy la comunicación ha revolucionado, logrando conectar familias, concretar negocios, entregar información oportuna que ha servido también para el desarrollo y crecimiento del mismo comercio, entre otras actividades. Toda la información que se difunde a través de redes sociales y en las páginas web, tiene la ventaja de interactuar de manera inmediata y con mayor eficacia, la prensa incluso hoy por hoy se mantiene a la vanguardia con sus medios electrónicos.

A pesar de que el derecho a la libre manifestación de ideas se encuentra estipulado en el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, eran muy pocos los que hacían valer este derecho, (Gobierno, líderes sindicales y demás organizaciones). En la actualidad el uso de las tecnologías ha beneficiado la expresión de las personas, grupos sociales que se manifiestan a través de las redes sociales y conforman vínculos con personas con la misma preocupación o afección logrando a través de las redes la manifestación de ideas.

2.4.1.1 Desarrollo en la infraestructura Educativa

La Declaración Universal de los Derechos Humanos busca la protección de los derechos así como de las libertades e igualdad del ser humano, el artículo 26 de la Declaración Universal de Derechos Humanos (DUDH) y el 3° Constitucional, expresan el derecho a la educación, la necesidad de que exista una preparación y por tanto el acceso a una educación digna y de calidad, lo que ha llevado a las naciones a revolucionar todas las formas en el desarrollo de la educación, anteriormente no todos tenían acceso a las aulas escolares. Fundación Telefónica (2014) indica que en estos tiempos los gobiernos de los países crean proyectos y brindan apoyo e infraestructura tecnológicas para proponer y crear un modelo de educación híbrida (presencial y en línea), entendiendo que la tecnología es una herramienta, un medio que permite ver a las escuelas de una manera más atractiva a los estudiantes y con ello buscan la reinserción de los niños que han abandonado sus estudios, generando con esto un aprendizaje extendido con nuevos modelos y métodos de enseñanza en la era digital.

La crisis sanitaria del año 2020 obligo a los Gobiernos a realizar una reingeniería a sus procesos educativos, hoy se han transformado en clases en línea y a distancia, a través de los múltiples dispositivos tecnológicos, tomar clases en línea, vía internet a través de diversas plataformas y tecnologías, que simulan aulas virtuales dentro del ciberespacio. El autor Pierre Levy (2007) habla de esta transformación del conocimiento a través de la interacción con el ciberespacio y como las plataformas tecnológicas las cuales juegan un papel fundamental en estas nuevas formas de aprendizaje, en donde esta convergencia promueve

vínculos entre diferentes grupos sociales de diferentes culturas, los cuales interactúan creando nuevas comunidades virtuales dando sentido a sus actos en esta nueva forma de enseñanza.

La interacción, dentro del ciberespacio, del alumnado ha expandido diversas formas impensables de adquirir información que décadas atrás, jamás se pensó. Las bibliotecas virtuales son un claro ejemplo, anteriormente una biblioteca limitaba el número de libros o la imposibilidad de conseguir títulos, era mucho muy difícil encontrar datos y de encontrarlos, era reducida la información que te podía enseñar una enciclopedia, no por ello le restamos la importancia, solo que hoy en día basta con consultar diversos metabuscadores, hacer un clic y la información requerida aparece, es mucho más fácil encontrar títulos, intercambiar ideas en foros educativos, investigar información en la web para realizar tareas, sin duda un gran beneficio que ayuda en el desarrollo de la educación (Pesce, 2011).

2.4.1.2 Desarrollo de las TIC´s en las instituciones encargadas de impartir justicia.

La Ley General que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública, en su artículo 10. Párrafo III, en donde precisamente habla de la operación y la modernización tecnológica de las instituciones de seguridad pública. Así como las conductas han ido avanzando en temas tecnológicos, también las instituciones encargadas de la impartición de justicia y prevención de los delitos, tienen que estar a la vanguardia, con equipos, Software especializado y tecnología de punta, creando con esto un cambio en los procesos, rompiendo las barreras culturales y desarrollando nuevas formas de interacción a nivel nacional e internacional en el empleo de las tecnologías, creando una mejora en los procesos de prevención y todo aquello que logre favorecer el esclarecimiento de los hechos delictivo y con ello se disminuya el índice delictivo.

2.4.1.3 Desarrollo de la TIC´s en la infraestructura Industrial

Las empresas industriales tenían entre sus principales preocupaciones las de contar con el personal suficiente que fuera capaz de solventar las necesidades de la empresa, en cuanto a elaboración de productos y manejo de la maquinaria, pero esto ha quedado atrás. Para Pérez (2008) la productividad de las empresas u organizaciones se verá reflejado principalmente por la adopción de una infraestructura tecnológica que renueve los procesos de producción, distribución y consumo, creando con estos cambios en los procesos de comunicación e interacción en la forma de interrelacionadas en el proceso económico, generando al interior una nueva cultura organizacional enfocada a la adopción de las TIC´s, como parte de sus actividades cotidianas.

Por otro lado, Galo y Cano (2018) señala que el enfoque tradicional ya no basta para lograr ser competitivo y permanecer a flote en esta nueva era tecnológica, pues los múltiples cambios que se han dado en todas las esferas sociales y los ámbitos laborales y del mercado, nos arrojan a otros cambios, no solo

tecnológicos, sino estructurales, culturales y de clima organizacional, motivo por el cual las TIC's en las empresas se han ido posicionando de manera importante y favorecedoras de múltiples ventajas a su adopción.

2.4.1.4 Desarrollo de las TIC´s en el Sector Salud

En este sentido Guanyabens (2020) destaca como las tecnologías de la información han transformado la forma en la que las áreas de salud brindan los diferentes servicios a los pacientes, son una herramienta estratégica que a través de software y equipo clínico de alta especialidad (hardware), con el fin de mejorar la atención que se le brinda a los pacientes, la información que se acopia de los diversos pacientes es automatizada, procesada y almacenada, permitiendo la creación de expedientes digitales para un fácil acceso a su consulta, formación de nuevas formas de comunicación con los pacientes, la salud intercultural se enfoca en la comunicación y dialogo como medio de intercambio y llegar a un acuerdo entre la enfermedad a tratar y el servicio prestado, respetando las creencias y costumbre de los pacientes, salvaguardando en todo momento la salud.

2.4.2 Impactos negativos de las TIC´s en la interacción humana

El desconocimiento de muchos es la ventaja de pocos, esto ha facilitado que el uso que se le da a las tecnologías de la información, no siempre sea el que se desea y por lo contrario surjan comportamientos que llegan a tener un impacto negativo, el cual se ve reflejado en conductas que amenazan la integridad de los usuarios de internet tales como:

Cyberbullyng: Acción mediante la cual un menor atormenta, hostiga, amenaza, humilla o molesta a otro/a menor mediante el uso de Internet, teléfonos móviles, videoconsolas online u otras (Morales et al., 2016).

Sexting: Envío de contenidos de tipo sexual (principalmente fotografías y/o vídeos) producidos por el/la propio/a remitente, a otras personas por medio de teléfonos móviles (e-legales, 2016).

Sextorsión: Chantaje a una persona por medio de una imagen de sí misma desnuda que ha compartido a través de Internet o móviles mediante sexting o que le ha sido robada (e-legales, 2016).

Grooming: Prácticas online de ciertos adultos para ganarse la confianza de un (o una) menor fingiendo empatía, cariño, etc., normalmente bajo una falsa identidad de otro/a menor, con fines de satisfacción sexual (e-legales, 2016).

Ciber-enamoramiento: comunicación que se entabla a través de la redes sociales, al ingresar a sitios específicos para encontrar pareja, donde se crea una contacto visual dando con esto paso a una nueva

forma de relaciones afectivas, en la búsqueda de personas con los mismos gustos y afinidades (Carrique, 2005).

Ciber-acoso: Acoso realizado principalmente mediante el uso de TIC´s, especialmente en internet (e-legales, 2016).

Suplantación de identidad: Hacerse pasar por otra persona, a través de diferentes formas, ya sea por teléfono, correo, plataformas sociales, entre otras, con el fin de acceder a cierta información y beneficios económicos o personales (Piragof, 2013).

Retos y juegos sociales: Tendencia viral en la que se invita al resto de la gente a realizar un reto, a hacer algo, ya sea por una causa benéfica o simplemente por diversión (Multiconversion, 2020).

Ingeniería social: técnicas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima (Hadnagy, 2011).

Siendo importante mencionar las variantes de esta conducta de riesgo:

Phishing: se caracteriza por el envío masivo de correos a diferentes empresas, organizaciones, Instituciones Bancarias, haciéndose pasar por una fuente confiable, con la finalidad de obtener datos sensibles y realizar un fraude en detrimento del patrimonio del o los usuarios (Hadnagy, 2011).

Spear-phishing: es una técnica dirigida a usuarios específicos a través del envío de correos electrónicos personalizados a la víctima, empresa, organización, Gobiernos, entre otras (Abu-Nimeh, y otros, 2009).

Smishing: es una práctica través del envío de mensajes de texto SMS o mensajería instantánea de tipo fraudulento, con el fin de obtener información confidencial (Abu-Nimeh, y otros, 2009).

Vishing: técnica en la cual hace uso de las líneas telefónicas para obtener información sensible por medio del engaño haciéndose pasar por alguien confiable (Abu-Nimeh, y otros, 2009).

Pharming: instalación de código malicioso en un dispositivo móvil o servidores, aparentando ser sitios reales de empresas o Instituciones financieras (Abu-Nimeh, y otros, 2009).

La siguiente tabla muestra las conductas de riesgo en el ciberespacio, las cuales nacen y son exponenciales dado el uso de las tecnologías de información y comunicaciones, de igual manera se describen sus características, los riegos y las formas de prevención:

Tabla 5. Conductas de riesgo especializadas.

Conducta de riesgo	Consiste en:	A través de:	Características de la conducta:	Riesgo a la salud:	Forma de prevención:
Cyberbullyng o ciberacoso	Acción mediante la cual una persona utiliza las TIC´s para atormentar, hostigar, amenazar, humillar, denostar o molestar a otra persona.	▪ Redes sociales ▪ Mensajería instantánea ▪ Mensajes de texto ▪ Foros y salas de chat ▪ Salas de juego ▪ Teléfonos móviles	▪ Acoso en redes sociales. ▪ Envió de memes. ▪ Insultos por mensajes. ▪ Perfiles falsos para ridiculizar. ▪ Adopción de roles imaginarios. ▪ Propagar rumores. ▪ Publicaciones ▪ Fotomontajes de la víctima.	▪ Desarrollo bajo de autoestima. ▪ Cambios de comportamiento ▪ Ausentismo escolar. ▪ Depresión. ▪ Suicidio. ▪ Dificultad al momento de relacionarse ▪ Dolores de estómago, cabeza. ▪ Problemas de sueño. ▪ Irritabilidad	▪ Gestión de las redes sociales. ▪ Aplicación de controles parentales. ▪ Concientización del uso seguro de las TIC´s. ▪ Dialogo, sobre la adquisición de valores como el respeto, empatía y la tolerancia. ▪ No responder a las provocaciones de los acosadores.
Sexting	Creación, difusión, reproducción y almacenamiento de fotografías o videos con contenido explícito.	▪ Redes sociales ▪ Mensajería instantánea ▪ Mensajes de texto ▪ Teléfonos móviles ▪ Correo electrónico ▪ Plataformas en línea	▪ Acoso ▪ Amenazas ▪ Extorsiones. ▪ Humillaciones. ▪ Grabadas de forma consentida u oculta. ▪ Abuso emocional ▪ Uso de perfiles falsos, para contactar a la víctima.	▪ Desarrollo de bajo autoestima. ▪ Cambios de comportamiento ▪ Ausentismo escolar. ▪ Depresión. ▪ Suicidio. ▪ Trastornos psicológicos. ▪ Problemas laborales.	▪ Gestión de las redes sociales. ▪ Evitar contactos con desconocidos. ▪ No publicar, ni enviar contenido íntimo en la red o por cualquier otro medio. ▪ Cambiar contraseñas periódicamente.
Sextorsión	Chantaje a una persona por medio de una imagen o videos con contenido íntimo. Su característica es la amenaza de publicar estos contenidos si no se cumplen las demandas del extorsionador.	• Redes sociales • Mensajería instantánea • Mensajes de texto • Teléfonos móviles • Videoconferencia • Correo electrónico • Sitios de citas en línea.	• Amenazas • Chantajear • Extorsionar • Manipulación emocional • Suplantación de identidad • Pago de dinero	• Desarrollo de bajo autoestima. • Cambios de comportamiento • Ausentismo escolar. • Depresión. • Suicidio. • Trastornos psicológicos • Problemas laborales	• Gestión de las redes sociales. • No publicar fotos o videos. • No proporcionar datos personales. • No publicar contenido intimo en la red. • No enviar contenido intimo por ningún medio. • Cambiar contraseñas periódicamente.
Grooming	Es una conducta de riesgo, en la que un adulto se hace pasar por un menor de edad, con el fin de ganarse la confianza y empatía, con fines sexuales.	• Redes sociales • Mensajería instantánea • Mensajes de texto • Foros y salas de chat • Juegos en línea • Llamadas telefónicas	• Empatía para generar un lazo de amistad. • Modificación de la identidad. • Seducción o provocación. • Envió de imágenes con contenido sexual. • Chantaje • Abandono del hogar.	• Desarrollo de bajo autoestima. • Cambios de comportamiento • Ausentismo escolar. • Depresión. • Suicidio. • Dificultad al momento de relacionarse. • Dolores de estómago y cabeza.	• Gestión de las redes sociales de los menores. • Aplicaciones de controles parentales. • Concientización sobre los riesgos en el uso de las TIC´s. • Evitar contactos con desconocidos. • Dialogo abierto.

					• Problemas de sueño. • Irritabilidad.	• Reportar estos comportamientos. • Supervisión por parte de los padres de familia.
Ciber-enamoramiento	Es una conducta en línea, donde a través de las diferentes interacciones en las plataformas sociales, se da una conexión emocional y romántica.	• Redes sociales • Mensajería instantánea • Mensajes de texto • Foros y salas de chat • Juegos en línea • Llamadas telefónicas • Aplicaciones de citas en línea	• Generar un lazo de amistad. • Intercambio de mensajes. • Llamadas telefónicas • Seducción o provocación. • Chantaje • Abandono del hogar.	• Cambios de comportamiento • Ausentismo escolar. • Depresión • Suicidio • Dolor de estomago	• Gestión de las redes sociales. • No busques relaciones por internet. • No proporciones información sensible. • No aceptar citas con extraños. • Verificar el contenido de un perfil que no sea falso.
Pornografía	Posesión, promover, producir y difundir por cualquier medio tecnológico imágenes con contenido sexual	• Redes sociales • Mensajería instantánea • Mensajes de texto • Foros y salas de chat • Juegos en línea • Dark web • Servicio de intercambio de archivos • Sitios WEB	• Publicaciones de videos o imágenes de dibujos animados en redes sociales. • Creación de perfiles falsos de venta o consulta. • Información en páginas para adultos. • Plataformas en línea. • Servicios de streaming	• Desarrollo de bajo autoestima. • Cambios de comportamiento • Ausentismo escolar. • Depresión. • Suicidio. • Dificultad al momento de relacionarse • Dolores de estómago, cabeza. • Problemas de sueño. • Ansiedad • Irritabilidad • Conductas inapropiadas	• Gestión de las redes sociales. • No publicar fotos, videos e información sensible. • Verificar el contenido de un perfil que no sea falso. • Software de filtrado • Reportar estos comportamientos. • Supervisión por parte de los padres de familia. • Concientización sobre los riesgos en el uso de las TIC´s.
Suplantación de identidad	Hacerse pasar por otra persona, a través de diferentes formas, ya sea por teléfono, correo, plataformas sociales, entre otras, con el fin de acceder a cierta información y beneficios económicos o personales.	• Redes sociales • Mensajería instantánea • Mensajes de texto • Pishing • Hacking • Robo de información • Software malicioso	• Se hacen pasar por otra persona en redes sociales. • Creación de perfiles falsos. • Robo de claves de cuentas bancarias. • Robo de contraseña de correo electrónico de la víctima. • Crear un perfil falso para contactar a las víctimas y recabar información personal.	• Depresión. • Dolores de estómago y cabeza. • Problemas de sueño. • Irritabilidad • Ansiedad. • Suicidio	• Gestión de las redes sociales. • Concientización del uso seguro y sano de las redes sociales. • Activar la doble autenticación para proteger todas tus cuentas. • No abrir mensajes ni mail sospechosos. • No compartir fotos o videos comprometedores • Cambiar contraseñas periódicamente. • Denunciar

Retos y juegos sociales	Son juegos que se plantean a los niños, a través de pruebas que deben ir pasando, algunos de ellos terminan con su vida	• Redes sociales • Mensajería instantánea • Foros y salas de chat. • Salas de juego • Teléfonos móviles	• Videos virales y peligrosos. • Se practican comúnmente por jóvenes en las escuelas, parques y lugares cerca de su domicilio. • Popularidad • Participación masiva • Difusión rápida	• Lesiones físicas • Presión psicológica • Suicidio. • Ansiedad • Irritabilidad • Dificultad al momento de relacionarse • Dolores de estómago y cabeza.	• Gestión de las redes sociales. • Aplicaciones de controles parentales. • Concientización del uso seguro y sano de las redes sociales • Constante dialogo, sobre la adquisición de valores como el respeto o la tolerancia. • No compartir estos retos. • Evitar contactos con desconocidos.
Ingeniería social	Tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima.	• Redes sociales • Mensajería instantánea • Mensajes de texto • Foros y salas de chat • Salas de juego • Teléfonos móviles	• Ataques dirigidos • Envió de correos electrónicos. • Llamadas telefónicas. • Envió de enlaces a páginas web. • Fraudes • Oferta de productos por debajo de su valor. • Envió de mensajes SMS o por mensajería instantánea.	• Estrés • Ansiedad • Depresión • Irritabilidad • Suicidio por pérdidas financieras • Problemas al relacionarse • Trastornos del sueño • Problemas digestivos	• Gestión de las redes sociales. • No abrir archivos de dudosa procedencia. • Validar la información del sitio WEB a consultar. • No descargar archivos adjuntos que no se conozca el remitente. • No conectarse de redes WIFI abiertas • Actualizar el sistema operativo, instalación de antivirus, parches de seguridad.
Phishing	Se caracteriza por el envío masivo de correos a diferentes empresas, organizaciones, Instituciones Bancarias, haciéndose pasar por una fuente confiable, con la finalidad de persuadir a las personas para obtener datos sensibles y realizar un fraude en detrimento del patrimonio del o los usuarios.	• Correo electrónico. • Mensajería instantánea • Mensajes de texto • Llamadas telefónicas • Sitios web falsos	• Nombres de empresas reales. • Imágenes corporativas • Nombres de empleados • Mensajes con cabeceras de asunto: urgente, facturación, instrucciones del jefe, temas fiscales. • Enlaces sospechosos • Mensajes con faltas de ortografía y mal redactados.	• Estrés • Ansiedad • Depresión • Irritabilidad • Suicidio por pérdidas financieras • Problemas al relacionarse • Trastornos del sueño • Problemas digestivos	• Instalación de sistemas de seguridad. • Capacitación al personal. • Confirmar la información. • Instalación de antivirus. • Políticas internas de seguridad informática. • Actualizaciones a los sistemas de seguridad. • No dar clic a enlaces sospechosos.

Speer phishing	Es una técnica dirigida a usuarios específicos a través del envío de correos electrónicos personalizados a la víctima, empresa, organización, entre otras	• Redes sociales • Mensajería instantánea • Mensajes de texto • Correo electrónico. • Llamadas telefónicas	• Enlaces a páginas web falsas. • Correos con modificaciones en el dominio • Fallas de seguridad internas. • Descarga de archivos adjuntos.	• Depresión. • Dolores de estómago, cabeza. • Enfermedades. • Problemas de sueño. • Suicidio.	• Instalación de sistemas de seguridad. • Capacitación al personal. • Confirmar la información. • Instalación de antivirus. • Políticas internas de seguridad informática.
Smishing	Es una práctica través del envío de mensajes de texto SMS o mensajería instantánea de tipo fraudulento, con el fin de obtener información confidencial.	• Mensajes de texto SMS	• Enlaces maliciosos con mensajes aparentemente confiables.	• Depresión. • Dolores de estómago, cabeza. • Enfermedades. • Problemas de sueño. • Suicidio.	• Instalación de antivirus. • Concientización sobre el uso de los dispositivos móviles. • Evitar responder los mensajes.
Vishing	Técnica en la cual hace uso de las líneas telefónicas para obtener información sensible por medio del engaño haciéndose pasar por alguien confiable.	• Llamadas telefónicas	• Información confidencial. • Familiares en problemas o secuestrados. • Extorsión	• Depresión. • Dolores de estómago, cabeza. • Enfermedades. • Problemas de sueño. • Suicidio.	• Confirmar la información. • Instalación de antivirus. • Concientización sobre el uso de los dispositivos móviles.
Pharming:	Instalación de código malicioso en un dispositivo móvil o servidores, aparentando ser sitios reales de empresas o Instituciones financieras.	• Sitios WEB	• Manipulación de sitios web. • Re direccionamiento del Router. • Envenenamiento en los DNS • Cambio del archivo del local host.	• Depresión. • Dolores de estómago, cabeza. • Enfermedades. • Problemas de sueño. • Suicidio.	• Sistemas de seguridad. • Capacitación. • Confirmar la información del sitio WEB. • Instalación de antimalware, antivirus y técnicas antipharming. • Políticas internas de seguridad informática.

Fuente: Elaboración propia con base en experiencia y en la literatura revisada (2020).

Derivado de lo plasmado en el cuadro se observa que la disrupción tecnológica ha venido a transformar las formas de comunicación y de interrelacionarnos en el ciberespacio, aunado al uso excesivo de las plataformas tecnológicas, el acceso a los dispositivos móviles, la conectividad y almacenamiento, con ello los riesgos asociados a su uso, dando paso surgimiento de violencia y de conductas de riesgos que afectan de diversas maneras a los usuarios, desde un simple cambio de conducta hasta llegar incluso a causar la muerte, por lo cual resulta imperante trabajar en una educación de protección adecuada al momento de interactuar y navegar en el ciberespacio, de aquí la propuesta de la creación de una cultura de ciberseguridad, buscando hacer del internet un espacio más seguro y confiable para la Sociedad Michoacana.

Para una mayor comprensión sobre las acciones y métodos utilizados por los ciberdelincuentes para comprometer los sistemas y la información de los usuarios, empresas o gobiernos, en el anexo 4 se muestran los principales vectores de ataque.

Por otra parte es necesario poner particular atención a las conductas nocivas que repercuten en la salud mental y emocional, que pueden estar presentando los usuarios de las TIC's, las cuales son resultado del contacto con los medios cibernéticos. Con la llegada de la pandemia por el virus SAR-COV 2, que obligó al confinamiento, se generaron diferentes cambios en la rutina diaria y en la forma de interactuar del mundo, originando con esto mayor tiempo de ocio, suscitando una sobredosis de estímulos digitales que hacen que la distracción aumente, reduciendo con esto la capacidad de atención y concentración, desencadenando alteraciones a la salud, como las que se enlistan a continuación:

2.4.3 Efectos psicológicos en el uso de las TIC´s

Aislamiento social: Para Oñate (2014) define como la ausencia de la vida social, dejando de lado las interacciones intrafamiliares y académicas, evitando todo contacto físico con el exterior, saliendo de su espacio solo para lo esencial, presentando cambios en su rutina, horas de sueño, hábitos alimenticios, llegando a desarrollar poca tolerancia, baja autoestima, inseguridad, causando con esto daños en su salud física y psicológica, ya que al no realizar otras actividades y al aislarse se pierde esa capacidad para desarrollar habilidades sociales y de interacción con el resto de la sociedad.

Por consiguiente, Desmurget (2020) menciona que con la incorporación de las TIC´s, como parte de la vida social, se favorece el desarrollo del aislamiento, mencionado anteriormente, dado que las nuevas TICS, así como el fácil acceso a los dispositivos permiten crear una nueva forma de comunicación de los individuos, absorbiendo más tiempo del habitual, dejando de lado actividades esenciales (estudiar, convivir con la familia, hacer ejercicio, entre otras), considerando que no es necesario la interacción cara a cara, creando con esto problemas de salud, como es: sedentarismo, depresión, problemas alimenticios, del sueño, afectando su desarrollo social y emocional.

Alteraciones cognitivas: Para Quijano et al. (2010) Bajo este concepto se contemplan alteraciones de las funciones cognitivas que no permiten concentrarse, falta de memoria para recordar, problemas para procesar la información, lenguaje, comunicación y falta de atención para desarrollar sus actividades con normalidad.

Por esta razón y con la interacción de las TIC´s como parte de nuestra vida cotidiana, Desmurget (2020) comenta que se puede desarrollar está alteración, ya que al utilizar de manera excesiva los dispositivos

móviles para consultar información, se deja de lado la habilidad de analizar y la falta de procesamiento de la información, generando con esto aprendizajes incompletos o erróneos, anulando habilidades de comunicación, pérdida de memoria de corto plazo al tener la información en los dispositivos evitamos esforzarnos en recordarla, lo que disminuye el rendimiento y la capacidad citica de análisis para desarrollar las actividades sin la ayuda de las TIC´s.

Trastorno del sueño: la Asociación Americana de Psiquiatría (2014) lo describe como todas aquellas alteraciones y problemas relacionados con el sueño, mismos que impiden que el descanso de una persona pueda ser el correcto, causado debido a diversos factores tales como: malestares clínicos, insomnio, dificultades para conciliarlo aun cuando se tiene sueño, depresión, ansiedad, entre otros, provocando en la salud, bajo rendimiento, cansancio, irritabilidad, mal humor, dificultad para concentrarse, afectando el rendimiento de la rutina habitual.

Del mismo modo para Patino (2020) la exposición desmedida a los diversos dispositivos móviles y a los contenidos que ofrecen como fuente de entretenimiento, provocan que se destine tiempo de sueño por seguir conectados a las diferentes plataformas sociales, video juegos, mensajería instantánea, contenidos audiovisuales en línea, descargando música, leyendo noticias, entre otras actividades, causando que la falta de descanso genere problemas para concentrarse, bajo rendimiento, irritabilidad, sueño intranquilo revisando si hay nueva actividad en el celular, afectando con esto la salud.

Trastorno del ánimo: para la Asociación Americana de Psiquiatría (2014) quien lo defino como las alteraciones en los estados emocionales del ser humano en periodos prolongados de tristeza, exaltación, depresión, irritabilidad, clasificándolo en depresivo y bipolar, poniendo en riesgo la salud y en algunos casos la vida de las personas e interfiriendo en su capacidad de desarrollar sus actividades habituales.

Como resultado de la interacción con las TIC´s y su uso excesivo, Echeburúa y De Corral (2010) comentan que provocan diversos estados de ánimo, como la irritabilidad al no poder conectarse a las redes sociales o ser limitado a su uso, tristeza al no obtener la respuesta que se espera en las diversas plataformas (desde no tener suficientes amigos en Facebook, no obtener likes o reacciones ante sus publicaciones, que sea dejado en visto al entablar comunicaciones por mensajería instantánea) ocasionando con esto un trastorno depresivo por todo el consumo de información que circula en el ciberespacio y la incitación para realizar retos y juegos virales que en muchas ocasiones terminan con la vida ya que son incitados al suicido aprovechando la alteración que presenta su estado de ánimo.

Identidad: para Ovejero (2015) quien la define como el conjunto de características que identifican a una persona y la distinguen de otras, por: su carácter, habilidades, virtudes, actitudes, temperamento,

mencionando que estás se van modificando con el paso del tiempo y desencadenas cambios en el ser humano a lo largo de su vida.

Con la aparición de las TIC´s, Ruiz y De Juanas (2013) refieren que los usuarios pueden interactuar a través de las diferentes plataformas sociales que coexisten en el ciberespacio, con la posibilidad de crear una personalidad diferente, distorsionada (falsa) de quien en realidad es, ocultándose a través de una pantalla, sintiéndose más libre de expresarse, de interactuar y de crear nuevas formas de comunicación, afectando con esto su desarrollo, presentado cambios de comportamiento, de ánimo o modificando incluso su carácter al posicionarse en una personalidad virtual.

Adicción: Sosa (2014) lo describe como determinadas sustancias y conductas que afectan al cerebro, volviéndose una enfermedad crónica, actuando de manera impulsiva para conseguir determinados estímulos que satisfacen la dependencia a ciertas drogas o conductas (juegos, apuestas, compras, videojuegos), afectando la salud y provocando cambios en el comportamiento.

De ahí que para Echerburúa y Requesens (2012), con el surgimiento de las redes sociales, se está presentando una inclinación desmedida a mantenerse conectado al ciberespacio o por el uso excesivo de algún dispositivo, videojuegos, Facebook, Instagram, TikTok, YouTube, Twitter, entre otras, causando una adicción en espera de nuevos mensajes, comentarios, reacciones, posteos, publicaciones manifestando la necesidad de mantenerse alerta de cualquier nuevo cambio que pueda darse, ya que es necesario estar informado de todo lo que sucede alrededor, satisfaciendo esa dependencia, ocasionado con esto afectaciones a la salud como: aislamiento, desinterés en otros temas, cambios de conducta, irritabilidad, afectando su salud, entre otros.

Derivado de lo antes expuesto y con el nacimiento de las TIC´s, en esta era digital emerge la cibercultura como una nueva forma de comunicación, interacción y entretenimiento, generando desarrollos políticos, sociales, económicos, entre otros, pero también como una fuente de conflicto social. Siendo importante crear en la sociedad una cultura digital ética que permita la interacción en el ciberespacio de una manera confiable, empática, armónica y responsable que guíen la actuación de los usuarios en su interacción en el ciberespacio.

2.5 Cibercrimen

Con el surgimiento de las Tecnologías de la Información y Comunicaciones (TIC´s) han nacido nuevas modalidades en la comisión de delitos, mismas que varios autores manejan como “ciberdelincuencia” “cibercrimen” o “cibercriminalidad” y, que no resultan ilícitos para nada nuevos, sino la adaptación de

estos a una nueva forma de vida, en la cual nos encontramos inmersos la mayoría como parte de nuestra evolución, lo que ha facilitado la existencia de las sociedades en términos de acceso a la información, comunicación, actualmente, basta con un clic para acceder a ingentes cantidades de información y diverso contenido (páginas web, sitios de mensajería instantánea, sitios de citas en línea, contenido no apto para menores de edad, videos, pornografía, entre otros), así como realizar actividades que permiten ser víctimas de este fenómeno que va en aumento y que conocemos como "cibercrimen", en el presente la falta de leyes que regulen este tipo de conductas no están actualizadas, o bien, ni siquiera existen algunas que sean capaces de reglamentar la navegación de las mismas en el ciberespacio.

Esta evolución tecnológica ha dado origen a nuevas modalidades delictivas derivadas de su uso, tales como: robo de información, suplantación de identidad, sabotajes informáticos, fraudes bancarios, falsificación de documentos digitales, divulgación de obras protegidas por derechos de autor, trata de personas, pornografía, ataques al honor, ataques a la imagen, violencia digital a la intimidad sexual, entre otros.

La delincuencia ha sido un tema de interés para los Gobiernos, durante el siglo XIX varios fueron los grupos de expertos pertenecientes cientistas sociales, juristas y penitenciarios que se preocupaban por descubrir aquello que movía al ser humano en la comisión de un delito y reformar las leyes penales que según Rodríguez (1981) basadas en el libre albedrío, principalmente buscaban entender el comportamiento delictivo y al mismo al autor del delito, por lo que varias escuelas influyeron y aportaron estudios referentes a la criminología, misma que revolucionó a partir de Cesare Lombroso y su aportación en cuanto a la clasificación del delincuente, Rafael Garofalo y su teoría de la pena, en donde la clasificación del delincuente por delitos era necesaria, ya que algunos delincuentes presentaban mayor peligrosidad y esto era dependiendo el delito que se hubiese cometido y la gravedad de este. Enrico Ferri, también perteneciente a la escuela positiva creía que existían factores de tipo social que rodeaban el ambiente y dotaban al individuo de una capacidad para delinquir.

De aquí que resulta importante conocer no solo los factores criminológicos, sino, las diversas teorías criminológicas de la ciberdelincuencia, así como, la criminogenésis y criminodinámica ya que son aspectos de gran importancia que atienden todo un estudio de la cibercriminalidad y, que nos dan la oportunidad de aportar un razonamiento para la prevención de los ciberdelitos, a partir del reconocimiento, de la importancia de las tecnologías de la información como factor determinante en la vida social, aunado al incremento de usuarios conectados y la utilización de este medio para el desarrollo de las actividades cotidianas, así como el incremento de delitos cibernéticos y la falta de una legislación que permita regular

y sancionar las conductas dentro del ciberespacio, empezaremos hablando de aquellos elementos que forman parte de la teoría de la anomia actual en Michoacán

2.5.1 Funcionalismo

El funcionalismo para Durkheim (1895) es una teoría socio-antropológica que explica los fenómenos sociales, por lo que una vez que llegamos a formar parte de esta sociedad, observamos que ésta ya cuenta con una estructura sólida, que cumple con funciones, de las cuales con el paso del tiempo vamos siendo parte, es decir, y como ya lo sabemos, el ser humano es un ser social por naturaleza, desde antes de su nacimiento "concepción" y hasta el día de su muerte "o aun después de ella", existen actividades, roles, normas y dentro de estás ultimas las hay de diversos tipos (religiosas, sociales, jurídicas y morales).

Entendiendo que ya existe una "forma" de "cómo hacer las cosas", es decir, a lo que Durkheim (1895), denominó "fenómenos que se desarrollan dentro de la sociedad" y éstos existen en "todas" las sociedades, es decir, en los diversos países, culturas, subculturas e inclusive dentro de las esferas pertenecientes a una comunidad "esferas sociales".

Durkheim (1895) hace la distinción de fenómenos determinados entre unas ciencias, explicando así el funcionalismo desde la ciencia sociológica, por lo cual ejemplifica que, el ser humano cumple con cierto tipo de tareas, las cuales podíamos denominar; "tareas personales", es decir, (como hermano, amigo, padre, etc.) así mismo, con aquellos compromisos que han sido adquiridos dentro de la sociedad y los deberes que han sido definidos a través de las "Leyes y Costumbres", aunque cabe señalar que, él no los ha creado, sino más bien le han sido conferidos a través de la educación, y así sucesivamente de generación en generación. Ya que previo al nacer, existe un sistema de creencias, lenguaje, "sistema de signos para expresar el pensamiento", estructura financiera, política, organización social y cultural y éstas "funcionan" independientemente del uso que cada individuo haga de los mismos, tenga conocimiento o desconocimiento de los mismos, es a este proceso imperativo y coercitivo a lo que Durkheim (1895) denominó "funcionalismo", habiendo comprendido el funcionalismo y con ello entendiendo que la organización social es trascendente dentro de las sociedades, y que el ser humano asume roles dentro de la misma para el desarrollo, es por ello que establece ciertas normas que regulen las conductas de convivencia de las sociedades, pero, estás conductas a veces llegan a ser desviadas y es por ello y, que al ser cometidas solo por unos cuantos y no por todos los miembros de una comunidad, Durkheim comienza a investigar este tipo de conductas, naciendo con ello su teoría de la anomia.

2.5.1.1 Teoría de la anomia Émile Durkheim.

Para poder comenzar con la teoría de la anomia es necesario conocer los antecedentes que dieron origen a la misma. La revolución Industrial trajo consigo transformaciones económicas y sociales considerables a

nivel mundial, pero en América Latina y en particular en México, durante el porfiriato la era de la revolución industrial llegó y dejó cambios radicales en la economía para su sostenimiento y desarrollo evolutivo, estos cambios repercutieron no solo en la vida económica del país, sino en diversos sectores como lo fue en la estructura de la sociedad.

El surgimiento de movimientos migratorios internos y externos, el aumento de la población, la modificación de las estructuras sociales y económicas y la desigualdad en actividades, oportunidades y beneficios fueron consecuencias considerables que marcaron éste período industrial.

Estos cambios sociales han sido la pauta que han motivado diversas teorías, ya que la era de la industrialización no ha sido propia de un Estado, sino que ha sido de impacto mundial, tomando en cuenta algunos de las teorías realizadas principalmente por Emile Durkheim y Robert Merton.

Para Durkheim (1895) la sociedad cumple con dos funciones, la primera es integradora, mientras que la segunda es regulatoria, si la función regulatoria no se ejerce adecuadamente, los individuos de una comunidad se encuentran frente a la anomia, que dicho en otras palabras es la ausencia de normas competentes en regular la convivencia y el actuar de los miembros de la misma.

Con ello Durkheim (1895), explica que dentro de la sociedad, las actividades realizadas por los miembros de la misma cumplen con una función, en donde se busca alcanzar su eficiencia a través de ideas y sentimientos que son comunes y prevalecen dentro de ésta, lo que Durkheim reconoce como "Solidaridad Social". Pero, la modernización y con ello el paso de una sociedad tradicional a una sociedad alcanzada por la modernización "sociedad moderna" ha ocasionado una transformación en su base y funciones, sobre todo en la regulación de ésta, con cambios considerables en las normas y conductas de los integrantes de la misma. Puesto que, en una sociedad tradicional el tipo de solidaridad se le reconoce como "mecánica", principalmente basa sus funciones en la uniformidad de creencias y costumbres, dicha sociedad se caracteriza por ser hermética y no aceptar alguna diferencia en cuanto a creencias o costumbres por verse amenazados, podemos considerarlo meramente convencional, por lo que castiga el comportamiento que atenta contra sus intereses protegiéndolos, mientras que las sociedades modernas que se caracterizan por la "solidaridad orgánica", se han visto considerablemente modificadas en su estructura, lo que ha repercutido directamente en la regulación, es decir, las reglas para regular las relaciones de los miembros de la misma, originando una anomia.

2.5.1.2 Teoría de la anomia Robert Merton.

Mientras que Durkheim ha explicado la anomia como una transición de la sociedad a una modernización, atribuyéndole la misma al cambio social que consigo ha dejado el proceso de la industrialización, Merton centra su atención no solo a la carencia de valores, sino debido al cambio en éstos y la falta de interés en

los mismos, es decir, una modificación en los valores, al fijarse como fin y obligación para todos los ciudadanos la acumulación de riquezas materiales, la obtención de estas pueden ser por cualquier medio sin importar si con ello infringen las leyes.

Por otra parte para Huertas (2010) quien hace una comparación sobre la teoría de la anomia de Durkheim y Merton, en donde se observa que mientras para Durkheim son "necesidades naturales" del individuo aquellas que se ven afectadas por la sociedad, para Merton estas necesidades son "culturales", es decir, dentro de un modelo de sociedad las diversas contradicciones internas entre los diversos grupos sociales ocasiona una disfunción estructural, que radica en cierto grupo de la sociedad.

Para Merton según Huertas (2010), las contradicciones existentes entre la "estructura social" y la "estructura cultural", originan una anomia dentro de la sociedad, aunque su principal estudio fue a la sociedad "norteamericana", la falta de oportunidades y desigualdad se puede observar en cualquier modelo social de cualquier país, pues toda sociedad en la búsqueda por alcanzar sus objetivos y metas culturales, precisa, regulariza y controla los medios para alcanzar dichos fines. Por otro lado, la socialización y el grado de la misma manifiestan la interiorización de los valores y las normas, mismos que hoy en día los seres humanos ya no respetan.

Si bien, la teoría de la anomia nos muestra una ausencia de normas desde la perspectiva de Durkheim, desde la de Merton, es una falta de regulación, por modificación de los valores y la desigualdad en la que se encuentra la sociedad en general. Centrando nuestra atención a los delitos de tipo cibernético o "ciberdelitos", se observa la ausencia de un marco normativo que permita una correcta impartición de la justicia en la regulación del ciberespacio, o bien, la falta de certeza jurídica conveniente que permita encuadrar los delitos en tipos penales apropiados que den la certeza a los usuarios en su interacción en el ciberespacio, lo que ha dado origen al aumento de los mismos en la sociedad de Michoacán, la génesis de los ciberdelitos podría atribuirse a la ausencia de leyes para dar respuesta a estos delitos de alta especialidad y complejidad. Por lo cual abordaremos los siguientes conceptos;

2.5.2 Teorías criminológicas de la ciberdelincuencia.

ara entender un poco más el fenómeno de la delincuencia a continuación se enlistaran las diversas teorías que han nacido de una ciencia criminológica tradicional para con ello atender los ciberdelitos, ya que por la necesidad actual se han tenido que apoyar de las bases de las teorías convencionales. Por lo que para Cámara (2020) son ocho teorías criminológicas explicativas de la ciberdelincuencia que a continuación se enlistan:

1.- Teoría del aprendizaje social y la asociación diferencial de Sutherland y Akers; según Hikal (2017) la teoría basada principalmente en el aprendizaje a través de la comunicación entre los individuos, estos individuos al encontrarse inmersos en el ciberespacio están en contacto con los ciberdelincuentes, aprendiendo de éstos últimos comportamientos desviados o conductas antisociales.

2.- Teoría de Control Social, de los vínculos sociales y de autocontrol Gottfredson y Hirschi),según Capace (2015) esta teoría hace referencia a un control personal débil socializador, principalmente relacionado a la formación de los hijos por parte de los padres, es decir, se han modificado mucho la forma de educación y de crianza, el ciberespacio nos ha envuelto dentro de su mundo y con ello los procesos de socialización se han visto afectados o modificados, por otro lado, la falta de supervisión por parte de los padres esto con relación a que cada vez los usuarios inmersos en el internet son muy jóvenes y por consiguiente vulnerables, también pueden desarrollar comportamientos delictivos dentro del ciberespacio.

3.- Teoría general de la tensión Agnew (1992), dicha teoría según Aebi (2008) deriva de la teoría de la anomia, en donde la frustración derivada de un estado afectivo negativo es la principal característica de ésta teoría, que son desencadenados por una dificultad para lograr las expectativas que desea alcanzar, la privación de estímulos positivos que desea tener o bien, estar sujeto a situaciones negativas, buscando la forma de liberarse de dichas tensiones a través de conductas delictivas en el ciberespacio, como pueden ser; “Grooming” y Ciberbullying”.

4.- Teoría de las ventanas rotas Wilson y Kellingdes desde el punto de vista de Rovira (2013) la falta de represión ante la comisión de alguna conducta que la ley señala como delictiva, al no castigar conforme a derecho, se sigue cometiendo el mismo, o incluso nuevos delitos debido a la inacción penal.

5.-Teoría de la disuasión Anwar y Loughran, en Kennedy (2016) esta teoría hace referencia a la necesidad de castigar o hacer cumplir las leyes en la comisión de los delitos, pero, dentro del ciberespacio la falta de jurisdicción e identificación del ciberdelincuente hacen que no siempre se pueda aplicar la ley, lo que sigue favoreciendo y aumentando la comisión de los ciberdelitos.

6.- Teoría de las actividades rutinarias Cohen y Felson y la teoría de la oportunidad de Cloward y Ohlin, en Aloisio (2016) dicha teoría está principalmente relacionada con la “cibervictimización” y tomando en cuenta tres factores que favorecen la victimización; “defensor motivado, víctimas propicias y la ausencia de guardianes” por un lado y por el otro, los ciberdelincuentes aumentan su motivación justamente al conocer la impunidad que existe en el ciberespacio debido a lo “anonimizador y “favorecedor” del medio, también cabe señalar que la falta de brechas legislativas y digitales son estudiadas y tomadas en cuenta por los ciberdelincuentes confieren a éstos oportunidades para la comisión de ciertos ciberdelitos.

7.- Teoría de las técnicas de neutralización, presenta Cámara (2020) que dentro de ésta teoría entran algunos ciberdelincuentes especializados como los "hackers", ya que dicha teoría propone que existe una conducta desviada que el mismo victimario rechaza como tal, al no reconocer que existe un daño ocasionado dentro de la misma, por el contrario justifican su conducta al creer que están favoreciendo y no cometiendo un ilícito, como lo es el caso de los "hackers" para mejorar el propio sistema.

8.- Teoría de la transición espacial Jaishankar según Cámara (2020) el comportamiento difiere de un espacio "real-físico" a otro "ciberespacio", 1).- existen personas con conductas delictivas reprimidas que no son capaces de cometerlas en un espacio físico "real", pero en el "ciberespacio" sí las pueden llegar a cometer; 2).- El anonimato que presenta el ciberdelincuente al estar inmerso dentro de un mundo virtual "un espacio no físico", le ayuda a cometer delitos sin que éste quede descubierto, pues sí bien, la mayoría de las personas podrían cometer delitos en un espacio real, pero los limita el hecho de ser descubiertos; 3).- algunos delitos comienzan cometiéndose en el ciberespacio y trastoca al mundo físico, como lo es el ciber enamoramiento y 4).- El ciberespacio y sus múltiples plataformas se ha convertido en un medio ideal para el "reclutamiento criminal" así como, la difusión de técnicas criminales.

2.5.3 Criminogénesis y criminodinámica.

Para conocer la criminogén7esis de la ciberdelincuencia es necesario conocer cada uno de los conceptos que dan origen a la misma y, que a continuación veremos y ejemplificaremos.

Para Rodríguez (1981)la criminogénesis y la criminodinámica se encuentran completamente ligadas, mientras que la criminogénesis explica el origen del delito a través de los factores y las causas criminógenas que han dado origen a una conducta delictiva, la criminodinámica explica los pasos que se llevaron a cabo para cometer dichas conductas.

Por otro lado, para Di Tullio (1966) la criminogénesis y criminodinámica no solo se limitan a explicar la conducta antisocial o delictiva, sino que también ayudan para el análisis del delincuente, así como de la criminalidad.

Explicaremos de manera breve los factores que inciden de manera significativa en la criminogénesis y la criminodinámica;

2.5.3.1 Factor criminógeno.

Desde el punto de vista de Rodríguez (1981) un factor criminógeno es todo aquello que contribuye a la comisión de las conductas antisociales o delictivas, mientras que para Mayorca como lo puntualiza Rodríguez, un factor criminógeno es aquel estímulo de tipo endógeno, exógeno o bien, mixto que favorece en la comisión de una conducta criminal.

Los factores criminológicos varían dependiendo el tipo de conductas delictivas, dentro de los delitos cibernéticos, pero para cada uno de estos factores criminológicos se extenderán y serán cada vez más precisos, por dar un ejemplo, los delitos de "violencia digital", un factor criminógeno sería el compartir fotografías con contenido explicito, desnudas o con poca ropa, o el simple hecho de tenerlas almacenadas en el celular o en algún dispositivo electrónico, dejarse tomar fotografías, grabarse en la intimidad y compartir esta información, sin duda favorecería la comisión de un delito.

2.5.3.1 Factor biológico.

La escuela positiva tuvo como principales exponentes a Cesare Lombroso, Rafael Garofalo y Enrico Ferri, con ello la constitución bio-psico-social del ser humano, por lo que comenzaron a tomar en cuenta Factores criminógenos de tipo biológicos, psicológicos y sociales, los factores biológicos atienden el carácter genético del individuo, la constitución biológica, aberraciones cromosomáticas, etapas evolutivas del ser humano, sistema endocrino, sistema nervioso, patologías según Rodríguez (1981)

Dentro del positivismo biológico y tratando de explicar las conductas antisociales desde una perspectiva biológica, los principales exponentes de esta corriente son Darwin y Comnte. Tal vez nos podríamos preguntar ¿Qué tipo de ciberdelitos podrían ser ocasionados por Factores Biológicos? y para ejemplificar, el "Ciberbullying" o el "Grooming", quienes representan conductas de riesgo en el ciberespacio, los cuales no son nuevos, solo han evolucionado como lo ha hecho la sociedad misma, entonces, el "ciberbullying" comúnmente se conoce como una acción para hostigar, humillar, someter o amenazar una persona a través de las diferentes plataformas sociales como lo menciona Santillán (2015), esto por medio de las tecnologías de información y comunicaciones, lo que le puede generar mayor irritabilidad y cambios en el ciclo del sueño y todas las consecuencias, así mismo, se puntualiza que la mayoría de las conductas del victimario son las mismas del bullying, pero sin la agresión física o directa.

Por otro lado, el "Grooming" atiende Factores de carácter sexual, que están relacionados directamente con factores biológicos, ya que esta conducta de riesgo ocurre entre un adulto y un menor, quien a través de la manipulación o el engaño busca ganar la empatía o la confianza de la víctima, para que realice él envío de imágenes con contenido explicito, para posterior ejecutar el chantaje para recibir más información, la siguiente etapa es la extorsión para obtener más contenido sexual a cambio de no revelar a familiares lo sucedido, el siguiente paso, es hacer que el menor salga por su propia voluntad de la casa para tener un encuentro sexual con su atacante.

2.5.3.2 Factor psicológico.

Para Rodríguez (1981)los factores psicológicos pueden ser individuales o colectivos, atendiendo temas de la personalidad, las emociones y pasiones, temperamento, procesos cognoscitivos, trastornos, entre otros.

Para ejemplificar como estos factores influyen en la ciberdelincuencias, se toma en cuenta el delito de corrupción de personas menores de edad, la creación de imágenes, distribución de vídeos y fotografías a través de sitios web, nos coloca frente a un victimario que fue víctima y normaliza este tipo de actos en contra de menores debido al quiebre emocional que sufrió en alguna etapa de su vida.

2.5.3.3 Factor sociológico.

En este sentido Rodríguez (1981) explica que los factores sociológicos se originan dentro de la sociedad y atienden hechos que se desarrollan en la misma y, que favorecen la comisión de las conductas antisociales, como lo son el medio ambiente cósmico y geográfico, la pareja delincuente, los diversos grupos primarios (pandillas), secundario (organizaciones criminales), terciario (religioso político), cuaternario (el Estado), las variables demográficas, la delincuencia urbana y rural, factor económico, espacio social, profesión, clases sociales, grupos étnicos, la familia, diversiones, guerra y postguerra, medio escolar, medios de difusión, anomalía social, subculturas, la marginalidad y desviación, las regularidades sociales de la delincuencia, entre otros.

Para explicar el factor sociológico, hablaremos del delito de fraude actualmente este delito es de los más comunes, cada vez son más los usuarios que son víctimas, previo a serlo, el ciberdelincuente hace un estudio de la víctima, pero también cuenta con conocimientos previos relacionados con las tecnologías de la información y comunicaciones o herramientas de los que se hace valer para llevar a cabo el ilícito, es decir, la profesión o preparación con la que cuenta el victimario es un factor social que tiene que ser tomado en cuenta.

2.5.3.4 Factor criminógeno de la ciberdelincuencia.

Nos encontramos ante un tema de gran importancia, pero que para algunas legislaciones carece de interés o no han sabido otorgarle el valor adecuado, en esta era tecnológica y de inteligencia artificial, el encontrarnos ante una situación en donde la Ley prevé el uso de las tecnologías a favor, inclusive los Derechos de la cuarta generación “Derechos Humanos”, están relacionados con garantizar el acceso de las TIC`s de todos los individuos, y recordemos que México forma parte de este tratado, pero, no basta con el solo hecho de avalar el acceso a internet en el país, sino, que la navegación dentro del mismo no signifique un riesgo para los usuarios del ciberespacio.

2.5.3.5 Causa criminógena.

Refiere Rodríguez (1981) que la causa Criminógena según las Naciones Unidas, es aquella condición determinante para la comisión de alguna conducta delictiva, relacionando la causa criminógena con un efecto, dando este último origen a la conducta delictiva. Una causa que se puede considerar dentro del delito de violencia digital a la intimidad sexual, aunque cabe manifestar que todas cambian aunque el

delito sea el mismo, las causas criminógenas dependen más del individuo que comete la conducta antisocial, estas puede variar aunque el tipo de conducta sea la misma.

2.5.4 Cibercriminalidad

Como se ha mencionado anteriormente con el surgimiento de las tecnologías de información y comunicación y su acelerado crecimiento, han cambiado la forma en la que las sociedades se relacionan, generando nuevas formas de conocimiento, creación de diversas aplicaciones, negocios en línea, servicios de entretenimiento, comercio electrónico, entre otras actividades que se realizan a través del ciberespacio que, como se ha mencionado, son soportadas por toda una infraestructura tecnológica (servidores, equipos de cómputo, redes de comunicación, protocolos, plataformas digitales, aplicaciones comerciales, usuarios, comunidades virtuales, enlaces de datos, redes, entre otros) como medio de comunicación que permite la hiperconexión de millones de usuarios.

Para lo cual analizáremos de manera breve el fenómeno de la sociología criminal, definida como la ciencia encargada de estudiar el delito y los factores sociales que lo producen, tratando de explicar le génesis de la conducta de quien comete el delito analizando a la sociedad.

De aquí la importancia de entender el fenómeno social, lo que nos ayudará a tener más claro todas aquellas conductas que derivan de una sociedad, es decir aquellos hechos sociales, el ser humano es un ser social por naturaleza, como bien lo dijo Aristóteles (1988) en su libro la política, el hombre es un animal social desde su concebimiento y su nacimiento llega a formar parte de una sociedad. Aristóteles concibe de esta forma al hombre y ve imposible que exista un ser insocial o que esté apartado de una sociedad o deje de pertenecer a una esfera social, ya que este sería un ser humano “no normal” al considerarlo inferior o superior, si bien el ser vivo desde su nacimiento forma parte de una esfera social (familia) y así con el paso del tiempo y durante su evolución humana propia llegará a formar parte de diversas esferas sociales más (escuela, trabajo, religión, entre otras), así se le van infiriendo al ser humano deberes y obligaciones que tendrá que in cumpliendo como el resto de los seres pertenecientes a una sociedad lo hacen y, que conocemos como normas que rigen una sociedad para que todos los seres humanos puedan vivir en armonía y paz. su parte para Durkheim (1895) los hechos sociales son aquellas formas de actuar, sentir o pensar que han sido impuestas al ser humano de una forma coercitivamente a partir de estos hechos sociales se desarrolla la forma de actuar del individuo a través de la percepción del mundo y la sociedad por eso para Durkheim no eran necesariamente individuales, sino sociales ya que estas son una base fundamental de la sociedad desde antes de formar parte de una sociedad, es decir, del nacimiento, ya existían formas de desarrollo dentro de una sociedad, formas de actuar ya establecidas en una sociedad, es

decir, ya existe una forma de hacer las cosas en cuanto a forma de trabajo, educación, o incluso de delinquir.

Motivo por el cual y a pesar de tener ideologías diferentes, Gabriel tarde considera que el ser humano manifiesta esos hechos sociales a través de la imitación considerando que a su vez esta se da por repetición, es decir, los hechos sociales son un reflejo que el individuo manifiesta a traes de la observación para posteriormente replicar esa conducta, cuando un ser comienza su vida social, es decir desde sus primeros años de vida, va desarrollando sus capacidades a través de la imitación y del aprendizaje

Mientras que Tarde (2011) menciona que toda relación humana que se da entre dos personas se encuentra regulada por lo que él llama influencia mental, en donde el ser humano busca a través de un modelo a seguir la imitación de una conducta deseada, otro elemento clave es la oposición, cuando existe un conflicto entre modelos y no se sabe cuál modelo es el que se quiere seguir y realiza una combinación de los dos, se le conoce como adaptación, es decir, todo nuevo delito es una invención cultural, en donde cada nueva motivación va inventando este nuevo delito o una nueva forma de comisión de un delito ya existente, todos estos hechos sociales no son meramente conductas del tipo social, sino que pueden desarrollarse conductas asociales, antisociales parasociales a través de las leyes de imitación desarrolladas por Gabriel Tarde.

Para Rodríguez (1981) la conducta social es aquella que cumple con todas las normas de convivencia establecidas en una sociedad (morales, sociales y jurídicas, es decir con el bien común, buscando preservar los valores que rigen a la misma (amor, respeto, amistad, entre otras), mientras que las conductas son asociales aquellas que no están relacionadas con la sociedad ni con el bien común, una vez que nos quedamos solos tienen cabida esta forma de conducta, mientras que la conducta parasocial no realiza el bien común pero tampoco llega a agredirlo, un ejemplo, las subculturas, modas usos o costumbres son un ejemplo de esta forma de conducta, y por último la antisocial, trasgrede el bien común, ya que atenta la estructura básica de la sociedad, destruyendo y lesionando las normas y valores que nos rigen como sociedad.

Menciona Tonkonoff, (2020) que los ambientalistas Lacassagne, Manouvreir, Topinard y Tarde convenían por una criminología sociológica, tratando de explicar el delito desde una interpretación sociológica, tomando en cuenta que el delito tiene una historia que tiene que ser tomada en cuenta ya que mostraran las invenciones delictivas y su propagación, el delito para Tarde es el comportamiento del individuo a través de la imitación o del aprendizaje y no algo nato como en su clasificación del delincuente Lombroso lo expuso.

Por lo antes expuesto y teniendo una visión más clara de lo que es el delito, sus antecedentes y su fenomenología, comenzaremos a describir el concepto del cibercrimen aplicado a los delitos informáticos.

Para Parada y Errecaborde (2018) desde la teoría criminalística existen dos puntos de vista en lo que a su naturaleza refiere esta conducta criminal: El primer lugar los delitos informáticos no son delitos nuevos o delitos complejos como en ocasiones se menciona, son delitos convencionales que toman nueva vida con el uso de instrumentos informáticos, aplicativos y servicios en internet. El segundo punto de vista confirma que el uso de las tecnologías de información y comunicaciones proporciona diversas herramientas para la comisión de delitos irreales, tales como virus, troyanos, gusanos, software malicioso, ataques a páginas Web, spyware, entre otros. También hay delitos habituales que toman nuevas formas a partir de equipos automatizados, como nuevas formas que no serían factibles de realizarse si no existiese el desarrollo de software, código malicioso o el almacenamiento digital para hacer que los sistemas o el hardware funcione de manera diferente a lo esperado.

Por otra parte abordaremos el concepto de delito informático, describiendo el concepto de delito, que de acuerdo con el Código Penal Federal es el siguiente:

“Artículo 7. Delito es el acto u omisión que sancionan las leyes penales.”

Enfocándonos al delito informático Téllez (2008), en su libro Derecho Informático, menciona el concepto típico de delitos informáticos: "son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin"; y en el concepto atípico menciona que "son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin". Desde un punto particular, se podría definir al delito informático como “el acto u omisión que es realizado utilizando cualquier medio electrónico y que es sancionado por las leyes penales”.

Refieren Tropinan y Callanan (2015) que, “el cibercrimen, cubre no solo los delitos cometidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, sino también los delitos de contenido (como las imágenes de abuso infantil y el contenido terrorista) y cualquier otro tipo de delitos cometidos en línea”.

Según Friedman (2014) el cibercrimen es el delito informático que “se define con mayor frecuencia como el uso de herramientas digitales por parte de delincuentes para robar o realizar actividades ilegales”.

Se entiende por “ciberdelito” o “cibercrimen” cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de

audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito Rayón y Gómez (2014).

Entendemos que la cibercriminalidad es la criminalidad que se genera en el ciberespacio por el uso de las tecnologías de la información y comunicaciones.

2.5.5 Ciberdelincuente.

Una vez que se analizaron las teorías criminológicas de la ciberdelincuencia y que conocemos que la cibercriminología no solo le interesa el estudio de los ciberdelitos, sino todo aquello relacionado con la conducta antisocial de tipo cibernético, como lo es el ciberdelincuente, pues al igual que la criminología, no solo es de interés la conducta social sino el individuo que las comete, realizando con ello una perfilación del mismo, por lo que de contar con una política preventiva, conociendo el modus operandi de los diferentes "ciberdelitos" con ello se facilitara la identificación de los ciberdelincuentes, siendo de esta manera más proactivos como sociedad que reactivos en el ciberespacio.

Por otra parte De la Cuesta et al., (2010), identifica que los conocimientos y el dominio del ciberdelincuente en el ámbito informático, se encuentran en ocasiones mayormente motivados por la publicidad y el reconocimiento que por el dinero, aunque no se puede generalizar el tipo de delitos, ya que existen algunos ciberdelitos en los que el móvil sigue siendo el factor económico.

Por otro lado, destaca Cámara (2020) como principal rasgo criminológico, las aptitudes que cierto grupo de ciberdelincuentes sirven de "puerta de entrada" para otros ciberdelincuentes menos capacitados.

Para Vidal (2016) En estos tiempos los jóvenes tienen gran acceso a internet y una habilidad en el dominio del mismo, pero así como los ciberdelincuentes "pueden" ser personas muy jóvenes, también un gran número de víctimas lo son, recordemos que el análisis de la cibervíctima será de bastante ayuda para la perfilación del ciberdelincuente y que, debido a estar inmersos dentro del ciberespacio, nos encontramos frente a una territorialidad nula, por lo que no se pueden tomar en cuenta los factores bio-psico-sociales líneas atrás descritos.

A continuación y como lo menciona Cámara (2020) es uno de los autores que ha contribuido a la ciberdelincuencia, realizando una clasificación de los ciberdelincuentes, con esto dando un panorama más amplio del cibercrimen;

Cuadro 1. Clasificación de ciberdelincuentes.

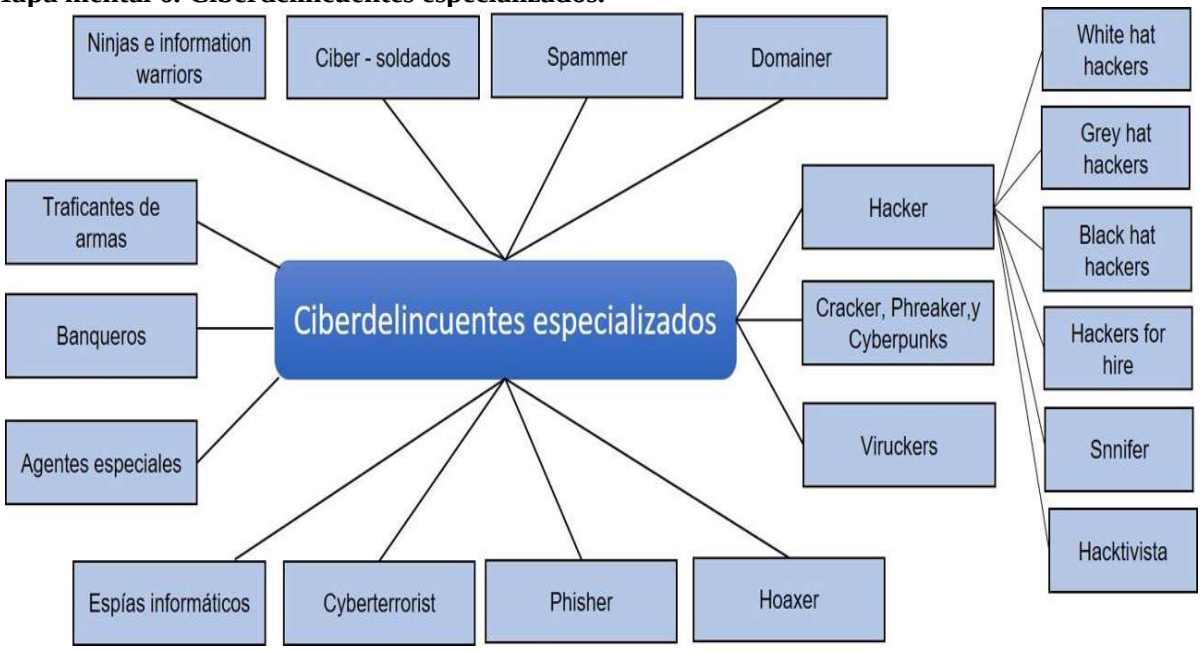
Clasificación	Objetivos y habilidades
Toolkit/newbies	Habilidades técnicas y conocimientos bajos, hacen uso de software ya existente.

Cyberpunks	Capacidad de escribir programas pequeños para alterar páginas web, envían correos spam y realizan actos vandálicos.
Internals	Empleados o ex-empleados que se aprovechan del conocimiento, el acceso a información para afectar a la organización.
Coders	Escriben códigos maliciosos con el propósito de dañar otros sistemas.
Old-guard hackers	Siguiendo los preceptos de la primera generación de hackers, se les denomina piratas informáticos, altamente calificados, sin una intención criminal.
Profesional criminals y cyberterrorist	Crakers con elevados conocimientos y especializados en el espionaje industrial y operaciones de inteligencia en contra de gobiernos, agencias de seguridad nacional, entre otros.

Fuente: Elaboración propia con base en la clasificación de Rogers (1999).

La clasificación del delincuente que realiza Royers está basada únicamente en los objetivos y habilidades, pero dado el crecimiento de los ciberdelitos dicha clasificación convendría más a una perfilación cibercriminal, por otro lado, Cámara (2020) ha hecho la diferenciación entre ciberdelincuentes especializados y no especializados por lo que a continuación se presentan en un mapa conceptual.

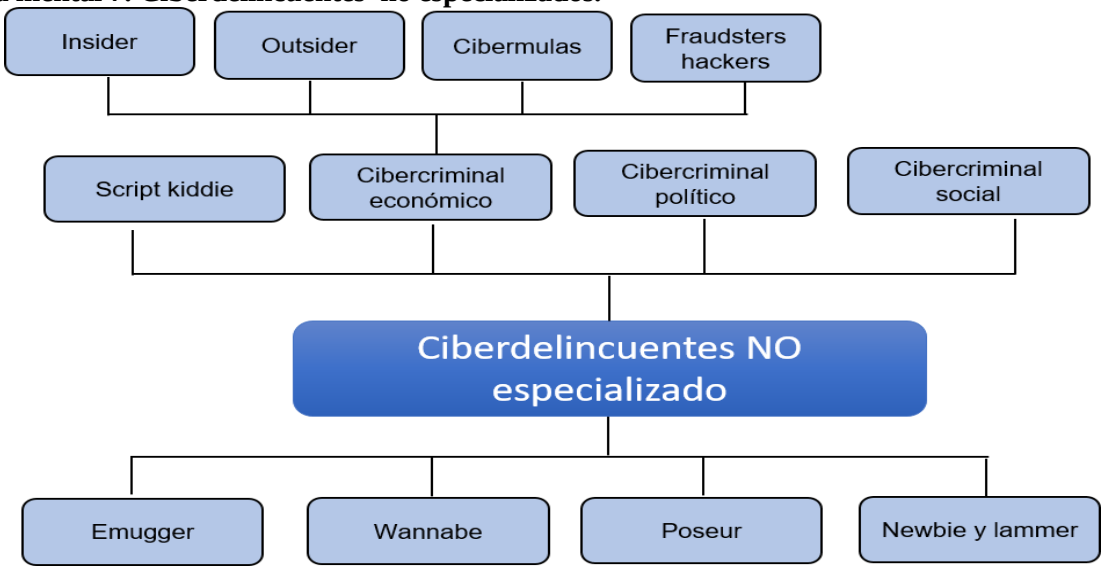
Mapa mental 6. Ciberdelincuentes especializados.



Fuente: Elaboración propia con base Cámara (2020).

El mapa nos permite apreciar el grado de especialización de cada cibercriminal, en donde el conjunto de habilidades, conocimientos técnicos, pericia, así como la experiencia en el ciberespacio le permiten realizar ataques dirigidos hacia ciertos usuarios, con vectores de ataques especializados que en muchos casos es imposible lograr obtener su trazabilidad dado al anonimato que brindas las plataformas digitales.

Mapa mental 7. Ciberdelincuentes no especializados.



Fuente: Elaboración propia con base en Cámara (2020).

Por otra parte en esta clasificación podemos apreciar que son personas que van iniciando su experiencia criminal en el ciberespacio, valiéndose de programas en el internet, a prueba y error, a través de técnicas de ingeniera social, con los cuales ponen a prueba sus habilidades, a provechándose en muchos casos del desconocimiento de los usuarios.

Para una mayor comprensión, en el Anexo 2 se desarrolló un cuadro comparativo con los tipos penales de algunos países, que se están involucrando en la Ciberseguridad y por consiguiente en la persecución de los delitos que se cometen a través de la utilización de las TIC´s, tales como: España, Estados Unidos, Rusia, México y Michoacán, se muestra la forma en que otras naciones están abordando este fenómeno en comparación con México.

2.6 Infraestructuras críticas

Las antiguas civilizaciones han buscado como protegerse en todos los ámbitos de su vida, el ser humano por sentido de supervivencia siempre ha buscado preservar su integridad. Las cosas han cambiado, pero persistentemente han existido conductas que han tenido siempre la misma intención de dañar, perjudicar o destruir, ¿Qué ha cambiado con el paso del tiempo? Sevillano et al., (2021) Expone que la evolución tecnológica ha modificado los espacios de acción social y con ello la estructura social y de Gobierno, está evolución ha trastocado nuestra vida en todos los ámbitos, ya que actualmente se depende de ciertas infraestructuras para el desarrollo de las actividades diarias de las sociedades, como puede ser: servicios de salud, banca en línea, semáforos, control aéreo, red electica, transporte, entre otros. Actualmente los vectores de ataque son más sofisticados, impensables años atrás, dado el surgimiento de las tecnologías de

la información y comunicaciones, que han permitido la automatización de los sistemas industriales, haciéndolos más eficientes en su gestión, se habla en la actualidad de infraestructuras críticas y de ciberseguridad.

Empezaremos por definir describir que la palabra infraestructura está formada por el prefijo infra (debajo) y estructura (esqueleto o partes que soportan un edificio). Podemos definir como aquello que da soporte a una estructura o sostiene a una organización.

Abordaremos el concepto de estrategia, el cual tiene diferentes acepciones dependiendo del campo de su aplicación.

Para Porter (1991) la estrategia la define como el establecimiento de una ventaja competitiva, diferente aportando un valor único.

La Ley General del Sistema Nacional de Seguridad Pública en su artículo 146, (2009) define a las instalaciones estratégicas, como todos aquellos activos y servicios (edificios, áreas estratégicas, servidores, bases de datos, Sistemas industriales, información, redes de datos, entre otros) que son vitales en las actividades diarias de una sociedad y las tendientes a salvaguardar la soberanía de un país.

Conjunto de acciones encaminadas a establecer las acciones y mecanismos necesarios para minimizar la probabilidad de riesgos y vulnerabilidades inherentes en el uso de las TIC para la gestión de infraestructuras críticas, así como para fortalecer la capacidad de resiliencia para mantener la estabilidad y continuidad de los servicios en caso de sufrir un incidente de ciberseguridad (Gobierno de la República, 2017).

En el mismo contexto el marco de referencia de infraestructura crítica de ciberseguridad del Instituto Nacional de Estándares y Tecnologías (NIST 2019) para reducir los riesgos y salvaguardar las infraestructuras críticas (Instituto de Nacional de Estándares y Tecnologías, 2019).

Para ENISA define las infraestructuras críticas como el conjunto de activos e infraestructura tecnológica que son indispensables para dar soporte a los servicios esenciales de una sociedad. Las infraestructuras pueden ser físicas, lógicas, enlaces de comunicación, redes de datos, bases de datos, sistemas automatizados, procesos entre otros componentes tecnológicos que soportan o mantienen estás infraestructuras disponibles para brindar servicios esenciales a la sociedad para los cuales no hay sustitutos (Mattioli y Levy, 2014).

En el contexto actual los activos estratégicos y procesos de las infraestructuras críticas son soportados tecnológicamente, por lo cual resulta indispensable protegerlos de las amenazas existentes, con el objetivo de garantizar la continuidad en la prestación de servicios esenciales para los ciudadanos y el Estado.

Derivado de lo anterior se comienza a utilizar la palabra cibeterrorismo como una forma de amenaza a través del cual se utilizan las tecnologías de la información y comunicaciones para poder afectar los intereses del estado y con ello crear pánico entre sus habitantes, como se mencionó en el planteamiento del problema estos ataques ya son frecuentes y reales, por otra parte el anonimato que brindan las plataformas permiten este tipo de incidentes, haciendo como esto más difícil su ubicación (Malagón y Herrera, 2019), se mencionan las características del ciberterrorismo.

- La destrucción de infraestructura de tecnologías de la información y comunicaciones.
- La pérdida o deterioro de información de las redes críticas del gobierno y la sociedad civil (Instituciones financieras, infraestructura de comunicaciones).
- Control de equipos tecnológicos (redes críticas: semáforos, plantas de energía, controladores. de tráfico aéreo, sitios gubernamentales).
- Propaganda o mensajes acerca de los daños causados por ataques terroristas.
- Atentados biológicos, tecnológicos o civiles.
- En los ataques terroristas existe presencia física, en el ciberterrorismo no es necesario.

2.6.1 Criterios para la clasificación de las infraestructuras críticas

Se elaboró un cuadro comparativo entre los países de España, Rusia, Estados Unidos y México, con el fin de identificar qué criterios define cada país para garantizar la continuidad de sus operaciones en la protección a las infraestructuras críticas.

Tabla 6. Criterios de clasificación en instalaciones estratégicas.

País	Criterios	Sectores	Fuente
España	• Personas afectadas • Consecuencias a la salud • Impacto económico • Impacto medioambiental • Impacto público y social	• Energía • Industria • Nuclear • TIC • Transporte • Agua • Alimentación • Salud • Sistema Financiero y Tributario Industria • Química • Espacio • Instalaciones de Investigación • Administración	https://INTERNET.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf
Rusia	• Transcendencia social • Importancia política • Importancia social. • Importancia ambiental • Seguridad y orden publico	• Instalaciones gubernamentales • Energía • Industria • Nuclear	http://www.consultant.ru/document/cons_doc_LAW_220885/

		• TIC • Transporte • Agua • Alimentación • Salud • Sistema Financiero • Química • Instalaciones de Investigación	
Estados Unidos	• Riesgo • Consecuencia • Amenaza • Población circundante	• Químico • Instalaciones comerciales • Comunicaciones • Fabricación • Represas • Industrial de defensa • Servicios de emergencia • Energético • Financiero • Instalaciones gubernamentales • Sanitario y salud publica • Tecnologías de la información • Transporte • Agua	https://www.cisa.gov/publication/cisa-services-catalog
México	• Riesgo desestabilizador directo y/o inmediato para la seguridad nacional. • Riesgo directo y/o inmediato de desestabilización para el país • Riesgo directo y/o inmediato de desestabilización a nivel local • Magnitud del daño. • Repercusiones. • Impacto. • Función.	• Correos • Telégrafos y radiotelegrafía • Petróleo, hidrocarburos y petroquímica básica • Minerales radioactivos y generación de energía nuclear • Electricidad • Las actividades que señales las leyes expedidas por el congreso de la unión • Aquellas que tienden a mantener la integridad, estabilidad y permanencia del Estado México.	https://www.segurilatam.com/seguridad-por-sectores/infraestructuras-criticas/instalaciones-estrategicas_20190829.html

Fuente: Elaboración propia con base en la información obtenida de las metodologías de los países analizados (2020).

Del estudio realizado podemos observar que cada país define en similitud los mismos criterios dando prioridad a la vida, los riesgos y amenazas de sus actividades esenciales, cada uno en su ámbito de competencia, dando prioridad a garantizar la continuidad de los servicios esenciales de un País.

2.6.1.2 Clasificación de infraestructuras

En México en el año 1995 en el gabinete de seguridad nacional se estableció un Grupo de Coordinación para la atención de las Instalaciones Estratégicas (GCIE) en el año 2000, de igual manera en la LGSNSP se estableció el 15 de agosto del 2006 que el GCIE sería la única instancia para realizar el inventario de las infraestructuras consideradas como estratégicas.

En el contexto anterior en la Ley de la Guardia Nacional en su Artículo 9, capítulo III Atribuciones y Obligaciones de la Guardia Nacional, se observa el listado de las instalaciones de la federación y de aquellas que son consideradas como estratégicas, dadas las amenazas naturales o físicas que su mal funcionamiento pueda afectar a los ciudadanos.

De lo anterior se desprende la clasificación identificándolas de acuerdo a su grado de estrategia para el país, con un total de 3,116 instalaciones (Manual de Seguridad a Instalaciones Vitales 2003: SEDENA), que por el orden de importancia se dividen de la siguiente manera:

- Nivel A 1930 instalaciones
- Nivel AA 625 instalaciones
- Nivel AAA 561 instalaciones

La clasificación se atiende de acuerdo a los siguientes criterios:

- Nivel **A** son aquellas cuya afectación o interrupción del proceso normal de operación repercute sólo en perímetros geográficos y poblacionales reducidos, sin que ello atente contra la estabilidad de la nación de manera directa y/o inmediata (nivel local).
- Nivel **AA** aquellas cuya interrupción del proceso normal de operación afecta a extensas e importantes zonas geográficas de la nación y no representa un riesgo directo y/o inmediato de desestabilización para el país (nivel regional).
- Nivel **AAA** son aquellas cuya afectación o interrupción del proceso normal de operación afecta en su totalidad a extensas e importantes zonas geográficas de la nación e implica un riesgo desestabilizador directo y/o inmediato para la seguridad nacional.

2.6.2 Vulnerabilidades de las Infraestructuras críticas

Cualquier Infraestructura que se encuentra dispersa geográficamente y soportada por una infraestructura tecnológica es susceptible de sufrir diversos ataques, una vulnerabilidad por tanto puede poner en riesgo la información y su operación, pero supone un riesgo mayor cuando se habla de instalaciones estratégicas, por lo tanto el Estado y las organizaciones deben proteger adecuadamente su ciberseguridad.

2.6.3 Marco de control NIST

Derivado de los ataques a infraestructuras críticas y del impacto que pueden provocar de llegar a materializarse en la seguridad nacional de Estados Unidos, el Ex presidente Barack Obama (2013) redacta la orden 13636 para la mejora de la ciberseguridad en las infraestructuras críticas, donde instruye al Instituto Nacional de Estándares y Tecnología (2021) la creación de un marco para gestionar los riesgos en el ciberespacio y enfrentar las amenazas latentes que puede presentan para las empresas y usuarios en general de los Estados Unidos.

El marco del NIST es una metodología, la cual incluye un conjunto de normas, directrices, estándares y las mejores prácticas en matera de ciberseguridad todas ellas orientadas a la gestión de los riesgos en infraestructuras críticas, para cualquier organización sin importar su , las cuales dependen de infraestructura tecnológica para soportar sus procesos de operación, aplicando las mejores prácticas en la gestión de riesgos y que en caso de verse comprometida la seguridad por un ataque cibernético tener la capacidad de recuperarse y llegar al punto óptimo qué permita la recuperación con los menores impactos (2021).

A continuación se describen de manera gráfica los objetivos del marco.

Ilustración 8. Objetivos del marco NIST.

Fuente: Elaboración propia con base en el NIST (2021).

2.7 Seguridad de la información

De acuerdo con la Real Academia Española (RAE), el termino seguridad se define como “libre o exento de todo peligro, daño o riesgo. (Real Academia Española, 2019).

Para Ellis y Mohan (2019), la Seguridad de información se enfoca en salvaguardar en todo momento la confidencialidad, integridad y disponibilidad de los datos en su totalidad, con el objetivo de satisfacer las necesidades de los usuarios de información. También incluye el aseguramiento de la información, que trata con los principios subyacentes de evaluar qué información puede o debe protegerse. La seguridad de la red, a su vez, se ocupa del diseño, implementación y operación de las redes, con el objetivo final de lograr la seguridad de la información en las redes dentro de las organizaciones y el sector Gobierno.

La norma internacional ISO 27001, define a la seguridad de la Información, como; las medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que garanticemos en todo momento la confidencialidad, integridad y disponibilidad de la información. (ISO, 2014).

Derivado de lo anterior podemos precisar que la seguridad de la información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información, con la finalidad de salvaguardar los activos de información críticos e infraestructuras tecnológicas de los riesgos y amenazas existentes en el ciberespacio y de forma física.

Es así que la Norma ISO 27001 creada en el año 2005 por la Organización Internacional de Estandarización y por la Comisión Electrónica Internacional, cuya utilización puede ser interna o externa, la cual tiene como finalidad brindar los requerimientos en el análisis, diseño, implementación y evaluación de un sistema de gestión de seguridad de la información dentro de una organización, en los cuales se involucra: gente, procesos y tecnología, a través de la adecuada gestión del riesgo. (ISO, 2014). Es así que se describen los principales de la seguridad de la información.

2.7.1 Principios

Estos principios son fundamentales para garantizar la seguridad de la información frente a las amenazas, riesgos o incidentes informáticos que puedan poner en peligro la operación de cualquier organización, empresa o la información personal de los usuarios. Los cuales se describen para mayor entendimiento:

2.7.1.1 Confidencialidad

ISO 27001 (2014) describe a la confidencialidad como aquella propiedad que la información tiene de no ser revelada a aquellas personas, entidades o procesos, con la finalidad de asegurar su acceso autorizado a la información.

Santos (2019) nos indica que la confidencialidad es el requisito de que la información no sea divulgada a individuos no autorizada por el propietario.

2.7.1.2 Integridad

ISO 27001 define a la integridad como la propiedad de que la información no sufra alteraciones o modificaciones por personas no autorizadas (ISO, 2014).

Por otra parte Santos (2019) define a la integridad es básicamente la capacidad de asegurarse de que un sistema y sus datos no se hayan alterado o comprometido. Eso garantiza que los datos sean una representación precisa y sin cambios de los datos seguros originales.

2.7.1.3 Disponibilidad

La disponibilidad en Santos (2019) establece que los sistemas, aplicaciones y los datos deben estar disponibles para los usuarios autorizados cuando las personas o procesos autorizados, tengan acceso a la información en tiempo y forma para la toma de decisiones.

2.7.1.4 Autenticación

Para Costas (2014) es comprobar quien elaboró o envía cierta información sea quien dice ser, a través de contraseñas, autenticación de dos pasos, criptografía, entre otros mecanismos.

2.7.1.5 Autenticidad

Costas (2014) la define como la característica de probar que quien ha enviado la información proceda de una fuente confiable y fidedigna, esto se logra por medio de firmas digitales, certificados SSL.

2.7.1.6 No repudio

Costas (2014) nos define que tiene relación estrecha con la autenticación, que prueba la comunicación entre emisor y receptor, donde alguno de ellos no puede negar que se recibió la información o que se dio la comunicación, se clasifica en:

No repudio en origen: el emisor del mensaje no puede negar el envió porque el destinatario tiene pruebas de esa emisión.

No repudio en destino: el receptor del mensaje no puede negar que recibió el mensaje porque el destinatario tiene pruebas de la recepción.

Esto se asegura a través del uso de criptografía, firmas digitales

2.7.2 ¿Qué es un activo de información?

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) (2012) que utiliza el Gobierno español para minimizar los riesgos en el uso de las TIC’s en sus operaciones

habituales, define un activo de información como algo que las organizaciones valoran y deben de proteger de las amenazas, ya que genera valor para los procesos internos, externos e incluso la imagen.

2.7.3 Clasificación de los activos de información

Los activos pueden clasificarse de acuerdo a su naturaleza, MAGERIT (2012) define tres etapas, se enlistan a continuación:

1.- Inventario de activos: que permita la identificación, ubicación, descripción y el dueño del activo quien define el grado de seguridad que requiere dicho activo, categorizándolos de la siguiente manera:

- Información que se gestiona en la organización.
- Servicios y procesos de negocio que brinda la organización.
- Aplicaciones informáticas de software.
- Infraestructura tecnológica equipos informáticos.
- Personal interno, proveedores, clientes, entre otros
- Redes de comunicaciones que brindan el soporte a la organización para la conectividad e interoperabilidad de los datos.
- Soportes físicos de información (servidores de aplicaciones, respaldo, telefonía).
- Equipamiento auxiliar soporte que da servicio a los sistemas de información.
- Instalaciones oficinas donde se almacena la información y sus procesos.

2.- Dependencia de los activos; los principales son la información y los servicios que proporciona la organización al interior o al exterior, sin embargos estos dependen de otros activos y de la infraestructura tecnología que permiten su correcta operación y funcionamiento, resulta imperante conocer la relación existente entre los activos superiores y los inferiores, con el fin de identificar la alta disponibilidad, en relación con el objetivo dentro de la organización, para recuperar su estado de operación a un punto óptimo.

3.- Valoración de los activos de información en función de la importancia que representan y del impacto que un incidente sobre el mismo pueda causar a la organización, a través de:

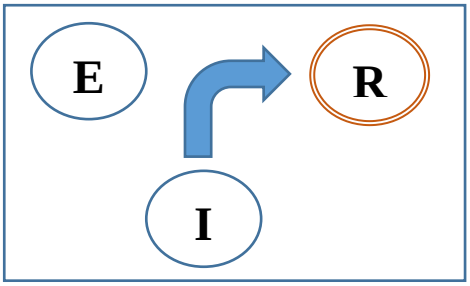
- Valoración cuantitativa, estimando el valor del activo.
- Valoración cualitativa, se establece de acuerdo a una escala del 0 al 10 o con valores: alto, mediano y bajo, se debe definir un criterio en base a las características principales de la información: confidencialidad, integridad y disponibilidad.

2.7.4 Amenazas a los activos de información

Los activos de información serán afectados por diversos factores, quebrantando su confidencialidad, integridad y disponibilidad, uno de los más importantes son los relacionados con los delitos cibernéticos, factores internos y externos, las acciones contra estos pueden ser:

- Fabricación: ingreso de información que antes no existía en el sistema, afectando la integridad de la información, ejemplo, transacciones en red, ingreso de registros a una base de datos, se muestra está amenaza de tipo activa en la ilustración 7.

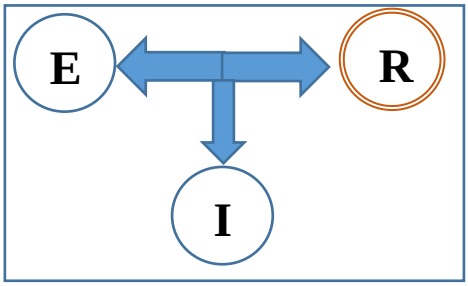
Ilustración 9. Ataque de fabricación de la información.



Fuente: Elaboración propia con base en Álvarez y Pérez (2004).

- Modificación: alteración de la información que ya vive en el sistema, aplicación o cuando viaja por algún canal de comunicación, simboliza un ataque contra la integridad, ya que el aplicativo funcionará de forma diferente o cambiar los datos que viajan por la red, ejemplo modificación de la nómina o de hardware, se muestra en la ilustración 8.

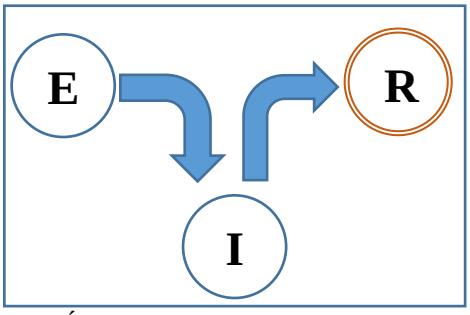
Ilustración 10. Ataque de modificación de la información.



Fuente: Elaboración propia con base en Álvarez y Pérez (2004).

- Intercepción: es un ataque contra la confidencialidad de la información, por medio de un aplicativo, proceso o usuarios que no estén autorizados y que logren acceder a los recursos, ejemplo: copia de información, escucha de información en línea, la ilustración 9 modela el ataque de tipo pasivo.

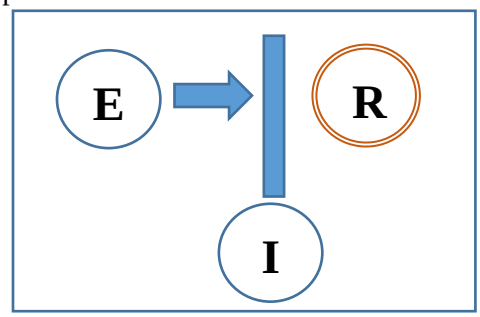
Ilustración 11. Ataque de intercepción a la información.



Fuente: Elaboración propia con base en Álvarez y Pérez (2004).

- Interrupción: alteración de la información, atentando contra la disponibilidad, dejando inutilizable o no una parte del sistema, ejemplo: borrado de datos, fallas en el sistema operativo, destrucción de hardware, la ilustración 10 muestra esta amenaza de tipo activa.

Ilustración 12. Ataque de interrupción a la información**.**



Fuente: Elaboración propia con base en Álvarez y Pérez (2004).

2.7.5 Protección a los ataques de la seguridad de la información

Las medidas de protección para garantizar la seguridad de la información ante los ataques descritos pueden ser diferentes, ya que esto lo determina el vector de ataque utilizado, el tipo de tecnología empleada, se enlistan los controles que permiten gestionar el riesgo en caso de una afectación al sistema, proceso o usuarios;

- Listas de control de acceso a la información.
- Cifrado de la información.
- Copias de seguridad.
- Borrado seguro de discos.
- Almacenamiento en la nube.
- Contratos de outsourcing.
- Equipo de respuesta a incidentes.
- Plan de recuperación.
- Políticas.
- Procedimientos.

2.7.6 Metodologías de análisis de riesgos

Con los avances tecnológicos y dada la automatización de los sistemas de información por parte de las organizaciones para eficientar sus actividades, se hace necesario contar con metodologías en la gestión de riesgos que permitan evaluar y medir el nivel de madurez en el manejo de la información a fin de garantizar la confidencialidad, integridad y disponibilidad de la información, el cual es un instrumento que evaluara los procesos involucrados en la gestión de dicha información.

Revisaremos las metodologías internacionalmente más conocidas

2.7.6.1 Norma ISO 27001

Norma creada en el año 2005 por la Organización Internacional de Estandarización y por la Comisión Electrónica Internacional, su utilización puede ser interna o externa, la cual tiene como finalidad brindar los requerimientos en el análisis, diseño, implementación y evaluación de un sistema de gestión de seguridad de la información dentro de una organización, para preservar la confidencialidad, integridad y disponibilidad de los activos, en los cuales se involucra: gente, procesos y tecnología, a través de la adecuada gestión del riesgo (2013) .

Esta norma establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. . Ofrece un enfoque estructurado para reconocer y manejar los riesgos relacionados con la seguridad de la información de manera metódica.

2.7.6.2 Norma ISO 27002

La norma ISO 27002, anteriormente conocida como ISO/IEC17799, se pública por primera vez en el año 2000. A la fecha cuenta con diversas revisiones, su última versión en el año 2013. Se enfoca en las prácticas recomendadas para la gestión de la seguridad de la información, actualmente, se destaca como una etapa crucial para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) sólido. De esta manera, se asegura la continuidad y el adecuado funcionamiento de los procesos de seguridad, alineados con los objetivos estratégicos de la organización. Es una guía complementaria a la ISO/IEC 27001 que ofrece una amplia lista de controles para que las organizaciones manejen los riesgos de seguridad de la información. (2013).

CAPÍTULO 3. CONCEPTUALIZACIÓN DE LAS POLÍTICAS PÚBLICAS

3.1 Introducción a las políticas públicas

Existe una diversidad de autores que han hecho aportaciones al tema de las políticas públicas, procediendo de la necesidad que existe dentro de la misma sociedad por dar solución a un considerable número de problemas, como ya lo hemos abordado anteriormente, el individuo es un ser social por naturaleza y está naturaleza le ha inferido la necesidad de establecer un orden social, aunque cabe señalar que ese orden no es natural como lo es la sociedad, por el contrario, este con el paso del tiempo se ha ido adhiriendo a la sociedad en busca de tener mejoras dentro de la misma, por lo que hablar de políticas públicas no es solo entender lo que son, o hablar solo de conceptos, es necesario conocer los antecedentes de las políticas públicas, momentos históricos en los que se han visto involucradas diversas teorías, la evolución que han presentado, y aquellos procesos sociales que se han derivado de diversas etapas, entender la importancia de los actores y la movilización de recursos que juegan un papel fundamental dentro de este tema, solo así podremos definir de manera propia el término de políticas públicas, la evolución y el ciclo de las políticas públicas, a pesar de que abordaremos el punto de vista de diversos autores, principalmente basado en la perspectiva del Doctor Luis F. Aguilar Villanueva y sus múltiples estudios y aportes a las políticas públicas en México, desde el punto de vista de diversos autores que han logrado aportar a este tema investigaciones que complementan a las políticas y sus ciclos, motivo por el cual abordaremos el ciclo de las políticas públicas a partir de tres momentos, el diseño, la implementación y evaluación.

Las políticas públicas, un tema controversial, complejo y de importancia fundamental para el desarrollo y el bienestar de grupos sociales, pero las decisiones que se llegan a plantear no siempre benefician a una mayoría, siendo en ocasiones solo algunos los privilegiados, aquellos que resultan con beneficios derivados de las mismas, ¿Cuáles son aquellos objetivos que imperan en las políticas para que puedan formar parte de la agenda de gobierno?

Para Aguilar (1992) Las políticas públicas son aquellas acciones del gobierno con objetivos de interés público, que buscan subsanar y satisfacer las necesidades de la sociedad, para lo cual se apoya de diversos modelos, teorías y ciencias, pero cabe señalar que no siempre fue así, ya que la evolución que muestra la sociedad nos ha dejado problemas cada vez con mayor complejidad, es por ello que a la par las políticas públicas han presentado cambios considerables, pues los elementos de un modelo tradicional, el cual se había visto con limitaciones en la resolución de conflictos, incluso en la colaboración de otras ciencias, el desarrollo de políticas públicas con procesos sistemáticos y la racionalidad sobre la que se sustentaba no eran determinantes para combatir esos múltiples fines conflictivos, el principal cambio del que fue objeto la ciencia de políticas, fue el surgimiento de nuevas ciencias, a las que Lasswell (1992) denominó ciencias

de políticas, que emergieron y se fueron adhiriendo conforme los intereses de la sociedad iban cambiando, ya que en todo momento consideró que era vital encontrarse un paso adelante de toda evolución social, debido a que la resolución de conflictos cada vez mostraría mayor complejidad, es necesario comenzar con los antecedentes de las políticas públicas para con ello ampliar nuestro criterio.

3.1.1 Antecedentes de las políticas públicas

El estudio de las políticas públicas ha tenido lugar en la segunda mitad del siglo XX, su objeto es la resolución de problemas públicos para lo cual son necesarios tener en cuenta aspectos políticos y de orden técnico, el antecedente directo y por tanto surgimiento de la ciencia política ocurrió en 1950, en los años de la gran depresión, con Lasswell y su programa de investigación "El conocimiento del proceso de la política y en el proceso de la política", en donde y, a través de una articulación de forma sistemática de las ciencias (interdisciplinares) y decisión de gobierno entendiéndose como democracia, pero la razón tenía un lugar de considerable importancia para él, ya que debido a las múltiples disciplinas en conjunción con esta última arroja un margen de error mínimo, debido a que el estudio se vuelve más preciso, pero la importancia no radica únicamente en el presente y su contexto actual, sino que el conocimiento del pasado se considera fundamental para precisar el futuro, ya que los problemas no solo serían abordados desde una ciencia social, sino desde las diversas ciencias que fuesen necesarias (economía, antropología, historia, filosofía, sociología, psicología social, analistas de sistemas, investigadores de operaciones, y politólogos). Conforme hemos ido evolucionando como sociedad, también lo hemos hecho en diversos temas, técnicas, métodos y por supuesto ciencias, que necesitan estar a la vanguardia y que, en su totalidad, tienen relación con la sociedad, motivo por el cual no se pueden dejar de lado en el estudio, elaboración e implementación de políticas (1992).

Continuando con los antecedentes en los años en los que tuvo lugar la guerra fría, tuvieron su origen planteamientos necesarios como: la posibilidad del empleo de recursos intelectuales con la más instruida economía; la función de la inteligencia buscando aumentar la racionalidad de la política; cómo lograr que los hechos y las interpretaciones influyan de manera efectiva en la toma de decisiones. Puntualiza Aguilar (1992) que fue durante los años de guerra que Laswell y otros economistas naturales se habían reunido para desarrollar modelos de "costo-beneficio" pero, aunque el congreso había aprobado la creación, no aprobó la incorporación de las ciencias sociales, Lasswell (1992) con firmeza sostenía que en aquellas ciencias sociales existía un interés progresivo por el proceso de la política, ya que la racionalidad se había perfeccionado en cuanto a decisión de políticas, pues gracias a las demás ciencias ahora el criterio se mostraba con más amplitud y se abordaba desde las diversas ciencias sociales que veían el problema desde su campo de estudio pero con perspectiva estrecha, estos años de guerra fueron decisivos y fundamentales

no solo para que se tomaran en cuenta a las ciencias sociales, si no aquellos métodos y técnicas, lo que los convertía en sustentables de observación, clasificación, formación de concepto e hipótesis, y protocolos de prueba, enfocados al proceso de la política y hacia las necesidades de inteligencia del proceso, siempre apoyándose de los métodos de investigación de las ciencias sociales y de la psicología, para después mejorar el contenido de la información y la interpretación, convirtiéndose en políticas.

Varios fueron los autores que apoyaron el modelo de Lasswell, como ha pasado en otros momentos, las doctrinas que van sucediendo son abordadas por expertos que contribuyen las bases de dichos modelos doctrinales y proponen desde su perspectiva fortalecer aquellas tesis doctrinales, como lo sucedido con la doctrina de Lasswell. Aguilar (1992) es de la firme convicción que la propuesta de Lasswell, va más allá de solo una propuesta o tesis doctrinal, es decir, no quedando en solo una doctrina más, ya que logra arrancar esa venda que muchos aún conservan, logrando que nuestro criterio sea más amplio y razonable, podemos observar la presencia de un contexto social del cual forman parte problemas que le confieren a la ciencia, tecnología y a la información, un claro ejemplo es lo sucedido en los años de gran depresión, la influencia Lasswelliana rompió fronteras y logró impactar a nivel mundial, en este caso nos es de interés conocer un poco sobre los antecedentes de las políticas públicas en México.

Los años de la gran depresión fue un periodo que impacto a través de una crisis también a Latinoamérica, Aguilar (1996) enfatiza lo sucedido en México, cuando la demanda social de la democratización y redimensionamiento, sucesos que consideró “vientos de la revolución y contrarrevolución”, momento en el que el aparato gubernamental burocrático crecía de forma paralela con el desbordamiento del autoritarismo, México atravesaba por una crisis de transición política, en donde el cambio de régimen era irreversible y necesario. En México, las formas de gobierno autoritarios lo habían sumergido en una profunda crisis y depresión, en donde el beneficio que se obtenía era para pocos, durante el periodo de los 70´s y 80´s, las crisis económicas que se vivieron obligaban a la reformulación de cuestiones, que envolvían temas de completo interés para el avance gubernamental y social del Estado Mexicano, pero para Aguilar (1996) no era otra cosa que “una patología”, es decir, gobiernos que venían arrastrando la misma problemática o peor aún, llevando a un gobierno que conducía a ciclos, sin darse cuenta que los problemas de su estado iban creciendo a pasos más apresurados que el mismo, lo que en un dado momento llevaría a un gobierno sin límites de poder y sin límites de recursos, a ampliar el gasto público invirtiendo en la economía (adquiriendo empresas) y así mismo incrementando las regulaciones y trámites.

Aguilar (1992) enfatiza que en México no solo creció el gobierno, su organización, aparato, personal, recursos, propiedades y programas, también lo hizo el Estado de Derecho, el ámbito de los poderes, las atribuciones y las normas generales que estrecharon el campo de acción de las libertades políticas y

económicas de los ciudadanos, y sigue siendo un tema que hoy en día se sigue observando, ya que no únicamente se ha ido incrementando el gobierno y todos sus componentes, es necesario el desarrollo que ha llevado a la evolución de un Estado de Derecho mexicano, gracias a los cambios que se han ido adhiriendo y el reconocimiento de este por formar parte de la ONU (1947) y de los tratados internacionales (1936), en donde las leyes mexicanas han sufrido algunos cambios considerables, principalmente las garantías individuales, que ahora son los derechos humanos "fundamentales", aunque el único cambio ha tenido lugar en aquellos "otros" derechos que se han ido agregando, es decir, que han ido surgiendo derivado de las nuevas necesidades sociales, y que ahora están previstos a lo largo de la Constitución Política de los Estados Unidos Mexicanos, ya que anteriormente las garantías individuales se encontraban únicamente previstas en los primeros veintinueve artículos, otro cambio considerable es aquel que se dio dentro de Sistema Penal Acusatorio, en donde la principal diferencia del Sistema Acusatorio Adversarial es "la presunción de inocencia y bajo los principios de publicidad, inmediación, concentración, continuidad y contradicción" o las leyes "Sustantiva y Adjetiva".

Estos cambios que han ido sucediendo han presentado no solo la evolución social, sino de pensamiento y raciocinio, ya que como puntualiza Aguilar (1992), es importante el sentido de racionalidad que envuelven estos temas de decisiones, ya que la responsabilidad de las elecciones públicas es de los gobernantes y hacia los gobernados, considera también que la democratización es importante para reconstruir la naturaleza pública del gobierno, los cambios de orden social se tienen que ir presentando, porque no se puede permanecer estáticos en modelos obsoletos, que no se encuentren a la par evolutiva de todo problema y contexto social, así mismo son necesarios para saber si van a funcionar o solo podrían llegar a ser buenas algunas ideas en busca de aceptación, una vez que hemos conocido los antecedentes de las políticas públicas, podemos comenzar a abordar lo que es una política pública y con ello conocer los conceptos de los que se rodean las políticas públicas, como ya lo hemos mencionado las políticas públicas buscan dar respuesta a problemas sociales.

De lo antes expuesto, podemos expresar que las políticas públicas son aquellas acciones de gobierno manifestadas a través del diseño y gestión de programas, así como una administración pública con el objetivo primordial de satisfacer las necesidades de la sociedad, para lo cual es necesario conocer dichas necesidades a través de propuestas que se estudian después de la exposición de estas en arenas, para con ello dar acomodo jerárquico y real a cada conflicto social, se auxilia de diversas teorías y modelos, así como de métodos que intentaran definir de manera adecuada un problema que previamente se incorporó a la agenda de gobierno y que es de interés público y por tanto se busca la creación, rediseño y posterior implementación de políticas públicas, buscando erradicarlo o tener un control sobre este. Desde el punto de vista de Aguilar (1996) las políticas públicas son un conjunto de acciones orientadas a llevar a cabo la

realización de objetivos que se plantearon con base a necesidades sociales, estas necesidades deben tener la característica de prioritarias, la resolución de problemas que se da a través de las políticas públicas expone el interés o beneficio público.

Otro objetivo de gran importancia en el análisis de Políticas Públicas que señala Aguilar (1996) es el de mejorar la calidad de vida de la sociedad a la que va dirigida, por lo cual es de gran importancia identificar la totalidad de las partes que conforman el problema y con esto garantizar el éxito en la intervención del Gobierno e incorporación a la agenda pública, dentro del análisis de Políticas Públicas, la comunicación juega un papel fundamental: "Entender y escuchar" permite generar más cooperación y coordinación entre las partes involucradas. Es decir, debemos pasar de una relación vertical potencialmente (impositiva-autoritaria) a una relación horizontal más cooperativa, que dé más legitimidad y efectos menos deseados al proceso de análisis.

Por otra parte Aguilar (1996) hace una compilación de conceptos que refieren la noción descriptiva de la política, en donde principalmente manifiesta la capacidad de la "noción descriptiva" de la política como una construcción de los datos de experiencia que se ha observado a través de las teorías, valorando e integrando algunos elementos de los fenómenos políticos y sus diversas categorías o divisiones, a través de las diversas políticas que se conocen, refiriendo que en la noción descriptiva se hace de un análisis derivado de la observación, para así poder llegar a un problema en específico, mencionando que algunos componentes son un reflejo común de una búsqueda entre varios conceptos; a) Institucional, la política es elaborada o decidida por una autoridad formal legalmente constituida en el marco de su competencia y es colectivamente vinculante; b) Decisorio, la política es un conjunto-secuencia de decisiones, relativas a la elección de fines y/o medios, de largo o corto alcance, en una situación específica y en respuesta a problemas y necesidades; c) Comportamental, implica la acción o la inacción, hacer o no hacer nada; pero una política es, sobre todo, un curso de acción y no sólo una decisión singular; d) Causal, son los productos de acciones que tienen efectos en el sistema político y social.

Aguilar (1996) menciona a la jurisdicción como un componente de gran importancia ya que juega un papel principal dentro de la elaboración de políticas, a través de la cual se toman decisiones que se derivan de una observación detallada que conlleva a la especificidad de una situación que busca respuestas y soluciones de problemas y necesidades, para lo cual es necesario tomar en cuenta la necesidad de actuar o de no actuar, esto de acuerdo con la situación frente a la que se encuentre, la inacción solo muestra la incapacidad de resolver un problema y por tanto aquellos hacedores de políticas no deberían ocupar su tiempo en problemas que no se pueden resolver, es decir, tratan de persuadir a la población, no por su ineficacia, sino por la complejidad y la falta de resolución de los problemas, ya que no todos los problemas

tienen una solución a través de la elaboración de las políticas, por lo cual se debe observar y comprender sobre la inacción o la acción de una política, esto conlleva a que las políticas reflejen efectos dentro del sistema político y social, siendo el impacto no siempre el que se espera, pero que se logra a través de la secuencia de decisiones y no de una en singular, así mismo la inacción se puede considerar por algunos autores como la mejor estrategia frente a alguna cuestión.

La elaboración de políticas públicas no depende solo de un actor gubernamental, sino de todos aquellos actores que se ven involucrados en la elaboración y que Aguilar Villanueva (1996) considera como "gubernamentales y extra gubernamentales", que a través de interacciones logran incorporar un análisis para lograr con ello llegar a una decisión "toma de decisión", gracias a los actores multidisciplinares, ya que todos los involucrados en la elaboración de las políticas públicas difieren en diversidad de opiniones, preferencias doctrinales, la percepción y el alcance que quieren lograr a través de la acción, por lo cual se presenta un elevado grado de complejidad a la hora de la toma de decisiones y de todo el proceso que sucede antes de la elaboración de las políticas, otro aspecto importante que Aguilar (1996) manifiesta es el "impacto alcanzado", y que el hacedor de políticas tiene que tomar en cuenta la posibilidad del error, derivado de esto la capacidad que muestre de resolución es el motivo de aquellas alternativas que ha contemplado, es decir "rehacer" una política o reajustar, con relación a la observación y análisis que se lleva a través de teorías y políticas, es necesario tomar en cuenta los efectos que resultan de las políticas.

Aguilar (1996) señala que en el ámbito político, la interacción desempeña un papel crucial, ya que el proceso de formulación de políticas involucra a múltiples actores con diversas formaciones doctrinales, afiliaciones políticas, percepciones e ideologías que han evolucionado a lo largo del tiempo. Por esta razón, la interacción se convierte en la característica central de las políticas, ya que se desarrollan después de una serie de procesos previos, pero antes de su formulación final. Para obtener la convicción total o parcial de los actores involucrados en la toma de decisiones, es necesario presentar argumentos sólidos que muestren cómo el problema es relevante y de interés público. Este argumento se expone y se busca persuadir al resto de los participantes en el proceso. Así, el problema se integra al ciclo de las políticas públicas y se acompaña de momentos clave en su desarrollo.

3.2 Ciclo de las políticas públicas

El ciclo de las políticas públicas se lleva a cabo a través de etapas que lo conforman, puntualiza Aguilar Villanueva (1996) que aquel motivo que convertía en un objeto de estudio externo al proceso decisorio de la política era que la autonomía principalmente se encontraba en la administración pública para la ciencia política general, por tanto, la hechura de la política dependía más de la administración pública, por lo cual el proceso de la elaboración de políticas no era un tema de estudio, análisis o simple interés. La ciencia

sociología política tenía más respuestas certeras ya que todo giraba en torno a la sociedad y los sociólogos de la época que conocían y estudiaban las relaciones sociales y por tanto de poder que existía en un sistema social, los sociólogos tenían mayor decisión que el mismo gobierno para la resolución de todos aquellos conflictos, por el simple hecho del conocimiento que tenían y por tanto no asumían preocupación en la elaboración de políticas, ya que no existía una ciencia que brindara el estudio de dichos procesos y la regulación y efectividad de los mismos, pero con el paso del tiempo se vio en la necesidad de optar por medidas alternas, ya que se demostró que no era suficiente conocer y estudiar a la sociedad para asumir el control absoluto, la sociedad necesitaba soluciones, no control, ya que y aunque principalmente el estudio se da en el sector social, no era suficiente solo tomar en cuenta las relaciones sociales, sino un estudio más exhaustivo y con mayor complejidad por lo cual era necesario abordar ciencias auxiliares, aunque las cuestiones a atender son sociales, ya había que regularse a través de normas de convivencia, implicando el contexto social, económico, geográfico, cultural, entre otras muchas que contribuyan a garantizar el orden y procuren el bienestar público.

En el contexto actual los intereses sociales han cambiado, los asuntos políticos son cada vez más específicos y la creciente población hacen cada vez más compleja la hechura de políticas, es fácil solo voltear a otros países y querer que el gobierno asuma las mismas acciones, responsabilidades y por tanto el mismo tipo de políticas que les ha funcionado, pero la realidad dista, ya que los asuntos públicos requieren un estudio más reforzado, a través de conocimiento especializado, cálculos precisos de costos, mostrando con ello un lado administrativo de las políticas y tomando en cuenta una evaluación causal de aquellas consecuencias probables a partir de las acciones y los medios de los que se disponga, es decir de un estudio de cada etapa del ciclo de las políticas públicas (1996).

El modelo secuencial de políticas públicas tuvo su origen a través de las reflexiones de Lasswell (1992), cuando creó las ciencias de las políticas, creía necesaria construir información, a la par que sostienen necesario un marco interpretativo, creando una secuencia de etapas, es decir un modelo teórico, remontándonos a 1970 y tomando como referencia el modelo secuencial de políticas públicas, se apoya nuevamente la teoría del ciclo “esquema analítico”, en donde las políticas públicas son un proceso que se retroalimenta permanentemente Anderson (1984) lo retoman a seis momentos, mientras que otros autores consideran cinco, y Aguilar Villanueva lo reduce a tres. A continuación describiremos de manera breve y entendida las fases del ciclo de las políticas públicas.

1.- **Identificación del problema**, se delimita el problema y se convierte en una cuestión pública, para lo cual y con relación a la identificación y definición de problemas, para Delgado Godoy (2009), los problemas sociales son un gran número que afecta a diversos sectores de la sociedad y que los gobiernos

buscan dar atención a través de políticas públicas para lo cual primero tiene que estudiar dichos procesos a través de una agenda, para buscar dar solución en un determinado tiempo. Los problemas son percibidos por los actores involucrados, siendo objeto de exploración, articulación y cuantificación (1996).

2. **Formulación de soluciones,** alternativas de políticas, tentativas de respuesta, puntualiza Delgado Godoy (2009), como la fase en donde el problema ha sido aceptado para dar una solución a través de políticas públicas, por lo cual se comienzan a desarrollar cursos de acción a través de propuestas viables para enfrentarse a problemas públicos. Cabe señalar que en esta fase se llevan a cabo cuatro actividades para que se lleve a cabo la formulación de soluciones; 1) establecimiento de metas y objetivos a alcanzar, los objetivos son aquel elemento sobre el que se centra la acción pública, otorgando un propósito y dirección a la organización, políticas y programas, cuando se va a identificar los objetivos, nos señala Delgado Godoy surgen dificultades a la hora de identificarlos ; 2) Detección y generación de alternativas que permitan alcanzar los objetivos, se le considera una lista de opciones de política pública, se da el caso de identificación cuando las opciones ya son conocidas, cuando estas son desconocidas, se generan opciones; 3) valoración y comparación de las alternativas, después de haber identificado las opciones, las ventajas y los inconvenientes se realiza un análisis costo-beneficio, con la finalidad de identificar costes, beneficios y la cuantificación económica; 4) Selección de una opción o combinación de ellas, el decisor público se apoya de las técnicas, pero el decisor público es el que optará por la mejor opción.

3. Adopción de la decisión, que es un hecho eminentemente político, seleccionan la elección publica diseñada, Delgado (2009), manifiesta que esta fase emana de la autoridad y ya llevo a cabo las otras tres fases.

4. **Implementación,** movilizan a un conjunto de actores para llevarlo a la acción. Impactos efectivos de la implementación., señala Delgado (2009) , se llevan a cabo movilización de recursos económicos y humanos con la finalidad de poner en práctica la política adoptada, se lleva a cabo la ejecución de las políticas, a través de una secuencia de acciones e involucra a un indeterminado número de actores y operaciones, con la finalidad de obtener los resultados esperados.

5.- Evaluación, en esta fase se lleva a cabo la evaluación del resultado, pero Sabatier (2000) manifiesta que la evaluación también es de todo el proceso de las políticas públicas, es decir debe evaluarse todo el ciclo de políticas.

3.2.1 Problemas públicos

Como ya hemos abordado las políticas públicas buscan dar respuesta a las demandas sociales a través de la implementación de estas, por lo que todos los actores involucrados juegan un papel fundamental en su elaboración, ya que como lo expuso Lasswell (2005) el trabajo interdisciplinario es fundamental para el éxito de las políticas, ya que los múltiples actores interdisciplinarios abordaran desde su perspectiva aquellas demandas sociales, por consiguiente el trabajo de un administrador es muy complejo, pues cae en él, la responsabilidad de la resolución de problemas a través del análisis de estos y elaborando políticas públicas idóneas para atacar el problema, pero si la política no consigue el éxito buscado jamás se logrará erradicar el problema, por lo cual es necesario definirlo, ya que solo de esa manera se lograrán observar una cadena de valores que siendo del interés o no del administrador deberían de enlistarse jerárquicamente, pero, ¿Cuál método es el más adecuado? ¿Es posible enlistar jerárquicamente una serie de valores que conduzcan al diseño de una política pública con éxito?

Para Lindblom (1959) era viable hacer ese listado a través de un análisis del contexto social actual y de los problemas públicos, como ya hemos mencionado antes, la racionalidad y la colaboración interdisciplinaria hacen que estos sean abordados desde una perspectiva analítica y profesional. Lindblom nos habla de una secuencia de valores a considerar para la formulación de una política que busque combatir ciertos problemas, cualquiera que el administrador tome en consideración, su análisis debe comenzar enlistando de manera jerárquica una secuencia de "valores" relacionados directamente con el problema y su contexto actual, social, y no limitarse a una sola resolución, es decir, tomar en consideración desde antes de su elaboración otras posibles políticas, tener más opciones, lo que se lograría a través del análisis realizado, los administradores tomarán en cuenta los valores que se han estudiado y entonces diseñaran todas las opciones posibles a su alcance, después del diseño, la comparación sistemática entre las diversas opciones que tiene en consideración le ayudara a elegir entre aquella que tiene mayor cantidad de valores, a través de estos tres pasos resultará más factible el diseño de una política, tratando de buscar el éxito gracias a una mejor revisión que se está llevando a cabo, aunque cabe mencionar que esto no quiere decir que el éxito sea rotundo, pues nunca se está exento al fracaso, pero el considerar más de una diseño ayudará a contar con un análisis integral y una mejor toma de decisiones.

Por otro lado, los problemas de interés público son sinónimo de complejidad, aunque cabe mencionar que esta complejidad se encuentra en unos más que en otros, motivo por el cual expone Lindblom (1959), dos métodos, haciendo la división de problemas en dos tipos, "los complejos y los relativamente simples". Las capacidades intelectuales, fuentes de información son elementos fundamentales y de gran influencia, así como también lo son el tiempo y dinero que debiera asignarse a los o a un problema de política, siendo

por lo general limitados, estos dos últimos, restringiendo con ello la atención en los valores y así mismo las pocas políticas alternativas. El primer método es considerado para la formulación de políticas que busca la resolución de problemas simples, es el paso a problemas contemplados a pequeña escala, mientras que el segundo método busca atacar el problema de raíz, construyendo su base sobre el pasado como lo manifiesta Lindblom exponiendo que el enfoque racional deductivo debe tener en cuenta una multiplicidad de variables de alta complejidad que a su vez interactúan todas entre ellas y requieren que uno vaya a la misma raíz de la "situación/problema." El enfoque deductivo presta fuerte atención a los valores y a su aplicación, y como resultado de ello acota lo que "se trata", y nos llevaría a un "enfoque sinóptico" para la toma de decisiones.

Lindblom (1959) expone el método de la raíz como el desacuerdo por parte de todos los actores involucrados en la elaboración de las políticas públicas y no solo de ellos sino de los miembros de la sociedad, con referencia a los valores u objetivos que este método considera fundamentales mismo que juega un papel muy importante debilitando la credibilidad de este. El administrador asume un criterio de decisión manifestando con ello la creencia en propios valores a considerar, pero ahora se encuentra frente a otra problemática, la de jerarquizar los valores que son considerados y que son parte del conflicto, ya que deberá tomar en cuenta después de una arduo análisis a cuál de los valores ha de sacrificar, ya que existen diversas circunstancias para que estos sean tomados en cuenta, motivo por el cual exponía que es esencial elegir las políticas que combinan estos valores y no calificar valores para con posterioridad elegir entre las políticas, así mismo considera dos aspectos en la determinación de valores; primero, la valoración y el análisis empírico, la segunda; centrar atención entre valores marginales e incrementales.

Por otro lado la limitación en cuanto al análisis denota dos elementos, principalmente la capacidad intelectual humana y la información a la que se tenga acceso, se considera que nadie puede practicar el método racional-exhaustivo debido a que los problemas presentan un alto grado de complejidad, pero la realidad es que el administrador haciendo uso de las capacidades intelectuales y de todo medio de información al que tenga alcance (doctrinas, teorías) tiene que ir presentando esa capacidad de análisis y raciocinio transformando la alta complejidad de un problema a través de estudios y diseños que puedan simplificar la complejidad del mismo, los administradores que participan en la formulación de políticas no son "todólogos", pero van adquiriendo el conocimiento sobre diversos temas, pero sobre todo la capacidad de simplificar las complejidad de los problemas ante los que se encuentren.

El error en este caso puede no ser anticipado, pero sí es importante estar preparado para enfrentarlo en caso de que ocurra. Como menciona Lindblom (1959), las democracias tienden a cambiar sus políticas mediante ajustes incrementales, lo que implica realizar análisis detallados para evitar políticas irrelevantes

y poco efectivas debido a la complejidad del problema. Es esencial simplificar el análisis y delimitar claramente el problema y su alcance antes de abordarlo.

Los administradores de políticas deben tener en cuenta tanto las políticas actuales como las del pasado, para realizar análisis exhaustivos y considerar diferentes modelos antes de abordar un problema complejo. Es importante evitar intentar resolver un problema general sin una definición clara y detallada del mismo.

En una sociedad con libertad de asociación, los "perros guardianes" son aquellos grupos y organizaciones que defienden intereses sociales y valores que pueden no ser tomados en cuenta por las instancias gubernamentales. Estos grupos juegan un papel crucial al velar por los intereses y demandas de la sociedad en general. Los procesos de ajuste mutuo y acuerdos entre estos grupos permiten atender las necesidades de la sociedad de manera más efectiva (1959).

Por otra parte “El método de irse por las ramas se hace y se rehace sin cesar” Lindblom (1959) manifiesta que no todo está dicho, en cualquier momento se va cambiando a la vez que salen a la luz nuevas consideraciones, se logra prever las consecuencias probables a través de políticas y del conocimiento que se tiene de las mismas en base a los pasos empleados, no espera con la política una resolución final sino la capacidad de reajuste, logrando con ello considerar la antelación de una respuesta por si se está frente a un error, sobre todo se tiene que tomar en cuenta que nadie está exento de errores, las alternativas y la capacidad de improvisación también es parte fundamental del diseñador de políticas.

Mientras que el “método de ir a la raíz”, lo expone Lindblom (1959) como primer paso no habla de objetivos que tiene que ser jerarquizados para alcanzar de una manera adecuada esos fines deseados, en donde se le debe de dar la importancia a cada valor u objetivo, pero cabe mencionar, que esa jerarquía no dependerá de una mayoría, sino de lo que aquel encargado de la elaboración de políticas crea, ya que difícilmente se va a llegar a acuerdos entre la definición principalmente de objetivos y después de la jerarquía que se da a estos, la única forma de lograr saber si la política es buena es que se cumplan los fines deseados, los que se establecieron.

3.2.2 Formulación de las políticas públicas

Dentro de la formulación de las políticas nos señala Roth (2002), que se tiene que considerar “el ser”, es decir la situación presente y “el deber ser” refiriéndose a aquella situación deseada a alcanzar, es decir cuál de las alternativas existentes nos ayudará a que no coexista tensión entre la situación presente y a lo que se desea llegar, mientras que Quintana (2014), nos señala que esta etapa intenta responder a dos preguntas de la política ¿Por qué? y ¿Cómo?, para con ello tener claro cuáles son las metas o los fines deseados de la política a diseñar, y con posterioridad dar precisión a los objetivos concretos, el objetivo

representa el "cómo". Roth hace referencia a una cascada de metas y objetivos, jerarquizando cada uno de estos, lo cual hace más fácil los niveles de intervención estatal, con posterioridad se determinan los efectos esperados y los indicadores para con ello poder conocer el grado de realización de la meta. A través de la planificación se busca alcanzar con coherencia los objetivos, con definición de prioridades, y jerarquía de los objetivos y de los medios necesarios, el plan se elabora en base al instrumento racional de integración de las diferentes políticas sectoriales, la reducción de la incertidumbre lleva implícito el conocimiento previo que se tiene del contexto y se lleva a cabo a través de recolección de datos, gracias a los instrumentos, Roth menciona tres elementos importantes "estadística social, económica y la contabilidad nacional." Los obstáculos a la planificación se pueden considerar como factores externos o internos (2002).

3.2.3 Agenda de gobierno

En el análisis de Políticas Públicas, la formación de la Agenda es fundamental en la actuación de los gobiernos en relación con la atención de ciertos problemas, ¿Qué define su importancia a la hora de seleccionar cierta alternativa? Esto dependerá de la importancia objetiva que esos problemas representan para la sociedad, ya que estos problemas dan la importancia al proceso de política en la elección y definición de problemas públicos. El análisis que se realiza en la formación de la agenda pública, entendiendo que esto conlleva todo un entramado en torno a su construcción; grupos involucrados, grupos de intereses, diversos actores y organismos interesados en una demanda social en cuestión, se presenta a través de la existencia de diversos problemas y de los cuales el Gobierno en base a un análisis decide sí interviene para su solución. Es importante que estos problemas reflejen de manera clara las prioridades y las preocupaciones mismas que son de interés público, es decir, que el problema planteado tenga esa visión de problema social, ya que el nivel de atención que se le dé, dependerá de los grupos de actores que están involucrados en el proceso de la creación de la agenda, es decir, que todos ellos comprendan la relevancia de formar parte de la Agenda de Gobierno, pues el éxito de su implementación dependerá de la coincidencia de un equipo multidisciplinario, problemas, soluciones y las oportunidades de elección.

La formación de la agenda, es un tema muy complejo, debido a los diversos actores que busca dar solución a los problemas sociales que repercuten en su gobierno, comprometidos desde su campaña política, aunque no siempre tomando en cuenta a los grupos sociales que son la voz de una minoría y que no siempre es escuchada, esto deriva que las relaciones tienen que ser estrechas y los conflictos sociales que afectan a un grupo, en diversas ocasiones no benefician a todos, el desacuerdo y la falta de análisis da paso a un proceso de ciclos, en donde a pesar de la reformulación del problema, no se logra erradicar, debido a que los grupos sociales no tienen las mismas oportunidades de ser escuchados, hay problemas que no reciben

solución, es el claro ejemplo de las "anarquías organizadas", en donde no todos los problemas tienen un acceso establecido en la agenda no cuenta con oportunidades para ser tratados, en las arenas públicas no se exponen los problemas por igual, pero como ya lo comentamos con anterioridad en ocasiones la mejor opción que se tiene es la inacción de dichos problemas públicos, pero aquellos que son de interés para los actores involucrados, se incorporan a la agenda pública a través de la identificación de estos, existen según para Delgado (2009) dos tipos de agenda; la agenda sistémica; la cual se conforma por un grupo de problemas que acontecen a un grupo determinado de la sociedad y necesitan ser atendidos a través de la autoridad gubernamental, estos problemas son de interés y preocupación de dicha sociedad. Por otra parte, la agenda de gobierno incorpora solo asuntos que fueron aceptados por aquellos miembros del gobierno, es decir, el gobierno cree que es necesario incorporarlos para dar solución a dichos problemas.

3.3 Diseño, implementación y evaluación de las políticas públicas en México

Durante el diseño, implementación y evaluación de las políticas, es decir, todo el ciclo que las conforma en múltiples ocasiones dichas políticas no tienen éxito y a decir verdad, el tema de "las promesas incumplidas" o "las esperanzas frustradas", no es un tema del todo nuevo y actualmente lo seguimos presenciando en la mayoría de las situaciones, principalmente en nuestro país, pero ¿cuál fue la realidad que llevo a los Estados Unidos de Norteamérica a las grandes decepciones en temas de política social? Por contextualizar Estados unidos al ser nuestro país vecino y por las estrechas relaciones que México mantiene, la repercusión también lo es para México, estos temas que han presentado frustración no son para nada nuevos resaltan entre ellas necesidades sociales de pobreza, desigualdad, discriminación, y surgen otras demandas sociales que a pesar de ser realmente necesarias, no se ha logrado establecer la importancia y repercusión que pueden ocasionar si no son atendidos, podríamos hacer una lista indeterminada e incluso de políticas que han fracasado, y es cuando pasa algo que causa revuelo, cuando nos damos cuenta de que las políticas siguen su curso y que la mayor parte del tiempo, no se dedican a la resolución de estos conflictos de tipo social, pero entonces, ¿Por qué hay tantas promesas sin cumplir por parte de los partidos gubernamentales que buscan posicionarse dentro del poder? En realidad, ¿este tipo de conflictos sociales no frenará? Los diversos estudios que acontecieron a esa época trataban de localizar el error del gobierno, entender ¿qué se tenía que hacer? Lo manifestado por Aguilar (1996) nos da respuesta a las cuestiones arriba mencionadas, pues plantea que durante los años de posguerra concibió los estudios desde una triada de ciencias, siendo estás la ciencia política, la economía y la sociología, el desarrollo fue considerable y muy importante para con ello pensar que las múltiples estadísticas que arrojaban pronósticos sobre las consecuencias de las decisiones y la estimación del costo-beneficio, el gobierno se proponía alcanzar los objetivos propuestos, cumpliendo con solución favorable de las demandas sociales, pues toda proposición científica era probada y los diseños de innovación se basaban

en “Investigación y Experimento” e “Investigación y desarrollo”. Pero la causa del problema real se encontraba principalmente en su implementación, todos aquellos programas y toda la inversión no se tiene la duda de que haya sido buena, pero carentes de objetivos específicos y sin conexiones entre las diversas operaciones llevadas a cabo, lo que en una infinidad de veces causó políticas públicas incapaces de cumplir con sus objetivos planteados. Tras una serie de investigaciones para lograr entender que había resultado mal, se encontraron con factores que pasaron desapercibidos anteriormente y que afectaban la puesta en marcha de las políticas gubernamentales, y que, hasta el día de hoy, siguen estando presentes es por ello que la promulgación de leyes y el buen diseño de un programa gubernamental no eran suficientes para que una política se lograra con éxito, el tomar en cuenta todos los pasos del proceso del ciclo de la política no arroja la eficiencia y efectividad en estas, pero como lo comento Lindblom (1959) y ya habíamos referido con anterioridad, es necesario saber que nos podemos encontrar ante el fracaso de estas, por lo cual se tiene que prever otras alternativas en caso de que la política fracase.

Por otro lado según Aguilar (1996), es necesario considerar tres puntos para tratar de llevar a cabo un programa funcional, ya que no es solo cuestión de pensar en un problema e intentar dar una solución, pese a todas las partes que conforman cada uno de los pasos del ciclo, podríamos encontrarnos ante el fallo de políticas públicas una y otra vez, pero todo lo que se involucra dentro de este proceso nos arrojaría a una política con más posibilidades de éxito, el principal error que se llega a dar por parte de los hacedores de políticas públicas es estar seguros que la política no fracasara, pues este es el principal punto a cambiar, para poder tener alternativas, el abordaje de las demandas sociales tiene que ser más preciso y no general, es decir saber el enfoque que se le dará, formar parte de la clasificación dentro de la misma demanda, es decir, desde que aspecto será tratada, por lo cual los tres puntos que Aguilar (1996) menciona favorecen a cambiar ese criterio de confianza, manifestándolo de la siguiente manera.: 1) Nos encontramos con el escepticismo respecto de los fundamentos intelectuales de la reforma liberal; 2) Enfatiza que aun sabiendo lo que se debe hacer y encontrando los líderes políticos dispuestos a hacerlos, el gobierno está probablemente mal cortado para llevar a cabo el trabajo, es probable que las estrategias regulatorias y burocráticas que han empleado con toda confianza los gobiernos sean ineficaces si no es que dañinas; 3) Si se sabe lo que se debe hacer, se encuentran los líderes políticos dispuestos a hacerlo y se puede diseñar una estrategia apropiada de intervención gubernamental, no se puede asegurar que la estrategia será bien llevada a cabo.

Si no se cambia la manera de pensar y concebir las cosas, nos seguiremos encontrando una y otra vez con políticas fallidas y tal vez la réplica de estas, predecir el futuro de las políticas públicas no solo es predecir su función, sino prever su fracaso, esto para adoptar opciones alternas desde que nos encontramos frente a la demandas sociales, ese cambio y amplitud de conocimiento es básico para que las políticas públicas

tomen una nueva orientación, y no solo se tomen modelos para replicar, pues recordemos que como ya lo expusimos, las políticas que han sido creadas para determinado país, no pueden ser adoptados por otros, no solo el contexto cambia, sino las condiciones, el tipo de gobierno, el abordaje y enfoque de las necesidades sociales, el tipo de territorio que presenta la sociedad, por solo mencionar unos cuantos, entonces los modelos pueden ser tomados en cuenta, pero para ello deberían de ser adaptados a cada Estado.

Los primeros estudios sobre la implementación.

Aguilar Villanueva (2000), nos habla de los primeros estudios sobre la implementación enlistando a un grupo de investigadores considerados de "la primera generación", dedicados a realizar los estudios sobre la implementación de las políticas, descubriendo y explicando con ello los defectos, conflictos, retrasos, distorsiones, entre otras, argumentando que hasta las políticas mejor diseñadas podrían mal lograrse, claro y tomando en cuenta que son años los que se necesitan para que el reflejo arrojados sea favorable, una vez implementados los programas, aunque los fracasos que envuelven a las políticas pueden ser diversos y de múltiples factores, la defectuosa implementación de las políticas es sin duda la base o el inicio de estos. Por lo tanto, no solo el diseño es importante sino también la implementación de una política es de vital importancia. Se llegó a pensar en la toma de decisiones, marcando la pauta del fracaso de una política, pero no solo era causa de la toma de decisiones, o de pensar en el diseño de la política como bueno, las causas del fracaso abarcaban más que ese tipo de factores o sus orígenes, es más bien un conjunto, no solo de decisión, o de diseño, si no también aborda aquellos factores que surgían de la implementación de las políticas, o el conjunto en general.

Los defectos y excesos de las políticas federales.

Su principal estudio y aporte fue para contestar una pregunta que a muchos nos ha dado inquietud ¿por qué fallan las políticas locales? Derthick (1970) aportó que la falta de influencia en los gobiernos locales se da debido a la resistencia de las autoridades y grupos locales considerados al momento que el programa sea puesto en operación. Así mismo la predisposición en la planeación de las metas ideales tuvo también consecuencias que se vieron reflejadas en el fracaso del o los programas, abarcando no solo un conflicto, sino queriendo a raíz de uno solventar varios, es decir, se buscaba la construcción de una sociedad modelo, para lo cual, la pobreza, el racismo y la criminalidad, principalmente se estarían combatiendo. Fuera del alcance quedaron los incentivos y el tema de una canalización de estos hacia el poder local, siendo necesario de haberse dado cuenta a tiempo y con ello se hubiera alcanzado el propósito federal deseado.

La complejidad de la acción conjunta.

Por otro lado y como ya es sabido, principalmente tanto Pressman y Wildavsky (1984), basaron sus estudios en aquellos errores que venían haciendo de las políticas implementaciones de estas que con seguridad dirigirán al fracaso, pero como anteriormente lo hemos visto, era necesario resolver que es lo que llevó a dichas políticas a fracasar, pero también conocer en dónde se encuentra el error y tratar de evitarlo, aunque con anterioridad se manejó que había sido problema de la ejecución, los fracasos correspondían a factores que tenían que ver por la frustración, ya que las políticas no tuvieron la oportunidad de expandirse y por tanto verse bien reflejados sus efectos ya que el programa no se había logrado con éxito, más bien su logro se vio truncado. Aunque no todos los fracasos tienen que atribuirse a la implementación, no se puede dejar de lado que los factores sociales que acontecen y que se ven reflejados en la implementación, igualmente ocasionan repercusiones que se manifiestan como fracasos de las políticas o programas gubernamentales. Otro aspecto importante para Pressman y Wildavsky (1973) Es trabajar en conjunto con el diseño y la implementación de las políticas públicas, y por otro lado se cree que la claridad en el diseño es lo que favorece a los programas a tener éxito y no recurrir una y otra vez al fracaso. Aunque cabe mencionar que no existe ni una implementación, ni una política perfecta. Ya que al diseño le confiere una sucesión de actos entre los que destaca el proceso de implementación a través de la cual se busca el desarrollo de un programa que busca solucionar a través de este sus objetivos deseados.

El juego de la implementación.

Otro aspecto importante es los mencionado por Bardach (1998) es "llegar a una concepción precisa del proceso de implementación, antes de intentar especificar sus problemas y especular sobre lo que se debe hacer para enfrentarlos" a través de lo que denominó el “proceso de ensamblaje”, se entendía perfectamente que aquella implementación era el proceso al que hacía referencia y que ensamblaba diversos pasos o procesos, siendo estos; “recursos financieros y procesos administrativos, las fuentes de los fondos, las dependencias públicas, empresas privadas proveedoras de bienes, servicios, los grupos de apoyo, las regulaciones de autoridades gubernamentales, la actitud de los beneficiarios o clientelas”

Por otro lado, agregó Aguilar (1993), que se logra a través de la negociación y de la persuasión, ya que cada uno de los elementos debería aportar lo propio a sus capacidades. Debido que al estar al mando un partido político, llega a ser condicionante para la estrategia y la táctica de la lucha. Por otro lado, analizando los diferentes puntos de vista de los diversos autores, no todos conciben los fracasos a los mismos factores, pero todos coinciden en que no se pueden seguir replicando doctrinas en donde el fracaso de las políticas se hace presente, entonces se debería de poner atención en cada uno de los elementos de las programas elaborados y tratar a toda costa de prever los fracasos, buscando en todo momento que la

diversidad de opiniones que existe entre todos los actores involucrados, se logre considerar y logre obtener mayor amplitud en sus ideales y no solo el mero convencimiento o capricho de hacer una voluntad propia en base a doctrinas erróneas o a ideales discrepantes entre los múltiples actores que se ven involucrados, y eso no involucra solo al proceso en la toma de decisiones, sino en cada uno de los pasos que conlleva a la implementación de un programa para así lograr cumplir con sus metas planteadas, a través de análisis previos o estudios precisos, empleando el argumento buscando proveer la información adecuada, con los medios a los que se tenga acceso y no solo por querer cumplir con políticas que abarquen problemáticas múltiples y sin poder cumplir aunque fuese un objetivo deseado.

En la toma de decisiones tanto como en la ejecución de las políticas, se tiene que enfocar el interés de no cometer errores, pues en la toma de decisiones no se puede generalizar sobre un tema, por lo que una adecuada delimitación tendría mejores resultados sobre políticas que actúen buscando las metas deseadas, es decir, no querer abarcar un sinfín de situaciones, y por el contrario ser conscientes del alcance que se tiene, con los medios involucrados, es decir, gasto público, grupos de interés social y gubernamental, siempre estaremos ante la presencia de problemas en los que la agenda pública no ponga interés, no por falta de programas o doctrinas o porque el problema no sea importante, sino que conlleva una serie de elementos que se tienen que considerar para obtener el efecto deseado y no solo la intención de dar solución a las demandas sociales, hoy en día temas de pobreza, racismo, delincuencia, drogadicción y nuevos temas con relación al uso de las redes y las tecnologías de la información y comunicaciones representan una demanda social respecto a la necesidad de una Política pública de ciberseguridad en México, aunque cabe mencionar que dichos temas sobrepasan fronteras, no son temas específicos de un solo país, pero se ha llegado a dar el caso que los problemas sociales que acontecen a un gobierno, llegan a perjudicar a otros más, trascendiendo en el tiempo o en el espacio. Dejando con ello claro que no porque existan dichos problemas, no se esté haciendo nada, tal vez los medios no son los idóneos, las políticas no son las adecuadas, o el desconocimiento al encontrarnos frente a nuevos temas, ya que como lo hemos mencionado, la evolución de la sociedad trae consigo, evolución de demandas sociales también, lo que es cierto es que, los hacedores de políticas vamos avanzando no junto con el desarrollo de un país, sino detrás de este, ¿Cuántos años? es un tema que tal vez resulte sorprendente, y pareciera de ¡nunca acabar!, pero la realidad es que el compromiso que hubo años atrás, no es el mismo, las doctrinas o leyes, no se pueden replicar tal cual, los programas que no favorecieron tienen que pronosticar y reajustarse, tantas veces fuese necesario, en algún momento se dijo que los hacedores de políticas, no son todólogos, nuestra verdad no es la única y hoy en día seguimos lidiando con esas ideologías que solo nos llevan una y otra vez al fracaso, porque es más fácil la lucha del poder que poder hacer algo por la lucha de erradicar dichos conflictos a través de políticas.

Por otro lado, un sistema centralizado recurre a más problemas ante los conflictos y a menos cumplimiento de los programas, lo que en alguna ocasión expuso Lindblom (1991) al argumentar que en un sistema descentralizado, los problemas parecían no ser olvidados, ya que existían grupos sociales a los que denominó “perros guardianes” y en donde, los grupos se encargaban de hacer ver los problemas a los que no se les ponía la atención adecuada, con ello, la mayoría de los conflictos sociales tenía una solución o eran temas que no se dejaban de tratar, ya que “los perros guardianes” se encargaban de cuidar sus intereses, estos grupos de interés sociales se hacen hoy en día más fuertes ya que usan los medios de comunicación y ahora con el uso de las redes sociales, se emplean para que aquellas demandas sociales sean expuestas a través de las múltiples plataformas y con ello tengan mayor impacto al estar haciendo presión en busca de una respuesta que de solución a determinada situación, justo nos damos cuenta que teorías y modelos estudiados años atrás siguen siendo presentes y manifestando la forma de abordar las políticas públicas con el conocimiento previo y las acciones necesarias y expuestas en este capítulo.

3.4 Políticas públicas en ciberseguridad

Por lo anterior expuesto el Estado debe reconocer la importancia de crear una Política pública de ciberseguridad, con el fin de garantizar y salvaguardar la integridad, confidencialidad y privacidad de los derechos de la sociedad, la protección a sus infraestructuras críticas y los servicios públicos que son soportados por las infraestructuras tecnológicas, todo esto como lo hace a través de las leyes generales que regulan la conducta humana, de lo contrario, seguirá creciendo la impunidad en los delitos cibernéticos, siendo blanco vulnerable que afectan no solo a una parte de la población, sino como ya se comentó pueden poner en riesgo la seguridad de un país.

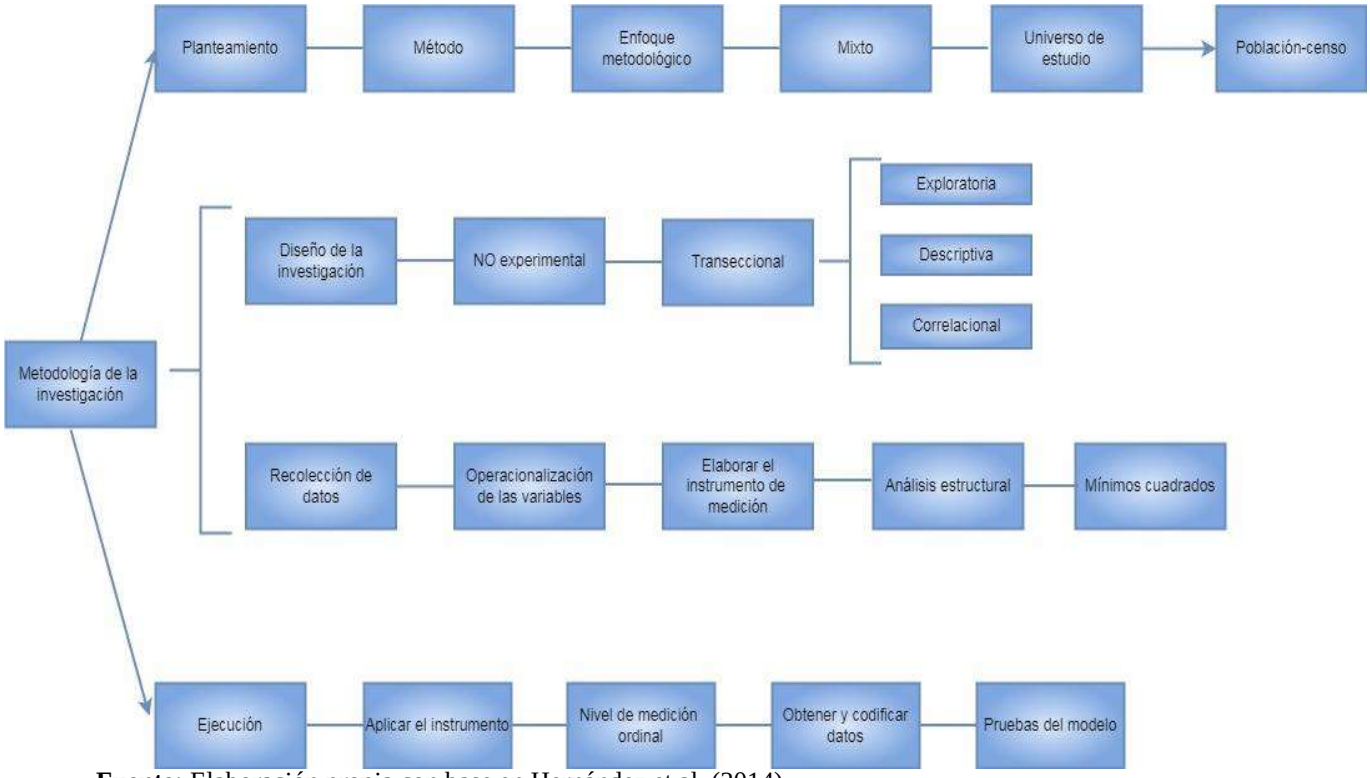
Las instituciones actualmente son susceptibles de cambios dado el contexto existente que se vive y que obliga en razón de su capacidad económica, política y social a realizar una reingeniería de sus procesos existentes, lo que involucra una serie de modificaciones a su estructura organizacional, por lo cual a partir del reconocimiento de la problemática mencionada, se debe implementar un marco de actuación que establezca la visión del Estado a partir del reconocimiento de los riesgos asociados al uso de las tecnologías como es el, diseño de una política pública de ciberseguridad en el Estado de Michoacán.

CAPÍTULO 4. DISEÑO DE LA INVESTIGACIÓN.

4.1 Introducción

Para el desarrollo de la presente investigación se emplea el método científico, a fin de garantizar la confiabilidad y veracidad de los resultados obtenidos, a partir de la recolección de datos cualitativos los cuales mediante un tratamiento matemático, permitirán poner a prueba las hipótesis planteadas en la presente investigación y cuyos resultados permitirán realizar una aproximación causal del fenómeno estudiado. La siguiente ilustración presenta la metodología a seguir en esta investigación, misma que se describirá a lo largo del capítulo.

Ilustración 13. Metodología de la investigación.



Fuente: Elaboración propia con base en Hernández et al. (2014).

El estudio actual se fundamenta en el empleo del método científico como base de la presente investigación. Tamayo y Tamayo (2004) lo define como un conjunto de pasos lógicos y procedimientos que se utilizan en la obtención de conocimiento verídico y comprobable del fenómeno objeto de estudio. Mientras que Bunge (2013) afirma que solo puede existir dentro del contexto de la ciencia, ya que el método científico es una parte integral de la actividad científica, en la adquisición de conocimiento por medio de técnicas especializadas para explicar la realidad.

De lo comentado en líneas anteriores se puede entender al método científico como una secuencia estructurada y organizada de etapas, que mediante la aplicación de principios, reglas y normas, buscan alcanzar el objetivo de la investigación y la validación de la hipótesis objeto de estudio.

4.2 Tipo de investigación

El enfoque de la investigación es mixto, ya que se combinaran los enfoques cualitativo y cuantitativo para la generación del conocimiento, ya que esto permite obtener una comprensión más amplia y profunda del fenómeno de estudio. En Hernández et al. (2010) Comprendido como una serie de etapas que se vale de la selección de datos de una muestra de la población para su posterior análisis, a través de un tratamiento matemático en la comprobación del hecho estudiado, mientras que en Tamayo y Tamayo (2004) nos refiere que es el contrapunto que un investigador puede realizar entre las diversas teorías actuales, tienen estrecha relación con las hipótesis que derivan de estas, ya que nos arrojan información importante para la realización de un muestreo al azar, pero siempre con el enfoque de aquella población o fenómeno social, en todo momento la investigación de tipo cualitativo y por tanto el investigador se vale para la obtención de información de distintos medios para el estudio del fenómeno a describir.

En tal sentido, mediante la recolección de datos se probará la hipótesis planteada con base en mediciones numéricas y análisis estadísticos dando el enfoque cuantitativo, de igual forma se contrastara y se complementara esos datos mediante la recolección de datos que nos describan cualitativamente el fenómeno estudiado.

4.2.1 Diseño de la investigación

Por consiguiente el tipo de investigación es de tipo no experimental. Hernández et al. (2010) Explica que en este tipo de investigación no existe manipulación alguna sobre las variables de estudio, si no que se observa el fenómeno a explicar en su ambiente natural para un posterior estudio, a partir de hechos ya existentes, que permitan explicar las variables y su incidencia sin la manipulación del investigador. El diseño es de corte transeccional debido a que la recolección de datos será en un único momento, este diseño de divide en tres tipos:

Exploratorios: existen fenómenos limitados en cuanto a exploración, por lo que el investigador tiene que sumergirse y ser parte de todo el contexto relacionado con los mismos, para con ello cumplir con el fin deseado de recolectar todo lo conducente para su investigación partiendo de una problemática y generando a través de todo un proceso nuevo conocimiento

Descriptivos: Los fenómenos que derivan de esta investigación tienen que ser detallados y definidos a través del análisis, para con ello tener un fácil manejo y adecuada comprensión de las variables.

Correlacionales: El investigador cuenta con una capacidad facultativa para relacionar sus variables, repercutiendo de manera directa en la comprensión del fenómeno objeto de estudio, confiriéndole mayor claridad y convirtiéndolo más práctico, lo que puede arrojar la dependencia entre causa - efecto.

Por lo cual el tipo de alcance en esta investigación será de tipo exploratorio ya que se intentará explicar un fenómeno poco explorado como lo es la Ciberseguridad, para lo cual se detallarán las distintas características que conformarán la Política Pública de Ciberseguridad, por otra parte de tipo descriptivo ya que definirá las propiedades y variables que conforman el estudio observado para facilitar la construcción del nuevo conocimiento y de manera correlacional cuyo principal objetivo es describir y analizar la correlación entre las tecnologías de la información y comunicaciones, los aspectos legales, la cibercultura, el cibercrimen, las infraestructuras críticas y la seguridad de la información en la generación de la Política pública de ciberseguridad.

4.2.2 Población y muestra

Como anteriormente se mencionó dentro del presente trabajo de investigación, la sociedad desempeña un papel crucial en la ciberseguridad al ser consciente de los riesgos asociados en su interacción en el ciberespacio, por lo que en esta investigación el universo de estudio, estará limitado a la población del Estado de Michoacán. Misma que presenta un número significativo de delitos cometidos a través de las tecnologías de información y comunicaciones.

Por otra parte en Hernández et al (2010) lo que él denomina como muestra va dirigido a un grupo específico de una población, es decir, a un grupo en particular que debido a sus características y elementos se reduce en tamaño. Asimismo Tamayo y Tamayo (2004) habla de muestra, y de censo, para reunir elementos generales de una población. La muestra se hará tomando en cuenta solo algunos elementos con la finalidad de indagar sobre una cuestión específica y delimitando a un sector o grupo específico de la población.

Por lo tanto, la muestra entendida como la selección de un determinado número de elementos del universo de estudio, permitirá la selección de una parte especifica de la población de interés.

En concordancia con lo anterior se señala en el plan nacional de desarrollo 2013-2018, en la meta México en Paz, objetivo 1.2 Garantizar la seguridad nacional, esto a través de la estrategia 1.2.3 como objetivo es fortalecer la inteligencia del Estado Mexicano para salvaguardar la seguridad nacional, con la finalidad de fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad (2013); aunado

al Programa Nacional de Seguridad Pública (2014) en el que se identifica la importancia de la ciberseguridad dado el incremento de delitos cibernéticos, que adicional a la Política de Seguridad Pública, se sentaron las bases para la coordinación entre los actores involucrados para la generación de una Política en materia de defensa y ciberseguridad, apoyándose de la estrategia: "2.7 Detectar y atender oportunamente los delitos cibernéticos"; dando como resultado la creación del Modelo Homologado de Unidades de Policía Cibernética (aprobado en su Cuadragésima Primera Sesión Ordinaria de la conferencia nacional de secretarios de Seguridad Pública, mediante acuerdo 06/XLI/16, celebrada el 20 de diciembre de 2016.) y en cumplimiento a los acuerdos 12/XL/16 del Consejo Nacional de Seguridad Pública y de la 7 de la XVI sesión ordinaria de la Conferencia Nacional de Secretarios de Seguridad Pública, con el que se aprueba el Modelo Homologado de las Unidades de Policía Cibernética que deberá ser implementado a partir del año 2017.

El Modelo Homologado de Unidades de Policía Cibernética nace para dar respuesta a la problemática que empezó a enfrentar México en su contacto con el ciberespacio, iniciando con conductas de riesgo y delitos cibernéticos, Actualmente en el territorio nacional existen 47 policías cibernéticas de las cuales 46 son de competencia estatal y una de la guardia nacional, las cuales se encuentran distribuidas de la siguiente manera:

Ilustración 14. Distribución de unidades de Policía cibernética

Fuente: Elaboración propia con imagen obtenida de Google Inc. (2021).

En relación a lo anterior es que se decide aplicar el instrumento de medición a las cuarenta y siete Unidades de Policía Cibernética pertenecientes al modelo homologado, a los cuales se les considera expertos en

materia de ciberseguridad, con base en su experiencia estos expertos poseen una perspectiva más amplia y enriquecedora del fenómeno de la ciberseguridad.

4.3. Tipo de muestra

La muestra es no probabilística, en el caso de la política pública de ciberseguridad, se selecciona un grupo específico de profesionistas en ciberseguridad que con base en su experiencia y conocimientos, identificarán que características están estrechamente relacionadas con el tema de estudio. Lo que les permitirá analizar de manera específica y detallada aquellos aspectos que tendrán un impacto directo en el tema de estudio.

4.3.1 Tamaño de la muestra

Para conocer la percepción en materia de ciberseguridad se realizará la investigación a través de una muestra estratificada a un grupo de cuarenta y siete expertos en ciberseguridad a nivel nacional, quienes de acuerdo a sus experiencia identificaran aquellas variables que deben ser incluidas en la política pública de ciberseguridad.

4.4 Técnicas e instrumento de recolección de datos

En la presente investigación se utilizó la recolección de datos mediante un instrumento de medición, el cual se aplicó a 106 (ciento seis) expertos en ciberseguridad pertenecientes a las 47 Unidades de Policía Cibernética pertenecientes a las Secretarías de Seguridad Pública, Fiscalías/Procuradurías de las 31 entidades federativas y la Ciudad de México y/o de la División General Científica de la Guardia Nacional[2].

Debido a la distancia con los especialistas en ciberseguridad, se tomó la decisión de utilizar un formulario de Google Forms, la cual es una herramienta en línea automatizada que permite la creación de cuestionaros personalizados y que estos se puedan compartir a través de un enlace, facilitando con esto la interacción a distancia y permitiendo el acopio de información de manera rápida y eficiente, se solicitará al entrevistado algunos datos generales que permitan identificar a que parte de la muestra corresponden: nombre, estado, sexo y correo electrónico, cuidando en todo momento la seguridad de la información recabada, tal y como lo muestra el enlace al formulario https://docs.google.com/forms/u/2/d/1dFDITpXf7erwjC6QqAqRXWA-YxvUbbHtb-FwXEFCOZc/edit, para mayor información se puede consultar el instrumento de medición en el Anexo 5.

[2] Listado de la Unidades de Policía Cibernética que participaron en el estudio en el Anexo 4.

La estrategia empleada para documentar esta investigación, es a través de un modelo de análisis multivariado (mínimos cuadrados) y con el empleo de diferentes herramientas automatizadas, se llevó a cabo el estudio y procesamiento de los datos: STATA, SPSS y Excel, cuya finalidad es probar la existencia de una correlación directa entre las variables independientes y la dependiente, para proporcionar un análisis más aproximado de la realidad en ciberseguridad, llevada a cabo con este grupo de expertos.

4.5 Descripción del instrumento

Dentro del cuestionario que se aplicó en la presente investigación existen apartados específicos para detectar todos aquellos datos que son relevantes, que ofrecerán un escenario más amplio de la incidencia delictiva y con ellos estar en condiciones de realizar análisis estadísticos y posteriormente correlacionarlos de manera que nos permitan realizar unas adecuadas conclusiones.

Para medir el instrumento se utilizó la escala tipo Likert, la cual asigna puntuación matemática a cada uno de los ítems lo que permite distinguir su grado de importancia, es un método utilizado en las ciencias sociales por Likert (1932) describe que este instrumento de medición es una herramienta en la recolección de datos de tipo cuantitativos para temas de investigación, cada uno de los ítem refleja lo que el investigador quiere medir de cada uno de los encuestados y las respuestas obtenidas tienen una calificación asignada, donde se le asigna un valor numérico que permite medir la importancia del tema objeto de estudio, en este caso particular, intentaremos explicar la importancia de la ciberseguridad.

4.6 Confiabilidad y validez del instrumento de medición

La confiabilidad y validez del instrumento de medición se define como el grado en que su aplicación muestra resultados consistentes y congruentes, lo que nos indica que su aplicación repetida en varias a ocasiones a los mismos sujetos genera resultados iguales. Para precisar la confiabilidad del instrumento de medición existen diferentes técnicas. Cronbach (1951) lo expone a través del método de consistencia interna denominado alfa de Cronbach, para conocer el grado de concordancia o discordancia de los 76 usuarios evaluados para determinar su opinión respecto al dominio de ciberseguridad.

La operacionalización de las variables se muestra en la siguiente tabla, donde se han definido y establecido como se medirán las dimensiones mediante indicadores, De izquierda a derecha, se presentan las variables independientes que son objeto de la presente investigación, seguidas de la variable dependiente, las dimensiones, los indicadores, los ítems y por último la clave que se utilizó para codificar los indicadores, lo que permitirá validar las hipótesis propuestas.

Tabla 7. Operacionalización de las variables

Apartado	Variables independientes	Dimensiones	Indicadores	ITEMS	key
I	Tecnologías de la información y de las comunicaciones	Hardware (equipos terminales). Software (servicios y redes de comunicación).	Amenazas lógicas	1	TIC-HWSW-A
			Protocolos	2	TIC-SW-ARC
			Fortalecimiento	3	TIC-SW-NE-VI
			Estándares , guías de buenas prácticas y	4	TIC-HWSW-D
			Actualizaciones	5	TIC-SW-SU
			Análisis de vulnerabilidades	6	TIC-HWSW-TE
II	Aspectos legales de la ciberseguridad	Legislación nacional, internacional y normativa.	Frecuencia y calidad de las actuaciones legales.	7	ALC-LN-VI
				8	ALC.AI-PD
				9	ALC-LN-PD
			Legislación en materia de cooperación internacional.	10	ALC-OISP-PD
				11	ALC-LT-CD
				12	ALC-AHC-V
III	Cibercultura	Conocimiento Aprendizaje	Nivel de conciencia Nivel de conocimiento Organizaciones públicas o privadas Campañas de concientización Guías de buenas prácticas	13	CIB-MC-DFC
				14	CIB-AP-PV
				15	CIB-CO-COPP
				16	CIB-AP-ME
				17	CIB-AP-CC
				18	CIB-AP-GBP
IV	Cibercrimen	Prevención Investigación Persecución Judicialización	Campañas de prevención	19	CC-PRE-DC
			Especialización técnica	20	CC-JUD-ET
			Equipamiento especializado	21	CC-PRE-EQE
			Creación de un órgano jurisdiccional	22	CC-PER-CODC
			Capacitación de los órganos	23	CC-PRE-COJ
			Creación de un centro de contención,	24	CC-INV-CCRI
V	Infraestructuras criticas	Esquema nacional	Catalogo Mecanismos de control y gestión Planes de recuperación	25	IC-EN-PAIC
				26	IC-EN-CA
				27	IC-ENDMEC
				28	IC-EN-IMIC
				29	IC-EN-PCDSW
				30	IC-EN-PRD
VI	Seguridad de la información	Educación proactiva Educación reactiva	Políticas	31	SI-EP-DSI
			Cultura de seguridad de la información	32	SI-EP-ASPR
			Equipos de respuesta a incidentes	33	SI-EP-DIBP
			Campañas de divulgación	34	SI-ER-CONT
			Medidas de seguridad y protección	35	SI-EP-PDSI
			Identificación de vulnerabilidades	36	SI-ER-ERI
VII	Variable dependiente	TIC´S Aspectos legales Cibercultura Cibercrimen Infraestructuras Criticas Seguridad de la información	Fortalecimiento TIC´s	37	PPC-IAG
			Marco normativo	38	PPC-CCD
			Capacitación y concientización	39	PPC-AJOC
	Ciberseguridad		Incremento de la ciberseguridad	40	PPC-INCC
			Protección de los datos	41	PPC-PDD
			Fortalecimiento de IC	42	PPC-FIC

Fuente: Elaboración propia con base en experiencia y metodología revisada 2023.

De manera resumida se muestra en la siguiente tabla con la estructura de la propuesta de instrumento de medición y la distribución en cuanto al número de preguntas.

Tabla 8. Estructura del instrumento por variables.

Variables		Dimensiones	Número de preguntas
Variables independientes.	Tecnologías de la información y comunicaciones	2	6
	Aspectos legales	3	6
	Cibercultura	2	5
	Cibercrimen	4	7
	Infraestructuras criticas	3	6
	Seguridad de la información	2	6
Variable dependiente.	Política pública de ciberseguridad	6	6
Total dimensiones y preguntas…….....		22	42

Fuente: Elaboración propia con base en la propuesta de instrumento 2023.

La escala permite medir el grado de concordancia o discordancia con respecto a cada de los ítems de cada uno de los encuestados, está definida por los siguientes valores:

1. Totalmente en desacuerdo
2. Bastante en desacuerdo
3. En desacuerdo
4. Ni de acuerdo ni en desacuerdo
5. De acuerdo
6. Bastante de acuerdo
7. Totalmente de acuerdo

4.7 Técnica de procesamiento y análisis de datos.

Una vez aplicado el instrumento de medición a los setenta y seis expertos en ciberseguridad se realiza el procesamiento de los datos recabados, a través de la modelización de ecuaciones estructurales.

4.7.1 Modelización de ecuaciones estructurales

De acuerdo Hair, et al. (2017) La modelización de ecuaciones estructurales es el resultado de una evolución a lo largo de varios años en el uso de herramientas estadísticas para desarrollar, explorar y confirmar teorías o conocimientos científicos por parte de los investigadores, especialmente en el ámbito de las ciencias sociales. Estos métodos estadísticos incluyen el análisis factorial y de regresión, ampliamente conocidos como métodos de primera generación, que fueron ampliamente utilizados durante la década de 1980.

Sin embargo, como consecuencia de la evolución, el cuestionamiento y la necesidad de abordar fenómenos sociales complejos, en la década de los 90 surgieron métodos de segunda generación, entre los cuales se destaca la modelización de ecuaciones estructurales con mínimos cuadrados parciales (partial least squares structural equation modeling, PLS-SEM). Este enfoque ha ganado reconocimiento y popularidad debido a su capacidad para manejar relaciones complejas entre variables latentes y observadas, y su flexibilidad para abordar muestras de tamaño reducido (Hair, et al., 2017).

Inicialmente, la estadística se basaba en modelos univariantes y bivariantes Hair, et al. (2017), para demostrar las relaciones entre variables. Sin embargo, la complejidad de muchos fenómenos sociales y el avance de los sistemas informáticos para el análisis estadístico de datos condujeron al surgimiento de modelos multivariantes. Estos modelos permiten analizar fenómenos en los que convergen múltiples variables, lo que brinda una perspectiva más completa y precisa de las interacciones y relaciones entre los diferentes elementos en estudio. Esta evolución ha sido fundamental para abordar la complejidad de la realidad y comprender de manera más precisa los fenómenos sociales en su totalidad.

Cuando se trata de métodos multivariantes Hair, et al. (2017) Han establecido diferentes clasificaciones que distinguen entre los métodos comúnmente utilizados en las ciencias sociales. Estas clasificaciones agrupan los métodos en dos categorías complementarias. Por un lado, se encuentran los métodos de primera y segunda generación, y por otro lado, los métodos principalmente exploratorios y confirmatorios. Estas categorías se presentan en la siguiente tabla, cada una con sus características.

Tabla 9. Clasificación de los métodos multivariantes.

Técnica	Principalmente exploratorios (predictivos)	Principalmente confirmatorios (probatorias)
Primera generación	• Análisis de conglomerados • Análisis clúster • Análisis factorial • Escalamiento multidimensional	• Análisis de la varianza • Regresión logística • Regresión múltiple • Análisis factorial confirmatorio
Segunda generación	PLS-SEM	CB-SEM

Fuente: Elaboración con base en Hair, et al. (2017).

Tanto las técnicas de primera generación como las de segunda generación se pueden emplear para llevar a cabo estudios de naturaleza exploratoria y confirmatoria. Los estudios exploratorios se realizan cuando existe un respaldo teórico limitado sobre las relaciones entre las variables, por lo que buscan identificar patrones que validen dichas relaciones. Por otro lado, los estudios confirmatorios tienen como objetivo poner a prueba hipótesis o realizar pruebas empíricas sobre teorías preexistentes (Hair, et al., 2017).

Las técnicas multivariantes de segunda generación tienen la capacidad de superar muchas de las limitaciones que presentan las técnicas de primera generación. Una ventaja destacada de la modelización de ecuaciones estructurales (SEM) radica en su capacidad para incluir variables observables o indicadores que miden variables no observables. En cuanto a los modelos SEM, existen dos tipos: el basado en la covarianza (CB-SEM) y el de mínimos cuadrados parciales (PLS-SEM), siendo este último el enfoque utilizado en la presente investigación (Hair, et al., 2017).

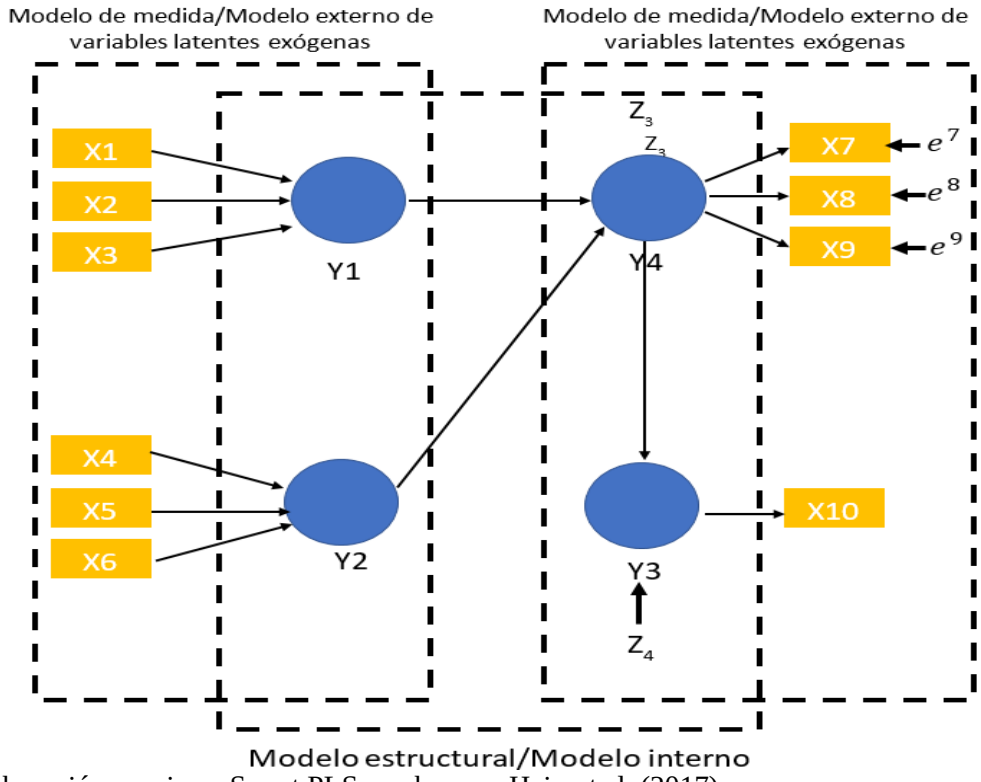
Aunque ambos modelos SEM tienen ventajas particulares dependiendo del tipo de investigación, existen consideraciones comunes al utilizar cualquiera de ellos: (1) los compuestos utilizados, (2) la medición de las variables, (3) las escalas de medida utilizadas, (4) la codificación de los datos y (5) la distribución de los datos. Es precisamente esta última consideración la que brinda una ventaja estadística significativa al elegir PLS-SEM en estudios exploratorios, ya que no requiere que los datos sigan una distribución normal (Hair, et al., 2017).

4.7.1.1 Aplicación de Partial Least Squares en la Modelización de ecuaciones estructurales

4.7.1.2 Nomograma

Una de las fortalezas de la modelización PLS-SEM, según Hair et al. (2017), reside en su capacidad y facilidad para visualizar las hipótesis de investigación y las relaciones entre variables dentro del modelo mediante el uso de nomogramas (modelos path). El nomograma representa visualmente las variables que no pueden medirse directamente como constructos, mostradas en forma de círculos, y las variables observables o ítems que actúan como indicadores de los constructos, representadas mediante rectángulos, en la ilustración siguiente se muestra el modelo interno y estructural.

Ilustración 15. Modelo estructural/Modelo interno.



Fuente: Elaboración propia en Smart PLS con base en Hair, et al. (2017).

Los nomogramas se componen de dos elementos principales: el modelo estructural o interno, y el modelo de medida o externo. El primero, representado por círculos, muestra las relaciones entre los constructos o variables latentes. El segundo muestra la relación entre los constructos y sus indicadores, representados por rectángulos. Esto implica la relación entre las variables observables (indicadores) y sus constructos subyacentes (variables latentes), así como la relación entre las variables observables externas y las variables latentes (Hair et al., 2017).

Los nomogramas, así como los modelos PLS-SEM en general, incorporan los términos de error asociados a los constructos endógenos y medidos de manera reflectiva, los cuales representan la varianza no explicada por el constructo. Sin embargo, en el caso de los modelos formativos, donde la relación va desde el indicador hacia el constructo, estos no incluyen términos de error (Hair et al., 2017).

4.7.2.3 Teoría de medida

Según Hair et al. (2017), la teoría de medida se refiere a la manera en que se realiza la medición de las variables no observables o latentes (constructos). Hay dos enfoques para llevar a cabo esta medición: los modelos de medida formativos, en los cuales la relación (flechas) se establece desde los indicadores hacia los constructos, indicando una causalidad de los indicadores hacia el constructo; y los modelos de medida reflectivos, en los cuales la relación se establece desde los constructos hacia los indicadores, lo que indica que el constructo causa la variación en el indicador.

Cuando se hace referencia a la teoría estructural, se está hablando de cómo se relacionan entre sí las variables latentes dentro del modelo. Estas relaciones, representadas por los caminos o "PATH" en los nomogramas, pueden basarse en teorías existentes, conocimientos previos o la experiencia del investigador. En el modelo estructural, se muestran las relaciones causales o los efectos entre las variables, donde generalmente se colocan las variables latentes exógenas o independientes en el lado izquierdo, y las endógenas o dependientes en el lado derecho. Es importante destacar que, en el caso de variables intermedias que actúan como exógenas con respecto a las variables independientes pero que a su vez dependen de otras variables exógenas, también se las denomina endógenas (Hair et al., 2017).

4.7.2 PLS-SEM

Existen múltiples beneficios al elegir PLS-SEM como método de investigación. Una de sus ventajas radica en su recomendación cuando la teoría subyacente es escasamente abordada o carece de una definición precisa. Es especialmente útil en casos donde el objetivo de la investigación es la explicación de los constructos clave del modelo y su capacidad predictiva. Mediante el uso de PLS-SEM, se busca obtener

una comprensión más profunda y precisa de las relaciones entre variables, permitiendo así realizar análisis más robustos y confiables (Hair, et al., 2017).

Presentan otra ventaja significativa al no requerir que los datos cumplan con los supuestos de normalidad. Esto significa que pueden ser aplicados a conjuntos de datos que no siguen una distribución normal. Además, estos modelos no necesitan grandes cantidades de observaciones para que sus resultados sean válidos y confiables. Aunque es importante destacar que a medida que aumenta el número de observaciones, se logra una mayor precisión en los resultados obtenidos. En resumen, los modelos PLS-SEM permiten flexibilidad en términos de requisitos de normalidad y tamaño de muestra, lo que facilita su aplicación en diversas investigaciones (Hair, et al., 2017).

El modelado PLS-SEM ofrece la capacidad de incorporar múltiples constructos en el análisis, lo que permite modelar relaciones complejas con múltiples relaciones estructurales. Esto incluye la capacidad de examinar los efectos de mediación y moderación en las relaciones entre variables. Al considerar estos efectos, se puede capturar de manera más precisa la complejidad de los fenómenos sociales estudiados. Esta capacidad de modelado enriquecida es especialmente relevante en investigaciones que buscan comprender las interacciones y relaciones complejas entre variables, lo que ayuda a proporcionar una visión más completa y detallada de los fenómenos sociales. En resumen, el modelado PLS-SEM brinda la flexibilidad necesaria para abordar relaciones complejas y reflejar de manera más precisa la complejidad de los fenómenos sociales (Hair, et al., 2017).

4.7.2.1 Modelo estructural

Según Hair, et al. (2017), el primer paso en el proceso de modelización PLS-SEM es la especificación del modelo estructural. Esto implica la creación de un diagrama que represente las hipótesis planteadas en la investigación y las relaciones entre los constructos o variables que se pretenden comprobar. La especificación del modelo debe estar fundamentada en la teoría subyacente y en la lógica que respalda la influencia de las variables entre sí. Es esencial que exista coherencia y cohesión en la representación del modelo, de modo que refleje de manera precisa las relaciones propuestas y las expectativas teóricas. Este proceso de especificación es crucial para establecer una base sólida y estructurada sobre la cual se llevará a cabo el análisis PLS-SEM (Hair, et al., 2017).

De acuerdo con el planteamiento del problema de la presente investigación denominada; “Principales factores determinantes de la Ciberseguridad en el estado de Michoacán”, El planteamiento del modelo estructural es el resultado de considerar las variables que se presentan a continuación y su interacción que se muestra en la siguiente ilustración.

Y = Ciberseguridad

X1 = Tecnologías de la información y comunicaciones (TIC´s).

X2 = Aspectos legales (AL).

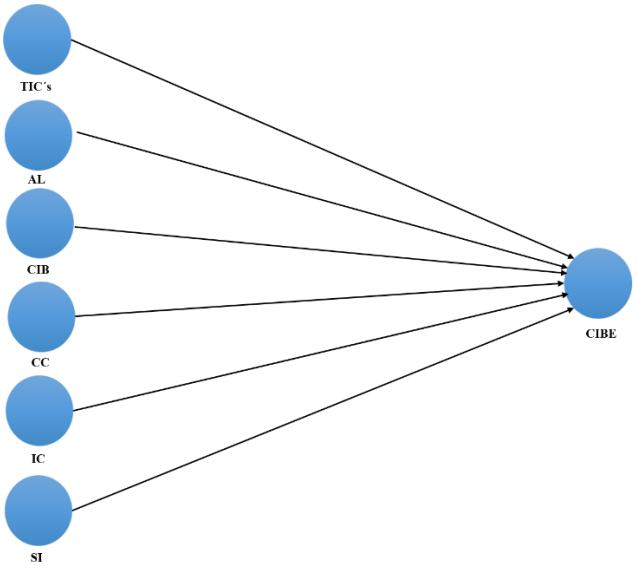
X3 = Cibercultura (CIB).

X4 = Cibercrimen (CC).

X5 = Infraestructuras criticas (IC).

X6 = Seguridad de la información (SI).

Ilustración 16. Nomograma de la ciberseguridad.



Fuente: Elaboración propia en Smart PLS con base en Hair, et al. (2017).

Como se observa se han modelado las variables independientes que muestran las relaciones entre las variables en el modelo estructural (tecnologías de la información y comunicaciones, aspectos legales, cibercultura, cibercrimen, infraestructuras críticas y seguridad de la información) a través de las líneas y flechas, se representan las conexiones hacia la variable dependiente (ciberseguridad), con la finalidad de visualizar de manera clara y concisa las relaciones causales propuestas en el modelo.

4.7.2.2 Modelo interno

El segundo paso en el proceso de modelización PLS-SEM, según lo planteado por Hair et al. (2017), implica la especificación del modelo de medida o modelo externo. En esta etapa, se representan las relaciones entre cada uno de los indicadores o variables exógenas y los constructos a los que afectan o causan, dependiendo de si se trata de un modelo reflectivo o formativo. Es importante destacar que la

selección de los indicadores más apropiados requiere una comprensión clara y fundamentada en sólidos principios teóricos de la teoría de medida del modelo. Estos indicadores deben ser elegidos cuidadosamente para garantizar una representación precisa y confiable de los constructos en cuestión.

En los modelos formativos, los indicadores son elementos que contribuyen o influyen en la formación del constructo endógeno, lo que implica que cada uno de ellos representa una dimensión clave para su construcción. Por otro lado, en los modelos reflectivos, los indicadores representan los efectos del constructo, lo que significa que estos indicadores pueden ser intercambiables o sustituibles entre sí Hair et al. (2017).

En el nomograma, se utiliza una representación gráfica para mostrar estas relaciones. En el caso de los modelos formativos, los indicadores se conectan al constructo mediante una flecha que apunta hacia él, indicando su influencia en la formación del constructo. En los modelos reflectivos, la flecha va desde el constructo hacia el indicador, representando la relación en la que el constructo causa los efectos observados en los indicadores, en la siguiente tabla se muestran los criterios para determinar el modelo de medida en una investigación.

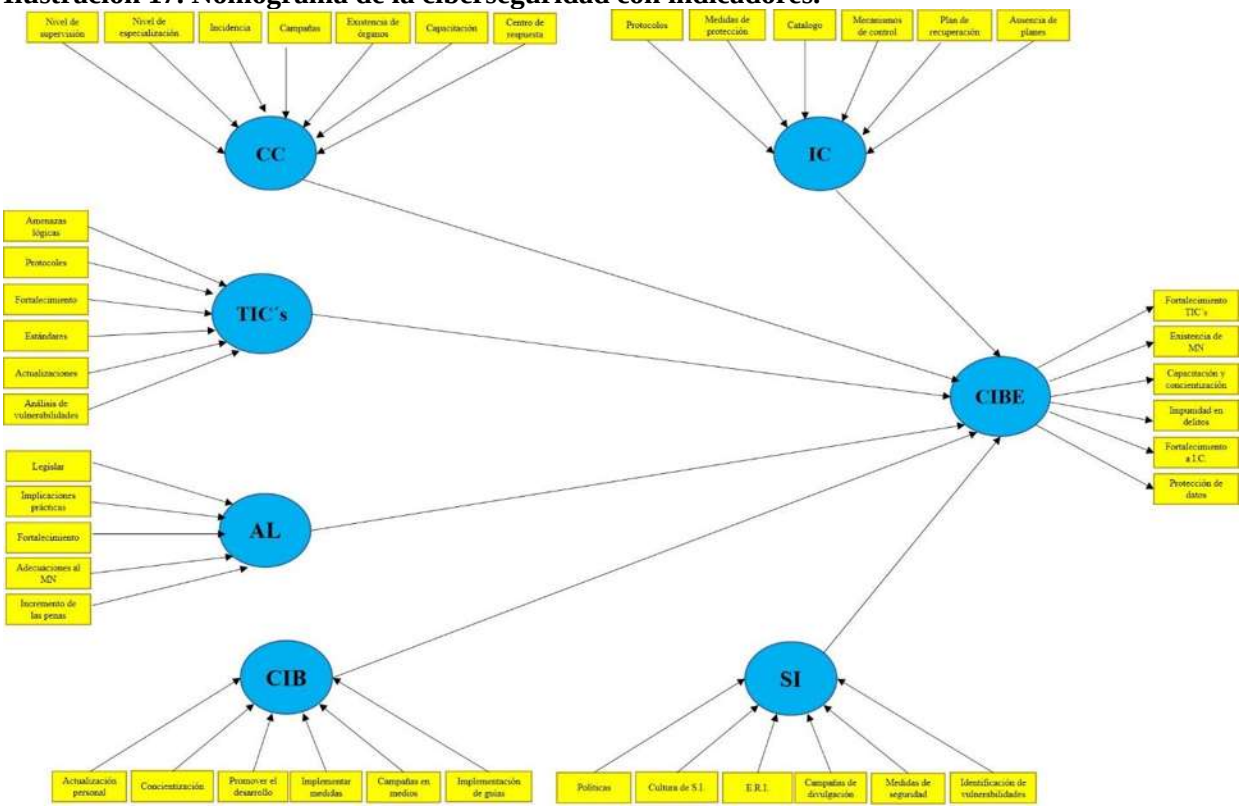
Tabla 10. Criterios para determinar el modelo de medida en una investigación.

Criterio	Modelos formativos	Modelos reflectivos
Relación entre los indicadores y el constructo.	Los indicadores forman o inciden en el constructo endógeno.	Los indicadores representan los efectos del constructo.
Intercambiabilidad de los indicadores	Cada indicador es una dimensión clave para la construcción del constructo.	Los indicadores son intercambiables o sustituibles entre sí.
Dirección de la flecha en el nomograma.	Flecha que apunta desde el indicador hacia el constructo.	Flecha que va desde el constructo hacia el indicador.
Teoría de la medida	Enfocada en la formación del constructo a través de los indicadores.	Enfocada en la relación causal del constructo con los indicadores.
Propósito de la investigación.	Explorar y construir el constructo a partir de los indicadores.	Validar y medir el constructo a través de los indicadores.

Fuente: Elaboración propia en Smart PLS con base en Hair, et al. (2017).

De acuerdo a los criterios identificados en la tabla y de acuerdo al tipo de investigación, el modelo a utilizar será con un enfoque formativo, que permitirá identificar y validar los conceptos relevantes que deben formar parte de la ciberseguridad. Esto permitiría avanzar en la construcción de una teoría o marco conceptual sólido para la ciberseguridad en el estado de Michoacán, a continuación se presenta el nomograma donde se observan las relaciones entre los indicadores y los constructos en el modelo de medida.

Ilustración 17. Nomograma de la ciberseguridad con indicadores.



Fuente: Elaboración propia en Smart PLS con base en Hair, et al. (2017).

4.7.3 Evaluación de resultados en modelos PLS-SEM (formativos)

Según Hair et al. (2017), para evaluar los resultados del modelado PLS-SEM en modelos formativos, es necesario realizar una evaluación inicial de la validez convergente del modelo de medida. Esto implica comparar la correlación formativa del constructo con una medida reflectiva del mismo. Este enfoque se utiliza para asegurarse de que cada indicador contribuya de manera similar al constructo o tenga el mismo efecto en la variable latente. Este paso también se conoce como análisis de redundancia, ya que su objetivo es distinguir entre lo que se mide en el modelo formativo y lo que se mide en el reflectivo, evitando así la duplicación de información.

En este primer paso, se examina la fuerza del coeficiente de camino (path) de cada uno de los constructos formativos en relación con sus respectivos indicadores formativos. En general, se espera que la fuerza del coeficiente de camino sea superior a 0.80. Sin embargo, el criterio mínimo para proceder con el análisis es que sea igual o superior a 0.7, lo que se traduce en un valor de R2 de 0.64 o al menos 0.05.

En la evaluación de los resultados de los modelos PLS-SEM, se lleva a cabo un segundo paso que implica examinar la colinealidad de los indicadores. Si se observa una correlación alta entre dos o más indicadores,

podría indicar la presencia de problemas de multicolinealidad en el modelo de medida. Una medida comúnmente utilizada para evaluar la colinealidad es el Factor de Inflación de la Varianza (VIF). La evaluación de la colinealidad entre los indicadores formativos de un constructo o variable latente implica asegurarse de que cada indicador esté midiendo una característica o aspecto diferente del constructo. Valores de VIF superiores a 5 indican un posible riesgo de colinealidad, lo que significa que los indicadores podrían estar capturando el mismo aspecto del constructo (Hair, et al., 2017).

Si el modelo experimenta dificultades de colinealidad debido a la fuerte correlación entre los indicadores de un mismo constructo, pero estos indicadores son esenciales desde el punto de vista teórico para la formación del constructo, se puede abordar el problema fusionando los elementos o empleando un modelo de constructos de orden superior o jerárquico de naturaleza formativa-formativa. Sin embargo, esta acción solo es factible si la teoría de medida lo permite y respalda dicha decisión (Hair, et al., 2017).

El tercer paso, según Hair, et al. (2017), implica evaluar la significancia y relevancia de cada indicador en la modelización. Esto implica analizar su contribución en la formación del constructo, lo cual se realiza mediante la evaluación de su peso. El peso de cada indicador representa su contribución relativa al constructo, por lo tanto, aquellos indicadores con pesos bajos serán menos significativos en la definición del constructo.

Para determinar si los indicadores formativos reflejan una parte fundamental del concepto, es necesario evaluar la significancia de los pesos externos en el modelo de medida, los cuales deben ser distintos de cero. Esta evaluación se lleva a cabo utilizando el proceso de bootstrap.

El método bootstrap permite determinar la significancia estadística de los indicadores mediante el cálculo de los valores t o los valores p teóricos. Como regla general, cuando el valor t es superior a 1.96, se puede interpretar que el coeficiente path es significativamente diferente de cero con un nivel de significancia del 5% para valores p α=0.05 en una distribución de dos colas.

4.7.3.1 Modelo estructural

Hair, et al. (2017), Indica que, al igual que en el modelo de medida externo, el primer paso para evaluar el modelo estructural implica analizar la colinealidad de manera independiente entre cada uno de los constructos predictores y las variables latentes dependientes. En general, si los valores de VIF son superiores a 5, esto indica problemas de colinealidad, por lo que se recomienda nuevamente fusionar los indicadores de los constructos o realizar un modelo de orden superior.

El segundo paso implica evaluar el coeficiente path, el cual representa las relaciones hipotéticas entre las variables latentes del modelo. Estos coeficientes suelen tener valores que van de +1 a -1, pudiendo ser

mayores o menores según el caso, lo que refleja relaciones positivas o negativas. Cuanto más se acerquen a 1, se considerarán relaciones fuertes, mientras que si se acercan a 0, indicarán relaciones débiles o poco significativas. Esta relación se evalúa nuevamente mediante la significancia estadística de los valores t y p utilizando el procedimiento de bootstrapping Hair, et al. (2017).

El tercer aspecto de análisis del modelo estructural, según Hair, et al. (2017), se centra en la evaluación del coeficiente de determinación R2, el cual mide los efectos conjuntos de las variables predictoras en la variable dependiente y, por lo tanto, la capacidad predictiva del modelo. Es importante destacar que el coeficiente de determinación R2 representa los efectos de todas las variables del modelo, desde las variables exógenas en el modelo de medida externo hasta las variables endógenas en el modelo estructural, y finalmente hacia la variable latente dependiente en su conjunto. Esto abarca tanto los valores reales como los valores de predicción estadística.

Dado la complejidad inherente de los modelos multivariantes, no existe una regla única para determinar los niveles aceptables del coeficiente de determinación. Sin embargo, se considera ampliamente aceptado que valores por encima de 0.2 son aceptables en teorías exploratorias o poco desarrolladas, mientras que en estudios confirmatorios se esperaría valores superiores a 0.5. Es importante destacar que estos valores pueden ser más altos si el modelo tiene un mayor número de relaciones o caminos path. Por esta razón, los investigadores suelen optar por modelos más parsimoniosos, con el objetivo de obtener una mayor explicación con un número mínimo de variables.

El cuarto paso de acuerdo con Hair, et al. (2017), implica la medición del efecto f2, que representa el impacto de cada constructo latente en el modelo y la variable de predicción al excluir cada uno de los constructos latentes en el cálculo. En otras palabras, el f2 muestra cuánto cambia el coeficiente de determinación R2 al omitir cada uno de los constructos endógenos. Si el valor del efecto f2 es menor a 0.02, indica que no hay un efecto significativo.

Si el valor del efecto f2 es mayor a 2, indica que el constructo latente tiene un efecto sustancial en la variable de predicción. Un valor de f2 mayor a 2 se considera una señal de un impacto significativo, lo que implica que el constructo latente tiene una influencia importante en la variable dependiente del modelo.

CAPÍTULO 5. RESULTADOS DE LA MODELIZACIÓN PLS-SEM Y ESTADÍSTICOS

En este capítulo, se presentan los resultados obtenidos en la investigación, los cuales se recopilaron mediante la aplicación de un instrumento de medición diseñado para evaluar los factores determinantes de la ciberseguridad. El objetivo principal de este apartado es presentar los hallazgos derivados de la metodología aplicada, así como proporcionar un análisis detallado de las variables objeto de estudio. Los resultados permitirán ofrecer una visión solida de los componentes que deben formar parte de la Ciberseguridad, una vez que hayan sido sometidos a un tratamiento estadísticamente y los cuales son presentados a continuación

5.1 Características de los encuestados

Se aplicaron 106 (ciento seis) cuestionarios a titulares y analistas de ciberseguridad pertenecientes a las 43 Unidades de Policía Cibernética pertenecientes a las Secretarías de Seguridad Pública, Fiscalías/Procuradurías de las 31 entidades federativas y la Ciudad de México y/o de la División General Científica de la Guardia Nacional, estas unidades forman parte del modelo homologado de Unidades de Policías Cibernéticas las cuales a su vez son miembros del Comité de ciberseguridad y que dentro de sus funciones desempeñan las siguientes actividades:

- Atención a las denuncias ciudadanas, fortaleciendo los canales de coordinación y las capacidades de investigación.
- Integración de estadísticas nacionales sobre ciberdelincuencia en nuestro país que permiten generar políticas públicas en materia de prevención.
- Coadyuvar con el Ministerio Público aportando pruebas fehacientes con tecnología e información para la integración de las carpetas de investigación.
- Realizar ciberpatrullajes en el ciberespacio para detectar y prevenir conductas de riesgo y delitos cibernéticos.
- Investigación y análisis de equipos informáticos, con el fin de reconstruir un evento donde pudo estar involucrado un dispositivo de cómputo a fin de generar los datos de prueba en investigaciones legales.
- Promover la cultura de la prevención de los delitos en los que se utilizan medios electrónicos para su comisión, así como la difusión del marco legal que sanciona los mismos y
- Generación y emisión de guías de buenas prácticas, cibertips, consejos y alertas cibernéticas.

5.2 Análisis descriptivo

En la presente investigación la variable dependiente denominada ciberseguridad está determinada por las variables independientes: Tecnologías de la información y comunicaciones, Aspectos legales,

Cibercultura, Cibercrimen, Infraestructuras críticas y Seguridad de la información, a continuación se presenta el análisis descriptivo por cada variable.

El primer paso para la evaluación de los resultados es el análisis y depuración de los datos obtenidos de la aplicación del instrumento de medición, cuyo resultado inicial consistió en 106 observaciones para 42 ítems, resultando que en las siguientes observaciones se encontraron respuestas atípicas en las que solo se tomó uno o dos valores de la escala en todo el cuestionario, convirtiéndose en respuestas binarias que impiden el tratamiento adecuado de los datos por las herramientas especializadas SPSS y Smart PLS.

De la revisión de los datos consistentes;

4, 9, 18, 19, 23, 24, 29, 31, 32, 33, 38, 39, 40, 44, 48, 49, 50, 51, 52, 54, 56, 62, 76, 81, 83, 87, 99, 103, 105 y 106.

Una vez identificadas y analizadas aquellas observaciones atípicas en las que se detectó que en una observación solo existía una y/o dos tipos de respuesta dentro de la escala de siete categorías; estas se descartaron como relevantes para el estudio pues se presume que no se analizó suficientemente los planteamientos realizados y se asignó una categoría dentro de la escala Likert sin necesariamente confirmar el grado de concordancia.

Se eliminan las observaciones mencionadas de la base de datos a analizar y dar el tratamiento matemático antes de ser cargadas dentro de los programas SPSS y Smart PLS-SEM, quedando 76 observaciones para los 42 ítems y teniendo 6 valores perdidos, los cuales fueron sustituidos por la media (valor promedio de los otros ítems de la escala).

5.2.1 Descriptivos de la variable dependiente, ciberseguridad

Los resultados de la medición de los datos obtenidos mediante el programa SPSS de la variable dependiente ciberseguridad incluye los valores obtenidos mediante una escala Likert y arrojados por cada una de las variables independientes, dimensiones e indicadores, los cuales se analizan a través de la información obtenida de la aplicación del instrumento de medición, conformado por los siguientes ítems:

Tabla 11. Dimensiones e indicadores variable dependiente: Ciberseguridad.

Dimensiones	Indicadores	Ítems
•Tecnologías de la información y comunicaciones. • Aspectos legales. • Cibercultura.	Fortalecimiento de las TIC´s.	La ciberseguridad es un reflejo del fortalecimiento de las Tecnologías de la información y comunicaciones.
	Marco normativo.	La ciberseguridad depende de la existencia de un marco normativo.
	Capacitación y concientización.	La ciberseguridad es un reflejo del número de personas capacitadas y concientizadas en una cultura digital y de seguridad de la información responsable.

• Cibercrimen. •Infraestructuras críticas. • Seguridad de la información	Incremento de la ciberseguridad. Protección de los datos Fortalecimiento de las infraestructuras críticas.	La menor impunidad de delitos cibernéticos es una reacción del incremento de la ciberseguridad. La protección de los datos y la información confidencial, son un reflejo del fortalecimiento de la ciberseguridad. La ciberseguridad depende del fortalecimiento de las infraestructuras críticas.

Fuente: Elaboración propia con la información obtenida del estudio de campo.

Una vez realizado el análisis descriptivo se obtienen los siguientes datos, los cuales se describen a continuación:

Tabla 12. Estadísticos descriptivos variable dependiente: Ciberseguridad.

Ciberseguridad	
N validos	76
Perdidos	0
Media	32.30
Error estándar de la media	.5694
Mediana	32.00
Moda	34.00
Desviación estándar	4.963
Varianza	24.64
Asimetría	-.247
Error estándar de asimetría	.276
Curtosis	.445
Error estándar de curtosis	.545
Rango	25.00
Mínimo	17.00
Máximo	42.00
Suma	2455

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

En la tabla se observan los valores obtenidos para las medidas de tendencia central y dispersión, correspondiente a la variable dependiente, donde se observa que la media tiene un valor de 32.30 puntos con relación al valor máximo posible para esta variable de 42, la mediana con un valor de 32 que presenta la distribución de los datos, la moda con un valor de 34 que representa el valor que se obtuvo con mayor frecuencia, por otra parte el valor de la desviación estándar 4.963 nos muestra una baja dispersión de los datos con respecto a la media, concentrando el 75% de datos a no más de una desviación estándar con respecto a la media de acuerdo con el teorema de Chebyshev (2008), este porcentaje indica la cantidad de entrevistados que se encuentran de acuerdo y bastante de acuerdo que los indicadores deben formar parte de la variable ciberseguridad.

Continuando con el análisis, el coeficiente de asimetría nos indica que tan alejados están los datos de la media, por lo que si $g1 < 0$ nos indica que se tiene una asimétrica negativa, lo que indica que la cola se

sesga a la izquierda, indicando que la mayoría de los datos se encuentran concentrados a la derecha, el coeficiente dio el siguiente resultado -.247. Por otra parte el coeficiente de curtosis nos indica que si Ck > 0, el grado de dispersión de los datos alrededor de la media, el valor obtenido es de .445, lo que nos indica que estamos ante una curtosis leptocúrtica, se observa un alto grado de concentración de los datos alrededor de las medidas de tendencia central.

En la siguiente tabla se muestra la tabla de distribución de frecuencias de la variable dependiente ciberseguridad.

Tabla 13. Distribución de frecuencias variable dependiente: Ciberseguridad.

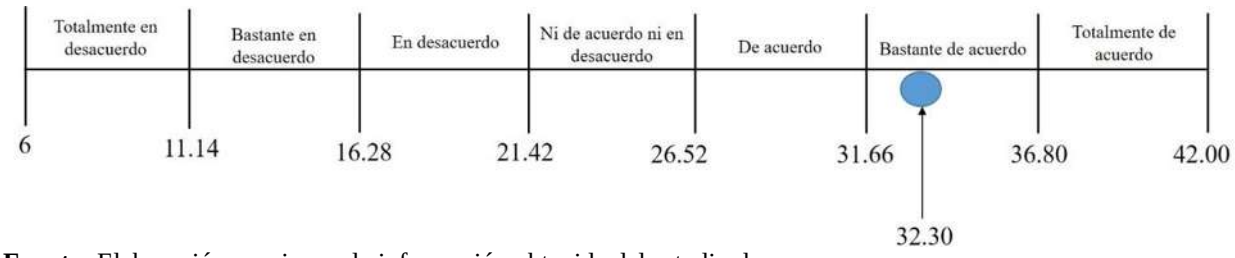
Ciberseguridad				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En desacuerdo	1	1.3	1.3	1.3
20	1	1.3	1.3	2.6
Ni de acuerdo ni en desacuerdo	2	2.6	2.6	5.3
25	1	1.3	1.3	6.6
26	2	2.6	2.6	9.2
De acuerdo	3	3.9	3.9	13.2
28	5	6.6	6.6	19.7
29	7	9.2	9.2	28.9
30	7	9.2	9.2	38.2
31	4	5.3	5.3	43.4
Bastante de acuerdo	8	10.5	10.5	53.9
33	3	3.9	3.9	57.9
34	9	11.8	11.8	69.7
35	3	3.9	3.9	73.7
36	5	6.6	6.6	80.3
Totalmente de acuerdo	3	3.9	3.9	84.2
38	4	5.3	5.3	89.5
39	1	1.3	1.3	90.8
40	3	3.9	3.9	94.7
41	1	1.3	1.3	96.1
42	3	3.9	3.9	100.0
Total	76	100.0	100.0	

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

La gráfica de distribución de frecuencias presenta la variable ciberseguridad de acuerdo al grado de concordancia o discordancia de los encuestados, donde se puede observar que a partir de la información que se obtiene, el valor mínimo arrojado es de 17 y el máximo puntaje obtenido es de 42, dando un rango de 25 puntos de distancia entre las respuestas, los valores que se encuentran por debajo del parámetro de acuerdo, equivalen a un 9.2% del total. La mayor parte de los datos, correspondiente al 90.8% de los encuestados se ubican en el área bastante de acuerdo, como se muestra en la tabla.

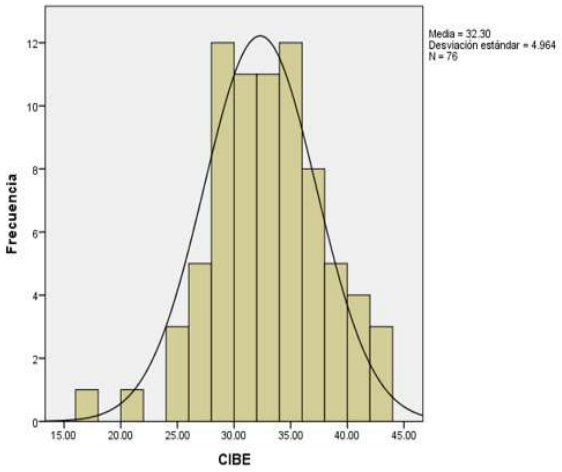
Se generó la gráfica de concordancia para evaluar el grado de acuerdo o desacuerdo por variable con respecto al total de encuestados, proporcionando una visión de la consistencia de las asignaciones, con una media de 32.30 que se encuentra en el rango de la escala bastante de acuerdo, como se muestra en la gráfica 10. Asimismo, se presenta el histograma de los datos de dicha variable, donde se aprecia un ligero sesgo izquierdo, lo que nos indica que algunos datos se encuentran ligeramente cargados a la derecha.

Gráfica 8. Concordancia de la variable dependiente: Ciberseguridad.



Fuente: Elaboración propia con la información obtenida del estudio de campo.

Gráfica 9. Histograma variable dependiente: Ciberseguridad.



Fuente: Imagen obtenida al procesar los datos en el software SPSS v.23.

5.2.2 Descriptivos de las variables independientes

Se realizó el análisis descriptivo de las variables independientes; Tecnologías de la información y comunicaciones, Aspectos legales, Cibercultura, Cibercrimen, Infraestructuras críticas y Seguridad de la información, las cuales se estudian para identificar cuál de ellas deben formar parte de la ciberseguridad. Los resultados de la medición de los datos obtenidos mediante el programa SPSS de dichas variables independientes; incluyen los valores obtenidos mediante una escala Likert y arrojados por cada una de las dimensiones e indicadores, los cuales se analizan a través de la información obtenida de la aplicación del instrumento de medición, a continuación se describe cada una de ellas.

5.2.2.1 Análisis de la variable independiente X1: TIC´s

En la siguiente tabla se muestran los indicadores, dimensiones e ítems que conforman dicha variable.

Tabla 14. Dimensiones e indicadores variable X1: TIC´s

Dimensiones	Indicadores	Ítems
		El incremento de amenazas lógicas y sistemas desactualizados provoca daños significativos a los equipos, infraestructura tecnológica e información.
		La ausencia de protocolos para abordar las amenazas físicas o lógicas, puede dificultar la recuperación después de un incidente de seguridad.
		El fortalecimiento a las tecnologías de la información y comunicaciones, podría incidir favorablemente en la disminución de vulnerabilidades que enfrentan los activos ante diversas amenazas.
		La implementación de medidas como estándares, guías de buenas prácticas y herramientas especializadas, resulta fundamentales en la identificación y mitigación de amenazas de los usuarios en su navegación. Implementar estrategias orientadas a promover y fomentar la actualización de hardware y software, reduce los riesgos asociados a la exposición de vulnerabilidades.
		Es importante que los creadores de tecnologías emergentes consideren de manera proactiva la seguridad, con el objetivo de prevenir y reducir el riesgo de vulnerabilidades y amenazas que puedan ser explotadas en su implementación.

Fuente: Elaboración propia con la información obtenida del estudio de campo.

Una vez realizado el análisis descriptivo se obtienen los siguientes datos, los cuales se describen a continuación:

Tabla 15. Estadísticos descriptivos variable X1: TIC´s.

Tecnologías de la información y comunicaciones	
N validos	76
Perdidos	0
Media	36.30
Error estándar de la media	.587
Mediana	37.00
Moda	42
Desviación estándar	5.122
Varianza	26.241
Asimetría	-1.037
Error estándar de asimetría	.276
Curtosis	1.396
Error estándar de curtosis	.545
Rango	25
Mínimo	17
Máximo	42
Suma	2759

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

En la tabla se observan los valores obtenidos de las medidas de tendencia central y dispersión, correspondientes a la variable independiente X1, donde se observa que la media tiene un valor de 36.30 puntos con relación al valor máximo posible para esta variable de 42, la mediana con un valor de 37 que presenta la distribución de los datos, la moda con un valor de 42 que representa el valor que se obtuvo con mayor frecuencia, por otra parte el valor de la desviación estándar 5.122 nos muestra una baja dispersión de los datos con respecto a la media, concentrando el 75% de datos a no más de una desviación estándar con respecto a la media de acuerdo con el teorema de Chebyshev, este porcentaje indica la cantidad de entrevistados que se encuentran de acuerdo, bastante de acuerdo y/o totalmente de acuerdo que los indicadores deben formar parte de la variable Tecnologías de la información y comunicaciones.

Continuando con el análisis el coeficiente de asimetría nos indica que tan alejados están los datos de la media, por lo que si $g1 < 0$ nos indica que se tiene una asimétrica negativa, lo que indica que la cola se sesga a la izquierda, indicando que la mayoría de los datos se encuentran concentrados a la derecha ya que el coeficiente dio el siguiente resultado -1.037. Por otra parte el coeficiente de curtosis nos indica que si $Ck > 0$, el grado de dispersión de los datos alrededor de la media, el valor obtenido es de 1.396, lo que nos indica que estamos ante una curtosis leptocúrtica lo que representa un alto grado de concentración de los datos alrededor de las medidas de tendencia central.

En la siguiente tabla se muestra la tabla de distribución de frecuencias de la variable independiente X1.

Tabla 16. Distribución de frecuencias variable X1: TIC´s.

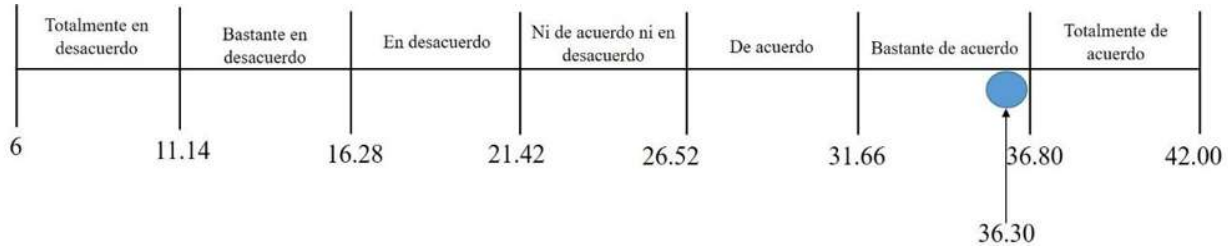
Tecnologías de la información y comunicaciones				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En desacuerdo	1	1.3	1.3	1.3
24	1	1.3	1.3	2.6
27	1	1.3	1.3	3.9
28	2	2.6	2.6	6.6
29	2	2.6	2.6	9.2
30	6	7.9	7.9	17.1
Bastante de acuerdo	1	1.3	1.3	18.4
32	3	3.9	3.9	22.4
33	3	3.9	3.9	26.3
34	4	5.3	5.3	31.6
35	6	7.9	7.9	39.5
36	5	6.6	6.6	46.1
Totalmente de acuerdo	4	5.3	5.3	51.3
38	6	7.9	7.9	59.2
39	6	7.9	7.9	67.1
40	4	5.3	5.3	72.4
41	7	9.2	9.2	81.6
42	14	18.4	18.4	100.0
Total	76	100.0	100.0	

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

La gráfica de frecuencias presenta la variable tecnologías de la información y comunicaciones de acuerdo al grado de concordancia o discordancia de los encuestados, donde se puede observar que a partir de la información que se obtiene, el valor mínimo arrojado es de 17 y el máximo puntaje obtenido es de 42, dando un rango de 25 puntos de distancia entre las respuestas, los valores que se encuentran por debajo del parámetro de acuerdo, equivalen a un 3.9% del total. La mayor parte de los datos, correspondiente al 96.1% de los encuestados se ubican en el área entre de acuerdo y totalmente de acuerdo, como se muestra en la tabla.

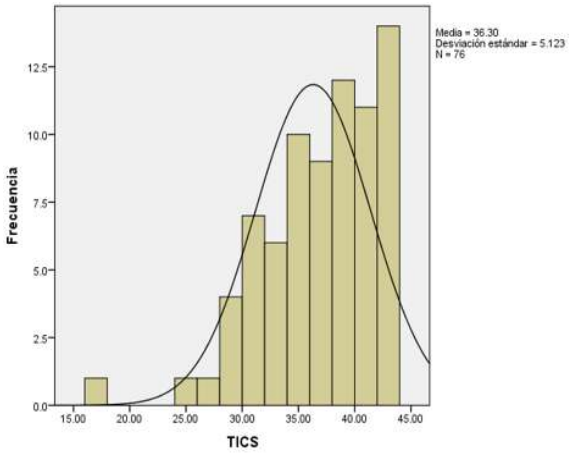
Adicionalmente, se generó la gráfica de concordancia que muestra el grado de acuerdo o desacuerdo por variable con respecto al total de encuestados, permitiendo evaluar la consistencia de las asignaciones, con una media de 36.30 la cual se encuentra en el rango de escala bastante de acuerdo como se modela en la gráfica 12. Asimismo, se presenta el histograma de dicha variable, donde se aprecia un ligero sesgo izquierdo, lo que nos indica que algunos datos se encuentran ligeramente cargados a la derecha.

Gráfica 10. Concordancia de la variable independiente X1: TIC´s



Fuente: Elaboración propia con la información obtenida del estudio de campo.

Gráfica 11. Histograma variable independiente X1: TIC´s.



Fuente: Imagen obtenida al procesar los datos en el software SPSS v.23.

5.2.2.2 Análisis de la variable independiente X2: Aspectos legales

En la siguiente tabla se muestran los indicadores, dimensiones e ítems que conforman dicha variable.

Tabla 17. Dimensiones e indicadores variable X2: Aspectos legales.

Dimensiones	Indicadores	Ítems
Legislación nacional, internacional y normativa.	Frecuencia y calidad de las actualizaciones legales.	Legislar sobre el diseño, fabricación y uso de las tecnologías de la información y comunicaciones, contribuiría a asegurar que estas tecnologías sean seguras y confiables.
		El desconocimiento de las implicaciones prácticas, técnicas y legales en el desarrollo y creación de tecnologías de la información y comunicaciones, conduce a la falta de legislación en este campo.
	Legislación en materia de cooperación internacional.	El fortalecimiento al marco normativo por parte de las autoridades, permitiría contar con mayores capacidades en la investigación, persecución y sanción de los delitos informáticos.
		La adecuación de la legislación local a los marcos y tratados internacionales podrá contribuir a la disminución de incidentes de ciberseguridad.
		Armonizar, tipificar e incrementar las penas con respecto a los delitos cometidos por medio de las tecnologías de la información y comunicaciones, contribuirá a disminuir los riegos de los usuarios.

Fuente: Elaboración propia con la información obtenida del estudio de campo.

Una vez realizado el análisis descriptivo se obtienen los siguientes datos, los cuales se describen a continuación:

Tabla 18. Estadísticos descriptivos variable X2: Aspectos legales

	Aspectos legales
N validos	76
Perdidos	0
Media	29.47
Error estándar de la media	.499
Mediana	30.00
Moda	34.00
Desviación estándar	4.358
Varianza	18.99
Asimetría	-.690
Error estándar de asimetría	.276
Curtosis	-.103
Error estándar de curtosis	.545
Rango	18.00
Mínimo	17.00
Máximo	35.00
Suma	2240

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

En la tabla se observan los valores obtenidos para las medidas de tendencia central y dispersión, correspondientes a la variable independiente X2, donde se observa que la media tiene un valor de 29.47 puntos con relación al valor máximo posible para esta variable de 35, la mediana con un valor de 30 que presenta la distribución de los datos, la moda con un valor de 34 que representa el valor que se obtuvo con mayor frecuencia, por otra parte el valor de la desviación estándar 4.358 nos muestra una baja dispersión de los datos con respecto a la media, concentrando el 75% de datos a no más de una desviación

estándar con respecto a la media de acuerdo con el teorema de Chebyshev, este porcentaje indica la cantidad de entrevistados que se encuentran de acuerdo y bastante de acuerdo que los indicadores deben formar parte de la variable aspectos legales.

Continuando con el análisis el coeficiente de asimetría nos indica que tan alejados están los datos de la media, por lo que si g1 < 0 nos indica que se tiene una asimétrica negativa, lo que indica que la cola se sesga a la izquierda, indicando que la mayoría de los datos se encuentran concentrados a la derecha ya que el coeficiente dio el siguiente resultado -.690. Por otra parte el coeficiente de curtosis nos indica que si Ck < 0, el grado de dispersión de los datos alrededor de la media, el valor obtenido es de -.103, lo que nos indica que estamos ante una curtosis platicúrtica lo que nos indica que los datos están poco concentrados alrededor de las medidas de tendencia central.

En la siguiente tabla se muestra la tabla de distribución de frecuencias de la variable aspectos legales.

Tabla 19. Distribución de frecuencias variable X2: Aspectos legales.

Aspectos legales				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En desacuerdo	1	1.3	1.3	1.3
Ni de acuerdo ni en desacuerdo	1	1.3	1.3	2.6
21	1	1.3	1.3	3.9
De acuerdo	6	7.9	7.9	11.8
24	4	5.3	5.3	17.1
25	3	3.9	3.9	21.1
26	3	3.9	3.9	25.0
Bastante de acuerdo	4	5.3	5.3	30.3
28	3	3.9	3.9	34.20
29	7	9.2	9.2	43.4
30	9	11.8	11.8	55.3
Totalmente de acuerdo	5	6.6	6.6	61.8
32	7	9.2	9.2	71.1
33	3	3.9	3.9	75.0
34	11	14.5	14.5	89.5
35	8	10.5	10.5	100.0
Total	76	100	100	

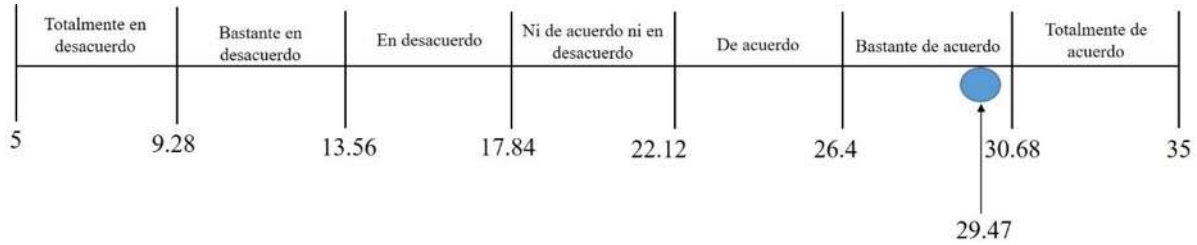
Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

La gráfica de frecuencias presenta la variable aspectos legales a partir de la información que se obtiene, el valor mínimo arrojado es de 17 y el máximo puntaje obtenido es de 35, dando un rango de 18 puntos de distancia entre las respuestas, los valores que se encuentran por debajo del parámetro de acuerdo, equivalen a un 3.9% del total. La mayor parte de los datos, correspondiente al 96.1% de los encuestados se ubican en el área bastante de acuerdo, como se muestra en la tabla.

De igual manera se generó la gráfica de concordancia que muestra el grado de acuerdo o desacuerdo por variable con respecto al total de encuestados, permitiendo evaluar la consistencia de las asignaciones y el valor de la media de 29.47 se encuentra en el rango de escala bastante de acuerdo como se muestra en la

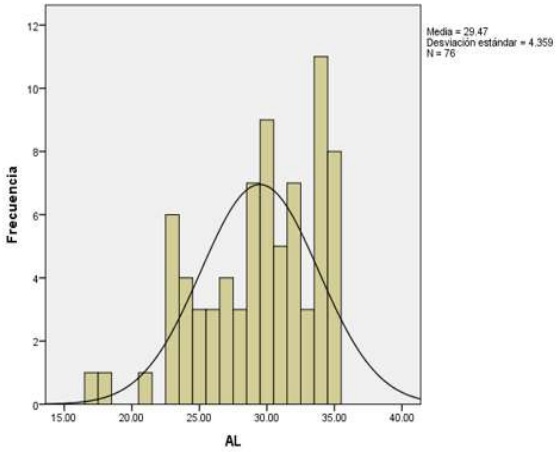
gráfica 14. Asimismo, se presenta el histograma de los datos de dicha variable, donde se aprecia un ligero sesgo izquierdo, lo que nos indica que algunos datos se encuentran ligeramente cargados a la derecha.

Gráfica 12. Concordancia de la variable independiente X2: Aspectos legales.



Fuente: Elaboración propia con la información obtenida del estudio de campo.

Gráfica 13. Histograma variable X2: Aspectos legales.



Fuente: Imagen obtenida al procesar los datos en el software SPSS v.23.

5.2.2.3 Análisis de la variable independiente X3: Cibercultura

En la siguiente tabla se muestran los indicadores, dimensiones e ítems que conforman dicha variable.

Tabla 20. Dimensiones e indicadores de la variable independiente X3: Cibercultura

Dimensiones	Indicadores	Ítems
Conocimiento Aprendizaje	Nivel de actualización.	La actualización personal sobre temas de seguridad en internet es básico para usarlo sin exponerse a riesgos.
	Nivel de conciencia.	Para evitar ser víctimas de los riesgos en el ciberespacio, es importante la concientización sobre las amenazas en línea y tomar medidas proactivas para protegerse.
	Nivel de conocimiento. Organizaciones públicas y privadas.	Para promover el desarrollo de una cultura digital, es importante considerar la creación de organizaciones, tanto públicas como privadas, que contribuyan a este objetivo.
	Campañas de concientización.	Es esencial implementar medidas que fomentan una comprensión profunda por parte de los usuarios, para evitar riesgos y vulnerabilidades al navegar en línea.

Guías de buenas prácticas.	Las campañas en diversos medios de comunicación para concientizar sobre la creación de una cultura digital, incrementaría la seguridad al momento de navegar.
	El desarrollo e implementación de guías de buenas prácticas para la navegación de los usuarios en el ciberespacio puede ser muy beneficioso y es un aspecto importante de la seguridad en línea.

Fuente: Elaboración propia con la información obtenida del estudio de campo.

Se realizó el análisis descriptivo obteniéndose los siguientes datos, los cuales se describen a continuación:

Tabla 21. Estadísticos descriptivos de la variable independiente X3: Cibercultura

	Cibercultura
N validos	76
Perdidos	0
Media	36.77
Error estándar de la media	.530
Mediana	38.00
Moda	42.00
Desviación estándar	4.626
Varianza	21.403
Asimetría	-.599
Error estándar de asimetría	.276
Curtosis	-.680
Error estándar de curtosis	.545
Rango	17.00
Mínimo	25.00
Máximo	42.00
Suma	2795

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

En la tabla se observan los valores obtenidos de las medidas de tendencia central y dispersión, correspondientes a la variable independiente X3, donde se observa que la media tiene un valor de 36.77 puntos con relación al valor máximo posible para esta variable de 42, la mediana con un valor de 38 que presenta la distribución de los datos, la moda con un valor de 42 que representa el valor que se obtuvo con mayor frecuencia, por otra parte el valor de la desviación estándar 4.626 nos muestra una baja dispersión de los datos con respecto a la media, concentrando el 75% de datos a no más de una desviación estándar con respecto a la media de acuerdo con el teorema de Chebyshev, este porcentaje indica la cantidad de entrevistados que se encuentran de acuerdo, bastante de acuerdo y/o totalmente de acuerdo que los indicadores deben formar parte de la variable cibercultura.

Continuando con el análisis el coeficiente de asimetría nos indica que tan alejados están los datos de la media, por lo que si $g1 < 0$ nos indica que se tiene una asimétrica negativa, lo que indica que la cola se sesga a la izquierda, indicando que la mayoría de los datos se encuentran concentrados a la derecha ya que el coeficiente dio el siguiente resultado -.599 Por otra parte el coeficiente de curtosis nos indica que si Ck

< 0, el grado de dispersión de los datos alrededor de la media, el valor obtenido es de -.680, lo que nos indica que estamos ante una curtosis platicúrtica lo que representa que no están estrechamente agrupados alrededor de las medidas de tendencia central.

Tabla 22. Distribución de frecuencias variable independiente X3: Cibercultura.

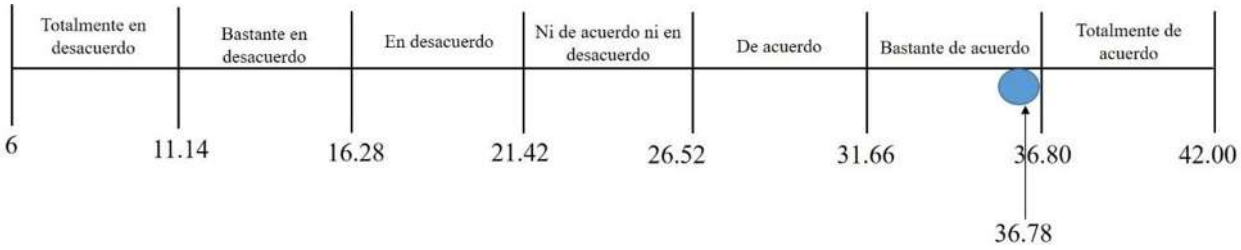
Cibercultura				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Ni de acuerdo ni en desacuerdo	1	1.3	1.3	1.3
26	1	1.3	1.3	2.6
28	1	1.3	1.3	3.9
29	1	1.3	1.3	5.3
30	7	9.2	9.2	14.5
De acuerdo	3	3.9	3.9	18.4
Bastante de acuerdo	3	3.9	3.9	22.4
33	2	2.6	2.6	25.0
34	5	6.6	6.6	31.6
35	4	5.3	5.3	36.8
36	3	3.9	3.9	40.8
Totalmente de acuerdo	4	5.3	5.3	46.1
38	9	11.8	11.8	57.9
39	4	5.3	5.3	63.2
40	7	9.2	9.2	72.4
41	4	5.3	5.3	77.6
42	17	22.4	22.4	100.0
Total	76	100	100	

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

La gráfica de frecuencias presenta la variable cibercultura de acuerdo al grado de concordancia o discordancia de los encuestados, donde se puede observar que a partir de la información que se obtiene, el valor mínimo arrojado es de 6 y el máximo puntaje obtenido es de 42, dando un rango de 36 puntos de distancia entre las respuestas, los valores que se encuentran por debajo del parámetro de acuerdo, equivalen a un 14.5% del total. La mayor parte de los datos, correspondiente al 85.5% de los encuestados se ubican en el área bastante de acuerdo, como se muestra en la tabla.

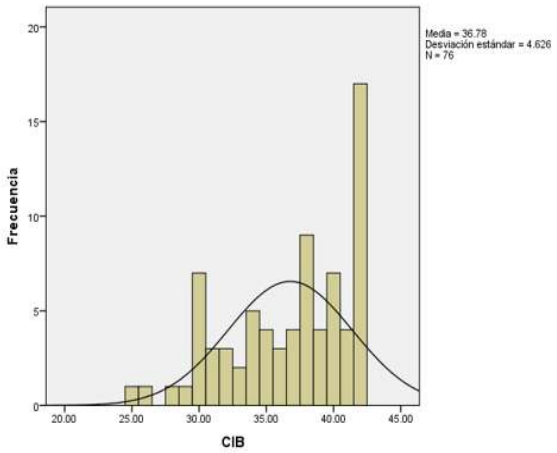
De igual manera se generó la gráfica de concordancia que muestra el grado de acuerdo o desacuerdo por variable con respecto al total de encuestados, permitiendo evaluar la consistencia de las asignaciones y el valor de la media de 36.78 se encuentra en el rango de la escala en bastante de acuerdo como se muestra en la gráfica 16. Asimismo, se presenta el histograma de los datos de dicha variable, donde se aprecia un ligero sesgo izquierdo, lo que nos indica que algunos datos se encuentran ligeramente cargados a la derecha.

Gráfica 14. Concordancia de la variable independiente X3: Cibercultura



Fuente: Elaboración propia con la información obtenida del estudio de campo.

Gráfica 15. Histograma de la variable independiente X3: Cibercultura



Fuente: Imagen obtenida al procesar los datos en el software SPSS v.23.

5.2.2.4 Análisis de la variable independiente X4: Cibercrimen

En la siguiente tabla se muestran los indicadores, dimensiones e ítems que conforman dicha variable.

Tabla 23. Dimensiones e indicadores de la variable independiente X4: Cibercrimen

Dimensiones	Indicadores	Ítems
Prevención Investigación Persecución Judicialización	Nivel de supervisión	La ausencia de una debida supervisión por parte de los padres de familia, propicia la realización de variadas acciones de riesgo durante la navegación en línea.
	Nivel de especialización	La falta de especialización técnica y capacitación de los investigadores encargados de perseguir delitos cibernéticos puede llevar a que los delincuentes queden impunes.
	Incidencias o casos registrados	El número de denuncias o incidentes cibernéticos, son un reflejo del estado de cibercriminalidad en Michoacán.
	Campañas	La ausencia de campañas de sensibilización sobre los riesgos en la navegación de los usuarios contribuye al aumento de la cibercriminalidad.
	Existencia de órganos especializados	La creación de un órgano judicial especializado en delitos cibernéticos, podría ser una estrategia efectiva para reducir la incidencia de la cibercriminalidad.
	Capacitaciones	
	Existencia o creación de centros de respuesta	

	La formación y capacitación de los órganos jurisdiccionales especializados en delitos cibernéticos, fortalece la capacidad de investigación y reduce la incidencia delictiva.
	La creación de un centro de contención, respuesta e investigación especializada de delitos cibernéticos ayudaría a disminuir la cibercriminalidad.

Fuente: Elaboración propia con la información obtenida del estudio de campo.

Se realizó el análisis descriptivo obteniéndose los siguientes datos, los cuales se describen a continuación:

Tabla 24. Estadísticos descriptivos de la variable independiente X4: Cibercrimen.

	Cibercrimen
N validos	76
Perdidos	0
Media	40.06
Error estándar de la media	.636
Mediana	40.50
Moda	42.00
Desviación estándar	5.552
Varianza	30.836
Asimetría	-.312
Error estándar de asimetría	.276
Curtosis	-.498
Error estándar de curtosis	.545
Rango	23.00
Mínimo	26.00
Máximo	49.00
Suma	3045

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

En la tabla se observan los valores obtenidos de las medidas de tendencia central y dispersión, correspondientes a la variable independiente X4, donde se observa que la media tiene un valor de 40.06 puntos con relación al valor máximo posible para esta variable de 49, la mediana con un valor de 40.50 que presenta la distribución de los datos, la moda con un valor de 42 que representa el valor que se obtuvo con mayor frecuencia, por otra parte el valor de la desviación estándar 5.552 nos muestra una baja dispersión de los datos con respecto a la media, concentrando el 75% de datos a no más de una desviación estándar con respecto a la media de acuerdo con el teorema de Chebyshev, este porcentaje indica la cantidad de entrevistados que se encuentran de acuerdo, bastante de acuerdo y/o totalmente de acuerdo que los indicadores deben formar parte de la variable Tecnologías de la información y comunicaciones.

Continuando con el análisis el coeficiente de asimetría nos indica que tan alejados están los datos de la media, por lo que si $g1 < 0$ nos indica que se tiene una asimétrica negativa, lo que indica que la cola se sesga a la izquierda, indicando que la mayoría de los datos se encuentran concentrados a la derecha ya que el coeficiente dio el siguiente resultado -.312 Por otra parte el coeficiente de curtosis nos indica que si $Ck<0$, el grado de dispersión de los datos alrededor de la media, el valor obtenido es de -.498, lo que nos

indica que estamos ante una curtosis platicúrtica los datos no muestran una concentración significativa alrededor de las medidas de tendencia central.

Tabla 25. Distribución de frecuencias de la variable independiente X4: Cibercrimen

Cibercrimen				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Ni de acuerdo ni en desacuerdo	1	1.3	1.3	1.3
28	2	2.6	2.6	3.9
30	1	1.3	1.3	5.3
De acuerdo	1	1.3	1.3	6.6
33	5	6.6	6.6	13.2
34	3	3.9	3.9	17.1
35	5	6.6	6.6	23.7
36	4	5.3	5.3	28.9
Bastante de acuerdo	2	2.6	2.6	31.6
38	6	7.9	7.9	39.5
39	2	2.6	2.6	42.1
40	6	7.9	7.9	50.0
41	5	6.6	6.6	56.6
42	8	10.5	10.5	67.1
Totalmente de acuerdo	3	3.9	3.9	71.1
44	3	3.9	3.9	75.0
45	3	3.9	3.9	78.9
46	5	6.6	6.6	85.5
47	4	5.3	5.3	90.8
48	3	3.9	3.9	94.7
49	4	5.3	5.3	100.0
Total	76	100	100	

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

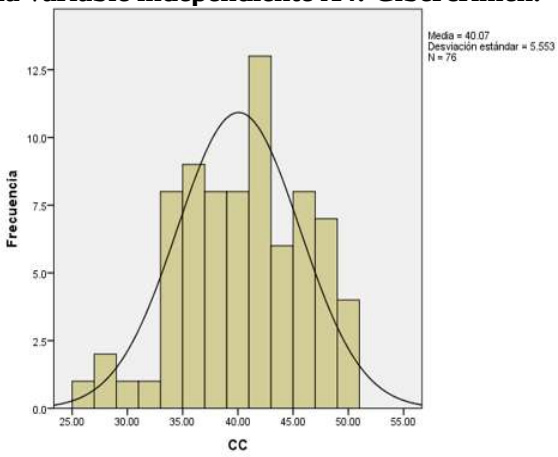
La gráfica de frecuencias presenta la variable cibercrimen de acuerdo al grado de concordancia o discordancia de los encuestados, donde se puede observar que a partir de la información que se obtiene, el valor mínimo arrojado es de 14 y el máximo puntaje obtenido es de 49, dando un rango de 35 puntos de distancia entre las respuestas, los valores que se encuentran por debajo del parámetro de acuerdo, equivalen a un 5.3% del total. La mayor parte de los datos, correspondiente al 94.7% de los encuestados se ubican en el área bastante de acuerdo, como se muestra en la tabla.

De igual manera se generó la gráfica de concordancia que muestra el grado de acuerdo o desacuerdo por variable con respecto al total de encuestados, permitiendo evaluar la consistencia de las asignaciones, el valor de la media de 40.07 se encuentra en el rango de la escala bastante de acuerdo como se muestra en la gráfica 18. Asimismo, se presenta el histograma de los datos de dicha variable, donde se aprecia un ligero sesgo izquierdo, lo que nos indica que algunos datos se encuentran ligeramente cargados a la derecha.

Gráfica 16. Concordancia de la variable independiente X4: Cibercrimen.

Fuente: Elaboración propia con la información obtenida del estudio de campo.

Gráfica 17. Histograma de la variable independiente X4: Cibercrimen.



Fuente: Imagen obtenida al procesar los datos en el software SPSS v.23.

5.2.2.5 Análisis de la variable independiente X5: Infraestructuras críticas

En la siguiente tabla se muestran los indicadores, dimensiones e ítems que conforman dicha variable.

Tabla 26. Dimensiones e indicadores de la variable independiente X5: Infraestructuras críticas.

Dimensiones	Indicadores	Ítems
Esquema nacional	Catálogo Mecanismos de control y gestión Planes de recuperación	Es importante establecer protocolos de actuación para las infraestructuras críticas, a fin de minimizar los riesgos y daños potenciales causados por eventos de sabotaje o ataques cibernéticos. La ausencia de medidas adecuadas de protección lógica y física para las infraestructuras críticas, podría resultar en vulnerabilidades de seguridad para Michoacán. La ausencia de un catálogo de las infraestructuras críticas dificulta la tarea de identificación y protección frente a eventuales amenazas de origen cibernético. La implementación de mecanismos para el control y gestión de las infraestructuras críticas por parte del Estado es esencial. Para proteger una infraestructura crítica ante un ataque cibernético es necesario disponer de un plan de recuperación de incidentes efectivo y adecuado.

	La creación de un centro de contención, respuesta e investigación especializada de delitos cibernéticos ayudaría a disminuir la cibercriminalidad.

Fuente: Elaboración propia con la información obtenida del estudio de campo.

Se realizó el análisis descriptivo obteniéndose los siguientes datos, los cuales se describen a continuación:

Tabla 27. Estadísticos descriptivos de la variable independiente X5: Infraestructuras críticas.

Infraestructuras críticas	
N validos	76
Perdidos	0
Media	35.94
Error estándar de la media	.6049
Mediana	37.00
Moda	42.00
Desviación estándar	5.273
Varianza	27.81
Asimetría	-.625
Error estándar de asimetría	.276
Curtosis	-.456
Error estándar de curtosis	.545
Rango	21.00
Mínimo	21.00
Máximo	42.00
Suma	2732

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

En la tabla se observan los valores obtenidos de las medidas de tendencia central y dispersión, correspondientes a la variable independiente X5, donde se observa que la media tiene un valor de 35.94 puntos con relación al valor máximo posible para esta variable de 42, la mediana con un valor de 37 que presenta la distribución de los datos, la moda con un valor de 42 que representa el valor que se obtuvo con mayor frecuencia, por otra parte el valor de la desviación estándar 5.273 nos muestra una baja dispersión de los datos con respecto a la media, concentrando el 75% de datos a no más de una desviación estándar con respecto a la media de acuerdo con el Teorema de Chebyshev, este porcentaje indica la cantidad de entrevistados que se encuentran de acuerdo, bastante de acuerdo y/o totalmente de acuerdo que los indicadores deben formar parte de la variable infraestructuras críticas.

Continuando con el análisis el coeficiente de asimetría nos indica que tan alejados están los datos de la media, por lo que si $g1 < 0$ nos indica que se tiene una asimétrica negativa, lo que indica que la cola se sesga a la izquierda, indicando que la mayoría de los datos se encuentran concentrados a la derecha ya que el coeficiente dio el siguiente resultado -.625. Por otra parte el coeficiente de curtosis nos indica que si $Ck < 0$, el grado de dispersión de los datos alrededor de la media, el valor obtenido es de -.456, lo que nos

indica que estamos ante una curtosis platicúrtica observándose que los datos están poco concentrados alrededor de las medidas de tendencia central.

Tabla 28. Distribución de frecuencias variable independiente X5: Infraestructuras críticas.

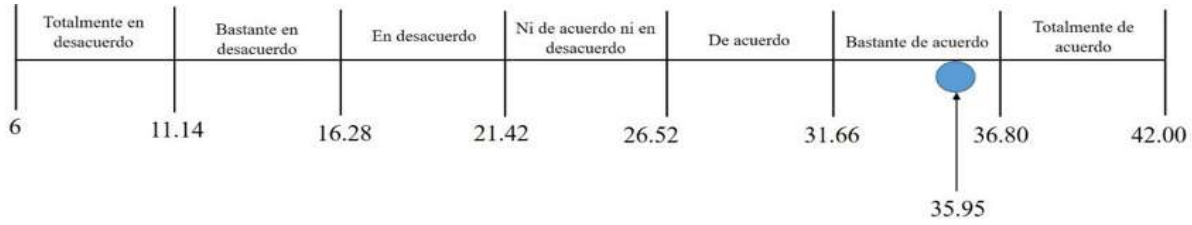
Infraestructuras críticas				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Ni de acuerdo ni en desacuerdo	1	1.3	1.3	1.3
24	1	1.3	1.3	2.6
De acuerdo	3	3.9	3.9	6.6
28	4	5.3	5.3	11.8
29	1	1.3	1.3	13.2
30	5	6.6	6.6	19.7
31	3	3.9	3.9	23.7
Bastante de acuerdo	4	5.3	5.3	28.9
33	1	1.3	1.3	30.3
34	5	6.6	6.6	36.8
35	1	1.3	1.3	38.2
36	8	10.5	10.5	48.7
Totalmente de acuerdo	4	5.3	5.3	53.9
38	6	7.9	7.9	61.8
39	4	5.3	5.3	67.1
40	5	6.6	6.6	73.7
41	4	5.3	5.3	78.9
42	16	21.1	21.1	100.0
Total	76	100	100	

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

La gráfica de frecuencias presenta la información obtenida de la variable infraestructuras críticas de acuerdo al grado de concordancia o discordancia de los encuestados, donde se puede observar que a partir de la información, el valor mínimo arrojado es de 21 y el máximo puntaje obtenido es de 42, dando un rango de 21 puntos de distancia entre las respuestas, los valores que se encuentran por debajo del parámetro de acuerdo, equivalen a un 2.6% del total. La mayor parte de los datos, correspondiente al 97.4% de los encuestados se ubican en el área entre de acuerdo y totalmente de acuerdo, como se muestra en la tabla.

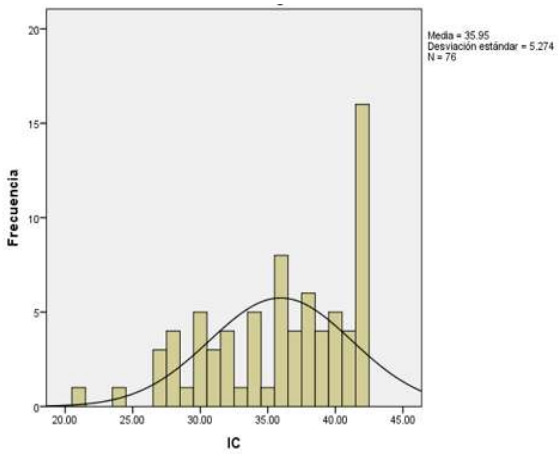
De igual manera se generó la gráfica de concordancia que muestra el grado de acuerdo o desacuerdo por variable con respecto al total de encuestados, permitiendo evaluar la consistencia de las asignaciones y el valor de la media de 35.71 que se encuentra en el rango de la escala bastante de acuerdo como se muestra en la gráfica 10. Asimismo, se presenta el histograma de los datos de dicha variable, donde se aprecia un ligero sesgo izquierdo, lo que nos indica que algunos datos se encuentran ligeramente cargados a la derecha.

Gráfica 18. Concordancia de la variable independiente X5: Infraestructuras críticas.



Fuente: Elaboración propia con la información obtenida del estudio de campo.

Gráfica 19. Histograma de la variable independiente X5: Infraestructuras críticas.



Fuente: Imagen obtenida al procesar los datos en el software SPSS v.23.

5.2.2.6 Análisis de la variable independiente X6: Seguridad de la información

En la siguiente tabla se muestran los indicadores, dimensiones e ítems que conforman dicha variable.

Tabla 29. Dimensiones e indicadores de la variable independiente X6: Seguridad de la información.

Dimensiones	Indicadores	Ítems
Educación proactiva Educación reactiva	Políticas	La generación de políticas que promuevan el aprendizaje significativo entre los usuarios y operadores de sistemas es esencial para la seguridad de la información.
	Cultura de seguridad de la información	Es importante fomentar la cultura de seguridad de la información por parte de los usuarios de sistemas informáticos, aplicativos y/o plataformas digitales.
	Equipos de respuesta a incidentes	Para asegurar la recuperación de la operación en seguridad de la información, es importante contar con equipos de respuesta a incidentes especializados.
	Campañas de divulgación	Los procesos de divulgación en materia de Seguridad de la Información son clave para fortalecer la seguridad de la información en una organización.
	Medidas de seguridad y protección	La implementación de medidas de seguridad y protección de datos es fundamental para evitar la exposición de privacidad y el uso indebido de información.
	Identificación de vulnerabilidades	Las auditorías a la infraestructura tecnológica y protocolos mejora la seguridad de la información.

Fuente: Elaboración propia con la información obtenida del estudio de campo.

Se realizó el análisis descriptivo obteniéndose los siguientes datos, los cuales se describen a continuación:

Tabla 30. Estadísticos descriptivos de la variable independiente X6: Seguridad de la información.

Seguridad de la información	
N validos	76
Perdidos	0
Media	36.06
Error estándar de la media	.5384
|Mediana	37.00
Moda	42.00
Desviación estándar	4.694
Varianza	22.03
Asimetría	-.303
Error estándar de asimetría	.276
Curtosis	-1.100
Error estándar de curtosis	.545
Rango	17.00
Mínimo	25.00
Máximo	42.00
Suma	2741

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

En la tabla se observan los valores obtenidos de las medidas de tendencia central y dispersión, correspondientes a la variable independiente X6, donde se observa que la media tiene un valor de 36.06 puntos con relación al valor máximo posible para esta variable de 42, la mediana con un valor de 37 que presenta la distribución de los datos, la moda con un valor de 42 que representa el valor que se obtuvo con mayor frecuencia, por otra parte el valor de la desviación estándar 4.694 nos muestra una baja dispersión de los datos con respecto a la media, concentrando el 75% de datos a no más de una desviación estándar con respecto a la media de acuerdo con el teorema de Chebyshev, este porcentaje indica la cantidad de entrevistados que se encuentran de acuerdo, bastante de acuerdo y/o totalmente de acuerdo que los indicadores deben formar parte de la variable seguridad de la información.

Continuando con el análisis el coeficiente de asimetría nos indica que tan alejados están los datos de la media, por lo que si $g1 < 0$ nos indica que se tiene una asimétrica negativa, lo que indica que la cola se sesga a la izquierda, indicando que la mayoría de los datos se encuentran concentrados a la derecha ya que el coeficiente dio el siguiente resultado -.303. Por otra parte el coeficiente de curtosis nos indica que si $Ck < 0$, el grado de dispersión de los datos alrededor de la media, el valor obtenido es de -1.100, lo que nos indica que estamos ante una curtosis platicúrtica lo que representa que los datos están poco concentrados alrededor de las medidas de tendencia central.

Tabla 31. Distribución de frecuencias de la variable independiente X6: Seguridad de la información

Seguridad de la información				
	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Ni de acuerdo ni en desacuerdo	1	1.3	1.3	1.3
De acuerdo	1	1.3	1.3	2.6
28	1	1.3	1.3	3.9
29	4	5.3	5.3	9.2
30	6	7.9	7.9	17.1
31	1	1.3	1.3	18.4
Bastante de acuerdo	7	9.2	9.2	27.6
33	4	5.3	5.3	32.9

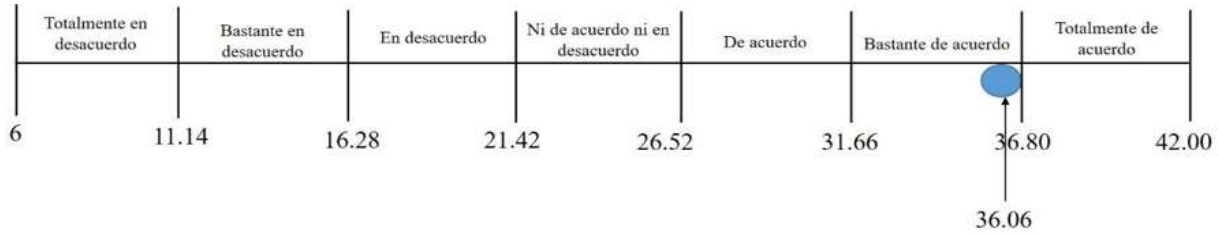
34	8	10.5	10.5	43.4
35	1	1.3	1.3	44.7
36	3	3.9	3.9	48.7
Totalmente de acuerdo	5	6.6	6.6	55.3
38	4	5.3	5.3	60.5
39	5	6.6	6.6	67.1
40	6	7.9	7.9	75.0
41	7	9.2	9.2	84.2
42	12	15.8	15.8	100.0
Total	76	100	100	

Fuente: Elaboración propia con la información obtenida en campo y procesada con SPSS.

La gráfica de frecuencias presenta la información obtenida para la variable seguridad de la información de acuerdo al grado de concordancia o discordancia de los encuestados, donde se puede observar que a partir de la información que se obtiene, el valor mínimo arrojado es de 10 y el máximo puntaje obtenido es de 42, dando un rango de 30 puntos de distancia entre las respuestas, los valores que se encuentran por debajo del parámetro de acuerdo, equivalen a un 1.3% del total. La mayor parte de los datos, correspondiente al 98.7% de los encuestados se ubican en el área bastante de acuerdo, como se muestra en la tabla.

De igual manera se generó la gráfica de concordancia que muestra el grado de acuerdo o desacuerdo por variable con respecto al total de encuestados, permitiendo evaluar la consistencia de las asignaciones y el valor de la media de 36.07 que se encuentra en el rango de la escala bastante de acuerdo como se muestra en la gráfica 22. Asimismo, se presenta el histograma de los datos de dicha variable, donde se aprecia un ligero sesgo izquierdo, lo que nos indica que algunos datos se encuentran ligeramente cargados a la derecha.

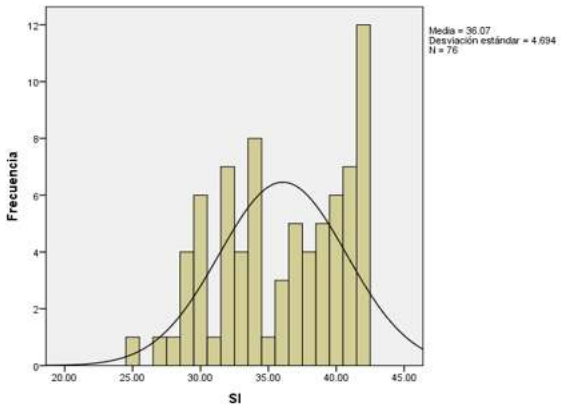
Gráfica 20. Concordancia de la variable independiente X6: Seguridad de la información



Fuente: Elaboración propia con la información obtenida del estudio de campo.

Como se aprecia en los resultados descriptivos la concordancia de los expertos con respecto a la influencia de las seis variables independientes hacia la dependiente ha sido alta, teniendo que en todas ellas por lo menos se ubicaron en la escala “bastante de acuerdo”, lo que reafirma la relevancia de dichas variables para la ciberseguridad en el estado de Michoacán.

Gráfica 21. Histograma de la variable independiente X6: Seguridad de la información.



Fuente: Imagen obtenida al procesar los datos en el software SPSS v.23.

Aunado a lo anterior la presente investigación combina este análisis estadístico descriptivo con un modelo PLS-SEM, brindando una mayor validez y robustez a la investigación científica en el campo de la ciberseguridad, lo que permitió obtener una mejor comprensión inicial de la naturaleza y la relación entre las variables de estudio, así como la evaluación de las diferentes respuestas obtenidas por los expertos en ciberseguridad, debido a que el análisis con un modelo de ecuaciones estructurales de mínimos cuadrados parciales al ser un método más potente de evaluación no solo se centra en el análisis de las relaciones entre las variables, si no que permite una comprensión más profunda del fenómeno de estudio al realizar validaciones cruzadas (bootstrapping) con diferentes iteraciones, mejorando con esto la capacidad predictiva del modelo; para ello en la siguiente sección se presentan los resultados obtenidos por la modelización en la que se podrán contrastar los resultados del análisis descriptivo y con los de la modelización por un método estadístico de segunda generación como lo es PLS-SEM .

CAPÍTULO 6. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS DE LA MODELIZACIÓN CON PLS-SEM

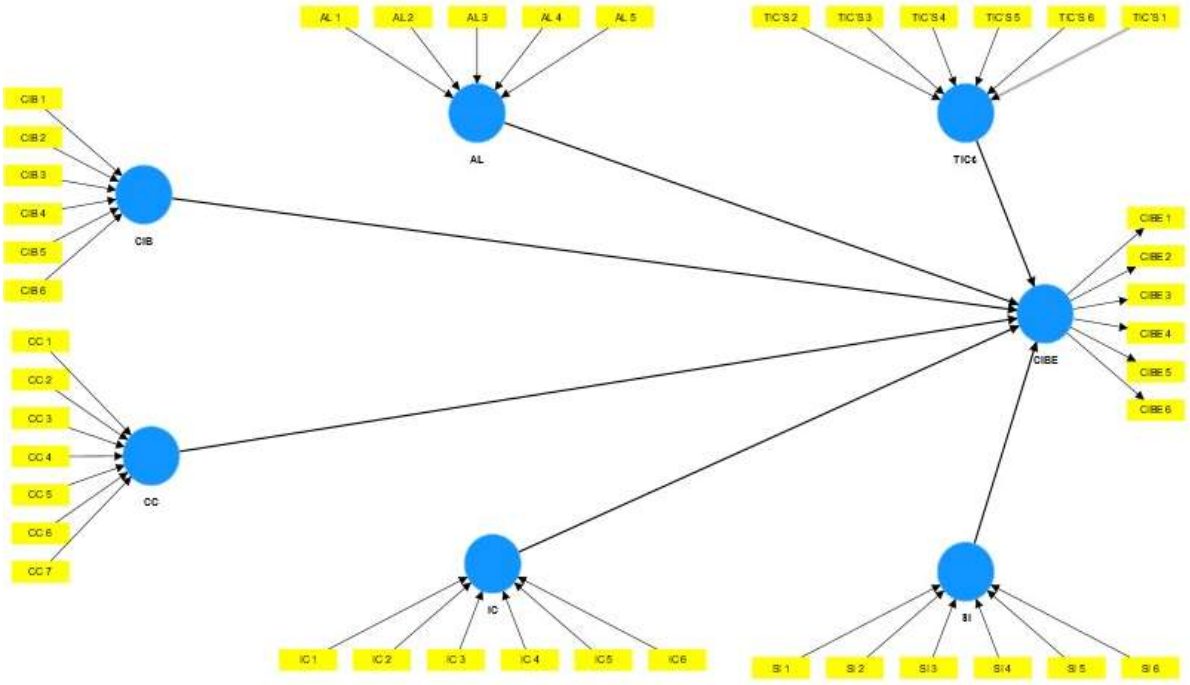
6.1 Resultados de la modelación con PL-SEM

Utilizando como base el método para desarrollar un modelo de ecuaciones estructurales mediante mínimos cuadrados parciales, en esta sección se proporciona una descripción detallada de los pasos realizados para estimar el modelo estructural propuesto por Hair et al. (2017) y verificar las hipótesis planteadas en la presente investigación. En primer lugar, se llevó a cabo una evaluación del modelo de medida externo y modelo estructural, seguida de una evaluación de los resultados obtenidos. Para ello, se hizo uso del software Smart PLS-SEM para llevar a cabo la estimación del modelo.

6.1.1 Evaluación del modelo de medida o externo

En la fase inicial de un proyecto de investigación, especialmente en el caso de esta investigación, en la que se utilizó el software estadístico SMART-PLS, versión 4, se modeló el nomograma que de manera gráfica permite visualizar las conexiones entre las variables (constructos) según la teoría de medida, de modo que se pueda visualizar la lógica de las relaciones hipotéticas que se intentarán comprobar. En la siguiente ilustración, se observan las relaciones estructurales entre las variables latentes y los indicadores, con la finalidad de mostrar las conexiones causales propuesta en el modelo.

Ilustración 18. Relación estructural variables latentes e indicadores Ciberseguridad.



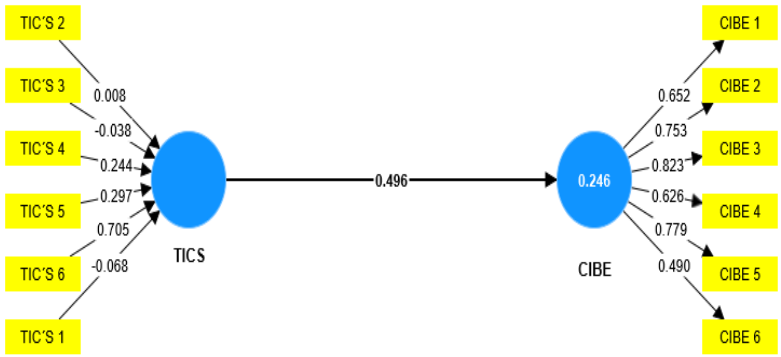
Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

De la ilustración anterior se observa que el modelo está conformado de seis variables latentes (constructos) los cuales son: Tecnologías de la información y comunicaciones (TIC´s), Aspectos legales (AL), Cibercultura (CIB), Cibercrimen (CC), Infraestructuras criticas (IC) y Seguridad de la información (SI) de las que se pretende demostrar si son factores determinantes de la ciberseguridad en el estado de Michoacán, que es la variable dependiente (CIBE) y sus respectivos indicadores. En la presente investigación se adoptó un enfoque formativo para el modelo utilizado, ya que los indicadores desempeñan un papel importante en la formación de las variables latentes.

Una vez cargados los datos en el software SMART-PLS, el procedimiento comienza con la validez convergente de las variables latentes y se procede a revisar la intensidad del coeficiente path que une los dos constructos, en donde se espera obtener valores superiores a 0,7, del coeficiente path, los cuales son aceptables en estudios exploratorios o en etapas tempranas donde se intenta probar nuevos conocimientos Hair et al. (2017).

En la siguiente ilustración se observa la variable independiente Tecnologías de la información y comunicaciones (TIC´s) y la variable dependiente Ciberseguridad (CIBE), donde se observa que el valor obtenido es de .496, presentando problemas de validez convergente.

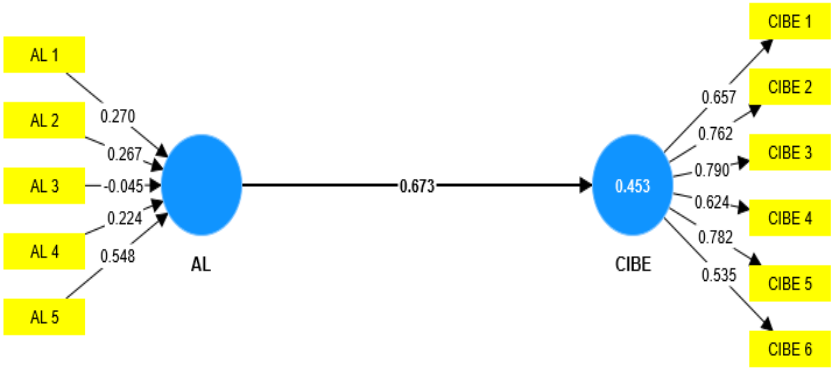
Ilustración 19. Fiabilidad variable TIC´s y CIBE.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

En la siguiente ilustración se observa la variable independiente (AL) y la variable dependiente (CIBE), donde se observa que el valor obtenido es de .673, presentando problemas de validez convergente.

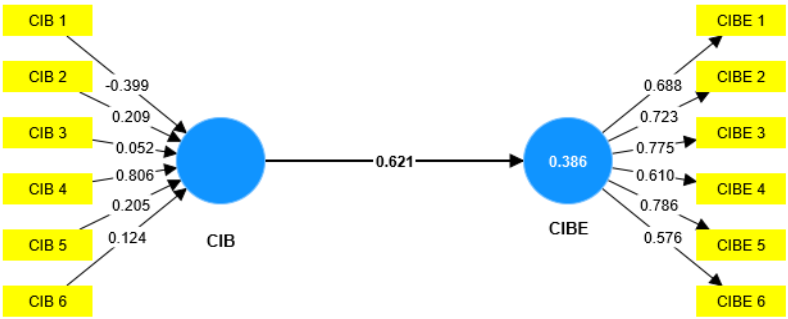
Ilustración 20. Fiabilidad variable AL y CIBE.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Se realiza el mismo cálculo para la variable independiente (CIB) y la variable dependiente (CIBE), donde se observa que el valor obtenido es de .621, presentando problemas de validez convergente.

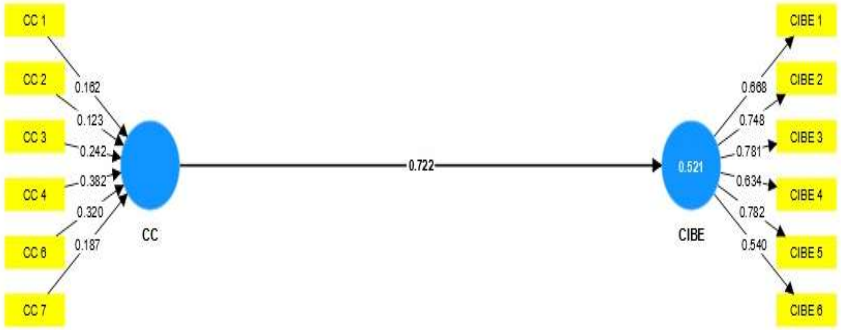
Ilustración 21. Fiabilidad variable CIB y CIBE.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

En lo que respecta a la variable independiente CC y la variable dependiente (CIBE), se observa que el valor obtenido es de .722 no presentando problemas de validez convergente, como se visualiza en la ilustración.

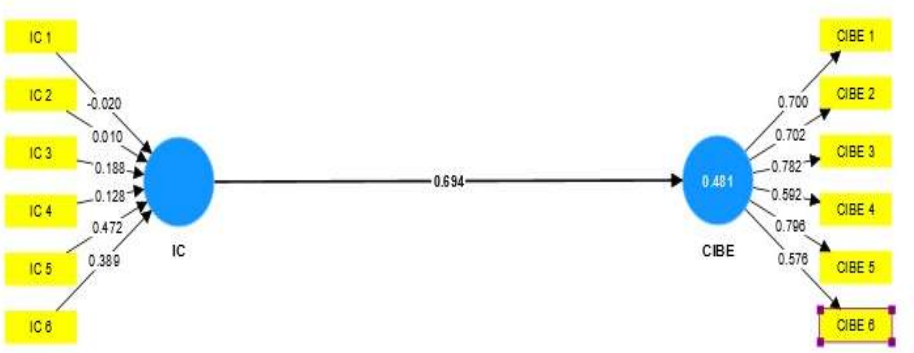
Ilustración 22. Fiabilidad variable CC y CIBE.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

El mismo procedimiento se aplicó sobre la variable independiente (IC) y la variable dependiente (CIBE), se obtiene un valor de .694, presentando problemas de validez convergente, como se aprecia en la ilustración siguiente.

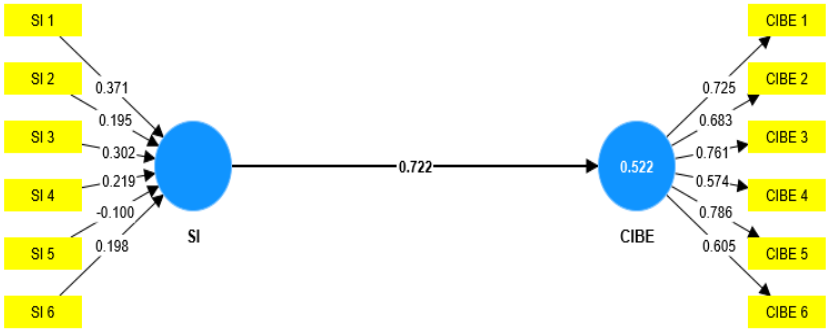
Ilustración 23. Fiabilidad variable IC y CIBE.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Finalmente con la variable independiente (SI) y la variable dependiente (CIBE), donde el valor alcanzado es de .722 no presentando problemas de validez convergente, como se aprecia en la siguiente ilustración.

Ilustración 24. Fiabilidad variable SI y CIBE.

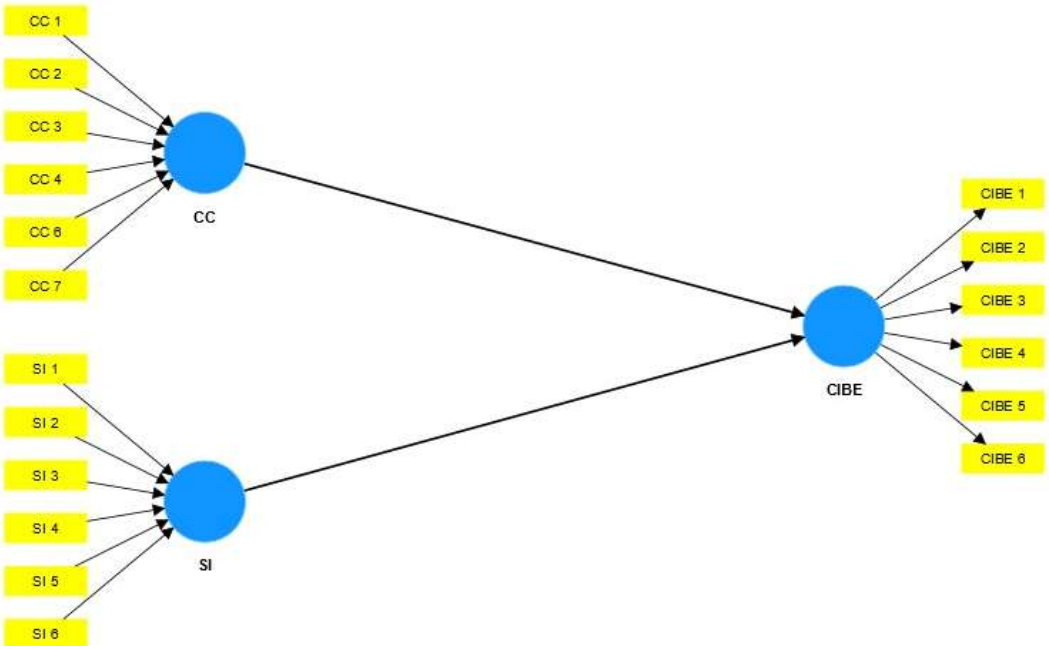


Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Después de verificar la validez convergente, se ha observado que únicamente los constructos CC y SI cumplen con los criterios establecidos en el análisis de redundancia. Debido a que los valores de los coeficientes path de las variables TIC´s AL, CIB e IC se encuentran por debajo del valor generalmente aceptado de 0.7, se decide eliminarlas del modelo y proceder el análisis con las variables que sí están reflejando con precisión el constructo subyacente.

En este análisis para la valoración del modelo se considerarán únicamente los constructos que no presentan problemas de validez convergente. Como resultado, el nuevo modelo queda expresado de la siguiente manera.

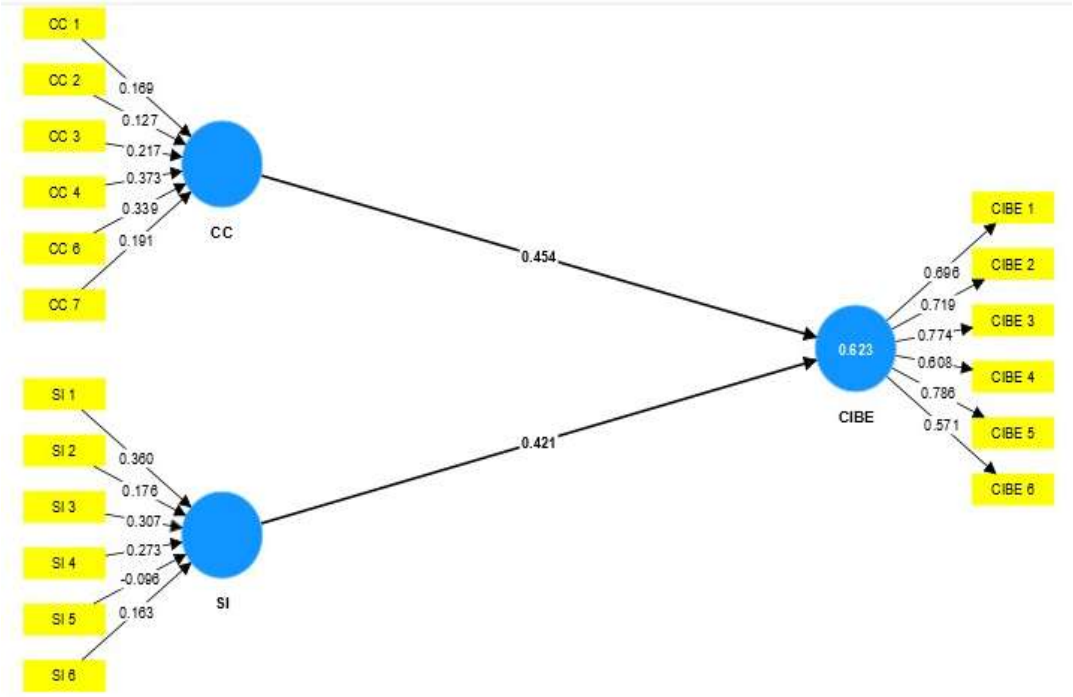
Ilustración 25. Nuevo modelo, sin las variables; TIC´s AL, CIB e IC.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Se calculan los coeficientes Path para conocer el grado de influencia o impacto que tienen los constructos sobre los indicadores, como lo muestra la siguiente ilustración.

Ilustración 26. Coeficiente Path.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

De la ilustración anterior se observa que el modelo está conformado de dos variables latentes (constructos) las cuales son: Cibercrimen (CC) y Seguridad de la información (SI), cuyos coeficientes path son de 0.454 0.421 respectivamente. No obstante que en estos resultados ya se puede apreciar una relación fuerte entre las variables, antes de hacer conclusiones es necesario realizar las pruebas necesarias para la evaluación de este tipo de modelos formativos.

Se procede a realizar el análisis de colinealidad bajo los valores VIF, el cual se calcula para cada indicador y proporciona una estimación de cuánto se infla la varianza de un estimador debido a la colinealidad con otros indicadores, donde se espera obtener valores menores a 5, como lo precisa la ilustración siguiente:

Ilustración 27. Estadísticos de colinealidad.

Estadísticos de colinealidad (VIF) - Modelo externo - Lista

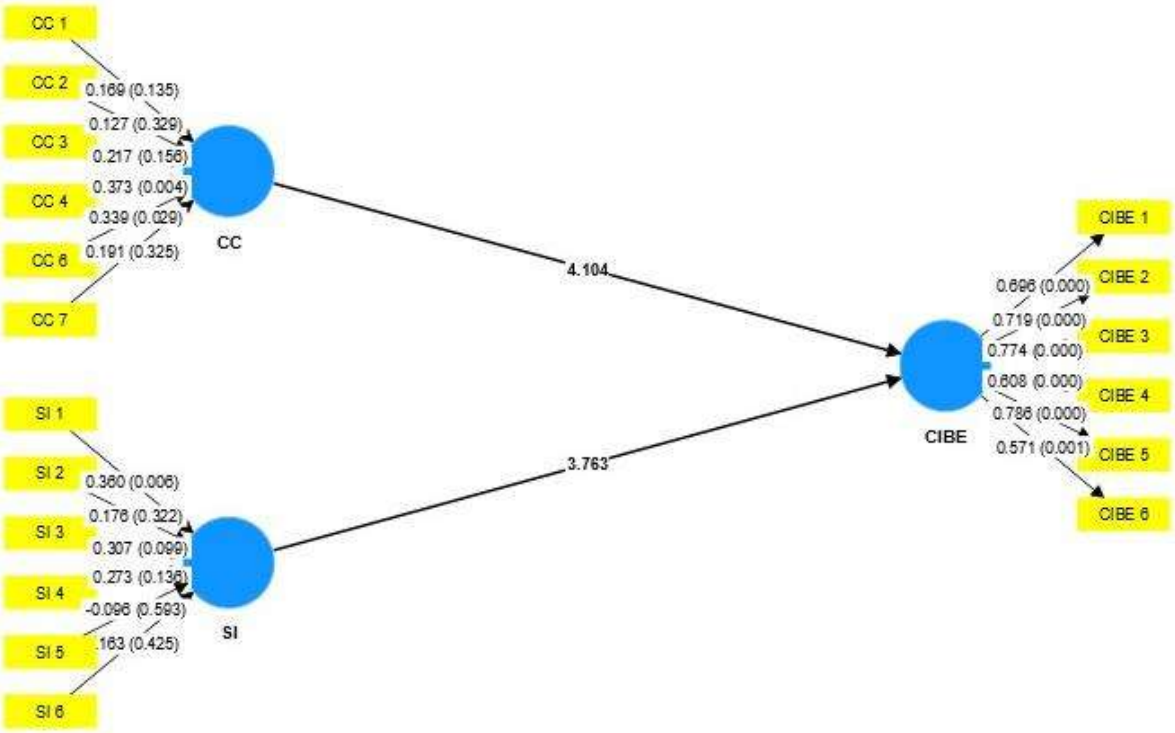
	VIF
CC 1	1.283
CC 2	1.340
CC 3	1.395
CC 4	1.493
CC 6	1.851
CC 7	1.766
CIBE 1	1.485
CIBE 2	1.584
CIBE 3	1.944
CIBE 4	1.435
CIBE 5	1.870
CIBE 6	1.329
SI 1	1.758
SI 2	2.140
SI 3	2.181
SI 4	2.147
SI 5	1.369
SI 6	1.976

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Se observa que el modelo interno de medida no presenta colinealidad entre las variables CC y SI, se observa que los indicadores propuestos están aportando información única y no son redundantes con respecto al constructo que se pretende medir.

El tercer paso es revisar la significancia de los pesos estadísticos de cada uno de los indicadores, donde se analiza la contribución de cada indicador al constructo y determinar si dicha contribución es estadísticamente significativa, como se observa en la siguiente ilustración.

Ilustración 28. Significancia de los pesos estadísticos en el nomograma.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Ilustración 29. Pesos externos.

Pesos externos - Media, desviación estándar, valores t, valores p Zoom (100%) Copiar a Excel Copiar a R

	Muestra original (O)	Media de la muestra (M)	Desviación estándar (STDEV)	Estadísticos t (|O/STDEV|)	Valores p
SI 5 -> SI	-0.096	-0.052	0.179	0.534	0.593
SI 6 -> SI	0.163	0.143	0.204	0.797	0.425
CC 2 -> CC	0.127	0.116	0.130	0.976	0.329
CC 7 -> CC	0.191	0.190	0.194	0.984	0.325
SI 2 -> SI	0.176	0.142	0.178	0.990	0.322
CC 3 -> CC	0.217	0.212	0.153	1.419	0.156
SI 4 -> SI	0.273	0.259	0.183	1.491	0.136
CC 1 -> CC	0.169	0.150	0.113	1.493	0.135
SI 3 -> SI	0.307	0.302	0.187	1.648	0.099
CC 6 -> CC	0.339	0.324	0.155	2.183	0.029
SI 1 -> SI	0.360	0.343	0.131	2.746	0.006
CC 4 -> CC	0.373	0.371	0.130	2.875	0.004
CIBE 6 <- CIBE	0.183	0.180	0.058	3.158	0.002
CIBE 4 <- CIBE	0.197	0.195	0.047	4.166	0.000
CIBE 2 <- CIBE	0.231	0.230	0.033	6.934	0.000
CIBE 5 <- CIBE	0.250	0.253	0.034	7.321	0.000
CIBE 1 <- CIBE	0.316	0.298	0.039	8.003	0.000
CIBE 3 <- CIBE	0.249	0.249	0.033	7.528	0.000

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

De lo anterior se aprecia que del indicado SI5, la significancia de sus pesos es mayor de .5, que es el criterio por debajo del cual se considera que los indicadores aportan y son significativos para el constructo, por lo que se procede a revisar la carga de dichos indicadores, como se aprecia en la siguiente ilustración.

La siguiente ilustración presenta el listado de cada uno de las cargas externas de los indicadores, que es el segundo criterio de decisión para eliminar o dejar que permanezcan los indicadores dentro del modelo.

Ilustración 30. Cargas externas.

Cargas externas - Lista

	Cargas externas
SI 5 -> SI	0.403
CC 1 -> CC	0.554
CIBE 6 <- CIBE	0.571
CC 2 -> CC	0.582
CIBE 4 <- CIBE	0.608
CC 3 -> CC	0.644
CIBE 1 <- CIBE	0.696
CC 7 -> CC	0.710
CIBE 2 <- CIBE	0.719
SI 2 -> SI	0.752
SI 6 -> SI	0.768
CIBE 3 <- CIBE	0.774
CC 4 -> CC	0.777
CIBE 5 <- CIBE	0.786
CC 6 -> CC	0.790
SI 4 -> SI	0.817
SI 1 -> SI	0.827
SI 3 -> SI	0.847

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Como se aprecia el indicador, SI5, la significancia de su pesos es baja, una vez revisada su carga externa se puede observar que únicamente el indicador seguridad de la información SI5, no contribuye al modelo estructural, ya que su peso está por debajo del criterio de .5, por lo que se procede a evaluar la significancia de su carga, como lo muestra la siguiente ilustración.

Ilustración 31. Significancia de las cargas externas.

Cargas externas - Media, desviación estándar, valores t, valores p Zoom (100%) Copiar a Excel Copiar a R

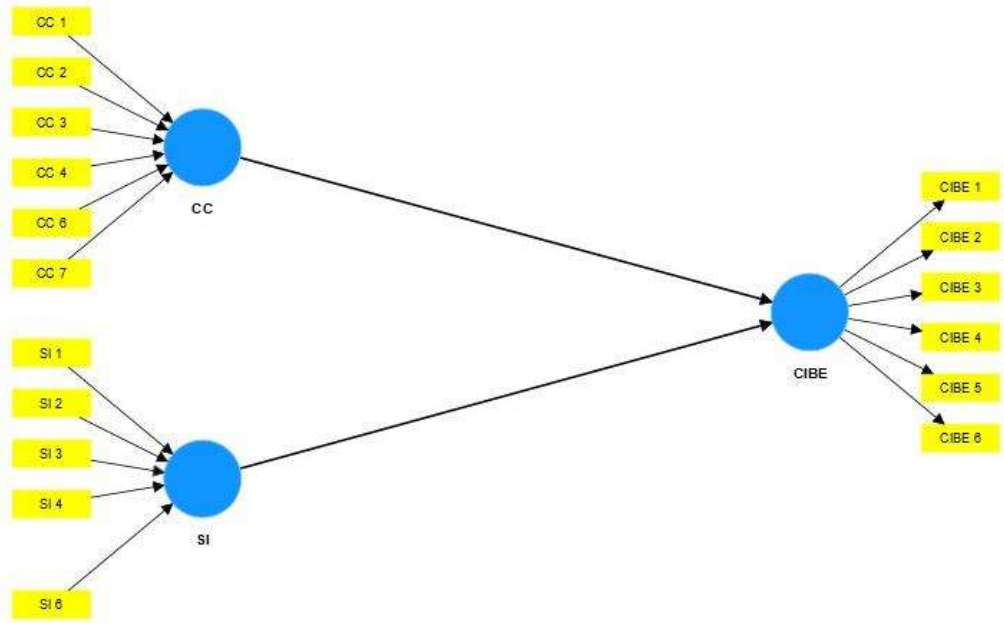
	Muestra original (O)	Media de la muestra (M)	Desviación estándar (STDEV)	Estadísticos t (|O/STDEV|)	Valores p
SI 5 -> SI	0.403	0.435	0.254	1.585	0.113
CIBE 6 <- CIBE	0.571	0.560	0.176	3.250	0.001
CIBE 4 <- CIBE	0.608	0.611	0.137	4.442	0.000
CC 2 -> CC	0.582	0.563	0.121	4.806	0.000
CC 1 -> CC	0.554	0.521	0.114	4.877	0.000
CC 7 -> CC	0.710	0.681	0.130	5.468	0.000
CC 3 -> CC	0.644	0.630	0.111	5.830	0.000
SI 6 -> SI	0.768	0.729	0.104	7.414	0.000
CC 4 -> CC	0.777	0.756	0.088	8.876	0.000
CC 6 -> CC	0.790	0.759	0.085	9.338	0.000
CIBE 1 <- CIBE	0.696	0.684	0.077	9.089	0.000
CIBE 2 <- CIBE	0.719	0.719	0.072	10.047	0.000
CIBE 3 <- CIBE	0.774	0.779	0.047	16.354	0.000
CIBE 5 <- CIBE	0.786	0.789	0.047	16.704	0.000
SI 1 -> SI	0.827	0.800	0.065	12.759	0.000
SI 2 -> SI	0.752	0.734	0.076	9.959	0.000
SI 3 -> SI	0.847	0.822	0.067	12.629	0.000
SI 4 -> SI	0.817	0.789	0.089	9.183	0.000

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Una vez revisada la significan de la carga, el valor del indicador obtenido para seguridad de la información SI5 con un valor de 0.113, lo que refleja que estos indicadores no contribuyen ni de forma relativa ni

absoluta al modelo, por lo que se toma la decisión de eliminar el indicador del modelo para mejorar su precisión y validez, quedando el nomograma como se presenta a continuación:

Ilustración 32. Nueva propuesta de monograma.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

6.1.2 Evaluación de modelo estructural o interno

Las siguientes pruebas permitirán determinar la calidad de ajuste del modelo y la validez de las relaciones entre las variables, por lo que el primer paso es revisar la colinealidad del modelo interno, donde se obtiene que la variable Cibercrimen y seguridad de la información IC-SI no presentan problemas de colinealidad, sus valores obtenidos de 1.703 y 1.703 respectivamente.

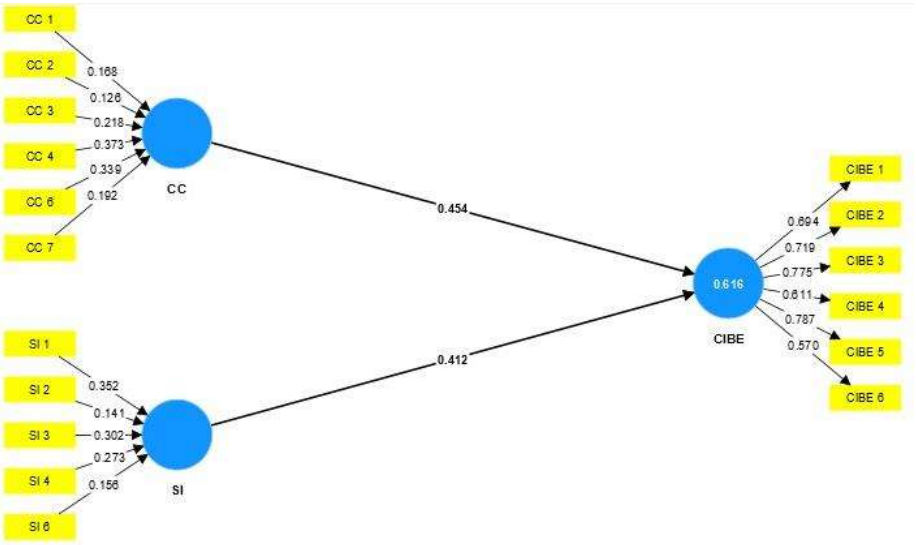
Ilustración 33. Estadísticos de colinealidad.

Estadísticos de colinealidad (VIF) - Modelo interno - Matriz

	CC	CIBE	SI
CC		1.703	
CIBE			
SI		1.703	

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Ilustración 34. Significancia de los caminos path.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Ilustración 35. Significancia de los caminos path.

Coeficientes path - Media, desviación estándar, valores t, valores p Zoom (100%) Copiar a Excel Copiar a R

	Muestra original (O)	Media de la muestra (M)	Desviación estándar (STDEV)	Estadísticos t (|O/STDEV|)	Valores p
CC -> CIBE	0.454	0.474	0.116	3.914	0.000
SI -> CIBE	0.412	0.413	0.112	3.662	0.000

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

De la anterior ilustración se observa la significación estadística de los coeficientes PATH, cuyos valores son 0.454 y 0.412 para las variables CC y SI respectivamente. Obteniéndose que las variables CC son significativas a un nivel de confianza de 0.00 reflejando un efecto estadísticamente relevante para el modelo.

El siguiente paso es calcular el coeficiente de determinación (R2) el cual refleja el poder predictivo de las variables independientes sobre la dependiente, obteniendo el resultado de .616, lo que nos indica que la variable dependiente ciberseguridad se explica en un 61.6 % por las variables independientes: cibercrimen y seguridad de la información (CC y SI).

Ilustración 36. Coeficiente de determinación R2.

R cuadrado - Resumen

	R cuadrado	R cuadrado ajustada
CIBE	0.616	0.605

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

El cuarto paso consiste en determinar el efecto del tamaño de F2, obteniéndose los valores que se muestran en ilustración siguiente.

Ilustración 37. F cuadrado.

f cuadrado - Matriz

	CC	CIBE	SI
CC		0.314	
CIBE			
SI		0.259	

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Donde se visualizan los siguientes coeficientes 0.314 y 0.259 respectivamente para las variables CC y SI, en el cual se aprecia que tienen un efecto medio sobre la variable dependiente, mostrando la contribución de cada una las variables al modelo.

6.1.3 Prueba de hipótesis

Estos valores permiten la comprobación o rechazo de las hipótesis del planteamiento del problema de investigación, con lo que se concluye que a pesar que el modelo teórico está formado por seis variables, no obstante de acuerdo a su nivel de significancia solo CC y SI se compruebe su relación hipotétizada con la ciberseguridad a un nivel de significancia del 0.0.

El valor obtenido por el coeficiente de determinación R2 es de .616 para la variable dependiente, se interpreta que en un 61.6% de las varianzas de las variables es explicada entre si, por lo que se puede asumir que dicho porcentaje del problema de la ciberseguridad es explicado por el modelo teórico.

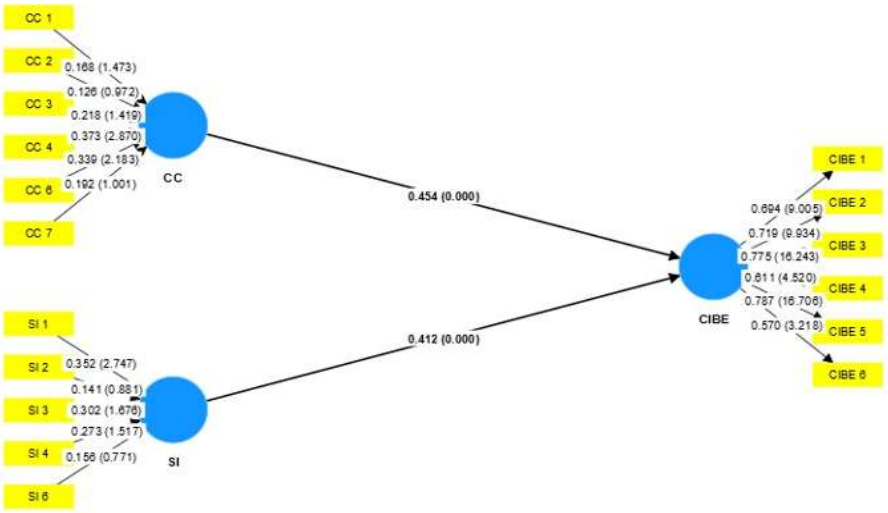
Una vez que se ha confirmado la relación de dependencia entre las variables, los coeficientes de la ruta (path) proporcionan una explicación sobre cómo se establece esta relación de dependencia. Se analiza el signo del coeficiente en relación con la hipótesis del modelo, demostrando que las variables si son significativas, mostrando una relación directa, ya que teniendo mayor perfeccionamiento en la disminución de la incidencia delictiva y seguridad de la información, podrán contribuir a incrementar la ciberseguridad en el Estado de Michoacán.

6.1.4 Coeficientes Path

De los resultados obtenidos de la modelización se puede concluir que dos de las seis variables son de gran relevancia para comprender y explicar el estado actual de la ciberseguridad. Siendo estas, de

acuerdo con su orden de importancia para la ciberseguridad: Cibercrimen con un coeficiente path de 0.403; seguido de Seguridad de la Información e Infraestructuras críticas con 0.233; y por último Aspectos legales con 0.226. Estos hallazgos constituyen una base sólida para la formulación y diseño de una Política Pública de Ciberseguridad efectiva y adecuada para el estado de Michoacán.

Ilustración 38. Coeficiente path.



Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

Asimismo, a partir de los resultados de la modelización se puede concluir que dos de las seis variables son factores determinantes para explicar la ciberseguridad en el estado de Michoacán, teniendo que las variables latentes cuyos coeficientes path son significativos a un 0.00 son Cibercrimen; y Seguridad de la información, cuya capacidad predictiva es alta, por lo que se procede con el análisis de cada uno de los indicadores formativos que las integran para así elegir a aquellos que sean más importantes para la política pública de ciberseguridad. A continuación se describen cada una de las variables.

Ilustración 39.Pesos de la variable cibercrimen

Pesos externos - Lista

	Pesos externos
CC 1 -> CC	0.168
CC 2 -> CC	0.126
CC 3 -> CC	0.218
CC 4 -> CC	0.373
CC 6 -> CC	0.339
CC 7 -> CC	0.192

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

De acuerdo con los pesos obtenidos, se concluye la capacidad explicativa de cada uno de los indicadores con respecto a la variable latente, teniéndose que cibercrimen (CC4, CC6, CC3, CC7, CC1 y CC2). Esto a su vez representa datos útiles para la toma de decisiones respecto a la política pública de ciberseguridad ya que el asignar orden por medio de los pesos nos ayuda a establecer las prioridades o las líneas de acción que más ayuden a mejorar la ciberseguridad.

Ilustración 40. Pesos de la variable Seguridad de la información.

Pesos externos - Lista

SI 1 -> SI	0.352
SI 2 -> SI	0.141
SI 3 -> SI	0.302
SI 4 -> SI	0.273
SI 6 -> SI	0.156

Fuente: Elaboración propia en Smart PLS con base en Hair et al., (2017).

De acuerdo con los pesos obtenidos, se concluye la capacidad explicativa de cada uno de los indicadores con respecto a la variable latente, teniéndose que seguridad de la información (SI5, SI3, SI4, SI6 Y SI2) representan el orden de importancia de mayor a menor de la variable.

Por lo que con este enfoque de PLS-SEM, los indicadores se convierten en elementos que guían las acciones concretas en el diseño de la Política Pública de Ciberseguridad.

CAPÍTULO 7. LA CIBERSEGURIDAD COMO PROPUESTA DE POLÍTICA PÚBLICA EN EL ESTADO DE MICHOACÁN

En capítulos previos de esta investigación, se ha examinado el problema de la ausencia de ciberseguridad, debido al surgimiento de las tecnologías de la información, su interacción en todos los aspectos de la sociedad y la dependencia tecnológica. En el contexto de México, se observa un aumento en la incidencia delictiva relacionada con la tecnología, a medida que esta crece y al mayor número de usuarios de las mismas. Esto se debe a varios factores, como la falta de conocimiento sobre estos incidentes y riesgos, el menoscabo de capacidades adecuadas para enfrentarlos, la ausencia de una legislación apropiada para su enmarcamiento y sanción, la escasez de una cultura de en ciberseguridad, protección de las infraestructuras críticas y la seguridad de la información que fluye por diferentes canales de comunicación, sin protección alguna y que afectan no solo a los usuarios, empresas, sino incluso al gobierno.

En el capítulo 3, se desarrolló un apartado para hablar de las políticas públicas, definiéndolas; como aquellas acciones del gobierno encaminadas a satisfacer las necesidades de la sociedad a través de programas públicos, a su vez se habla del ciclo de las políticas; diseño, implementación y evaluación que buscan generar un impacto positivo en la sociedad, en el caso que nos ocupa una política pública de ciberseguridad permitirá al estado de Michoacán contar con un instrumento para garantizar y proteger la integridad y los derechos de la sociedad, así como salvaguardar las infraestructuras críticas y los servicios públicos en materia de telecomunicaciones, preservación y protección de los activos informáticos tanto del Estado como de los particulares

Una vez analizados los resultados planteados en la presente investigación, es crucial que el Estado reconozca la necesidad de crear una Política Pública de Ciberseguridad. La cual debe llevarse a cabo mediante la implementación de leyes generales y una serie de acciones interrelacionadas, por medio del: Marco legal, Normas y estándares, Gobernanza, Colaboración en el sector público y privado, Investigación y desarrollo, Inversión en tecnología y cooperación internacional, todo esto desde un enfoqué holístico, con el fin de garantizar una ciberseguridad sólida y eficiente para el Estado de Michoacán.

Las instituciones actualmente son susceptibles de cambios dado el contexto existente que se vive y que obliga en razón de su capacidad económica, política, social y cultural a realizar una reingeniería de sus procesos existentes, lo que involucra una serie de modificaciones a su estructura organizacional, por lo cual a partir del reconocimiento de la problemática mencionada, se debe implementar un marco de actuación que establezca la visión del Estado adaptada y congruente con los riesgos asociados al uso de las tecnologías en cuanto a la protección de la información y los ciudadanos en el ciberespacio.

Esta visión adaptada a la realidad y congruente desde la perspectiva de la ciencia, se ha materializado en la presente investigación en la que se analizaron aquellos elementos teóricos y empíricos de los factores que afectan a la ciberseguridad, dilucidando dentro de estos, a aquellos que tienen mayor impacto y capacidad predictiva mediante la modelización de ecuaciones estructurarles de mínimos cuadrados parciales PLS-SEM en la ciberseguridad, por medio de sus variables explicativas planteadas. A partir de estos resultados se presenta una propuesta de diseño de P**olítica Pública de Ciberseguridad para el Estado de Michoacán**.

7.1 Alineación de la propuesta de Política Pública al Plan Nacional de Desarrollo 2019–2024

La propuesta de diseño de la Política Pública de Ciberseguridad para el Estado de Michoacán se ajusta a la visión del Gobierno Federal, tal como se refleja en el Plan Nacional de Desarrollo 2019 – 2024. Dicha propuesta se encuentra en correspondencia con el eje estratégico: Política y Gobierno (2019), la cual se describe a continuación.

7.1.1. Eje 1. Política y Gobierno

Combatir y erradicar la corrupción en el Gobierno, lo que incluye la transferencia de recursos públicos a manos de terceros y prácticas corruptas que debilitan a las Instituciones. Para garantizar esto, se propone tipificar esta conducta como una falta grave, eliminar muchos de los privilegios a los funcionarios, promover la colaboración internacional contra paraísos fiscales y fortalecer los mecanismos de fiscalización. Por otra parte se destaca la necesidad de terminar con los lujos y derroches de recursos de los funcionarios en el gobierno, buscando en todo momento un gobierno más eficiente y transparente en la ejecución del gasto público (2019), estableciéndose los siguientes objetivos:

Ilustración 41. Eje 1. Política y Gobierno.

Meta	Estrategia Nacional de Seguridad Pública
Objetivo I	Erradicar la corrupción y reactivar la procuración de justicia.
Objetivo VIII	Articular la seguridad nacional, la seguridad pública y la paz.
Objetivos estratégicos	
8.1	Coordinar la ejecución del Programa para la Seguridad Nacional del Gobierno, por medio del Consejo de Seguridad Nacional.
8.2	Establecer un Sistema Nacional de Inteligencia.

8.3	Actualizar el catálogo y clasificación de Instalaciones Estratégicas.
8.4	Promover el concepto de cultura de Seguridad Nacional postulado por el gobierno para contribuir al conocimiento colectivo sobre el tema.
8.5	Mejorar las capacidades tecnológicas de investigación científica en los ámbitos de seguridad pública, seguridad interior, generación de inteligencia estratégica y procuración de justicia.
Objetivo IX	Repensar la seguridad nacional y reorientar a las Fuerzas Armadas. Los soldados y marinos de México son pueblo uniformado.

Fuente: Elaboración con base en el PND 2019 – 2023 (2019).

7.2 Alineación de la propuesta de Política Pública en el estado de Michoacán al Plan de Desarrollo Integral del Estado de Michoacán 2021-2027

La presente propuesta de diseño de **Política Pública de Ciberseguridad para el estado de Michoacán,** queda alineada al Plan de Desarrollo Integral 2021-2027, alineada a los ejes estratégicos: Armonía, paz y reconciliación y al eje Bienestar (2021) en los cuales refleja la visión del estado de Michoacán, a través de ejes, objetivos, metas y acciones, los cuales se describen.

7.2.1 Eje 1. Armonía, paz y reconciliación

"Una política de seguridad ciudadana que garantice el respeto a los derechos humanos y el bienestar, que priorice la prevención social de la violencia, lo que requiere un esfuerzo interinstitucional y corresponsable con distintos actores sociales" (2021).

"Problemas de orden básico de convivencia social: violencia intrafamiliar, escolar, contra las mujeres, abuso del alcohol y consumo de drogas" (2021).

"Nuestra estrategia comienza por el fortalecimiento institucional desde lo local, mayor colaboración y cooperación con la fiscalía para la investigación, eficaz atención a víctimas del delito y acompañamiento permanente para garantizar el acceso a la justicia, tal como lo ha señalado el presidente" (2021).

Ilustración 42. Eje 1. Armonía, paz y reconciliación.

1.	Armonía, paz y reconciliación.
1.1.	Fortalecer la gobernabilidad y cultura democrática.
1.1.1.	Fortalecer el Estado Constitucional de Derecho, cultura democrática, de legalidad, y la coordinación entre poderes.

Meta	En 2021, la entidad se colocó en el lugar 27 a nivel nacional en el índice de desarrollo democrático, mostrando un desarrollo democrático mínimo. Para el 2027, se espera posicionar a Michoacán entre las primeras 10 entidades con mayor índice a nivel nacional.
Indicador	Índice de Desarrollo Democrático.
Acciones	
1.1.1.1.	Impulsar la cultura democrática y de legalidad.
1.1.1.2.	Favorecer, fortalecer y defender la libertad de expresión.
1.1.1.3.	Fortalecer y democratizar los medios de comunicación del Gobierno del Estado.
1.1.1.4.	Favorecer la conciliación entre las partes.

Fuente: Elaboración con base en el PLADIEM (2021).

1.3.1. Preservar la seguridad pública y fomentar la prevención social de la violencia y la delincuencia en el estado.

Ilustración 43. Eje 1.3.1. Preservar la seguridad pública y fomentar la prevención social de la violencia y la delincuencia en el estado.

Meta	En 2020 se cometieron casi 190 delitos de alto impacto por cada 100 mil habitantes. Para el 2027, se plantea reducir la cifra al menos por una tercera parte, colocando a la entidad entre los 5 estados con menor tasa a nivel nacional**.**
Indicador	Tasa de incidencia delictiva de alto impacto.
Acciones	
1.3.1.3.	Implementar la cultura de paz, iniciando con campañas en los niveles educativos para la prevención del delito, así como pláticas motivacionales entre los jóvenes para el fomento del deporte, el arte y la cultura.
1.3.1.6.	Capacitar a servidores públicos del área de seguridad en materia de prevención social del delito, cultura de la paz y reconstrucción del tejido social.
1.3.1.8.	Incentivar e incrementar la corresponsabilidad de actores sociales y de la ciudadanía en general en la prevención social de la violencia y la delincuencia.
1.3.1.9.	Establecer mecanismos de participación ciudadana a nivel comunitario y vecinal que promuevan la cultura de la paz y la mediación de conflictos.
1.3.1.10.	Implementar programas de profesionalización en prevención social de la violencia y la delincuencia, dirigidos a servidores públicos, policías municipales y ciudadanía en general.

Fuente: Elaboración con base en el PLADIEM (2021).

1.3.2. Fortalecer el estado de fuerza, su profesionalización y equipamiento.

Ilustración 44. Eje 1.3.2. Fortalecer el estado de fuerza, su profesionalización y equipamiento.

Meta	En el 2020, Michoacán no reportó la cantidad de elementos de seguridad pública que aprobó la evaluación para obtener el Certificado Único Policial. Como parte de las iniciativas de transparencia gubernamental, durante la presente administración se reportará esta cifra anualmente, manteniendo al menos un 95% de personal con evaluaciones aprobatorias.
Indicador	Personal de la institución encargada de la función de seguridad pública, por entidad federativa según estatus de evaluación.
Acciones	
1.3.2.1.	Implementar un fondo económico para el fortalecimiento de la paz para mejorar los cuerpos policiales con equipamiento e infraestructura, y apoyar acciones de prevención social de la violencia, adicciones y delincuencia.
1.3.2.6.	Fortalecer en los programas de formación y profesionalización los temas de derechos humanos, prevención de la violencia a las mujeres, perspectiva de género, inclusión, atención a grupos vulnerados y énfasis en la perspectiva infantil y adolescente, todo ello con base en estándares establecidos por los organismos internacionales.
1.3.2.8.	Fortalecer el equipamiento técnico y táctico de los cuerpos de seguridad policial estatal y municipal y, en su caso, su actualización y mantenimiento, así como ampliar la cobertura de la red de comunicaciones al interior del estado.

Fuente: Elaboración con base en el PLADIEM (2021).

7.1.2 Eje 2. Bienestar

"Con este nuevo enfoque de desarrollo social garantizaremos el pleno respeto a los derechos humanos, para lograr una transformación con igualdad, equidad, justicia social, reconocimiento de la diversidad y pluralidad, cohesión comunitaria e integración social, que abarque a todas y todos, prioritariamente a los que han sido marginados, discriminados y excluidos del desarrollo, para que tengan acceso a una vida digna" (2021).

Ilustración 45- Eje 2. Bienestar.

2.1.	Garantizar el acceso a los derechos sociales a grupos históricamente vulnerados para reducir las brechas de desigualdades sociales y territoriales.
2.1.1.	Brindar atención prioritaria a los grupos históricamente vulnerados. Meta En 2020, 34.8% de la población michoacana es vulnerable por carencias sociales. Para 2027 se espera reducir al menos una tercera parte de la población en esta condición.
Meta	En 2020, 34.8% de la población michoacana es vulnerable por carencias sociales. Para 2027 se espera reducir al menos una tercera parte de la población en esta condición.
Indicador	Población vulnerable por carencias sociales.

Acciones	
2.1.1.3	Armonizar el marco normativo vigente en materia de bienestar.
2.1.1.4	Crear espacios para la ciudadanía generadores de bienestar y armonía social que fortalezcan la confianza en las instituciones y reconstruyan el tejido social.
2.1.1.7.	Desarrollar campañas de información y concientización tendientes a eliminar la discriminación, la exclusión y la xenofobia.
2.1.1.8.	Promover capacitación y formación con perspectiva de género e interculturalidad a funcionarios.

Fuente: Elaboración con base en el PLADIEM *(2021).*

"Transitaremos a una nueva agenda digital en los servicios educativos. Llevaremos internet gratuito a las escuelas públicas para apoyar los nuevos modelos de aprendizaje, como las clases virtuales o vía remota, que permitirán expandir las fronteras del conocimiento de los alumnos. En las áreas administrativas el empleo de herramientas tecnológicas facilitará los trámites en línea, lo que abatirá la corrupción y evitará tortuosos procesos burocráticos; en este contexto avanzaremos en la credencialización y en la nómina digital" (2021).

2.2.4. Fortalecer la infraestructura y planeación para la mejora educativa.

Ilustración 46. Eje 2.2.4 Fortalecer la infraestructura y planeación para la mejora educativa.

Meta	En 2021, sólo 22 de cada 100 escuelas de educación primaria, secundaria y media superior cuentan con internet, sólo 10 de cada 100 escuelas tienen adaptaciones para personas con discapacidad y el 23 por ciento carecen de servicios sanitarios. Al término de la administración se incrementará en al menos un punto porcentual por ciclo escolar en dicha infraestructura.
Indicador	Porcentaje de escuelas y planteles según disponibilidad de servicios básicos.
Acciones	
2.2.4.3.	Adecuar la infraestructura educativa con una visión incluyente y de igualdad.
2.2.4.6.	Impulsar contenidos y actividades educativas conforme que incluyan el cuidado ambiental, la sana alimentación, la educación física y el deporte, el autocuidado de la salud, la igualdad sustantiva, el respeto a la dignidad humana, la cultura, el arte y la responsabilidad social.
2.2.4.8.	Fomentar el desarrollo científico y tecnológico, a través de la innovación y la investigación aplicada. Generar vinculación entre instituciones de educación superior, centros de investigación, iniciativa privada, productores y sector gubernamental.
2.2.4.10	Fortalecer la infraestructura y los esquemas de colaboración científica.

Fuente: Elaboración con base en el PLADIEM (2021).

7.1.3 Eje transversal. Gobierno digital, honesto, eficaz y transparente.

"Haremos lo necesario para que prevalezca el Estado de derecho y la cultura de la legalidad en Michoacán" (2021).

"En la Secretaría de Finanzas y Administración, además de reorganizar las funciones de cumplimiento de su objeto para eficientar las tareas de ingreso y rectoría en el ejercicio del gasto, se le confirieron facultades para hacer realidad el gobierno digital como elemento fundamental para incrementar la eficiencia administrativa" (2021).

"La Secretaría de Educación se fortaleció al consolidar las funciones que atienden a la educación básica; se creó un área específica para atender la agenda digital y se sentaron las bases para la creación del Instituto de Educación Media Superior y Superior" (2021).

"Las capacidades de digitalización de los servicios y la inclusión digital se convierten en esenciales para hacer más resilientes a las instituciones públicas frente a futuras crisis. Así lo entendemos, por lo que hemos emprendido esta iniciativa que requiere la participación de los tres órdenes de gobierno y los diferentes sectores" (2021).

"En este contexto, respaldaremos la Estrategia Digital Nacional, que considera para Michoacán otorgar servicio de telecomunicaciones en zonas sin cobertura, particularmente áreas rurales a las que el sector privado no atiende por no serle rentable. Nuestra lógica no es la de mercado, es la del derecho que tienen las personas al acceso a servicios de telecomunicaciones, incluido Internet, al que solo tienen acceso el 51% de las familias en Michoacán" (2021).

"Para este fin, facilitaremos la implementación del programa Internet para todos de CFE–Telecomunicaciones, que instalará radiobases de telefonía celular y puntos de conexión satelital gratuitas en zonas sin cobertura y antenas para el acceso, sin costo, en escuelas, bibliotecas y unidades médicas de zonas rurales de Michoacán" (2021).

"El gobierno digital permite modernizar la relación entre los ciudadanos y las instituciones públicas, por lo que creamos un área específica de atención de la agenda digital, desde donde se promoverá el tránsito hacia la firma electrónica certificada, la digitalización de trámites y servicios de la administración estatal; la digitalización de documentos y el impulso a la interactividad y atención en línea, con criterios de inclusión y accesibilidad" (2021).

"Para concretar la agenda digital, buscaremos adecuar el marco jurídico para que el Estado pueda migrar al uso intensivo de tecnologías de la información y así establecer lineamientos de uso, con el propósito de garantizar la conectividad entre las plataformas informáticas gubernamentales y el uso de las mejores herramientas disponibles" (2021).

Ilustración 47. Eje transversal. Gobierno digital, honesto, eficaz y transparente.

Objetivo General	Ser un gobierno honesto, eficaz y eficiente, que aplique principios de austeridad y racionalidad en el manejo de los recursos públicos, que transite hacia la transformación digital en Michoacán.
Criterios	
9.	Contribuir a reducir las brechas de desigualdad en el acceso al uso de las TIC´s, con criterios de inclusión y accesibilidad.
10.	Transitar hacia el uso de la firma electrónica certificada, la reducción de documentos físicos y la digitalización de trámites y servicios.

Fuente: Elaboración con base en el PLADIEM (2021).

En concordancia con la visión nacional de erradicar la corrupción y promover la eficiencia en el gasto público, es imperativo que a nivel estatal, como lo refleja el Plan de Desarrollo Integral del estado de Michoacán, se implementen políticas para fortalecer la ciberseguridad. Esto asegurará la protección de datos, sistemas informáticos, infraestructuras críticas, la confidencialidad, integridad y disponibilidad de la información, al tiempo que refuerza la confianza de la sociedad en los servicios digitales. De lo anterior resulta imperante que se desarrolle una Política Pública en Ciberseguridad que le permita al Estado contar con un instrumento estratégico y estructurado que aborde y mitigue los riesgos de una manera efectiva, es así, como de la presente investigación, surge la siguiente propuesta.

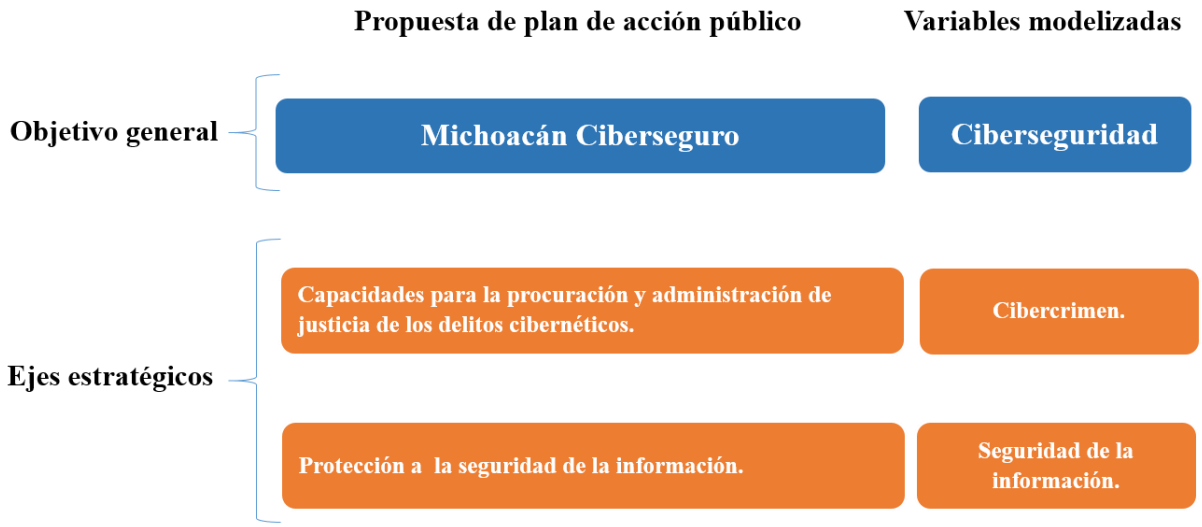
7.3 Propuesta de Política Pública de ciberseguridad en el estado de Michoacán

A continuación se describe el objetivo general, los ejes estratégicos y las acciones que se seguirán, con el fin de alcanzar el objetivo de un Michoacán Ciberseguro y que se resume gráficamente en la ilustración marcada con el número 50.

Objetivo general: **Michoacán Ciberseguro**

Incrementar la capacidad de adaptación frente a situaciones cibernéticas desafiantes en el ciberespacio al Estado, empresas y sociedad, lo que involucra salvaguardar los sistemas de información, asegurar la protección digital de ciudadanos, empresas y gobiernos frente a las amenazas y riesgos.

Ilustración 48. Esquema de iniciativa de Política Pública



Fuente: elaboración propia con base en la literatura.

Los dos ejes estratégicos son el resultado del diagnóstico realizado en la presente investigación y de la importancia de las variables dependientes, las cuales se transforman en estos ejes y sus dimensiones e indicadores forman a su vez objetivos estratégicos y acciones estratégicas. Se describen las acciones estratégicas que se deberán implementar para abordar los desafíos y oportunidades identificadas en cada eje estratégico para lograr una Política Púbica de Ciberseguridad exitosa.

7.3.1 Capacidades para la procuración y administración de justicia de los delitos cibernéticos.

Sustentado en mejorar las habilidades y recursos de las instituciones encargadas de la procuración y administración de justicia para dar una respuesta efectiva a los delitos cibernéticos.

Ilustración 49. Eje 1. Capacidades para la procuración y administración de justicia de los delitos cibernéticos.

Objetivo	Fortalecer las capacidades institucionales y legales para investigar y sancionar eficazmente los delitos cibernéticos.
Acciones estratégicas	
7.2.1.1	Capacitar a los padres de familia para una adecuada supervisión de sus hijos durante la navegación en línea.
7.2.1.2	Brindar especialización técnica y capacitación a los investigadores encargados de perseguir delitos cibernéticos.
7.2.1.3	Disminuir el número de denuncias o incidentes cibernéticos, en el Estado de Michoacán.

7.2.1.4	Concientizar sobre la cibercriminalidad en Michoacán, para evitar que más ciudadanos se conviertan en víctimas.
7.2.1.5	Implementar campañas de sensibilización sobre los riesgos en la navegación de los usuarios para la reducción de la cibercriminalidad.
7.2.1.6	Formar y capacitar a los miembros de los órganos jurisdiccionales especializados en delitos cibernéticos para fortalecer la capacidad de investigación y reducir la incidencia delictiva.

Fuente: elaboración propia con base en los resultados obtenidos en la investigación.

7.3.2 Protección a la seguridad de la información.

Basado en fortalecer la ciberseguridad de las infraestructuras críticas y proteger la seguridad de la información.

Ilustración 50. Eje 2. Protección a la seguridad de la información.

Objetivo	Mejorar y reforzar las medidas de ciberseguridad aplicadas a la infraestructura critica, así como garantizar la seguridad de la información en dichos sistemas.

Acciones estratégicas

7.2.2.1	Crear políticas que fomenten el aprendizaje significativo entre los usuarios y operadores de sistemas de información.
7.2.2.2	Promover la conciencia y adopción de una cultura de seguridad de la información entre los usuarios de sistemas informáticos, aplicaciones y plataformas digitales.
7.2.2.3	Fomentar la creación de equipos de respuesta a incidentes especializados para la pronta recuperación de la operación ante daños cibernéticos.
7.2.2.4	Divulgación los procesos en materia de Seguridad de la Información.
7.2.2.5	Fomentar la realización de auditorías a la infraestructura tecnológica y protocolos entre las organizaciones públicas y privadas.

Fuente: elaboración propia con base en los resultados obtenidos en la investigación.

Por lo tanto el diseño de la propuesta de Política Pública en ciberseguridad, requiere dotar de atribuciones, capacidades, competencia técnica a las diversas instituciones con las que cuenta el Estado. Esto resulta esencial para asegurar una implementación efectiva y coordinada de la Política.

La siguiente ilustración describe el análisis de involucrados, para identificar y comprender a todas las partes interesadas, actores clave que desempeñan un rol en la ciberseguridad, lo cual resulta fundamental para garantizar su pertinencia, legitimidad y efectividad, ya que promoviendo la participación activa de los diferentes involucrados permitirá contar con una política pública más inclusive y exitosa en beneficio de la sociedad.

Ilustración 51. Análisis de involucrados.

Fuente: Elaboración propia con base en los resultados obtenidos en la investigación.

La característica principal de esta propuesta de Política, es que se plasma bajo un documento dinámico, susceptible de modificaciones conforme avance la tecnología, brindando a la sociedad Michoacana la confianza y a la vez el conocimiento sobre el manejo de su información y las tecnologías, para lograr un "**Michoacán ciberseguro**".

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

El presente estudio integra un análisis estadístico descriptivo con un modelo PLS-SEM, lo que proporciona una mayor validez y robustez a la investigación científica en el ámbito de la ciberseguridad. Esta combinación metodológica permitió obtener una comprensión más completa de la naturaleza y las relaciones entre las variables de estudio, así como evaluar las diversas respuestas proporcionadas por los expertos en ciberseguridad a nivel nacional.

En una primera etapa se analizaron las variables Tecnologías de la información y comunicaciones; Aspectos legales; Cibercultura; Cibercrimen; Infraestructuras críticas; y Seguridad de la información, cuyos resultados descriptivos mostraron concordancia de los expertos en ciberseguridad con respecto a la influencia de las seis variables independientes hacia la dependiente la cual fue alta, teniendo que en todas ellas por lo menos se ubicaron en la escala “bastante de acuerdo”, lo que reafirma la relevancia de estas variables para la ciberseguridad en el estado de Michoacán.

En contraposición, el análisis mediante un modelo de ecuaciones estructurales de mínimos cuadrados parciales se revela como un enfoque más potente de evaluación. Este método no solo se enfoca en el análisis de las relaciones entre las variables, sino que también permite una comprensión más profunda del fenómeno de estudio. Esto se logra mediante la realización de validaciones cruzadas (bootstrapping) con múltiples iteraciones, lo que mejora significativamente la capacidad predictiva del modelo.

Al permitir una evaluación más exhaustiva y robusta de las relaciones entre las variables, el análisis con este método ofrece una visión más completa y precisa del modelo de estudio, siendo así que únicamente las variables Cibercrimen y Seguridad de la información influyen significativamente en la ciberseguridad en el estado de Michoacán.

El método de ecuaciones estructurales de mínimos cuadrados parciales (PLS-SEM), A través del análisis matemático permitió identificar los factores determinantes que permiten explicar la ciberseguridad en el contexto de estudio, demostrando la importancia de las variables independientes, al convertirse en dos ejes estratégicos generales: Capacidades para la procuración y administración de justicia de los delitos cibernéticos (Cibercrimen) y Protección a la seguridad de la información (Seguridad de la información), transformándose en líneas generales de acción que guiarán el diseño de la propuesta de Política Pública de Ciberseguridad en el estado de Michoacán.

El modelo PLS-SEM muestra a través del coeficiente de determinación (R2) el poder predictivo de las variables independientes (Cibercrimen y Seguridad de la información) sobre la dependiente

(Ciberseguridad), obteniendo el resultado de .616, lo que nos indica que la variable ciberseguridad se explica en un 61.6% por las variables independientes, comprobándose la fortaleza de las relaciones entre estas.

La combinación de ambas técnicas ha permitido validar las hipótesis planteadas en la presente investigación desde diferentes perspectivas. Esto refuerza la fiabilidad de los resultados y la solidez del marco teórico sobre el que se sustenta la presente tesis.

Por otra parte las implicaciones de los resultados conseguidos en esta investigación son de gran relevancia para la formulación, elaboración y mejora de políticas públicas de ciberseguridad en Michoacán. En primer lugar, la variable Cibercrimen destaca la importancia de Fortalecer las capacidades institucionales y legales para investigar y sancionar eficazmente los delitos cibernéticos.

En segundo lugar, la variable Seguridad de la recalca la necesidad de salvaguardar la protección de datos, activos y sistemas informáticos, así como promover la conciencia sobre la importancia de la seguridad de la información. En este sentido, las políticas públicas deberían orientarse en fortalecer la infraestructura de seguridad de la información, concientizar y crear una cultura de seguridad digital en la sociedad sobre las buenas prácticas y desarrollar estrategias que fortalezcan la ciberseguridad en el estado.

Las conclusiones destacan la contribución de la tesis doctoral al conocimiento actual en el campo de la ciberseguridad para el estado de Michoacán. Se ha logrado una comprensión más integral de los factores determinantes que afectan a la seguridad cibernética y se han identificado enfoques efectivos para abordar estos desafíos, asegurando la protección en el entorno digital. Destacando la relevancia de las variables Cibercrimen y Seguridad de la información en el contexto actual del Estado. Dichos hallazgos acentúan la necesidad de abordar la incidencia delictiva y proteger la información, así como la promoción de guías de buenas prácticas en la protección de la información, la seguridad de los ciudadanos y los activos del estado frente a los múltiples riesgos y amenazas existentes en el ciberespacio. En conjunto está investigación ofrece una base sólida para futuras investigaciones que fortalezcan la ciberseguridad y salvaguarden los intereses de la sociedad michoacana en el ciberespacio.

RECOMENDACIONES

Se identifican áreas que podrían requerir más investigación para una comprensión más profunda del tema de la ciberseguridad, una de ellas, derivada de la omisión de las variables: Tecnologías de la información y comunicaciones, Aspectos legales, Cibercultura e Infraestructuras críticas dentro del modelo por su falta de validez convergente, que a pesar de la importancia de cada una de ellas al soportan los servicios, aplicaciones y comunicaciones que dan vida al ciberespacio, marco normativo para regular las interacciones de los usuarios, la protección de los datos personales, privacidad, nuevas formas de comunicación y la protección a los activos que son indispensables para el funcionamiento de una sociedad y que a pesar de tener una relevancia teórica, tuvieron que ser excluidas del modelo.

Por lo anterior una posible línea de investigación futura, podría ser el explicar ¿Por qué las Tecnologías de la información y comunicaciones, Aspectos legales, Cibercultura e Infraestructuras críticas no resultaron factores determinantes para explicar la ciberseguridad en el estado de Michoacán?

Del valor obtenido del R2, de la presente investigación podemos concluir que existe un 38.4% de relaciones causales que afectan a la ciberseguridad y que no están contempladas en este modelo, por lo cual, futuras líneas de investigación seria identificar ¿Cuáles son estas variables que pudieran explicar de una mejor manera la ciberseguridad en el estado de Michoacán?

La presente investigación enfrento ciertos desafíos respecto a la construcción del marco teórico debido a la falta de información y estudios científicos relaciones con la ciberseguridad dentro de las fronteras nacionales y adecuadas al contexto nacional, por lo que otras futuras líneas de investigación sería realizar estudios más profundos que aborden problemáticas específicas de la ciberseguridad para seguir avanzando en la protección y la seguridad digital.

Las líneas de investigación futuras permitirán profundizar y alcanzar una mejor comprensión de la ciberseguridad y las políticas públicas identificando área de oportunidad para optimizar la seguridad en el ciberespacio en el estado de Michoacán.

La presente investigación resalta la necesidad de una constante evolución en las técnicas y metodologías utilizadas en la investigación en el campo de la ciberseguridad, dado el dinamismo y la complejidad de las amenazas, riesgos y ataques cibernéticos, por lo cual resulta fundamental que los investigadores y expertos en este campo estén a la vanguardia en el empleo de métodos estadísticos y modelos avanzados para abordar estos desafíos de manera integral.

En el contexto actual, la ciberseguridad se ha convertido en una prioridad esencial, sin embargo, las amenazas evolucionan constantemente. Aunque la presente investigación iniciada en el año 2020 no contempla la inteligencia artificial (IA) como amenaza, se reconoce la necesidad de incorporarla en futuras investigaciones, considerando su potencial en la generación de amenazas tales como fake news, suplantación de identidad, generación de imágenes, clonación de la voz y otros ataques cibernéticos.

Analizar la capacidad de la inteligencia artificial para la detección de amenazas cibernéticas en la actualidad e incorporarla para fortalecer la ciberseguridad y que permita contrarrestar los riesgos y amenazas de una manera más eficiente, ya que permite la identificación por medio de patrones maliciosos y anomalías en tiempo real, lo que ayudaría en la detección de ataques cibernéticos y fortalecería la seguridad en el ciberespacio.

BIBLIOGRAFÍA

3ciencias. (10 de agosto de 2012). *3ciencias*. Obtenido de https://www.3ciencias.com/

Abu-Nimeh, S., Becher, M., Fogie, S., Hernacki, B., Morales, J., & Wright, C. (2009). *Mobile Malware Attacks and Defense*. Estados Unidos de América: Syngress Publishing, Inc.

ACUERDO A/009/15 . (12 de febrero de 2015). Diario Oficial de la Federación. México, México: H. CONGRESO DE LA UNIÓN.

ACUERDO por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal. (6 de septiembre de 2001). Diario Oficial de la Federación. México, México: H. Congreso de la Unión.

Aebi, M. F. (2008). *Delincuencia Juvenil.* Catalunya: UOC.

AFCL. (5 de Mayo de 2020). *eluniversal.com.mx*. Obtenido de eluniversal.com.mx: https://www.eluniversal.com.mx/estados/linchan-dos-presuntos-delincuentes-en-puebla

Aguilar, L. F. (1992). *El Estudio de las Políticas Públicas: Colección Antologías de Políticas públicas.* México: Porrúa. Obtenido de Aguilar Villanueva L. F. (1992), ,1992, México, Miguel Ángel Porrúa.

Aguilar, L. F. (1996). *Problemas públicos y agenda de gobierno.* México: Miguel Ángel Porrúa.

Akhgar, B., Gercke, M., Vrochidis, S., & Gibson, H. (2021). *Dark Web Investigation.* Suiza: Springer.

Alberto, B., Eric, M., & Flippo, O. (2018). Evil twins and WPAE enterprisee: a coming security disaster. *Computer & Security*, 18.

Almenara, J. (1998). *Impacto de las nuevas tecnologías de la información y la comunicación en las organizaciones.*

Aloisio, T. &. (2016). La racionalidad en las teorías. *Artículos Académicos* , 280-294.

Altamirano, G. (2017). *Los Derechos Humanos de Cuarta Generación "Un Acercamiento"*. México: CESOP.

Álvarez, G., & Pérez, P. (2004). *Seguridad informática para empresas y particulares.* España: Mc Graw Hill.

Anderson, D., Sweeney, D., & Williams, T. (2008). *Estadística para administración y economía.* Alemania: CENGAGE Learning Editores S.A. de C.V.

ARIMETRICS. (15 de julio de 2021). *arimetrics.com*. Obtenido de https://www.arimetrics.com/glosario-digital/ecommerce

Arimetrics, Agencia Digital. (30 de junio de 2020). *Arimetrics, Agencia Digital*. Recuperado el 8 de agosto de 2022, de arimetrics.com: https://www.arimetrics.com/glosario-digital/evento

Aristoteles. (1988). *Política.* Madrid, España: Gredos.

Asociación Americana de Psiquiatría. (2014). *Guía de consulta de los criterios diagnósticos del DSM 5.* Estados Unidos: Medica Panamericana.

Banco de México. (2018). *Información sobre los ataques a participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI).* Ciuda de México: Banco de México.

Banco Interamericano de Desarrollo. (2020). *Reporte Ciberseguridad 2020.* Washington: Banco Interamericano de Desarrollo.

Barceló, M. (2008). *Una historia de la informática.* Barcelona: UOC.

Bardach, E. (1998). *Los ocho pasos para el análisis de políticas públicas. Un manual para la práctica.* México: Cide - Porrúa.

Barrio, M. (2017). *Ciberdelitos Amenazas criminales del ciberespacio.* Madrid: REUS.

Beekman, G. (2005). *Introducción a la Informática.* Madrid, España: Pearson Prentice Hall.

Bunge, M. (2013). *La Ciencia su Método y su Filosofía.* España: Laetoli.

Cabrera, M. Á. (2010). *Evolución tecnológica y cibermedios.* Sevilla, España: Comunicación Social S.C.

Calder, A. (2013). *A pocket guide.* Estados Unidos: IT Governance Publishing.

Calderón, B. (2017). *Deep & Dark Web.* Río de Janiero : Alta Books.

Callanan, C., & Tropina, T. (2015). *Self-and Coregulatión in Cybercrime, Cybersecurity and National Security.* Londres: Springer.

Càmara Arroyo, S. (2020). Estudios Criminòlogicos contemporàneos (IX): La Cibercriminologìa y el perfil del ciberdelincuente. *Derecho y Cambio Social*, 470-512.

Capace Gómez, A. L. (08 de 06 de 2015). *Crimipedia*. Recuperado el 28 de 06 de 2022, de Crimipedia: https://crimipedia.umh.es/topics/teoria-del-control-gottfredson-y-hirschi/

Carbonell, M. (2014). *México en la encrucijada: ¿modernidad o barbarie?* México: Floreseditor.

Carbonell, M., & Vázquez, R. (2003). *Poder, derecho y corrupción.* México: Siglo XXI editores Argentina S.A. de C.V.

Carrique, A. (2005). El ciberamor y sus estrategias. *redalyc.org*, 27.

Centeno, D. (2018). México Y El Convenio De Budapest Posibles Incompatibilidades. En D. Centeno, *México Y El Convenio De Budapest Posibles Incompatibilidades* (pág. 3). México: R3D Y DERECHOS DIGITALES DE AMÉRICA LATINA.

Centro de estudios en técnicas de Evaluación Legislativa. (2014). *Impacto social y económico de la implementación de política públicas en la sociedad.* Bogota: Univesidad Militar Nueva granada.

Chávez , G. (8 de Julio de 2020). *Expansión "Tecnologia"*. Obtenido de Expansión "Tecnologia": https://expansion.mx/tecnologia/2020/07/08/que-implicaciones-tuvieron-los-ciberataques-a-banxico-y-condusef

CISCO Secure. (Julio de 2020). *CISCO Secure*. Obtenido de CISCO Secure: https://www.sonicwall.com/resources/2020-cyber-threat-report-mid-year-update-pdf/

CN-CERT. (febrero de 2007). *CN-CERT*. Obtenido de CN-CERT: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=196.html

Código Penal Federal. (24 de Enero de 2020). Diario Oficial de Federación . México: Cámara de Diputados H. Congreso .

Código penal para el Estado de Michoacán. (19 de noviembre de 2022). Diario Oficial de la Federación. México, Michoacán, México: CONGRESO DE MICHOACÁN DE OCAMPO.

Comisión permanente dek Ho. Congreo de la Unión. (2017). *Convenio de Budapes.* México: H. Congreso de la Unión.

Constitución Política de los Estados Unidos Mexicanos. (08 de Mayo de 2020). Diario Oficial de la Federación . México: Cámara de Diputados del H. Congreso de la Unión .

Coordinación General de Protección Civil. (15 de julio de 2021). *Coordinación General de Protección Civil*. Obtenido de cgproteccioncivil.edomex.gob.mx: https://cgproteccioncivil.edomex.gob.mx/fenomenos_perturbadores

Costas, J. (2014). *Seguridad y alta disponibilidad.* España: Ra-Ma.

Council of Europe. (2001). *Convenio sobre la Ciberdelincuencia.* Hungría: Council of Europe.

Cronbach, , L. (1951). Coefficient alpha and the internal structure of tests. psychometrika. *Psychometrik*, 37.

De la Cuesta, J. L., Pérez , A., & Guillén, C. (2010). Ciberdelincuentes y cibervíctimas. En *Aspectos criminológicos y victimológicos.*

De Leeuw, K., & Bergstra, J. (2007). *The History of Information Security.* Amsterdam: Elsevier.

De Sosa, J. (2014). ¿Qué es una adicción? desde las adicciones con sustancias a las adicciones comportamentales. *Revista digital de medicina psicosomática y psicoterapia*, 28.

decide. (20 de junio de 2022). *decidesoluciones.es*. Obtenido de https://decidesoluciones.es/encicloped-ia/#ii

Definición.DE. (15 de julio de 2021). *Definición.DE*. Obtenido de https://definicion.de/

Delgado , L. (2009). ocumentación sobre gerencia pública, del Subgrupo A2, Cuerpo Técnico, especialidad de Gestión Administrativa, de la Administración de la Junta de Comunidades de Castilla-de la Mancha. *Escuela de Administración Regional.*

Desmurget, M. (2020). *La Fábrica de cretinos digitales Los peligros de las pantallas para nuestros hijos.* Francia: Grupo Planeta.

Deutsch, V. (2022). *Ciber seguridad para Directivos.* España: Almuzara.

Di Tullio, B. (1966). *Principios de Criminologia Clínica y Psiquiatría Forense.* Madrid, España: Aguilar.

Diario Oficial De La Federación. (06 de Noviembre de 2013). Obtenido de Diario Oficial De La Federación: https://www.dof.gob.mx/nota_detalle.php?codigo=5301941&fecha=11/06/2013

Diario Oficial De La Federación. (04 de Febrero de 2016). Obtenido de Diario Oficial De La Federación: http://dof.gob.mx/nota_detalle.php?codigo=5424367&fecha=04/02/2016

Diccionario de la lengua española. (18 de abril de 2019). *Real academia española*. Obtenido de https://dle.rae.es/ciber-

Díez, C. (2005). Procesos culturales, una apoximación desde la antropología social y cultural. *Norba Revista de Historia*, 24.

Digital Jurista. (30 de 01 de 2020). *Ciber & Law*. Obtenido de Ciber & Law: https://aicyberlaw.com/2020/01/iniciativa-busca-reconocer-ataques-ciberneticos-como-amenazas-a-la-seguridad-nacional/

Dimas, G. A. (2017). *Los Derechos Humanos De Cuartageneración "Un Acercamiento"*. México: CESOP.

Durkheim, E. (1895). *Las reglas del método sociológico.* México: Fondo de cultura económica México.

Echeburúa, E., & De Corral, P. (2010). Adicción a las nuevas tecnologías y a las redes sociales en jóvenes: un nuevo reto. *Adicciones*, 7.

Echeburúa, E., & Requesens, A. (2012). *Adicción a las redes socilaes y nuevas tecnologías en niños y adolescentes.* Madrid, España: Pirámide.

Echeverria, B. (2013). *¿Qué es la modernidad?* México: Unam (Universidad Nacional Autonoma De Mexico).

Ecomipedia. (12 de julio de 2021). *Ecomipedia haciendo facíl la economía*. Obtenido de https://economipedia.com/definiciones/activo.html

EDEX CRC. (09 de febrero de 2016). *e-legales*. Obtenido de e-legales: https://e-legales.net/glosario-de-terminos/

El mundo.es. (21 de Marzo de 2009). Obtenido de El mundo.es: https://www.elmundo.es/elmundo/2009/04/21/navegante/1240297753.html

El sol de Morelia. (15 de agosto de 2022). Obtenido de www.elsoldemorelia.com.mx: https://www.elsoldemorelia.com.mx/local/sin-protocolos-ni-medidas-de-prevencion-gobiernos-de-michoacan-expuestos-a-ciberataques-8738275.html

Ellis, R., & Mohan, V. (2019). *Rewire Cibercecurity Governance.* USA: Wiley .

ENDUTIH, INEGI e IFT. (31 de Julio de 2023). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares.* Ciudad de México: INEGI. Obtenido de https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/15%2BEstudio%2Bsobre%2Blos%2BHa_bitos%2Bde%2Blos%2BUsuarios%2Bde%2BInternet%2Ben%2BMe_xico%2B2019%2Bversio_n%2Bpu_blica.pdf

ESET. (25 de Septiembre de 2020). *welivesecurity.com.* Obtenido de welivesecurity.com: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

Estado, G. d. (2015-2021). *Plan De Desarrollo Integral Para El Estado De Michoacán.* Michoacán De Ocampo.

Estrada, A. C. (2017). *Ciberseguridad Una Estrategia Informatico DigitaL.* Madrid: DARFE.

Expansión. (09 de Julio de 2020). *Expansión* . Obtenido de Expansión : https://expansion.mx/economia/2020/07/09/sat-ataque-cibernetico-descarta-danos-a-contribuyentes#:~:text=El%20SAT%20sufre%20ataque%20cibern%C3%A9tico%3B%20descarta%20da%C3%B1os%20a%20contribuyentes,-El%20Servicio%20de&text=El%20SAT%20destac%C3%B3%20que%20l

Federación Rusa. (2021). *Política Estatal de la Federación de Rusia.* Rusia.

Fernández, B. (2010). *Las redes sociales: lo que hacen sus hijos en internet.* España: Club Universitario.

Fernández, N. (7 de octubre de 2008). *Retro Informática El Pasado Del Futuro*. Obtenido de Retro Informática El Pasado Del Futuro: https://www.fib.upc.edu/retro-informatica/historia/internet.html

Ferreyra, E. (2018). *La Convención De Cibercrimen De Budapest Y De América Latina (Volumen 1).* Creative Commons.

Ficha Técnica Ley Olimpia. (s.f.). Obtenido de http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

Franco, F. (2018). *El lado oscuro de las redes Sociales: Amenazas, peligros y riesgos en el uso de las redes sociales.* España: Independently published.

Friedman, S. P. (2014). *Cybersecurity and cyberwar "what everyone needs to know".*

Frieiro, R., P, P., & X, P. (Junio de 2017). *Deloitte México*. Obtenido de Deloitte México: https://www2.deloitte.com/mx/es.html

Fundación Telefónica. (2014). *Las TIC en la educación digital del tercer milenio* . Madrid, España: Ariel S.A. de C.V.

Galindo, L. (2006). Cibercultura, sistémica y comportamiento contemporaneo. En G. L.J, *Explotando las posibles fuentes conceptuales de un pensamiento emergente.* Colombia: Revista Q.

Galo, E., & Cano, P. (2018). Las TICS en las empresas: Evolución de la Tecnología y cambio estructural en las organizaciones. Ecuador: Dominio de las Ciencias.

García, M. C., Rojas, A., Cuadro, I., García, M., Fernández, J., Navas, M., . . . Sánchez, J. (2004). *Estrategias y actitudes de aculturación:la perspectiva de los inmigrantes y de los autóctonos en Almería.* España: Ediciones Al Sur, s.c.a.

Gartner. (17 de Junio de 2022). *gartner.com*. Obtenido de gartner.com: https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem

Gerardo, P., & Emilio, D. P. (2001). *Auditoría Informática un enfoque práctico.* Madrid, España: RA-MA.

Gob.mx. (2019). *www.gob.mx*. Obtenido de www.gob.mx: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

Gobierno Constitucional del Estado de Michoacán de Ocampo. (2020). *Acuerdo número 78.* Morelia, Michoacán: Secretaría de Gobierno.

Gobierno de España. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica.

Gobierno de España. (2019). *Estrategia de Ciberseguridad Nacional.* España: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019.

Gobierno de Estados Unidos de América. (2018). *National Cyber Strategy.* Estados Unidos.

Gobierno de la República. (2017). *Estrategia Nacional de Ciberseguridad*. Obtenido de gob.mx

Gobierno de México. (2019). *Plan Nacional de Desarrollo 2019 - 2024.* México: Secretaría de Hacienda y Crédito Público.

Gobierno de México. (15 de julio de 2021). *Gobierno de México*. Obtenido de https://www.gob.mx/cenapred/articulos/sabes-que-es-una-emergencia-radiologica?idiom=es

Gobierno de Michoacán. (2021). *Plan de Desarrollo Integral del Estado de Michoacán 2021-2027.* Morelia, Michoacán: Gobierno de Michoacán.

González , N. (14 de Noviembre de 2019). *Excelsior*. Obtenido de Excelsior: https://www.excelsior.com.mx/nacional/pemex-no-pagara-por-ciberataque-lopez-obrador-hackeo-no-fue-tan-grave/1347669

Goodman, M. (2016). *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World.* Estados Unidos: Anchor Books.

Google Inc. (20 de agosto de 2021). *Google maps.* Obtenido de https://www.google.com/maps/place/M%C3%A9xico/@23.3128659,-107.1825221,6z/data=!4m9!1m2!2m1!1sgoogle+maps+mapa+de+la+republica+mexicana!3m5!1s0x84043a3b88685353:0xed64b4be6b099811!8m2!3d23.6344598!4d-102.5518799!15sCilnb29nbGUgbWFwcyBtYXBhIGRlIGxhIHJlcHVi

Granadillo, A. (2019). *Tería del delito y el Estado Social y Democrático de Derecho.* Barcelona: Bosch Editor.

Guanyabens, J. (2020). Las TIC y la salud. *Universidad Oberta de Catalunya*, 52.

Gutiérrez, E. (2021). *Delitos informáticos: Análisis detallado de las conductas delictivas más comunes en el entorno informático.* España: Colex reader.

Gutiérrez, F. (4 de junio de 2003). *fergut.com*. Obtenido de https://www.fergut.com/sobre-las-reformas-y-adiciones-a-diversas-disposiciones-de-la-legislacion-federal-mexicana-en-materia-de-comercio-electronico/

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking.* Indianapolis, Indiana: Wiley Publishing, Inc.

Hair, J., Black, W., Babin, B., & Anderson, R. (2017). *Análisis de datos multivariados.* Estados Unidos: Pearson Prentice Hall.

Hair, J., M. Hult, T., Ringle, C., Sarstedt, M., Castillo, J., Cepeda, G., & Roldán, J. (2017). *Manual de Parcial Least Squares Structural Equation Modeling.* Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE Publications, Inc.

Harris, M. (1989). *Teorías sobre la cultura en la era posmoderna.* España: ed-critiica.es.

Hernández, R., Fernández, C., & Baptista, P. (2010). *Metodología de la investigación.* México: Mc Graw Hill.

Hidglobal.mx. (18 de julio de 2021). *www.hidglobal.mx*. Obtenido de https://www.hidglobal.mx/products/all-categories/hid-proximity

Hikal, W. (2017). La Teoría de la asociación diferencial para la explicación de la criminalidad y la articulación de una política criminal. *Derecho y Cambio Social*, 1-15.

Huertas Díaz, O. (2010). Anomia, normalidad y función del crimen desde la perspectiva de Robert Merton y su incidencia en la criminología. *Revista Criminalidad*, 365-376.

Huidobro, J. (2020). *Wi-fi 6 y 7 / Móviles 5G y 6G Redes de fibra óptica.* México.: Alfaomega.

Ibarra, R., & Serrano, M. (1999). *Principios de teoría de las comunicaciones.* México: Limusa S.A. de C.V.

IBM. (25 de noviembre de 2021). *¿Qué es la ciberseguridad?* Obtenido de IBM: /www.ibm.com/mx-es/topics/cybersecurity

Incibe. (1 de abril de 2019). *incibe.es*. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Incibe.es. (31 de octubre de 2020). *incibe.es*. Obtenido de incibe.es: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Instituto de Nacional de Estándares y Tecnologías. (2019). *Ciberseguridad marco NIST.* EEUU: White paper series edición 5.

Instituto Nacional de Antropología e Historia. (2015). *Guía para emitir documentos normativos 2015.* México: INAH.

ISO. (30 de Diciembre de 2014). *Normas ISO*. Obtenido de Normas ISO: https://www.normas-iso.com/iso-27001/

ISO 9000:2015. (15 de agosto de 2005). *ISO*. Obtenido de iso.org: https://www.iso.org/obp/ui/es/#iso:std:iso:9000:ed-3:v1:es

itmastersmag. (22 de septiembre de 2020). *www.itmastersmag.com*. Obtenido de https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/

Jara, H., & Pacheco, F. (2012). *Ethical hacking 2.0.* Buenos Aires, Argentina: Fox Andina.

Jessop, B. (2014). El Estado y el poder. *Utopía y Praxis Latinoamericana*, 19-35.

Jessop, B. (2017). *El Estado. Pásado, presente, futuro.* Madrid, España: Los libros de la Catarata.

Kalaharshaa, P., & Mehtr, M. (2021). Detecting Phishing Sites - An Overview. *Cornell University*, 13.

kaspersky.com. (18 de julio de 2021). *https://latam.kaspersky.com*. Obtenido de https://latam.kaspersky.com/resource-center/definitions/biometrics

Kelsen, H. (2020). *Teoría pura del Derecho.* Buenos Aires: Universitaria de Buenos Aires.

Kennedy M, D. (2016). *Disuasión y prevención del delito. reconsiderando la expectativa de la pena.* Madrid.

La Voz de Michoacán. (24 de agosto de 2021). *La Voz de Michoacán.com.mx*. Obtenido de https://www.lavozdemichoacan.com.mx/michoacan/morelia-appmobil/hackean-al-ayuntamiento-de-morelia-ciberdelincuentes-piden-rescate-en-bitcoins/

Laniel, J. (2021). *Diez razones para borrar tus redes sociales de inmediato.* Estados Unidos: Penguin Random House.

Lasswell , H. (2017). *El futuro de la ciencia política.* Nueva York: Routledge.

Lasswell, H. (2005). *The Future of Political Science.* Estados Unidos: Routledge.

Lenoir, R. (02 de Octubre de 2017). *El Confidencial*. Obtenido de El Confidencial: https://www.elconfidencial.com/mundo/2017-10-02/batalla-estatua-estonia-ciberguerra-rusia_1451408/

León, M. (2004). *Diccionario de Informática, telecomunicaciones y ciencias afines.* España: Edigrafos S.A.

Lévy, P. (2007). *Cibercultura.* México: Anthropos.

Lewis, J. A. (2016). *Experiencias avanzadas en politicas y practicas de ciberseguridad.* Miguel Ángel Porrúa .

LEXICO. (15 de julio de 2021). *www.lexico.com*. Obtenido de https://www.lexico.com/es/definicion/post

Ley General de Protección Civil. (6 de junio de 2012). Diario Ofcial de la Federación. México, México: H. Congreso de la Unión.

LGSNSP. (2 de enero de 2009). Diario Oficial de la federación. México, México: CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN.

Lindblom, C. (1959). *La ciencia de salir del paso teoría de la organización.* Public Administration Review,. Obtenido de Lindblom e. Charles, la ciencia del «salir del paso», Teoría de la organización 1959, Public Administration Review,

LISA Institute. (28 de Octubre de 2019). *Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación*. Obtenido de LISA Institute: https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

LLamas, J. (14 de septiembre de 2020). *Foro jurídico*. Obtenido de https://forojuridico.mx/el-estatus-de-mexico-y-el-convenio-sobre-la-ciberdelincuencia-de-budapest/

Luna, A. (2014). *Administración Estratégica.* México: Grupo Patria.

Malagón, D., & Herrera, L. (2019). *Ciberterrorismo: La jerarquia y evolución del poder.* España: Academia española.

Martínez, M. (12 de noviembre de 2018). *BBC NEWS*. Obtenido de https://www.bbc.com/mundo/noticias-america-latina-46178633

Mattioli, R., & Levy, C. (2014). *Methodologies for the identification of Critical Information Infrastructure assets and service.* Grecia: Unión Europea.

McKinsey & Company and COMEXI. (2018). *Perspectiva de Ciberseguridad en México.* México: McKinsey & Company and COMEXI.

Mendoza, G. E. (2006). *Teoria y ciclo de las políticas publicas.*

México, G. d. (2019). *Plan Nacional De Desarrollo Estado De México 2019-2024.* México.

Miguel, J. C. (2015). *Protección de datos y seguridad de la información.* España: Ra-Ma.

Mittelman, J. H. (2002). *El Síndrome de la Globalización (Transformación y resistencia).* México: Siglo veintiuno editores.

Molano, O. (2007). Identidad cultural un concepto que evoluciona. *Opera*, 69-84.

Molina, J., & Vecina, P. (2015). *Bullying, ciberbullying y sexting, ¿Cómo actuar ante una situación de acoso?* España, Madrid: Pirámide.

Molist, M. (21 de Enero de 2016). *elconfidencial.com*. Obtenido de https://www.elconfidencial.com/: https://www.elconfidencial.com/tecnologia/2016-01-21/amenazas-en-la-oscuridad-como-los-hackers-pueden-provocar-un-apagon-en-tu-ciudad_1138837/

Morales, T., Serrano, M., & Santos, A. (2016). *Ciberbullying y delitos invisibles Experiencias psicopedagógicas.* Ciudad de México: Universidad Autónoma del Estado de México.

nist.gov. (12 de junio de 2021). *https://www.nist.gov/*. Obtenido de https://www.nist.gov/

Oliva, J., & Escobedo, A. (2013). El concepto de impunidad, su abordaje en los instrumntos de Derecho Internacional de los Derechis Humano, Derecho Internacional Humanitario y Derecho Penal Internacional. *Universidad Carlos III de Madrid*, 260.

Oñate, M. (2014). Aislamiento y Patología inherente. *Aequitas*, 83.

Ortíz, D. M. (2012). *Diversidad Cultural.* Estado de México: Red Tercer Milenio S.C.

Ovejero, A. (2015). Psicología Social e Identidad: Dificultades para un análisis Psicosociológico. *Papeles del CEIC*, 18.

Pacheco, M. L. (2012). *Tecnología de información y comunicación.* Ciudad de México: Visión tipográfica editores S.A. de C.V.

Páez, D., González, J., Torres, N., & Zubieta, E. (2000). *Identidad cultural, Aculturación y Adaptación de los Inmigrantes Latinoamericanos (chilenos).* Chile: Centro Cultural Chileno PABLO NERUDA.

Parada, R. A., & Errecaborde, J. D. (2018). *Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet.* Buenos Aires, Argentina: ERREIUS.

Patino, B. (2020). *La civilización de la memoria de pez.* Madrid: Alianza.

Pérez, L. (2016). CARTAS O EPÍSTOLAS Y CORREOS ELECTRÓNICOS. *Revista de Direito da Faculdade Guanambi*, 11-43 file:///C:/Users/lap3/Downloads/Dialnet-CartasOEpistolasYCorreosElectronicos-7065405.pdf.

Pérez, S. M. (2008). LA INFRAESTRUCTURA Y LA COPETITIVIDAD DE MÉXICO. En S. M. PÉREZ, *LA INFRAESTRUCTURA Y LA COPETITIVIDAD DE MÉXICO.* MÉXICO: CESOP.

Pesce, L. (2011). La contribución de la Cibercultura a la educación en línea. *Dialnet*, 8.

Pessino, M. (2017). Las políticas en ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN). *(Tesis de Licenciatura).* Universidad Siglo 21, Argentina.

Pierre, L. (2007). *Cibercultura La cultura de la sociedad digital.* México: Anthropos.

Piragof, D. (2013). La suplantación de identidad. *Visión Criminológica-criminalística*, 147.

Plan de Desarrollo Integral para del Estado de Michoacán 2015-2021. (2015). Michoacán de Ocampo: Gobierno del Estado de Michoacán de Ocampo.

Popper , N., & Conger, K. (20 de JULIO de 2020). *infobae*. Obtenido de infobae: https://www.infobae.com/america/the-new-york-times/2020/07/20/los-hackers-cuentan-la-historia-del-ataque-intestino-a-twitter/

Porter, M. E. (1991). *Ventaja Competitiva.* Buenos Aires, Argentina: Rei Argentina S.A.

Presidencia de la República . (2019). *Plan Nacional De Desarrollo Estado De México 2019-2024.* México.

Puig, E. (2017). *El dorado. Una historia critica de internet.* Madrid, España: Clave intelectual ci.

Quijano, M. C., Arango, J. C., & Cuervo, M. T. (2010). Alteraciones cognitivas, emocionales y comportamentales a largo plazo con trauna craneoencefálico en Cali, Colombia. *Revista Colombiana de Psiquiatría*, 16.

Ramírez, C. (2010). *Fundamentos de Administración.* Bogota, Colombia: ECOE.

Rayón , M., & Gómez, J. (2014). Cibercrimen: particularidades en su Investigación y Enjuiciamiento. *Anuario Jurídico y Económico Esculiarense*, 209-234.

Real Academia Española. (2019). *Diccionario de la Lengua Española.* Madrid.

Reglamento de la Ley General de Protección Civil. (9 de agosto de 2015). Diario Oficial de la Federación. México, México: Cámara de Diputados H. Congreso.

República de Estonia. (22 de 04 de 2020). *https://www.mkm.ee/et*. Obtenido de https://www.mkm.ee/et: https://www.mkm.ee/en/objectives-activities/cyber-security

Resiliencia Sísmica. (15 de julio de 2021). *www.resilienciasismica.unam.mx*. Obtenido de https://www.resilienciasismica.unam.mx/conceptos.html#:~:text=La%20capacidad%20de%20un%20sistema,una%20mejor%20protecci%C3%B3n%20futura%20y

Reyes, L. (2012). *Introducción al estudio del Derecho.* México: Red Tercer Milenio.

Rodríguez Manzanera, L. (1981). *Criminología.* México: Porrua.

Rodríguez, D. (2016). *Aplicaiones de Google.* Madrid, España: RA-MA.

Roth, A. (2002). *Políticas Públicas: Formulación, Implementación y Evaluación.* Bogotá: Ediciones Aurora.

Rovira, Á. (27 de Mayo de 2013). *Álex Rovira*. Recuperado el 20 de 06 de 2022, de Álex Rovira: https://www.alexrovira.com/soluciones/articulo/la-teoria-de-las-ventanas-rotas

Ruiz, M., & De Juanas, Á. (2013). Redes sociales, identidad y adolescencia: nuevos retos educativos para la familia. *Estudios sobre la educación*, 21.

Rusa, C. d. (12 de 04 de 2021). *http://www.scrf.gov.ru/*. Obtenido de http://www.scrf.gov.ru/: http://www.scrf.gov.ru/security/information/document114/

Sala de Comisiones de la Cámara de Senadores . (2021). *Dictamen de la comisión de relaciones exteriores (https://comisiones.senado.gob.mx/relaciones_exteriores/reu/docs/dictamen3_250221.pdf).* México: Senado de la República.

Santillán, M. L. (12 de 01 de 2015). *Ciencia UNAM.* Recuperado el 26 de 06 de 2022, de Ciencia UNAM: https://ciencia.unam.mx/leer/418/Ciberbullying_perfil_de_victimas_y_victimarios#:~:text=Alguien%20que%20es%20v%C3%ADctima%20de,est%C3%A1%20hablando%20sobre%20su%20persona.

Santos, O. (2019). *Developing Cybersecurity Programs and Policies.* Estados Unidos: Pearson Education, Inc.

Sanz, E., & Fernandez, D. (2021). *Tratado de Delincuencia Cibernética.* España: ARANZADI / CIVITAS.

Schneier, B. (2019). *Haz clic aquí para matarlos a todos.* Estados Unidos: Ediciones temas de hoy.

Secrataría de Gobernación. (24 de 03 de 2020). *https://www.dof.gob.mx*. Obtenido de https://www.dof.gob.mx/nota_detalle.php?codigo=5590339&fecha=24/03/2020#gsc.tab=0

Secretaría de Comunicaciones y Transportes. (2019). *Estudio sobre hábitos de los usuarios en ciberseguridad en México.* México: Secretaría de Comunicaciones y Transportes.

Secretaría de Comunicaciones y Transportes. (2019). *Hábitos de los usuarios en ciberseguridad en México* . México: SCT.

Secretaría de Gobernación. (2013). *PLAN NACIONAL DE DESARROLLO 2013-2018.* México: Secretaría de Gobernación.

Secretaría de Gobernación. (2014). *PROGRAMA NACIONAL DE SEGURIDAD PÚBLICA 2014-2018.* México: Secretaría de Gobernación.

Segundo , O. (27 de Junio de 2017). *CB Televisión*. Obtenido de CB Televisión: https://cbtelevision.com.mx/el-virus-golden-eye-obliga-a-cerrar-parte-del-puerto-de-lazaro-cardenas/

Senado de la República. (04 de Mayo de 2021). *http://comunicacion.senado.gob.mx*. Obtenido de http://comunicacion.senado.gob.mx: http://comunicacion.senado.gob.mx/index.php/informacion/boletines/50936-senado-pide-informe-sobre-estrategia-de-ciberseguridad.html

Serra, A. (2016). *Ciencia Política la proyección actual de la teoría general del Estado.* México: Porrua.

Serrano, M. M. (2007). Evolución e Historia en el desarrollo de la comunicación humana. En *Evolución e Historia en el desarrollo de la comunicación humana.* Madrid, España: McGraw-Hill .

Sevillano, F., Rodríguez, A., Valencia, A., Echave, E., Sánchez , S., Matilla, E., & De Pablo, E. (2021). *Ciberseguridad Industrial e Infraestructuras Críticas.* Bogotá, Colombia: RA-MA.

Siobhan, G., August, C., & Dreazen, Y. (21 de Abril de 2009). *The Wall Street Journal*. Obtenido de https://www.wsj.com/: https://www.wsj.com/articles/SB124027491029837401

SonicWall. (2022). *Cyber Threat Report.* Estados Unidos: SonicWall.

Sonicwall. Inc. (2022). Informe de amenazas cibernéticas. *Sonicwall*, 66.

Steinberg, J. (2019). *Cybersecurity for dummies.* Estados Unidos: Wiley India.

Strauss, L. (1958). *Antropología estructural.* París: Plon, París.

Suárez, R. (2007). *Tecnologías de la Información y la Comunicación.* Madrid, España: Ideaspropias.

Tamayo y Tamayo, M. (2004). *El proceso de la investigación científica.* México: LIMUSA NORIEGA EDITORES.

Tarde, G. (2011). *Las leyes de la imitación y la sociología.* Madrid: Centro de investigaciones sociológicas.

Tecno Accesible. (15 de julio de 2021). *Tecno Accesible*. Obtenido de www.tecnoaccesible.net: https://www.tecnoaccesible.net/technology/computing-platform#:~:text=En%20inform%C3%A1tica%2C%20una%20plataforma%20es,con%20los%20que%20es%20compatible.&text=Al%20definir%20plataformas%20se%20establecen,o%20interfaz%20de%20usuario%20compatibles.

Téllez, J. (2008). *Derecho Informático.* México: Mc Graw Hill.

The White House. (12 de enero de 2013). *obamawhitehouse.archives.gov*. Obtenido de https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Tonkonoff, S. (2016). La sociología criminal de Gabriel Tarde. *Delito y Sociedad, revista de ciencias sociales.*, 22.

Tonkonoff, S. (2020). La sociología criminal de Gabriel Tarde. *Delito y Sociedad, revista de ciencias sociales.*, 22.

UNESCO. (20 de mayo de 2012). *Oficina de la UNESCO en México*. Obtenido de http://www.unesco.org/new/es/Mexico/work-areas/culture#:~:text=...la%20cultura%20puede%20considerarse,sociedad%20o%20un%20grupo%20social.

Unión Internacional de Telecomunicaciones. (Noviembre de 2010). *Unión Internacional de Telecomunicaciones*. Obtenido de Unión Internacional de Telecomunicaciones: https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

Valle, R. R. (1986). *Tecnologías de la información: electrónica, informática y telecomunicaciones.* Madrid : FUNDESCO.

Velásquez , R. (Junio de 2009). *www.redalyc.org*. Obtenido de https://www.redalyc.org/: https://www.redalyc.org/pdf/3596/359633165006.pdf

Véliz, C. (2021). *Privacidad es poder: Datos, vigilancia y libertad en la era digital.* España: Debate.

Vergara, M., & Huidobro, J. M. (2016). *Las tecnologías que cambiaron la historia.* España: Ariel, S.A.

Vidal Herrero-Vior, M. (2016). *Delincuencia Juvenil "online": el menor infractor y las tecnologías de la información y la comunicación.* Lisboa: Juruá.

Villar, A. M. (2006). *Introducción a la Informática y al uso y manejo de aplicaciones comerciales.* España: Ideaspropias.

Watkins, S. (2013). *An introduction to Information Security and ISO27001:2003.* Estados Unidos: IT Governance Publishing.

X-Force Threat. (2018). *ibm.com/security*. Obtenido de https://www.ibm.com/security

Anexo 1. Aspectos legales.

Se describe a continuación el marco legislativo en materia de Ciberseguridad en México y en el Estado de Michoacán que soporta la presente investigación;

Constitución Política de los Estados Unidos Mexicanos.

Actualmente en el Estado Mexicano, los tratados internacionales de los que el Estado Mexicano sea aparte se encuentran en igualdad jerárquica con la constitución política de los Estados Unidos Mexicanos, así como de las garantías que le protegen, dentro de la legislación mexicana se busca prevalecer el acceso de igualdad, gracias a los derechos humanos de la cuarta generación, pero en ningún momento en la legislación mexicana, existen leyes que regulen todas las conductas delictivas cometidas a través de los dispositivos digitales.

El artículo 6° de la Constitución Política de los Estados Unidos, párrafo III, "El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios" (Constitución Política de los Estados Unidos Mexicanos, 2020).

Pero en ningún momento habla de legislación que regule el uso de las tecnologías de la información, solo se menciona el libre acceso al que todos tengan la posibilidad respetando el derecho de la igualdad, pero olvidando brindar seguridad e información adecuada sobre el uso de los dispositivos digitales.

Ley de Seguridad Nacional

Con la iniciativa del 29 de enero del 2020, por parte de la diputada María Eugenia Hernández, quien propone hacer una reforma a los artículos 5 y 6 de la Ley de Seguridad Nacional, para adicionar a dichos artículos las fracciones XIV y XV al artículo 5 y la fracción VI, al artículo 6, con la finalidad de: Reconocer a los ataques cibernéticos como amenazas a la seguridad Nacional, Crear una estrategia de defensa a los ataques cibernéticos y Fomentar la cooperación internacional en torno a la ciberseguridad como política exterior. (Digital Jurista, 2020).

Ley General del Sistema Nacional de Seguridad Pública

Artículo 19.- El Centro Nacional de Información será el responsable de regular el Sistema Nacional de Información y tendrá, entre otras, las siguientes atribuciones:

- Determinar los criterios técnicos y de homologación de las Bases de Datos que conforman el Sistema Nacional de Información;
- Emitir los lineamientos de uso, manejo y niveles de acceso al Sistema Nacional de Información;

- Conocer, integrar y analizar las Bases de Datos del Sistema Nacional de Información, en términos de los lineamientos que al efecto emita;
- Vigilar el cumplimiento de los criterios de acceso a la información y hacer del conocimiento de las instancias competentes cualquier irregularidad detectada;
- Brindar asesoría a las Instituciones de Seguridad Pública para la integración y uso de la información de las Bases de Datos al Sistema Nacional de Información (Gob.mx, 2019).

Código Penal Federal.

Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que, sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.
Artículo 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

Artículo 211 Bis. - A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Capitulo II Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien, estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno (Código Penal Federal, 2020).

Dentro de las reformas que se han hecho a la legislación mexicana, hablaremos de la denominada “Ley Olimpia”, misma que no se refiere a una ley en particular, sino la reforma de un conjunto de legislaciones enfocadas al reconocimiento de la violencia digital, así como la sanción de los delitos que violen la intimidad sexual de las personas a través de los medios digitales “Ciber violencia” Entre los Estados que han tipificado la conducta; Aguas Calientes, Baja California, Baja California Sur, Chiapas, Ciudad de México, Coahuila, Durango Guanajuato, Guerrero, Estado de México, Michoacán, Nuevo León, Oaxaca, Puebla, Querétaro, Veracruz, Yucatán y Zacatecas. (Ficha Técnica Ley Olimpia).

Plan Nacional de Desarrollo 2013 – 2018.

El gobierno mexicano ha plasmado la problemática que desea combatir, pero dentro de sus lineamientos, solo hace alusión a la cobertura amplia del internet, jamás brindando herramientas para el uso de las tecnologías, o asumiendo la responsabilidad y el compromiso que tiene con la sociedad y no ve más allá que el combatir el derecho a la igualdad, dejando de lado la protección dela información a través de leyes o reformas a estas que puedan brindar seguridad a la nación misma, dentro del plan nacional podemos darnos cuenta que, “El Plan Nacional de Desarrollo (PND) es, en esta perspectiva, un instrumento para enunciar los problemas nacionales y enumerar las soluciones en una proyección sexenal”. (México, 2019, pág. 5).

Que en traducción de Jessop (Jessop B. , 2014) , los problemas que al gobierno en turno le interesan para ser solucionados, son específicos, quedando otros sin la posibilidad de generar una política o simplemente de formar parte de la agenda pública del gobierno, tal parece que el Estado no logra ver la situación real y preocupante con el incremento de las conductas delictivas empleadas a través del uso de las tecnologías y los grandes problemas y detrimentos económicos que afectan al Estado, y que solo dan lugar a más índice delictivo y no soluciones reales.

A pesar de que el Plan Nacional de Desarrollo refiere que a través de un documento plasmara los objetivos que se propone alcanzar y los medios para lograrlo, en materia de cibercriminalidad y del uso de las Tecnologías no hubo acción alguna que vaya a adoptar para dar solución a ese tipo de problemas, es decir, dentro de la agenda no se encuentra plasmado.

Código Penal Del Estado de Michoacán.

En la actualidad existen delitos que se pueden considerar "tradicionales", pero que se dan a través de dispositivos digitales y que los servidores públicos del Estado de Michoacán buscan encuadrar en las leyes penales, para que puedan ser combatidos. (Ley No. 355, Periódico Oficial del Estado de Michoacán, 13 enero 2020).

Plan De Desarrollo Integral del Estado de Michoacán.

El plan de Desarrollo Integral del Estado de Michoacán 2015-2021, en su eje estratégico Tranquilidad, Justicia y Paz. "La tranquilidad y paz es una aspiración de cualquier sociedad. Proteger los derechos humanos de los ciudadanos está en el centro de las acciones de cualquier gobierno Para lograr lo anterior se plantea dentro de su línea estratégica 2.2.3 Abatir la violencia y la delincuencia y en la acción 2.2.3.3 Utilizar las TIC's para difundir la paz y resolución de conflictos" (Estado, 2015-2021).

"las tecnologías de la información y comunicaciones son herramientas que permiten nuevas formas de gestión gubernamental, contribuyen a la eficiencia de los servicios públicos, favorecen la cooperación a distancia entre distintos actores y fortalecen la confianza y la seguridad entre sociedad y gobierno. Esta transformación del gobierno y la modernización de su gestión, fortalecen la democracia participativa". (Plan de Desarrollo Integral para del Estado de Michoacán 2015-2021, 2015).

Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones

El 8 de Mayo del 2014, se publicó en el Diario Oficial de la Federación (DOF) el acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional en materia de Tecnologías de la Información y Comunicaciones , y en la de seguridad de la Información, así como establecer el

Manual Administrativo de Aplicación General en dichas materias, donde se establecen los mecanismos para el almacenamiento y gestión de información sensible y de seguridad nacional que manejan las Instituciones de Gobierno. (Diario Oficial De La Federación, 2016)

MAAGTICSI es el principal Manual en materia de Tecnologías de la Información y Comunicación (TIC) de la Administración Pública Federal (APF) en México, ya que establece nuevas obligaciones derivadas del Plan Nacional de Desarrollo 2013-2018 (PND), decreto de disciplina presupuestaria y sus respectivos lineamientos en materia de TIC.

De acuerdo con el decreto publicado en el Diario Oficial de la Federación el 11 de junio de 2013, el Estado Mexicano garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. (Diario Oficial De La Federación, 2013).

Anexo 2. Comparación de códigos penales.

En cada tabla se describe la similitud en la manera de aborda los ciberdelitos en los países que se analizaron, lo que permitirá ver la forma de abordar los delitos que se cometen en el ciberespacio.

Tabla 32. Cuadro comparativo tipo penal: Ataques al honor.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Ataques al honor.	Código Penal y Legislación Complementaria. Delitos contra el honor cometidos mediante transmisiones electrónicas. Artículos. 30, 205, 206 y 207.	Difamación (No existe normativa federal en esta materia, por lo que sólo se regula a nivel estadual y de (Common law.) Art. 499-a.	El Código Penal de la Federación Rusia Difamación. Artículo.130 Calumnia. Artículo 128.1.	Código Penal Federal Artículo. 282. (Delitos contra la paz y seguridad de las personas.) Delitos contra el honor. (Derogado).	Ataques al honor Artículo 192. (Artículo 193. Punibilidad) Código penal del Estado de Michoacán.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

La calumnia para España, ataques al honor para México y Michoacán, difamación para Rusia, es el mismo delito que obedeciendo a su contexto social actual busca que la reputación de un individuo no se transgreda, mientras que Rusia y Michoacán incorporan en este delito el empleo de cualquier medio de difusión, no obstante en México no se cuenta con mecanismos de vinculación que obliguen a los proveedores de las plataformas digitales a proporcionar la información o al retiro de la misma, aunado el anonimato que estas ofrecen, vuelven compleja la posibilidad de su imputación.

Tabla 33. Cuadro comparativo de tipo penal: Fraude.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Fraude.	Código Penal y Legislación Complementaria. Defraudación mediante telecomunicación y uso ilegal de equipo terminal de telecomunicación. Artículos. 255, 256 y 623.4 Estafa por medios informáticos. Código Penal y Legislación Complementaria. Estafa por medio informático. Artículo. 248	Fraude y falso testimonio. Artículos 1028, 1028 a, 1029-30, 1037. Fraude por correspondencia y otros delitos de fraude. Artículo 1343.	El Código Penal de la Federación de Rusia. Fraude**.** Artículo 159.	Código Penal Federal. Fraude. Artículo 386.-	Código Penal del Estado de Michoacán. Fraude. Artículo. 217.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

Los delitos que se cometen en las legislaciones Estadounidense, Rusia y española especifican los medios o dispositivos electrónicos, para la comisión de delitos, adicional en su legislación, España contempla la Estafa por medios informáticos en la comisión de este delito, los principales elementos son el engaño y el

error del que se hacen valer el o los sujetos activos para poder llevar aquel acto que termine dañando al sujeto pasivo, la manipulación informática se encuentra implícito dentro de este articulo como un apartado, así mismo habla de aquel que fabrique posea o facilite programas informáticos que tengan la finalidad para la comisión de estafas.

En México no existe la legislación necesaria para enfrentarse a esta nueva modalidad de delitos a través de medios cibernéticos, los cuales se dan a través del empleo de las TIC´s, con el envió de un correo electrónico, un link o un código malicioso para aprovechar el desconocimiento o error de los usuarios y afectarlos en su patrimonio.

Tabla 34. Cuadro comparativo de tipo penal: Ataques a la imagen.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Ataques a la imagen.	Código Penal y Legislación Complementaria. Artículo 197. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio capítulo I del descubrimiento y revelación de secretos.	Injurias calumniosas. Artículos 491, 492 y 494	El Código Penal de la Federación de Rusia. Usar a un menor con el propósito de hacer materiales o artículos pornográficos. Artículo 242.2.	No tipificado	Código Penal del Estado de Michoacán. Ataques a la imagen**.** Artículos 196 y 197.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

A comparación de las legislaciones estadounidense, rusa y española, la legislación mexicana y la michoacana se han enfocado en aquellos ataques contra la intimidad por medios cibernéticos, mientras que las demás, en aquellos medios electrónicos que se vean involucrados para dañar la imagen de las personas, ya sea para atacar la imagen propia, intimidad, descubrir algún secreto personal o familiar. Este avance es significativo, sin embargo es importante la creación de mecanismos de vinculación los proveedores de servicios, con la finalidad de aportar la información del perfil o cuenta y que esta información pueda ser retirada de las plataformas digitales.

Tabla 35. Cuadro comparativo de tipo penal: Ataques a la intimidad.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Ataques a la intimidad.	Código Penal y Legislación Complementaria Artículo 197. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Del descubrimiento y revelación de secretos.	Código penal de la policía civil nacional. Artículos. 300 y 559	Ley Federal de la Federación Rusa. Acerca de datos personales.	No tipificado	Código penal del Estado de Michoacán. Art. 194. Ataques a la intimidad

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

Las cinco legislaciones revisadas tipifican el delito de ataques a la intimidad como el acto de revelar datos personales, aunque la legislación española señala la extracción de datos personales a través del correo electrónico, así como la intercepción de telecomunicaciones, se han logrado avances significativos en este delito en el Estado de Michoacán, sin embargo se requieren; modificaciones a las leyes, mecanismos de vinculación, para que los proveedores de servicio, proporcionen la información y el retiro del contenido publicado.

Tabla 36. Cuadro comparativo de tipo penal: Pornografía infantil.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Pornografía infantil.	Código Penal y Legislación Complementaria. Artículo 189. De los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores. Particularmente la difusión de pornografía infantil a través de la red.	Código de los Estados Unidos. Articulo. 1466 a. Representaciones visuales obscenas del abuso sexual de niños.	Código Penal de la Federación de Rusia. Artículo 242.2. Usar a un menor con el propósito de hacer materiales o artículos pornográficos.	Código Penal Federal. Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo. Artículos 202 y 202 bis.	Código Penal del Estado de Michoacán. Pornografía de personas menores de edad. Artículo. 158.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

La tipificación de este delito muestra similitud de elementos en las legislaciones, los componentes claves y que igualan a la tipología son la forma de divulgar el contenido, que se hace a través de las diversas plataformas digitales de manera masiva, mensajería instantánea, así como la complejidad para la imputación del hecho dado el anonimato que brinda la red.

Tabla 37. Cuadro comparativo de tipo penal: Trata de personas.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Trata de personas.	Código Penal y Legislación Complementaria. Artículo 188, 607 Bis. 9 De los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores.	Código de los Estados Unidos. . Articulo. 1591. Tráfico sexual de niños o por la fuerza fraude o coerción.	Código Penal de la Federación de Rusia Trata de personas. Artículo 127.1.	Código Penal Federal. Artículo 205. (Derogado.) 205-bis y 206 Bis.	Código Penal del Estado de Michoacán. Artículos. 161 y 162 Trata de personas.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

Las cinco legislaciones tienen parecido en cuanto a las características que describen el delito, pero en la actualidad el uso del internet como medio de comunicación ofrece el anonimato, donde se hacen pasar por

otra personas para contactar a personas desde cualquier parte del mundo, permite a los tratantes establecer contacto para captar a niños, adolescentes con ofertas de empleo, estudios, modelaje, desencadenando en secuestro, rapto o desaparición, sin elementos que permitan sancionar este delito cuando se comete por medios cibernéticos.

Tabla 38. Cuadro comparativo de tipo penal: Amenazas.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Amenazas.	Código Penal y Legislación Complementaria. Artículos 169, 170 y 171. De las amenazas.	Código penal de la policía civil nacional. Artículos. 322 y 596.	No tipificado	Código Penal Federal Artículo 282 343 bis, 343 ter, 283, 284 y 284 bis.	Código Penal del Estado de Michoacán. Amenazas. Art.187

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

La característica del delito es el intento de causar daño, por medio de amenazas. En España si especifica incluso si estas se realizan por teléfono u otro medio de comunicación o de reproducción, y en el caso de México y Michoacán no se hace referencia cuando el medio empleado es a través de redes sociales, mensajería instantánea o equipos móviles, es necesario reformas leyes para q crear una regulación específica por la modalidad que presentan.

Tabla 39. Cuadro comparativo de tipo penal: Instigación o ayuda al suicidio.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Instigación o ayuda al suicidio.	Código Penal y Legislación Complementaria. Del homicidio y sus formas Artículo. 143.	Código de los Estados Unidos. De la apología del delito. Artículo 387.	El Código Penal de la Federación de Rusia. Inducir o facilitar el suicidio**.** Artículo 110.1.	Código Penal Federal. Reglas comunes para lesiones y homicidio Artículo 312, 313.	Código Penal del Estado de Michoacán. Inducción al suicidio. Artículo 138 y139. Inducción o ayuda al suicidio de persona menor de edad. Artículo 140.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

La legislación rusa hace referencia a los consejos, instrucciones o información que se le pudiera brindar a la víctima (aunque no precisa a través de que medio), por otro lado, la legislación michoacana, tipifica en su artículo 140. Inducción o ayuda al suicidio o de persona menor de edad, señalándolo como homicidio calificado o en su defecto de no haberse llevado acabo por lesiones calificadas, pero no especifica en relación a utilizar el ciberespacio como medio de instigación al suicidio, los retos virales que utilizan las

TIC´s bajo la apariencia de juegos inofensivos han causado la muertes a niños y jóvenes, por eso es necesario legislar al respecto contra quienes los crean y fomentan en el ciberespacio.

Tabla 40. Cuadro comparativo de tipo penal: Ciberacoso/sexual

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Ciberacoso/ sexual **Acoso sexual.**	Código Penal y Legislación Complementaría. Artículo 184.	No tipificado	No tipificado	No tipificado	Código Penal del Estado de Michoacán. Acoso sexual Artículo. 169 Bis.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

El principal elemento es la relación laboral que ya se mantienen o que se está buscando y por consecuente todas aquellas situaciones emocionales y hasta psicológicas por las que la víctima puede llegar a pasar, otro elemento importante es la vulnerabilidad de la víctima, en la legislación mexicana no se contempla cuando este acto se realiza a través de redes sociales, mensajería instantánea o dispositivos móviles.

Tabla 41. Cuadro comparativo de tipo penal: Sexting.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Sexting.	Código Penal y Legislación Complementaria. Artículo 183 De los abusos y agresiones sexuales a menores de dieciséis años.	No tipificado	El Código Penal de la Federación de Rusia. Usar a un menor con el propósito de hacer materiales o artículos pornográficos. Artículo 242.2.	Código Penal Federal. Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo. Artículo 202, 202 Bis.	Código penal del Estado de Michoacán. Violencia digital a la intimidad sexual. Artículo 195.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

En la era digital, el sexting empezó como una conducta de riesgo con el surgimiento de las TIC´s y que se da como un acto de intercambio de mensajes de contenido sexual, presente en todas las edades. Por lo que la respuesta de algunas de las legislaciones aquí presentes ha sido favorable, al incluir esta conducta en la agenda pública y ver la necesidad de modificar las leyes y que esta conducta sea castigada.

Tabla 42. Cuadro comparativo de tipo penal: Delitos contra la libertad y el normal desarrollo psicosexual.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Delitos contra la libertad y el normal desarrollo psicosexual	Código Penal y Legislación Complementaria	No tipificado	No tipificado	Código Penal Federal.	Código Penal del Estado de Michoacán.

(hostigamiento sexual, abuso sexual, estupro y violación).	De los abusos sexuales artículos 181 y 182. De los abusos y agresiones sexuales a menores de dieciséis años. Artículo 183 y 183 Bis.			Hostigamiento sexual, abuso sexual, estupro y violación. Artículo 259 Bis.	Hostigamiento sexual. Art 169.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

El hostigamiento sexual en México y Michoacán es perseguido de oficio, por otro lado para España y su legislación sí se encuentra una gama más amplia en su legislación, no solo de acoso, sino la manera de abuso en donde los elementos que maneja la tipología de este delito describe desde la forma "no violenta" de cometerlo, "la violenta" y además especifica el contacto que puede existir entre un adulto con un menor de 16 años de edad y dependiendo la finalidad que sea del adulto para con este, así será el castigo. México y Michoacán han avanzado en este tema al incluirlo en la agenda pública y el cual ya está siendo incluido en los tipos penales de los estados.

Tabla 43. Cuadro comparativo de tipo penal: Extorsión.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Extorsión.	Código Penal y Legislación Complementaria. De la extorsión. Artículo 243.	No tipificado	No tipificado	Código Penal Federal. Extorsión. Artículo 390.	Código Penal del Estado de Michoacán. Extorsión. Artículos. 224 y 225.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

Los elementos principales de este ilícito son la violencia o la intimidación y, aunque últimamente la forma de cometer muchos delitos, el surgimiento de las TIC´s ha permitido que los delincuentes naveguen por los perfiles para seleccionar a sus víctimas, obtener datos, incluso fotografías, y así una vez con la información necesaria proceden a la consecución del delito, que en el mejor de los casos termina con un depósito en una tienda de conveniencia y en otros logran que la víctima salga de su domicilio para encentrarse con ellos y posteriormente ser secuestrados, situación por la cual se vuelve imperante el legislar sobre esta modalidad en el delito de extorsión.

Tabla 44. Cuadro comparativo de tipo penal: Violación de correspondencia.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Violación de correspondencia.	Código Penal y Legislación Complementaria. Artículo 535. De los delitos cometidos por los funcionarios públicos contra la	No tipificado	No tipificado	Código Penal Federal. Artículos 173.	Código Penal del Estado de Michoacán. Artículos. 294

	inviolabilidad domiciliaria y demás garantías de la intimidad**.** Del descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional Artículo 603. De la detención y apertura de la correspondencia escrita y telegráfica artículo 579.			Violación de correspondencia.	Violación de correspondencia o información.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

España, México y Michoacán cuentan con la tipificación del delito de violación de correspondencia, en el primero, con la creación de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD), se protege la intimidad, integridad y privacidad de sus ciudadanos, sin embargo en la legislación mexicana y michoacana se especifica que solo el tutor puede realizar esta acción sin que se cometa el delito. Por otra parte, la legislación hace la tipificación del delito en temas de defensa nacional, secuestro, delincuencia organizada, extorsión, así como la justificación mediante orden judicial, sin embargo no se habla de cuando estas se realicen a través de medios cibernéticos y en qué casos es permitida la conservación de datos.

Tabla 45. Cuadro comparativo de tipo penal: Violación de comunicación privada.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Violación de comunicación privada.	Código Penal y Legislación Complementaria. Artículo 560. De los desórdenes públicos	Intercepción de comunicaciones electrónicas y por cable e intercepción de comunicaciones orales. Artículos 2510-22. Comunicaciones almacenadas por cable y electrónicas y acceso a registros transaccionales. Artículos 2701-2712.	No tipificado	Código Penal Federal Artículos 165, 166, 166 Bis. Ataques a las vías de comunicación y violación de correspondencia.	Código Penal del Estado de Michoacán. Articulo. 295. Violación de comunicación privada.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

La interrupción de la comunicación privada es un delito, en donde se especifica que aquella persona que irrumpa en las comunicaciones privadas y que además emplee la información obtenida en beneficio propio, en el caso de México se deben especificar los casos y particularidades, debido a que cuando se trata de las comunicaciones por correo electrónico, se debe garantizar la protección legal de la comunicación, que actualmente no está definida en el CNPP.

Tabla 46. Cuadro comparativo de tipo penal: Corrupción de personas menores de edad.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Corrupción de personas menores de edad.	Código Penal y Legislación Complementaria. Artículo 188 y 189. De los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores.	Ley no. 105 De los delitos de proxenetismo y corrupción de menores. Art… 2	El Código Penal de la Federación de Rusia, Artículo 242.2. Usar a un menor con el propósito de hacer materiales o artículos pornográficos.	Código Penal Federal Artículo 200, 201 y 201 Bis. Corrupción de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo.	Código Penal del Estado de Michoacán. Articulo. 156 Corrupción de personas menores de edad. Artículo 157. Corrupción de personas menores de edad mediante su empleo.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

La tipificación de este, delito corrupción de menores, muestra similitud de elementos en las legislaciones. La aparición del internet ha permitido nuevas formas de comunicación, interacción y con ello; la creación y distribución de videos, fotografías, revistas, sitios web a través de la red, al amparo del anonimato que ofrecen las plataformas digitales, situación que en México no se contempla, lo que hace más difícil la imputación de este tipo de conductas.

Tabla 47. Cuadro comparativo de tipo penal: Acceso ilícito a sistemas y equipo de informática.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Acceso ilícito a sistemas y equipos de informática.	Código Penal y Legislación Complementaria. Daños a datos, programas o documentos electrónicos. Artículo. 264.2.	No tipificado	El Código Penal de la Federación de Rusia Acceso ilegal a información informática. Artículo 272.	Código Penal Federal. Acceso ilícito a sistemas y equipos de informática. **A**rtículos 211 bis al 211 bis 7.	No tipificado

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

La tipificación de esta conducta delictiva en la legislación de Rusia tiene implícitos los siguientes elementos: la destrucción, bloqueo, modificación o copia de información informática y daño importante cometido por interés egoísta. Para la legislación española los elementos de este delito son: a quien borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos ajenos, que la acción haya ocasionado daños o consecuencias en la infraestructura y esto a su vez pusiera en peligro grave la seguridad del estado europeo. Mientras que dentro de la legislación mexicana los elementos son, la destrucción, modificación o pérdida de información contenida en equipos informáticos protegidos por

algún mecanismo de seguridad, pero se deben hacer modificaciones, en caso de que el equipo no tenga mecanismo de seguridad no se impondrá sanción, con lo que contradice la importancia del bien jurídico que es la información contenida en sistemas informáticos.

Tabla 48. Cuadro comparativo de tipo penal: Sabotaje.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Sabotaje.	No tipificado	Código de Estados los Unidos Artículos. 2151, 2152, 2152, 2154, 2155 y 2156	El Código Penal de la Federación de Rusia Sabotaje. Artículo 281.	Código Penal Federal. Sabotaje. Artículo 140.	Código penal del Estado de Michoacán. Sabotaje. Artículo 314.

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

Esta acción delictiva repercute principalmente en el sector económico de los países, ya que las tres legislaciones la rusa, la mexicana y la michoacana tipifican este delito como una acción cometida en contra del Estado, ya que obstaculiza las vías de comunicación, edificios gubernamentales, afectando diversas clases de actividades, como lo son la exportación, importación y demás producciones que son necesarios para el país, siendo importante que se adicione incluyendo las TIC´s en la comisión de este tipo de delito.

Tabla 49. Cuadro tipo penal: Impacto inadecuado en la infraestructura de la información.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Impacto inadecuado en la infraestructura de información	No tipificado	No tipificado	El Código Penal de la Federación de Rusia. Impacto inadecuado en la infraestructura de información crítica de la federación de Rusia. Artículo 274.1.	**Infraestructuras críticas.** Artículo 5 fracción XII Ley de seguridad nacional México.	No tipificado

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

Rusia en su legislación considera que el uso, creación y la distribución de programas informáticos podría dar un golpe considerable en su infraestructura, por eso es necesario estar protegidos en temas de Seguridad Nacional que puedan llegar a ser un problema real para la nación, mientras que para la legislación mexicana surge la preocupación de todas aquellos temas que puedan llegar a obstaculizar su actuar en temas de defensa Nacional, sin considerar la distribución, utilización, replica de programas informáticos para atentar contra la confidencialidad, integridad y disponibilidad de los sistemas de información e infraestructura tecnológica.

Tabla 50. Cuadro comparativo tipo penal: Delitos contra la propiedad intelectual.

Delitos /legislaciones	España	Estados unidos	Rusia	México	Michoacán
Delitos contra la propiedad intelectual de los programas o **Contra la neutralización de sus dispositivos de protección.**	Código Penal y Legislación Complementaria. Delitos contra la propiedad intelectual de los programas o Contra la neutralización de sus dispositivos de protección. **Artículo 270.**			Código Penal Federal. Artículo 424 bis	

Fuente: Elaboración propia con base en los códigos penales revisados (2010).

La legislación española enlista la reproducción, el plagio, la distribución o publicación de alguna obra literaria, artística, artística o científica y como principal elemento es la obtención de un beneficio económico a cambio , siendo este de forma directa o indirecta, por otro lado, la legislación mexicana, busca proteger aquellas obras, evitando su reproducción, introducción, transporte, distribución, venta, a aquel que fabrique de forma dolosa y con la finalidad de desactivar un dispositivo de protección de un programa de computación, es necesaria la autorización del derecho de autor.

Del análisis realizado podemos observar la discrepancia entre los diferentes tipos penales con los que cada país aborda el fenómeno de la ciberdelincuencia. México desde 1999 en su capítulo III, denominado Acceso Ilícito a Sistemas y Equipo Informático del Código Penal Federal ha incluido algunos de los delitos y cada entidad federativa cuenta con su propio Código Penal, cada uno de ellos legisla los delitos como mejor lo considera, donde observamos que las legislaturas de cada entidad están trabajando en esta materia para regular estos delitos, muchas de ellas tomando como modelo el Código Penal Federal.

Aunado a lo anterior en el cuadro se presentan diferentes conductas típicas, antijurídicas y punibles que nos son consideradas como tal por las diferentes demarcaciones territoriales y geopolíticas, sin embargo esto no implica que dichas conductas no se lleven a cabo dentro del Estado de Michoacán.

Anexo 3. Prueba piloto (mayo 2021).

Como un primer momento se realizó una prueba piloto en la presente investigación, se utilizó la recolección de datos mediante un instrumento de medición, que se aplicó a diecisiete expertos en ciberseguridad. Dada la distancia se empleó el uso de Google Forms, herramienta automatizada que permite la interacción a distancia, se le solicito a los encuestados algunos datos generales que permitan identificar a que parte de la muestra corresponden: nombre, estado, dependencia en la que laboran, tal y como lo muestra el formulario https://docs.google.com/forms/d/e/1FAIpQLSfbdWMQuIs5tWwWCnqApciqG5oKCEe0R2CC3W_Ta6I_TKTQzQ/viewform, cuidando en todo momento la seguridad de la información recabada.

La estrategia que se va a emplear para documentar esta investigación, es a través de un modelo de análisis multivariado (mínimos cuadrados), con el software STATA, cuya finalidad es probar la existencia de una correlación directa entre las variables independientes y la dependiente, para proporcionar un análisis más aproximado de la realidad en ciberseguridad, realizada a este grupo de expertos.

4.4.1 Descripción del instrumento

Dentro del cuestionario que se aplicó en la presente investigación existen apartados específicos para detectar todos aquellos datos que son relevantes, que ofrecerán un escenario más amplio de la incidencia delictiva y con ellos estar en condiciones de realizar análisis estadísticos y posteriormente correlacionarlos de manera que nos permitan realizar conclusiones acertadas.

Para medir el instrumento se utilizó la escala tipo Likert, la cual asigna puntuación matemática a cada uno de los ítems lo que permite distinguir su grado de importancia, es un método utilizado en las ciencias sociales por Likert (1932) quien explica que es un instrumento de medición en la recolección de datos de tipo cuantitativos para temas de investigación, cada uno de los ítem refleja lo que el investigador quiere medir de cada uno de los encuestados y las respuestas obtenidas tienen una calificación asignada, donde se le asigna un valor numérico y medir la importancia del tema objeto de estudio, en este caso intentaremos explicar la importancia de la ciberseguridad.

En la siguiente tabla se presenta la operacionalización de las variables, en las que se muestra de izquierda a derecha, en primer lugar la variable dependiente objeto de la presente investigación, variables independientes, definiciones conceptuales, dimensiones, indicadores y por último los ítems, para comprobar la hipótesis de esta investigación.

Tabla 51. Operacionalización de las variables

Apartado	Variable dependiente	Variables indepedientes	Definición conceptual	Dimensiones	Indicadores	ITEMS	key
I	POLÍTICA DE CIBERSEGURIDAD EN EL ESTADO DE MICHOACÁN	Tecnologías de la información y de las comunicaciones	Pacheco (2012) define a las tecnologías de la información y comunicación como el conjunto de principios y teorías que facilitan la interacción de datos entre usuarios y dispositivos conectados en distintos puntos geográficos y esto es posible a la automatización de los datos, para aplicarles un valor el cual posteriormente es almacenado, procesado y difundido a través de señales electromagnéticas por distintos medios de comunicación.	Hardware (terminales, medios de transmisión y redes) y Software	Políticas	1	THFSRC
					Lineamientos, estrategias o	2	TMTRIMI
					Normas y estandares	3	TSNERC
					Virus, caballos de troya,	4	TSVCRC
					Desarrollos de Hardware y Softwa	5	TSDSRV
					Ataques	6	THARCPC
					Riesgos	7	THSRAC
					Conexione y enlaces	8	TSDWRC
					Inteligencia artificial y el IOT	9	TSIAITRC
II		Aspectos Legales de la Ciberseguridad	Contar con marcos normativos adecuados al contexto actual, capaces de regular los actos que se generan en el ciberespacio, a partir del reconocimiento del uso de las tecnologías de la información y comunicaciones, garantizando los bienes jurídicos, tales como; el patrimonio, la vida, integridad y la privacidad.	Legislación nacional, legislación internacional y normativa	Legislación técnica	10	ALTPC
					Cooperación internacional	11	ALCIPD
					Normativa	12	ANPDC
					Protección de datos personales	13	ALNIPDP
					Proveedores de ISP	14	ALNIPISP
					Delitos	15	ALDCVU
III		Cibercultura	Para Marvin Harris (1989), la cultura es el conjunto de prácticas y formas socialmente aprendidas de la vida, que se construye en las sociedades de acuerdo a sus vivencias diarias, las cuales incluyen una mezcla de sentimientos, pensamientos, conducta y el desenvolvimiento de los integrantes de una sociedad.	Conocimiento Aprendizaje	Cultura	16	CCDCMC
					Prevención	17	CAPRI
					Incorporación a planes	18	CCIPEC
					Aprendizaje	19	CAPRCI
					Concientización	20	CACCMC
IV		Cibercrimen	Téllez (2008), en su libro Derecho Informático, menciona el concepto típico de delitos informáticos: "son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin"; y en el concepto atípico menciona que "son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin". Desde un punto particular, se podría definir al delito informático como "el acto u omisión que es realizado utilizando cualquier medio electrónico y que es sanción.	Conductas especializadas Computadoras como medio o fin	Cibercriminalidad	21	CCECCRI
					Riesgos seguridad nacional	22	CCERSN
					Intervención de comunicaciones	23	CCEINTC
					Legalidad	24	CCETIC
					Conductas especializadas	25	CCMFLL
					Mecanismos estratégicos	26	CHSME
					Clasificación de delitos		
					Marcos normativos	27	CCEMNV
V		Infraestructuras criticas	La Ley General del Sistema Nacional de Seguridad Pública en su artículo 146, (2009) define a las instalaciones estratégicas, como todos aquellos activos y servicios (edificios, áreas estratégicas, servidores, bases de datos, Sistemas industriales, información, redes de datos, entre otros) que son vitales en las actividades diarias de una sociedad y las tendientes a salvaguardar la soberanía de un país.	Tipos de riesgos Amenazas Nivel de impactos Tipo de activo Protocolos	Ataques	28	ICSSIAIC
					Esquemas de ciberseguridad	29	ICENSPA
					Activos	30	ICCAPA
					Clasificación	31	ICCAC
					Mecanismos estratégicos	32	ICGMEC
					Servicios críticos	33	ICSCCE
					Protocolos industriales	34	ICGPIIC
					Planes de recuperación	35	ICPRIAIC
VI		Seguridad de la información	Según Rayan y Vivek, "la Seguridad de información está preocupada por la protección de la confidencialidad, integridad y disponibilidad de información en general, para satisfacer las necesidades del usuario de información aplicable". También incluye el aseguramiento de la información, que trata con los principios subyacentes de evaluar qué información puede o debe protegerse.	Educación proactiva Educación reactiva	Divulgación	36	SIEPDSI
					Aprendizaje	37	SIEPGAS
					Políticas	38	SIEPPSI
					Protocolos	39	SIEPFSO
					Buenas prácticas	40	SIERBPSI
					Controles	41	SIERCSFL
					Procesos	42	SIERPDSI
					Equipos de respuesta	43	SIERERI
					Planes de recuperación	44	SIERPR
VII		Política de Ciberseguridad	Perspectiva del Gobierno Mexicano partiendo del surgimiento de las TIC´S como vehículo para el desarrollo político y económico de la nación, la penetración de internautas y su interconectividad en el ciberespacio, aunado a los riesgos asociados a su utilización y la creación de una cultura de ciberseguridad (Gobierno de la República, 2017).	TIC´s, AL, CC, CCRI, IC, SI	Agenda de Gobierno	46	PCAG
					Dimensiones económicas	47	PCDE
					Cultura digital	48	PCCD
					Ambiente de seguridad	49	PCAS
					Problemas sociales	50	PCPS

Fuente: Elaboración propia con base en experiencia y metodología revisada 2021.

En la siguiente tabla se muestra la propuesta de instrumento de medición que se utilizó para la recolección de datos, misma que se utilizara para realizar los diagnósticos necesarios para la consecución del Diseño de una política en ciberseguridad en el Estado de Michoacán, el instrumento está dividido en siete rubros,

del I al VI son las variables independientes y en el apartado VII la variable dependiente, como se muestra a continuación:

Tabla 52. Propuesta de instrumento de medición.

Apartado	Variable dependiente	Variables independientes	Dimensiones	Indicadores	Mencione que tan de acuerdo está con las siguientes afirmaciones o enunciados. para la Política de Ciberseguridad	Núm. ITEM
I	CIBERSEGURIDAD	Tecnologías de la información y de las comunicaciones	Hardware (equipos terminales), Software (servicios) y redes de comunicación.	Amenazas lógicas	El incremento de amenazas lógicas y sistemas desactualizados provoca daños significativos a los equipos, infraestructura tecnológica e información.	1
				Protocolos	La ausencia de protocolos para abordar las amenazas físicas o lógicas, puede dificultar la recuperación después de un incidente de seguridad.	2
				Fortalecimiento en las TIC´s.	El fortalecimiento a las tecnologías de la información y comunicaciones, podría incidir favorablemente en la disminución de vulnerabilidades que enfrentan los activos ante diversas amenazas.	3
				Estándares, guías de buenas prácticas y herramientas especializadas.	La implementación de medidas como estándares, guías de buenas prácticas y herramientas especializadas, resulta fundamentales en la identificación y mitigación de amenazas de los usuarios en su navegación.	4
				Actualizaciones	Implementar estrategias orientadas a promover y fomentar la actualización de hardware y software, reduce los riesgos asociados a la exposición de vulnerabilidades.	5
				Análisis de vulnerabilidades	Es importante que los creadores de tecnologías emergentes consideren de manera proactiva la seguridad, con el objetivo de prevenir y reducir el riesgo de vulnerabilidades y amenazas que puedan ser explotadas en su implementación.	6
II	CIBERSEGURIDAD	Aspectos Legales de la Ciberseguridad	Legislación nacional, internacional y normativa.	Frecuencia y calidad de las actualizaciones legales. Legislación en materia de cooperación internacional.	Legislar sobre el diseño, fabricación y uso de las tecnologías de la información y comunicaciones, contribuiría a asegurar que estas tecnologías sean seguras y confiables.	7
					El desconocimiento de las implicaciones prácticas, técnicas y legales en el desarrollo y creación de tecnologías de la información y comunicaciones, conduce a la falta de legislación en este campo.	8
					El fortalecimiento al marco normativo por parte de las autoridades, permitiría contar con mayores capacidades en la investigación, persecución y sanción de los delitos informáticos.	9
					La adecuación de la legislación local a los marcos y tratados internacionales podrá contribuir a la disminución de incidentes de ciberseguridad.	10
					Armonizar, tipificar e incrementar las penas con respecto a los delitos cometidos por medio de las tecnologías de la información y comunicaciones, contribuirá a disminuir los riegos de los usuarios.	11
III	CIBERSEGURIDAD	Cibercultura	Conocimiento Aprendizaje	Nivel de conciencia Nivel de conocimiento Organizaciones públicas y privadas. Campañas de concientización Guías de buenas prácticas	La actualización personal sobre temas de seguridad en internet es básico para usarlo sin exponerse a riesgos.	12
					Para evitar ser víctimas de los riesgos en el ciberespacio, es importante la concientización sobre las amenazas en línea y tomar medidas proactivas para protegerse.	13
					Para promover el desarrollo de una cultura digital, es importante considerar la creación de organizaciones, tanto públicas como privadas, que contribuyan a este objetivo.	14
					Es esencial implementar medidas que fomentan una comprensión profunda por parte de los usuarios, para evitar riesgos y vulnerabilidades al navegar en línea.	15
					Las campañas en diversos medios de comunicación para concientizar sobre la creación de una cultura digital, incrementaría la seguridad al momento de navegar.	16
					El desarrollo e implementación de guías de buenas prácticas para la navegación de los usuarios en el ciberespacio puede ser muy beneficioso y es un aspecto importante de la seguridad en línea.	17

Fuente: Elaboración propia con base en experiencia y metodología revisada 2021.

IV	CIBERSEGURIDAD	Cibercrimen	• Prevención • Investigación • Persecución • Judicialización	Nivel de supervisión	La ausencia de una debida supervisión por parte de los padres de familia, propicia la realización de variadas acciones de riesgo durante la navegación en línea.	18
				Nivel de especialización	La falta de especialización técnica y capacitación de los investigadores encargados de perseguir delitos cibernéticos puede llevar a que los delincuentes queden impunes.	19
				Incidencias o casos registrados	El número de denuncias o incidentes cibernéticos, son un reflejo del estado de cibercriminalidad en Michoacán.	20
				Campañas	La ausencia de campañas de sensibilización sobre los riesgos en la navegación de los usuarios contribuye al aumento de la cibercriminalidad.	21
				Existencia de órganos especializados	La creación de un órgano judicial especializado en delitos cibernéticos, podría ser una estrategia efectiva para reducir la incidencia de la cibercriminalidad.	22
				Capacitaciones	La formación y capacitación de los órganos jurisdiccionales es	23
				Existencia o creación de centros de respuesta	La creación de un centro de contención, respuesta e investigación especializada de delitos cibernéticos ayudaría a disminuir la cibercriminalidad.	24
V	CIBERSEGURIDAD	Infraestructuras críticas	Esquema nacional	Protocolos	Es importante establecer protocolos de actuación para las infraestructuras críticas, a fin de minimizar los riesgos y daños potenciales causados por eventos de sabotaje o ataques cibernéticos.	25
				Medidas de protección lógicas y físicas	La ausencia de medidas adecuadas de protección lógica y física para las infraestructuras críticas, podría resultar en vulnerabilidades de seguridad para Michoacán.	26
				Catálogo	La ausencia de un catálogo de las infraestructuras críticas dificulta la tarea de identificación y protección frente a eventuales amenazas de origen cibernético.	27
				Mecanismos de control y gestión	La implementación de mecanismos para el control y gestión de las infraestructuras críticas por parte del Estado es esencial.	28
				Planes de recuperación	Para proteger una infraestructura crítica ante un ataque cibernético es necesario disponer de un plan de recuperación de incidentes efectivo y adecuado.	29
					La ausencia de planes de recuperación en caso de ataques a infraestructuras críticas puede representar una amenaza para la estabilidad y seguridad del estado de Michoacán.	30
VI	CIBERSEGURIDAD	Seguridad de la información	Educación proactiva Educación reactiva	Políticas	La generación de políticas que promuevan el aprendizaje significativo entre los usuarios y operadores de sistemas es esencial para la seguridad de la información.	31
				Cultura de seguridad de la información	Es importante fomentar la cultura de seguridad de la información por parte de los usuarios de sistemas informáticos, aplicativos y/o plataformas digitales.	32
				Equipos de respuesta a incidentes especializados	Para asegurar la recuperación de la operación en seguridad de la información, es importante contar con equipos de respuesta a incidentes especializados.	33
				Campañas de divulgación	Los procesos de divulgación en materia de Seguridad de la Información son clave para fortalecer la seguridad de la información en una organización.	34
				Medidas de seguridad y protección de datos	La implementación de medidas de seguridad y protección de datos es fundamental para evitar la exposición de privacidad y el uso indebido de información.	35
				Identificación de vulnerabilidades	Las auditorias a la infraestructura tecnológica y protocolos mejora la seguridad de la información.	36
VI	Ciberseguridad		• Fortalecimiento Tic´s • Aspectos legales • Cibercultura • Cibercrimen • Infraestructuras criticas •Seguridad de la información		La ciberseguridad es un reflejo del fortalecimiento de las Tecnologías de la información y comunicaciones.	37
					La ciberseguridad depende de la existencia de un marco normativo.	38
					La ciberseguridad es un reflejo del número de personas capacitadas y concientizadas en una cultura digital y de seguridad de la información responsable.	39
					La menor impunidad de delitos cibernéticos es una reacción del incremento de la ciberseguridad.	40
					La protección de los datos y la información confidencial, son un reflejo del fortalecimiento de la ciberseguridad.	41
					La ciberseguridad depende del fortalecimiento de las infraestructuras críticas.	42

Fuente: Elaboración propia con base en experiencia y metodología revisada 2021.

De manera resumida se muestra en la siguiente tabla la estructura de la propuesta de instrumento de medición y su distribución en cuanto al número de preguntas.

Tabla 53. Estructura del instrumento por variables.

Variables		Dimensiones	Número de preguntas
Variables independientes.	Tecnologías de la información y comunicaciones	2	9
	Aspectos Legales de la Ciberseguridad	3	6
	Cibercultura	2	5
	Cibercrimen	2	8
	Infraestructuras criticas	5	8
	Seguridad de la información	2	9
Variable dependiente.	Política pública de ciberseguridad	6	5
Total dimensiones y preguntas……....		22	50

Fuente: Elaboración propia con base en la propuesta de instrumento.

La escala que permite medir el grado de satisfacción o insatisfacción de cada uno de los encuestados, estará definida por los siguientes valores:

1. Muy de acuerdo
2. De acuerdo
3. Neutral
4. En desacuerdo
5. En total desacuerdo

El instrumento de medición consto de 50 preguntas organizadas en siete secciones, las cuales corresponden a cada una de las variables dependientes y la independiente, presentado en el apartado anterior, se validó antes de ser aplicado para probar su confiabilidad. Cronbach (1951) lo expone a través del método de consistencia interna denominado alfa de Cronbach, para conocer el grado de satisfacción de los 17 usuarios evaluados para determinar su opinión respecto al dominio de ciberseguridad.

El instrumento disponible en línea, se distribuyó a los participantes por medio de la dirección electrónica: http://107.180.68.127/tmp/.tesis_survey/login.php, a continuación se muestran los resultados obtenidos.

Por lo cual una vez recolectados los datos se les dio el tratamiento matemático en Excel 2013, para determinar la fiabilidad y consistencia del instrumento y para lo cual se utilizó la siguiente formula del alfa de cronbach.

$$\alpha = \frac{K}{K-1}\left(\frac{\sum_{i=1}^{K}\sigma_{Y_i}^2}{\sigma_X^2}\right)$$

Donde:

k= número de los ítems

Vi= varianza de cada ítem

Vi= varianza de la suma de los ítem

a= coeficiente del alfa de Cronbach

En la siguiente imagen se muestran los datos obtenidos:

Tabla 54. Análisis de datos obtenidos.

Usuario	ESCALA DE LIKERT																																																	
	Tecnologías de la información y comunicaciones									Aspectos legales						Cibercultura					Cibercrimen								Infraestructuras críticas								Seguridad de la información									Política de Ciberseguridad				
	item	item	inte	it3m	item	item	item	item	item	item	ietm	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item	item
Usuario 1	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	5	4	5	5	5	5	5	5	5	5	5	4	5	4	5
Usuario 2	4	5	5	4	4	4	5	4	5	4	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5	5	5	5	5	5	5	4	4	5	4	5	5	5	5	5	5	4	5	4	5	5	5	5
Usuario 3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Usuario4	3	4	4	4	5	4	5	3	5	3	4	5	5	5	4	5	4	5	5	5	4	5	5	4	4	3	3	4	4	4	4	4	4	3	3	5	5	4	4	3	4	5	3	5	4	5	5	4	5	5
Usuario 5	5	4	5	5	4	5	5	4	5	5	5	4	3	5	4	5	5	3	5	5	4	5	5	4	5	5	5	4	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Usuario6	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	4	4	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	4	5
Usuario7	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Usuario8	5	3	4	4	5	5	3	5	4	4	4	5	5	5	5	5	5	5	5	5	5	4	4	4	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	4	5	5	5	4	5	3	5	5	5	5
Usuario9	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5
Usuario 10	5	3	4	4	5	5	3	5	4	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4
Usuario 11	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	5	5
Usuario 12	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	5	4	5	5	5	4	4	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5
Usuario 13	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4
Usuario 14	5	4	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	5	5	5	5	5	4	5	5	4	4	5	5	5	5	5	5	5
Usuario 15	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
Usuario 16	5	5	4	4	5	4	4	4	5	5	5	5	5	4	4	4	4	5	5	4	5	4	5	4	5	4	5	5	4	4	5	4	4	4	5	4	4	4	4	4	5	5	4	5	4	5	5	5	5	5
Usuario 17	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Fuente: Elaboración propia, a partir del resultado obtenido en Excel 2021.

Para calcular alfa de Cronbach se despejo la formula, donde k es el número de ítem=17, sumatoria de la varianza de los ítems (sumatoria de la varianza individual de cada ítem), posteriormente calculamos la varianza de la suma de los ítems y finalmente el cálculo del alfa de Cronbach. En la siguiente tabla se muestra los resultados obtenidos.

Tabla 55. Calculo del alfa de Cronbach.

Número de ITEM	50
Sumatoria de la varianza de los item	11.4632353
Varianza de la suma de los item	175.992647

Alfa de Crombach	0.95
	0.95

Rangos	Magnitudes
0,81 a 1	Muy alta
0,61 a 0,80	Alta
0,41 a 0,60	Moderada
0,21 a 0,40	Baja
0,01 a 0,20	Muy baja

Fuente: Elaboración propia, a partir del resultado obtenido en Excel 2013.

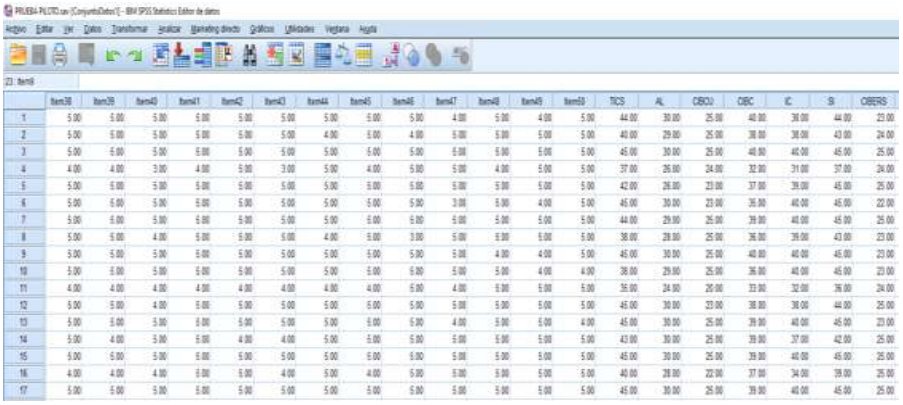
Una vez realizados los cálculos, el valor obtenido es de 0,95, dentro de la tabla se ubica en un rango de confiabilidad de 0,81 a 1, lo que nos indica que la consistencia del instrumento es muy alta, por lo tanto puede ser tomando en cuenta para su aplicación, ya que resulta valido y consistente, como lo muestra la gráfica siguiente:

4.4.3 Técnicas de procesamiento y análisis de datos.

Una vez aplicada la prueba piloto a una muestra menor, la cual fue seleccionada de forma discrecional, con la intención de detectar errores en el propio instrumento y corregirlos antes de que se aplique en la muestra seleccionada se obtuvieron los siguientes resultados preliminares:

Ingresamos al software SPSS versión 23, para cargar los datos y generar la base, una vez que se realizó la recolección de los datos, como se muestra en la siguiente imagen:

Tabla 56. Base de datos en SPSS.



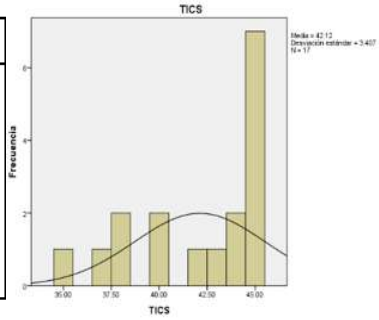
Fuente: Elaboración propia, a partir de cargar la base de datos en SPSS v.23

Posteriormente se realizó el análisis de frecuencias, donde podemos observar que la variable Tecnologías de la información y comunicaciones muestra que al menos el 94.1% están de acuerdo y totalmente de acuerdo que está debe ser incluida en la Política pública de ciberseguridad. Así mismo se presenta el histograma de los datos de dicha variable, donde se aprecia un sesgo izquierdo.

Tabla 57. Variable Tecnologías de la información y comunicaciones.

TICS

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	35.00	1	5.9	5.9	5.9
	37.00	1	5.9	5.9	11.8
	38.00	2	11.8	11.8	23.5
	40.00	2	11.8	11.8	35.3
	42.00	1	5.9	5.9	41.2
	43.00	1	5.9	5.9	47.1
	44.00	2	11.8	11.8	58.8
	Totalmente de acuerdo	7	41.2	41.2	100.0
	Total	17	100.0	100.0	



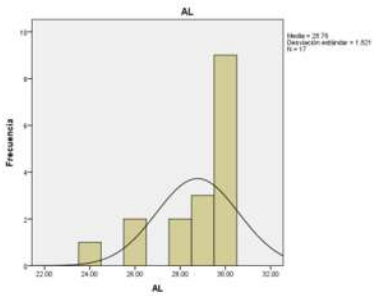
Fuente: Elaboración propia, resultado de procesar la información en SPSS v.23

En lo que respecta a la variable Aspectos legales muestra que al menos el 94.1% están de acuerdo y totalmente de acuerdo que está debe ser incluida en la política pública de ciberseguridad. Así mismo se presenta el histograma de los datos de dicha variable, donde se aprecia un sesgo izquierdo.

Tabla 58. Variable Aspectos legales.

AL

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	1	5.9	5.9	5.9
	26.00	2	11.8	11.8	17.6
	28.00	2	11.8	11.8	29.4
	29.00	3	17.6	17.6	47.1
	Totalmente de acuerdo	9	52.9	52.9	100.0
	Total	17	100.0	100.0	



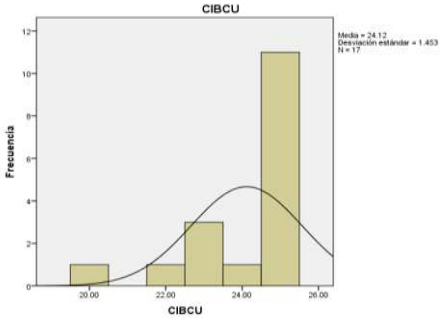
Fuente: Elaboración propia, resultado de procesar la información en SPSS v.23

En relación a la variable Cibercultura muestra que al menos el 94.1% están de acuerdo y totalmente de acuerdo que está debe ser incluida en la política pública de ciberseguridad. Así mismo se presenta el histograma de los datos de dicha variable, donde se aprecia un sesgo izquierdo.

Tabla 59. Variable Cibercultura.

CIBCU

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	1	5.9	5.9	5.9
	22.00	1	5.9	5.9	11.8
	23.00	3	17.6	17.6	29.4
	24.00	1	5.9	5.9	35.3
	Totalmente de acuerdo	11	64.7	64.7	100.0
	Total	17	100.0	100.0	



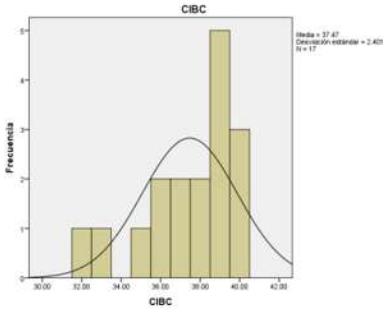
Fuente: Elaboración propia, resultado de procesar la información en SPSS v.23

La variable Cibercrimen indica que al menos el 94.1% están de acuerdo y totalmente de acuerdo que está debe ser incluida en la política pública de ciberseguridad. Así mismo se presenta el histograma de los datos de dicha variable, donde se aprecia un sesgo izquierdo.

Tabla 60. Variable Cibercrimen.

CIBC

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	1	5.9	5.9	5.9
	33.00	1	5.9	5.9	11.8
	35.00	1	5.9	5.9	17.6
	36.00	2	11.8	11.8	29.4
	37.00	2	11.8	11.8	41.2
	38.00	2	11.8	11.8	52.9
	39.00	5	29.4	29.4	82.4
	Totalmente de acuerdo	3	17.6	17.6	100.0
	Total	17	100.0	100.0	



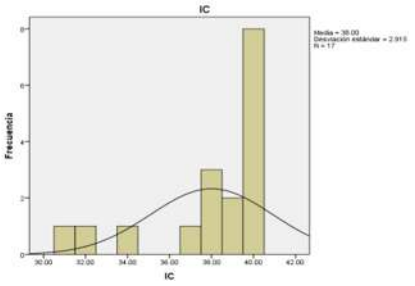
Fuente: Elaboración propia, resultado de procesar la información en SPSS v.23

Por su parte la variable Infraestructuras criticas indica que al menos el 94.1% están de acuerdo y totalmente de acuerdo que está debe ser incluida en la política pública de ciberseguridad. Así mismo se presenta el histograma de los datos de dicha variable, donde se aprecia un sesgo izquierdo.

Tabla 61. Infraestructuras críticas.

IC

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	31.00	1	5.9	5.9	5.9
	De acuerdo	1	5.9	5.9	11.8
	34.00	1	5.9	5.9	17.6
	37.00	1	5.9	5.9	23.5
	38.00	3	17.6	17.6	41.2
	39.00	2	11.8	11.8	52.9
	Totalmente de acuerdo	8	47.1	47.1	100.0
	Total	17	100.0	100.0	



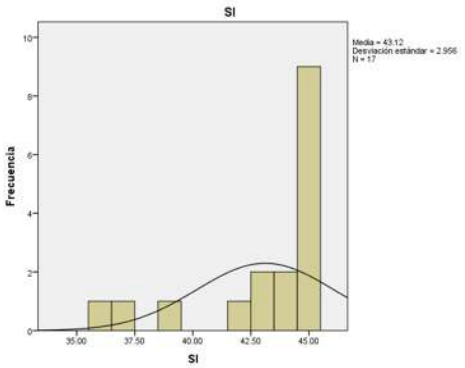
Fuente: Elaboración propia, resultado de procesar la información en SPSS v.23

En lo que respecta a la variable Seguridad de la información indica que al menos el 94.1% están de acuerdo y totalmente de acuerdo que está debe ser incluida en la política pública de ciberseguridad. Así mismo se presenta el histograma de los datos de dicha variable, donde se aprecia un sesgo izquierdo.

Tabla 62. Seguridad de la información.

SI

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	36.00	1	5.9	5.9	5.9
	37.00	1	5.9	5.9	11.8
	39.00	1	5.9	5.9	17.6
	42.00	1	5.9	5.9	23.5
	43.00	2	11.8	11.8	35.3
	44.00	2	11.8	11.8	47.1
	45.00	9	52.9	52.9	100.0
	Total	17	100.0	100.0	



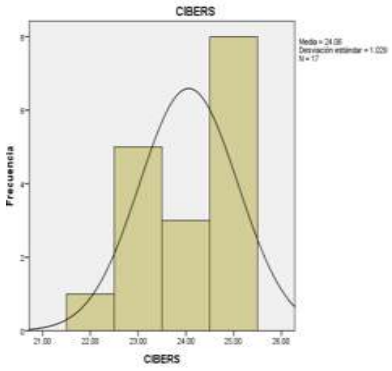
Fuente: Elaboración propia, resultado de procesar la información en SPSS v.23

Finalmente la variable de ciberseguridad indica que al menos el 94.1% están de acuerdo y totalmente de acuerdo que está debe ser incluida en la política pública de ciberseguridad. Así mismo se presenta el histograma de los datos de dicha variable, donde se aprecia un sesgo izquierdo.

Tabla 63. Variable Política pública de ciberseguridad.

CIBERS

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	22.00	1	5.9	5.9	5.9
	23.00	5	29.4	29.4	35.3
	24.00	3	17.6	17.6	52.9
	25.00	8	47.1	47.1	100.0
	Total	17	100.0	100.0	



Fuente: Elaboración propia, resultado de procesar la información en SPSS v.23

4.4.4. Análisis de regresión múltiple

Este análisis permite estudiar la relación ente la variable dependiente y las variables independientes, por lo cual se propone utilizar la metodología de mínimos cuadrados que nos permita estimar los coeficientes del modelo (MCO), con el fin de estimar los parámetros de la población a través de una muestra de datos observados (Anderson, Sweeney, & Williams, 2008).

Para lo cual haremos uso de la función poblacional.

Anexo 4. Listado de Unidades de Policías Cibernéticas que participaron en el estudio.

Unidad de análisis	Estados	Fiscalías Estatales y/o Procuradurías	Secretarías de Seguridad Pública	Guardia Nacional	SEXO		Titulares	Especialistas en ciberseguridad
					M	H		
1	Aguascalientes		25		11	14	1	25
2	Baja California		1			1	1	1
3	Baja California Sur		2		2		1	2
4	Campeche		4			4	1	4
5	Chiapas		1			1	1	1
6	Chihuahua	1				1	1	1
7	Ciudad de México		5	2	2	5	2	7
8	Coahuila		5		4	1	1	5
9	Colima		4		2	2	1	4
10	Durango	1				1	1	1
11	Estado de México		2			2	1	2
12	Guanajuato		1			1	1	1
13	Guerrero		1			1	1	1
14	Hidalgo		15		6	9	1	15
15	Jalisco	1				1	1	1
16	Michoacán	7	1		3	5	1	8
17	Morelos		1			1	1	1
18	Nayarit		1			1	1	1
19	Nuevo León		2			2	1	2
20	Oaxaca		3		1	2	1	3
21	Puebla		1			1	1	1
22	Querétaro		2			2	1	2
23	Quintana Roo	3			2	1	1	3
24	San Luis Potosi		1			1	1	1
25	Sinaloa	1				1	1	1
26	Sonora		1			1	1	1
27	Tabasco	1				1	1	1
28	Tamaulipas		2			2	1	2
29	Tlaxcala		4		3	1	1	4
30	Veracruz		2			2	1	2
31	Yucatán	1				1	1	1
32	Zacatecas		1			1	1	1
Totales…….		16	88	2	36	70	33	106

Fuente: Elaboración propia con base en la información recolectada, 2023.

Anexo 5. Instrumento de medición.

Actualmente en el Estado de Michoacán no se cuenta con una Política pública de ciberseguridad que sirva como un instrumento de investigación y concientización para la sociedad a partir del reconocimiento de la importancia de las tecnologías de la información como factor determinante en la vida social, que se encargue de regular las conductas y sancionar los delitos que se cometen en el ciberespacio. Esta política estará conformada de seis temas que son relevantes (Tecnologías de la información y comunicaciones, Aspectos legales, Cibercultura y Seguridad de la información, Cibercrimen e Infraestructuras críticas), los cuales se dividen en 40 aspectos, por lo que solicito su apoyo para contestar cada una de las siguientes afirmaciones. (Rellenar solo un ovalo):

Nombre:

Correo electrónico:

Estado de la República Dependencia:

Tecnologías de la información y comunicaciones.

1.- El incremento de amenazas lógicas y sistemas desactualizados provoca daños significativos a los equipos, infraestructura tecnológica e información.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

2.- La ausencia de protocolos para abordar las amenazas físicas o lógicas, puede dificultar la recuperación después de un incidente de seguridad.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

3.- El fortalecimiento a las tecnologías de la información y comunicaciones, podría incidir favorablemente en la disminución de vulnerabilidades que enfrentan los activos ante diversas amenazas.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

4.- La implementación de medidas como estándares, guías de buenas prácticas y herramientas especializadas, resulta fundamentales en la identificación y mitigación de amenazas de los usuarios en su navegación.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

5.- Implementar estrategias orientadas a promover y fomentar la actualización de hardware y software, reduce los riesgos asociados a la exposición de vulnerabilidades.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

6- Es importante que los creadores de tecnologías emergentes consideren de manera proactiva la seguridad, con el objetivo de prevenir y reducir el riesgo de vulnerabilidades y amenazas que puedan ser explotadas en su implementación.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

Aspectos legales.

7.- Legislar sobre el diseño, fabricación y uso de las tecnologías de la información y comunicaciones, contribuiría a asegurar que estas tecnologías sean seguras y confiables.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

8.- El desconocimiento de las implicaciones prácticas, técnicas y legales en el desarrollo y creación de tecnologías de la información y comunicaciones, conduce a la falta de legislación en este campo.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

9.- El fortalecimiento al marco normativo por parte de las autoridades, permitiría contar con mayores capacidades en la investigación, persecución y sanción de los delitos informáticos.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

10.- La adecuación de la legislación local a los marcos y tratados internacionales podrá contribuir a la disminución de incidentes de ciberseguridad.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

11.- Armonizar, tipificar e incrementar las penas con respecto a los delitos cometidos por medio de las tecnologías de la información y comunicaciones, contribuirá a disminuir los riegos de los usuarios.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

Cibercultura

12.- La actualización personal sobre temas de seguridad en internet es básico para usarlo sin exponerse a riesgos.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

13.- Para evitar ser víctimas de los riesgos en el ciberespacio, es importante la concientización sobre las amenazas en línea y tomar medidas proactivas para protegerse.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

14.- Para promover el desarrollo de una cultura digital, es importante considerar la creación de organizaciones, tanto públicas como privadas, que contribuyan a este objetivo.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

15.- Es esencial implementar medidas que fomentan una comprensión profunda por parte de los usuarios, para evitar riesgos y vulnerabilidades al navegar en línea.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

16.- Las campañas en diversos medios de comunicación para concientizar sobre la creación de una cultura digital, incrementaría la seguridad al momento de navegar.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

17.- El desarrollo e implementación de guías de buenas prácticas para la navegación de los usuarios en el ciberespacio puede ser muy beneficioso y es un aspecto importante de la seguridad en línea.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

Cibercrimen

18.- La ausencia de una debida supervisión por parte de los padres de familia, propicia la realización de variadas acciones de riesgo durante la navegación en línea.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

19.- La falta de especialización técnica y capacitación de los investigadores encargados de perseguir delitos cibernéticos puede llevar a que los delincuentes queden impunes.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

20.- El número de denuncias o incidentes cibernéticos, son un reflejo del estado de cibercriminalidad en Michoacán.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

21.- La ausencia de campañas de sensibilización sobre los riesgos en la navegación de los usuarios contribuye al aumento de la cibercriminalidad.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

22.- La creación de un órgano judicial especializado en delitos cibernéticos, podría ser una estrategia efectiva para reducir la incidencia de la cibercriminalidad.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

23.- La formación y capacitación de los órganos jurisdiccionales especializados en delitos cibernéticos, fortalece la capacidad de investigación y reduce la incidencia delictiva.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

24.- La creación de un centro de contención, respuesta e investigación especializada de delitos cibernéticos ayudaría a disminuir la cibercriminalidad.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

Infraestructuras críticas.

25.- Es importante establecer protocolos de actuación para las infraestructuras críticas, a fin de minimizar los riesgos y daños potenciales causados por eventos de sabotaje o ataques cibernéticos.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

26.- La ausencia de medidas adecuadas de protección lógica y física para las infraestructuras críticas, podría resultar en vulnerabilidades de seguridad para Michoacán.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

27.- La ausencia de un catálogo de las infraestructuras críticas dificulta la tarea de identificación y protección frente a eventuales amenazas de origen cibernético.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

28.- La implementación de mecanismos para el control y gestión de las infraestructuras críticas por parte del Estado es esencial.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

29.- Para proteger una infraestructura crítica ante un ataque cibernético es necesario disponer de un plan de recuperación de incidentes efectivo y adecuado.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo

( ) ( ) ( ) ( ) ( ) ( ) ( )

30.- La ausencia de planes de recuperación en caso de ataques a infraestructuras críticas puede representar una amenaza para la estabilidad y seguridad del estado de Michoacán.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

Seguridad de la información.

31.- La generación de políticas que promuevan el aprendizaje significativo entre los usuarios y operadores de sistemas es esencial para la seguridad de la información.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

32.- Es importante fomentar la cultura de seguridad de la información por parte de los usuarios de sistemas informáticos, aplicativos y/o plataformas digitales.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

33.- Para asegurar la recuperación de la operación en seguridad de la información, es importante contar con equipos de respuesta a incidentes especializados.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

34.- Los procesos de divulgación en materia de Seguridad de la Información son clave para fortalecer la seguridad de la información en una organización.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

35.- La implementación de medidas de seguridad y protección de datos es fundamental para evitar la exposición de privacidad y el uso indebido de información.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

36.- Las auditorías a la infraestructura tecnológica y protocolos mejora la seguridad de la información.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

Ciberseguridad.

37.- La ciberseguridad es un reflejo del fortalecimiento de las Tecnologías de la información y comunicaciones.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo

( ) ( ) ( ) ( ) ( ) ( ) ( )

38.- La ciberseguridad depende de la existencia de un marco normativo.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

39.- La ciberseguridad es un reflejo del número de personas capacitadas y concientizadas en una cultura digital y de seguridad de la información responsable.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

40.- La menor impunidad de delitos cibernéticos es una reacción del incremento de la ciberseguridad.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

41.- La protección de los datos y la información confidencial, son un reflejo del fortalecimiento de la ciberseguridad.

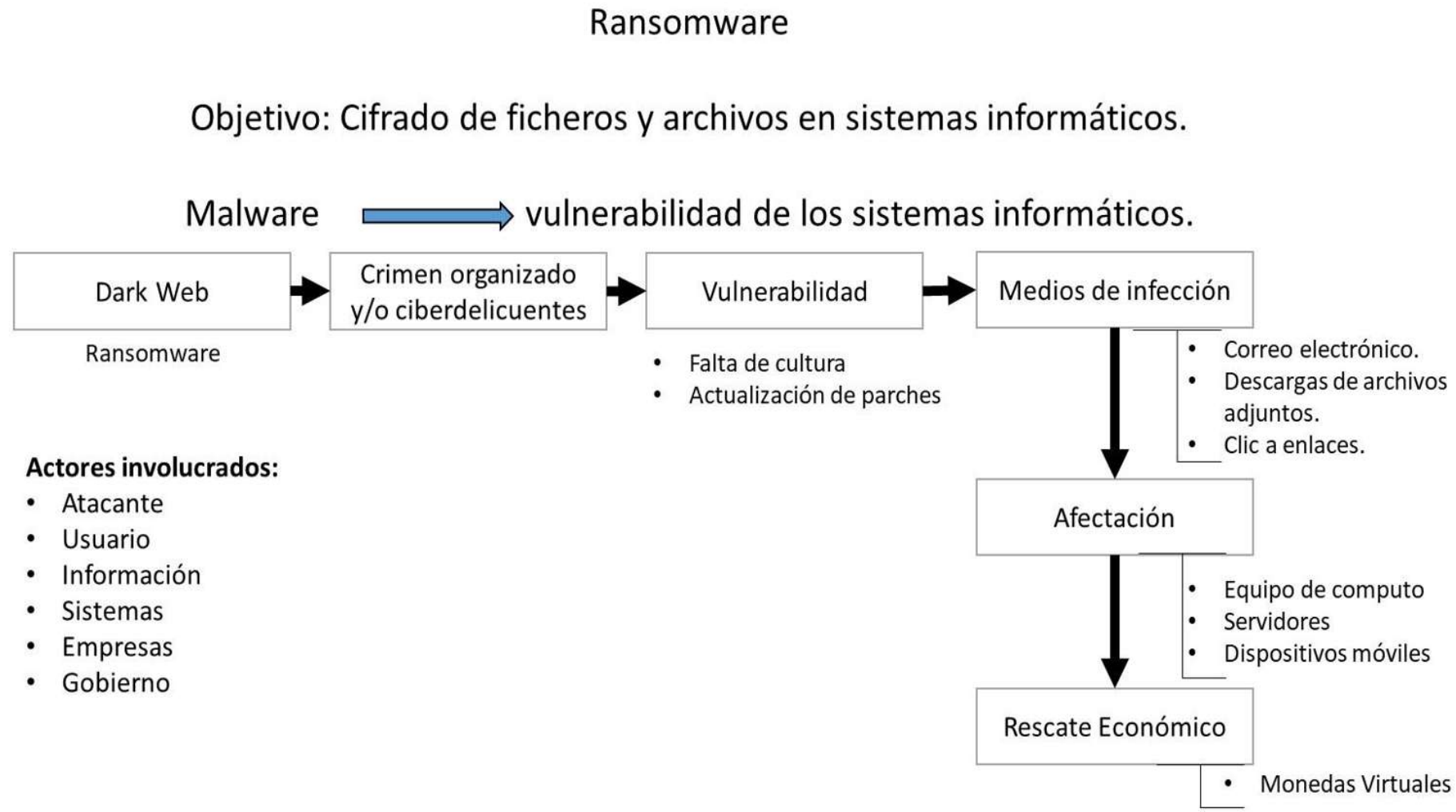
Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

42.- La ciberseguridad depende del fortalecimiento de las infraestructuras críticas.

Totalmente en desacuerdo	Bastante en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Bastante de acuerdo	Totalmente de acuerdo
( )	( )	( )	( )	( )	( )	( )

Anexo 6. Vectores de ataque en conductas de riesgo y ataques cibernéticos.

Ficha 1, vector de ataque:

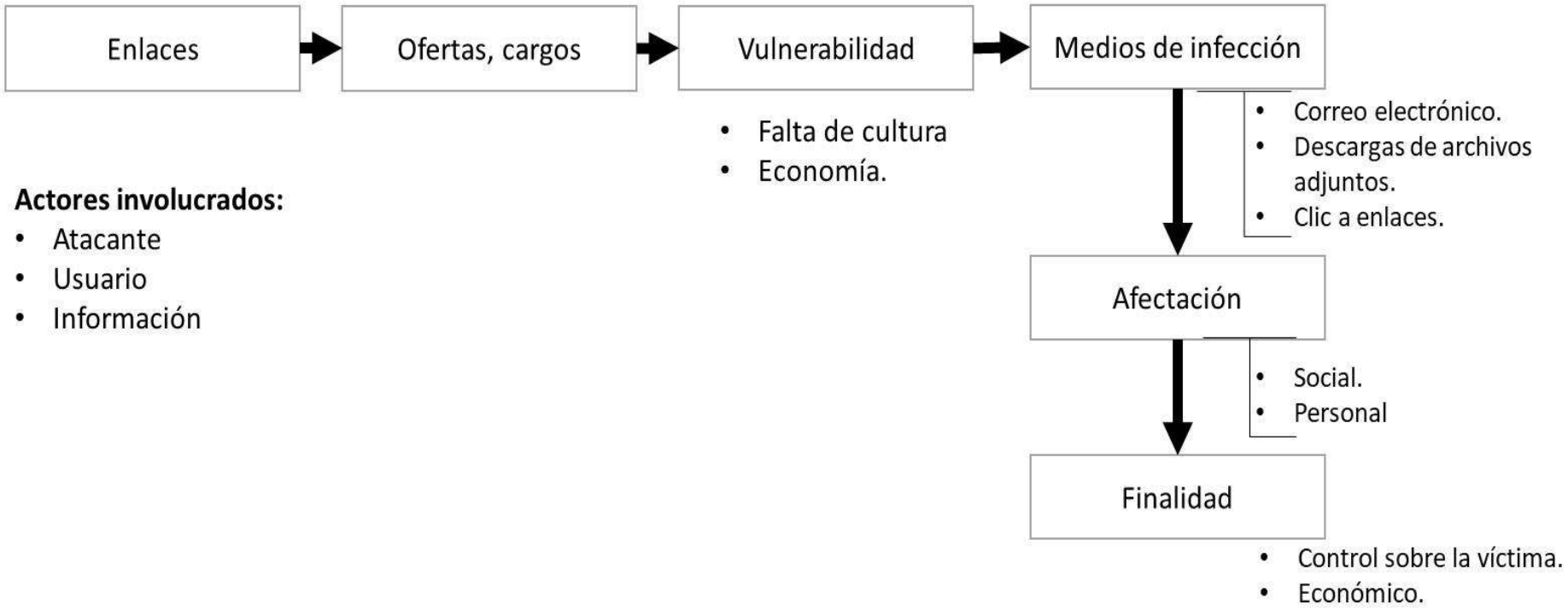


Ficha 2, vector de ataque:

Phishing, Smishing, vishing

Objetivo: obtener información personal y/o infectar de malware.

Ingeniería social ⟹ Engaño mediante afinidad con el usuario.



Actores involucrados:

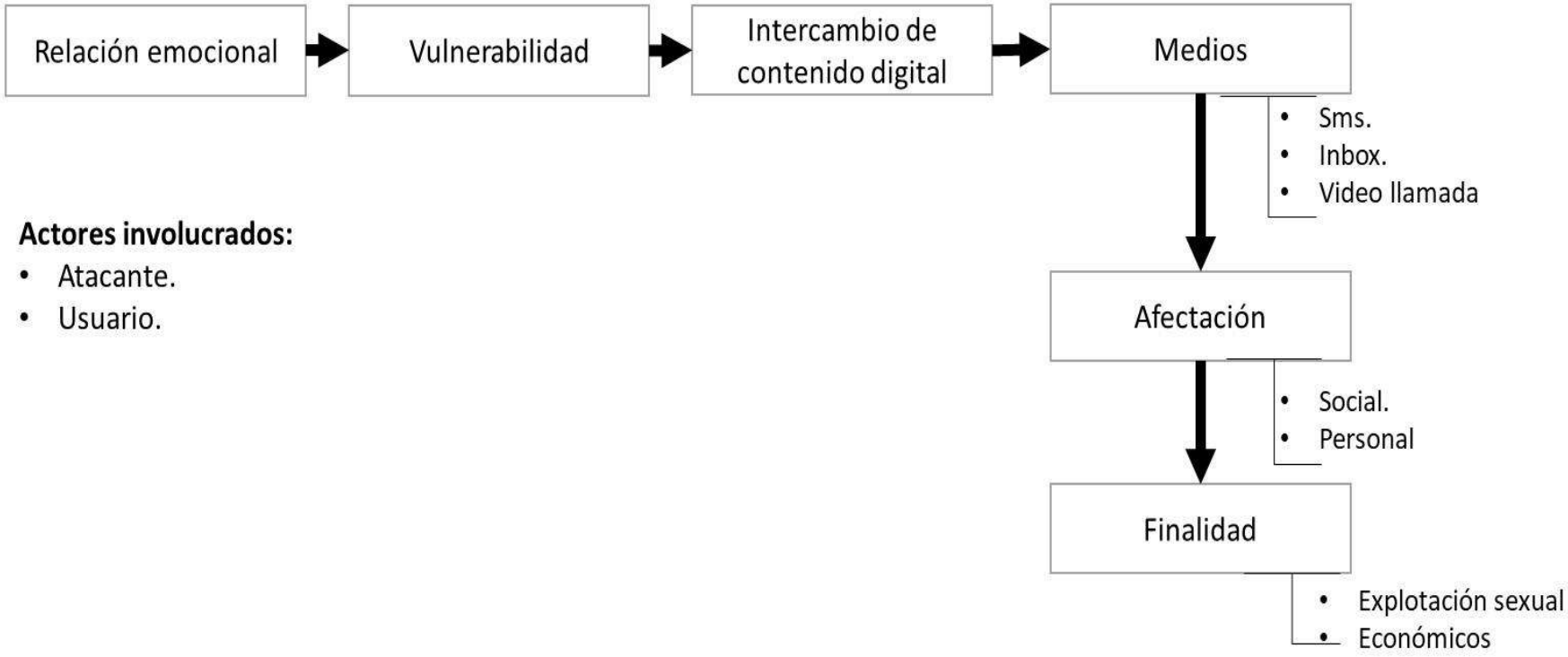
- Atacante
- Usuario
- Información

Ficha 3, vector de ataque:

Sexting

Objetivo: obtener fotografías, videos de contenido explicito

Ingeniería social → Engaño mediante afinidad con el usuario.



Actores involucrados:

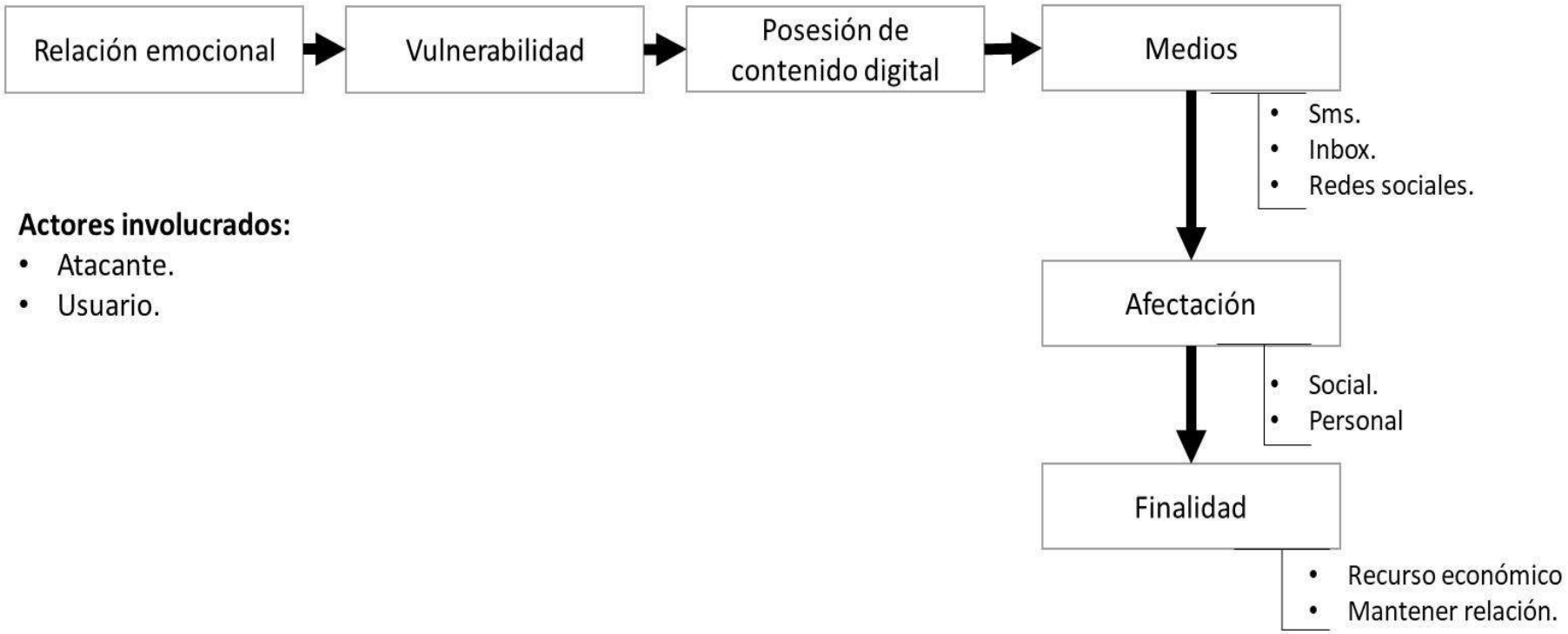
- Atacante.
- Usuario.

Ficha 4, vector de ataque:

Violencia a la Intimidad digital sexual

Objetivo: obtener beneficio económico, emocional, laboral.

Extorsión ⟹ Amenazas con hacer publico contenido.



Actores involucrados:

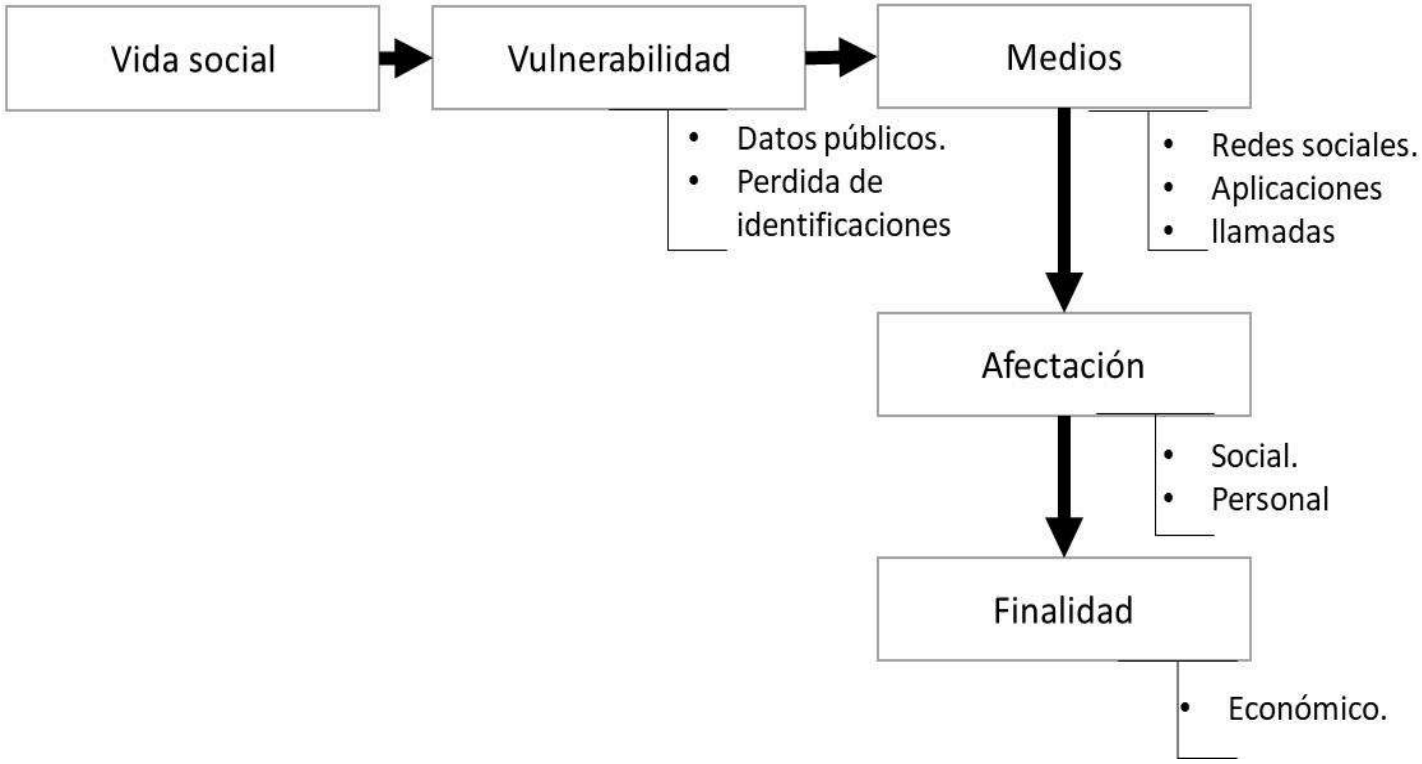
- Atacante.
- Usuario.

Ficha 5, vector de ataque:

Usurpación de identidad

Objetivo: obtener beneficio económico, difamar, dañar.

Fraude ⇒ utilizar la identidad de una persona ajena .



Actores involucrados:

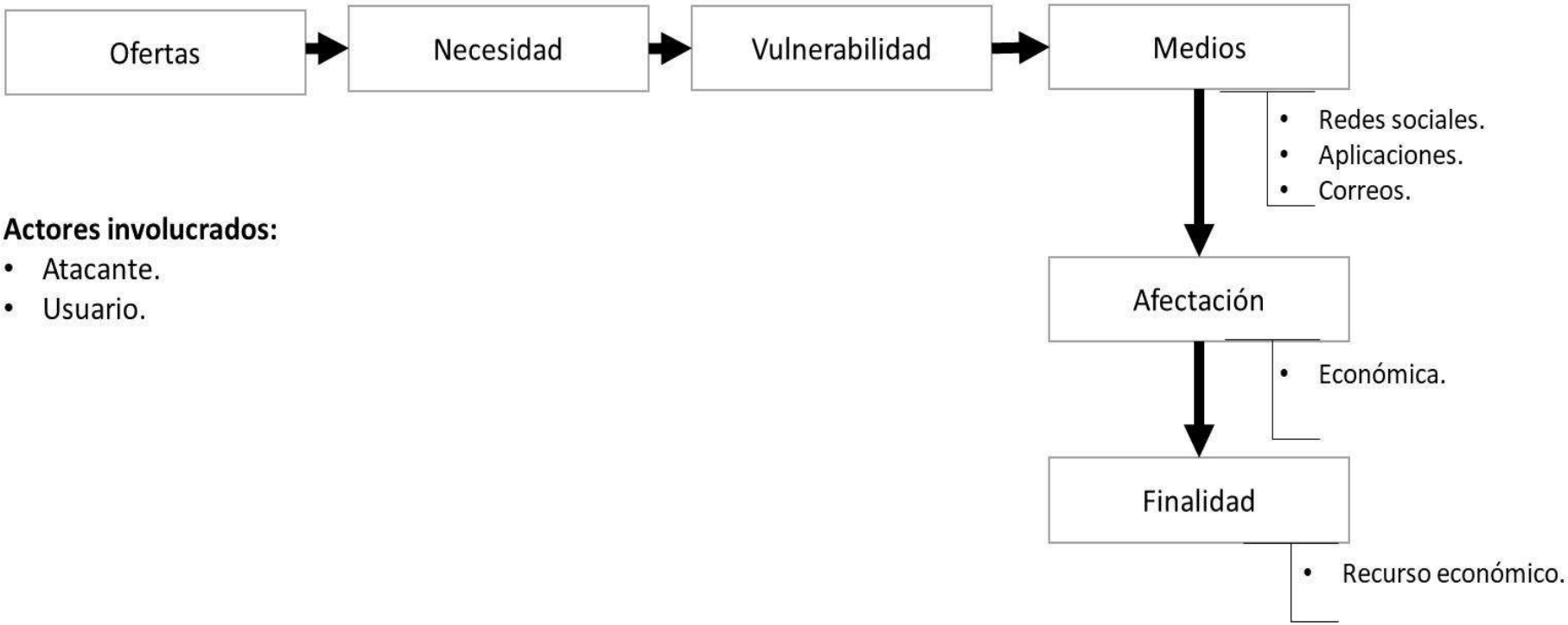
- Atacante.
- Usuario.

Ficha 6, vector de ataque:

Fraude

Objetivo: obtener beneficio económico.

Engaño ⟹ marketing para atraer a posibles victimas.



Actores involucrados:

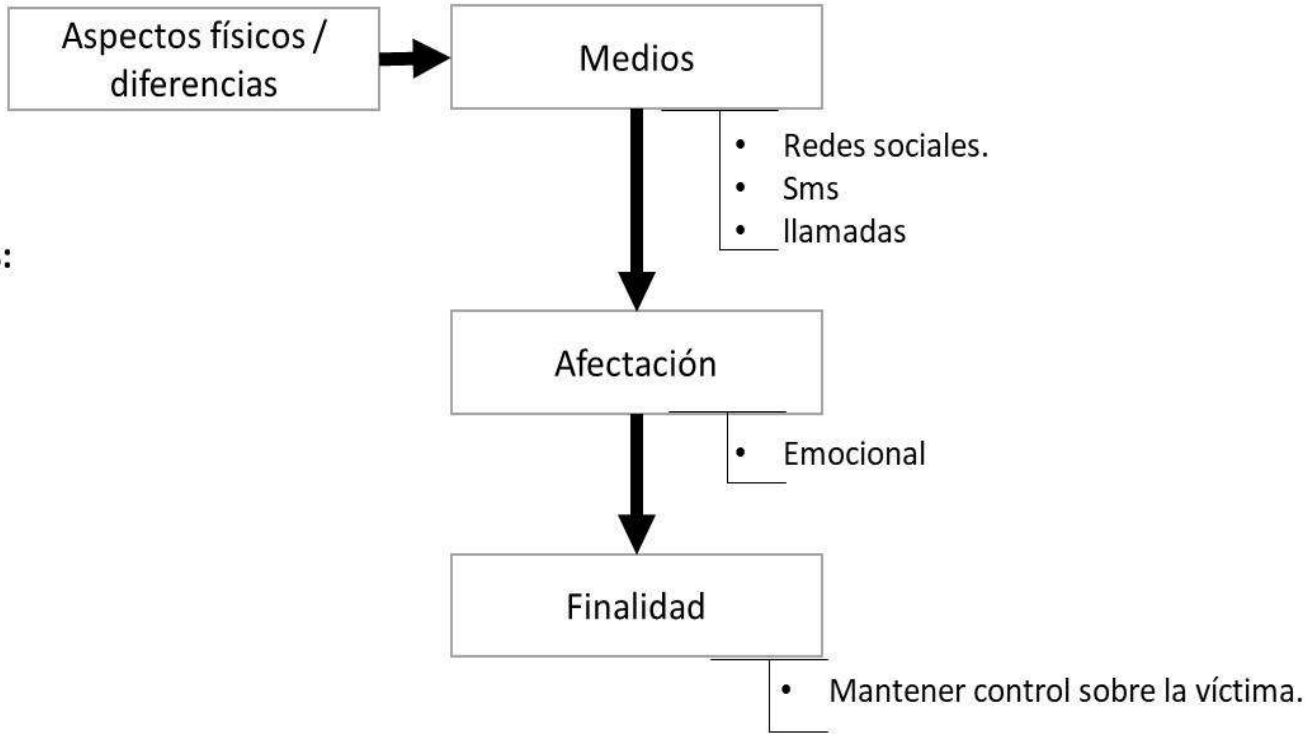
- Atacante.
- Usuario.

Ficha 7, vector de ataque:

Ciberbullyng

Objetivo: atacar a una persona a través de plataformas digitales

Acoso ⟹ envió de mensajes, creación de fotografías que denigren la imagen.



Actores involucrados:

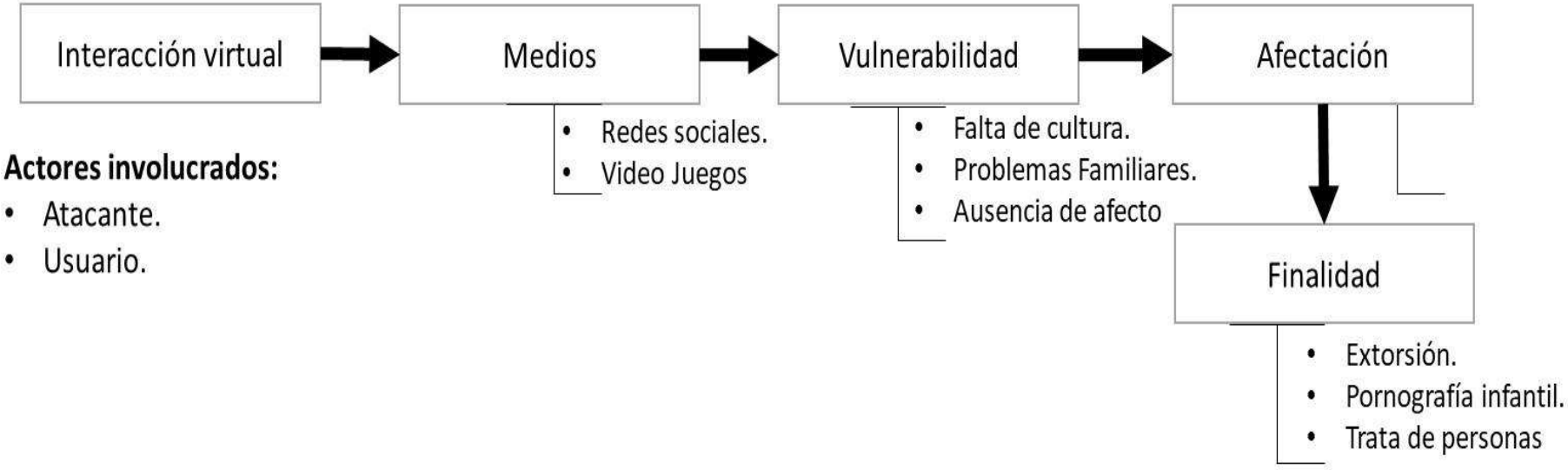
- Atacante.
- Usuario.

Ficha 8, vector de ataque:

Grooming

Objetivo: obtener información personal, fotografías, videos o hacer que el menor abandone su hogar.

Ingeniería Social ⟹ Crear afinidad para que la victima aporte los datos que necesita el delincuente.



Actores involucrados:

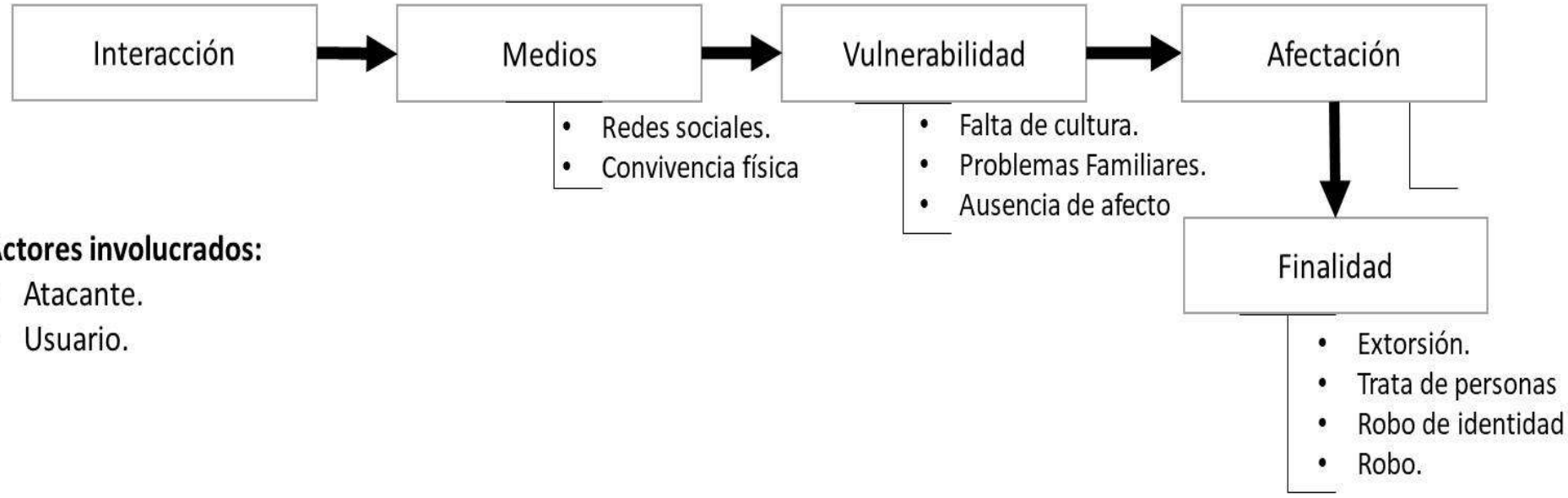
- Atacante.
- Usuario.

Ficha 9, vector de ataque:

Ingeniería social

Objetivo: obtener información personal, financiera, fotografías, videos.

Afinidad ⟹ compartir gustos, intereses para que la victima aporte los datos que necesita el delincuente.



Actores involucrados:

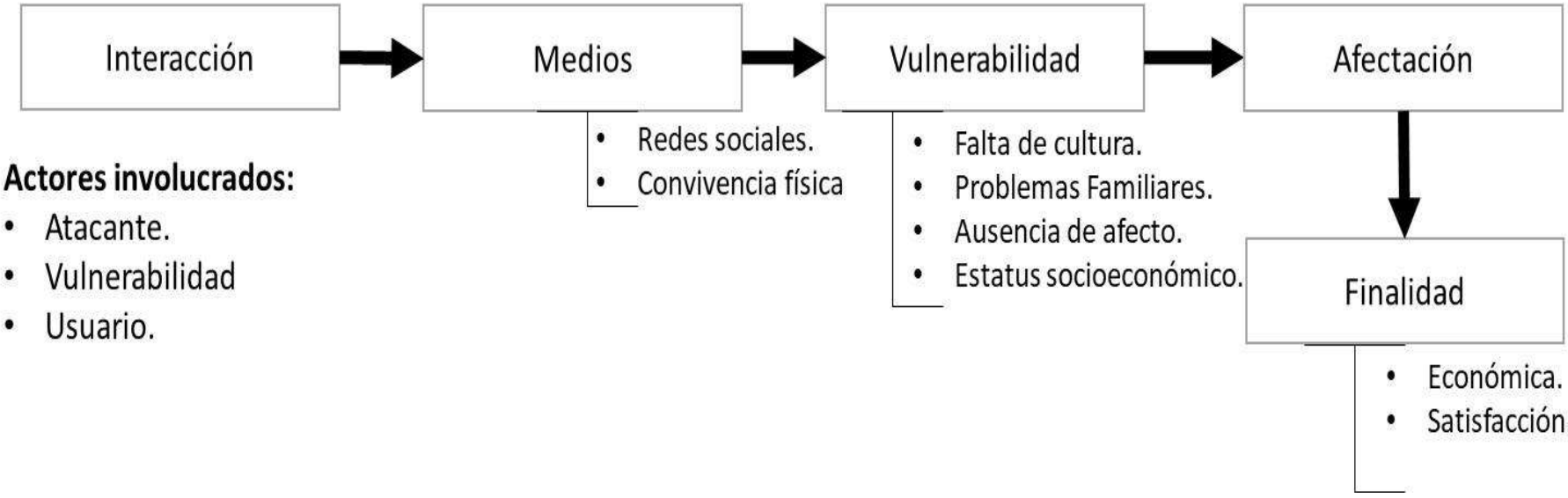
- Atacante.
- Usuario.

Ficha 10, vector de ataque:

Pornografía infantil

Objetivo: crear, poseer, distribuir contenido de índole sexual con personas menores de edad.

Ingeniería social, Extorsión → obtener la confianza de la victima, para obligar, amenazar para que realice ciertas acciones.



Actores involucrados:

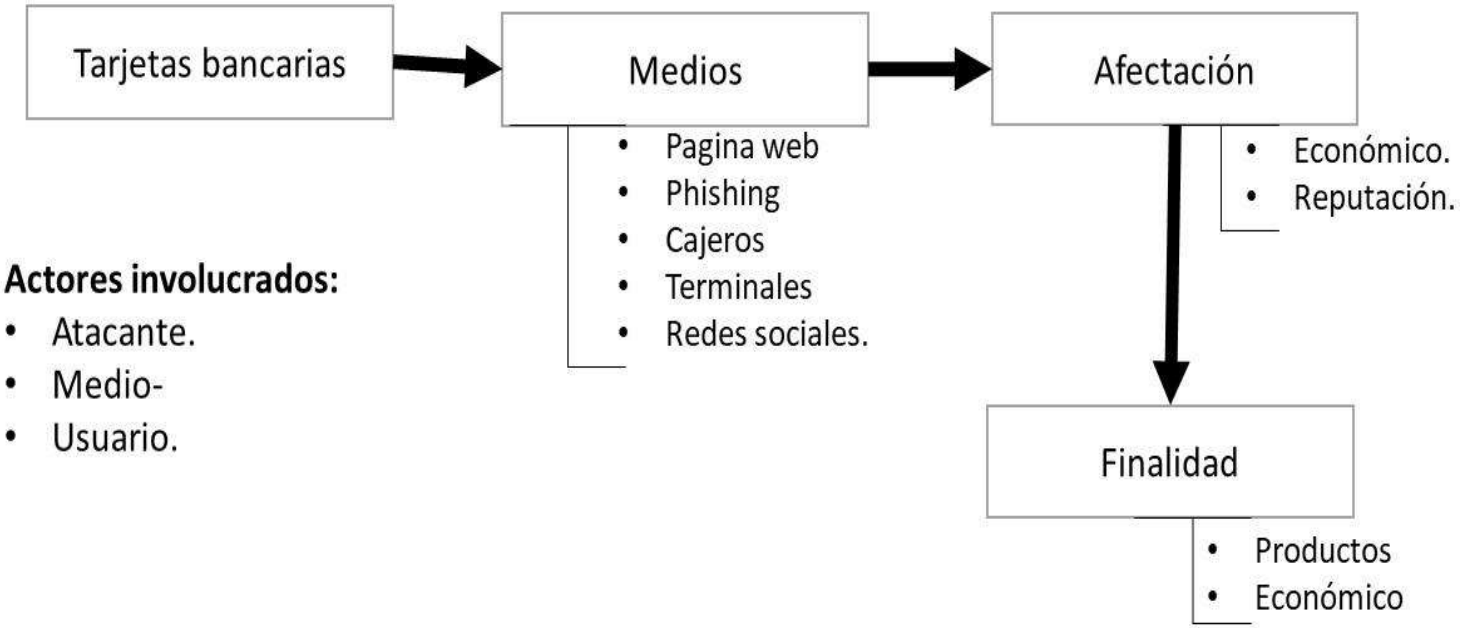
- Atacante.
- Vulnerabilidad
- Usuario.

Ficha 11, vector de ataque:

Carding

Objetivo: obtener los datos de tarjetas de debito, crédito y realizar una clonación.

Fraude → realizar compras con tarjetas ajenas.



Actores involucrados:

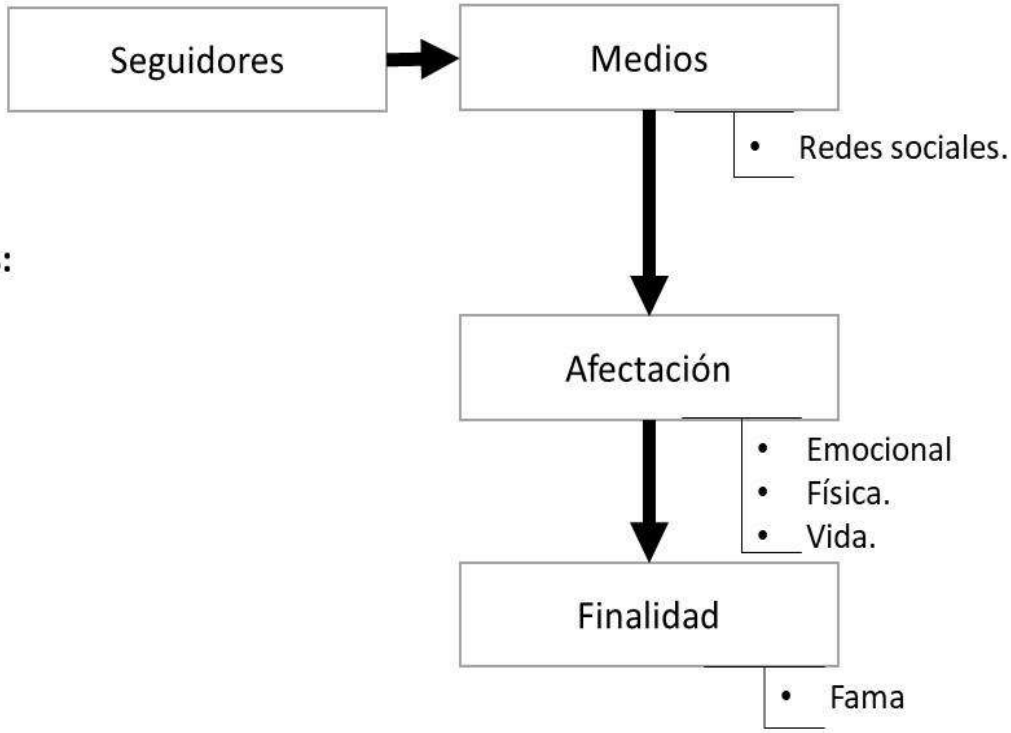
- Atacante.
- Medio-
- Usuario.

Ficha 12, vector de ataque:

Retos y juegos

Objetivo: realizar acciones con el fin de ganar popularidad en redes sociales

Redes Sociales ⟹ videos cortos realizando acciones riesgosas y/o novedosas.



Actores involucrados:

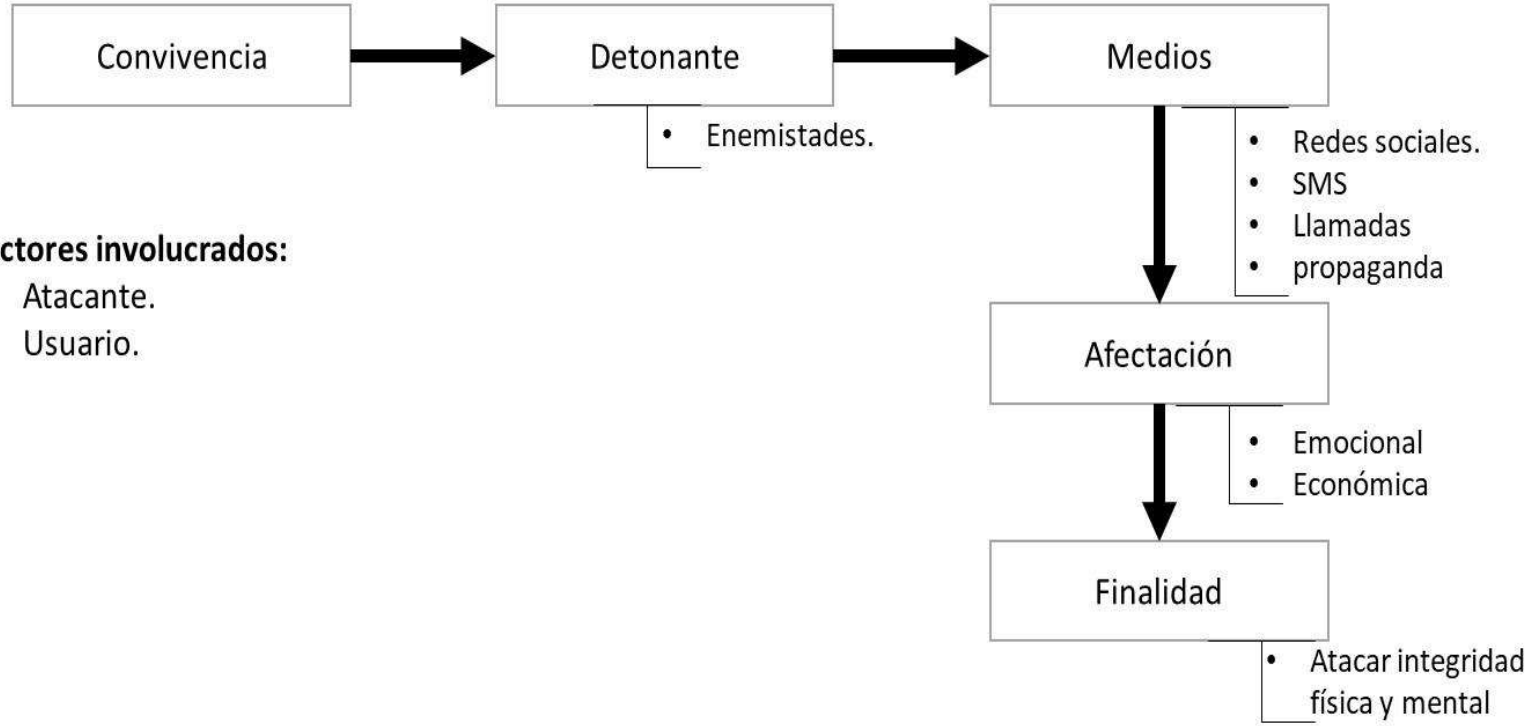
- Atacante.
- Usuario.

Ficha 13, vector de ataque:

Doxing

Objetivo: Acosar mediante la revelación de datos personales.

Ingeniería social, Acoso ⟹ Obtener datos personales para posterior revelarlos con el fin de exponer a la persona a diversas situaciones.



Actores involucrados:

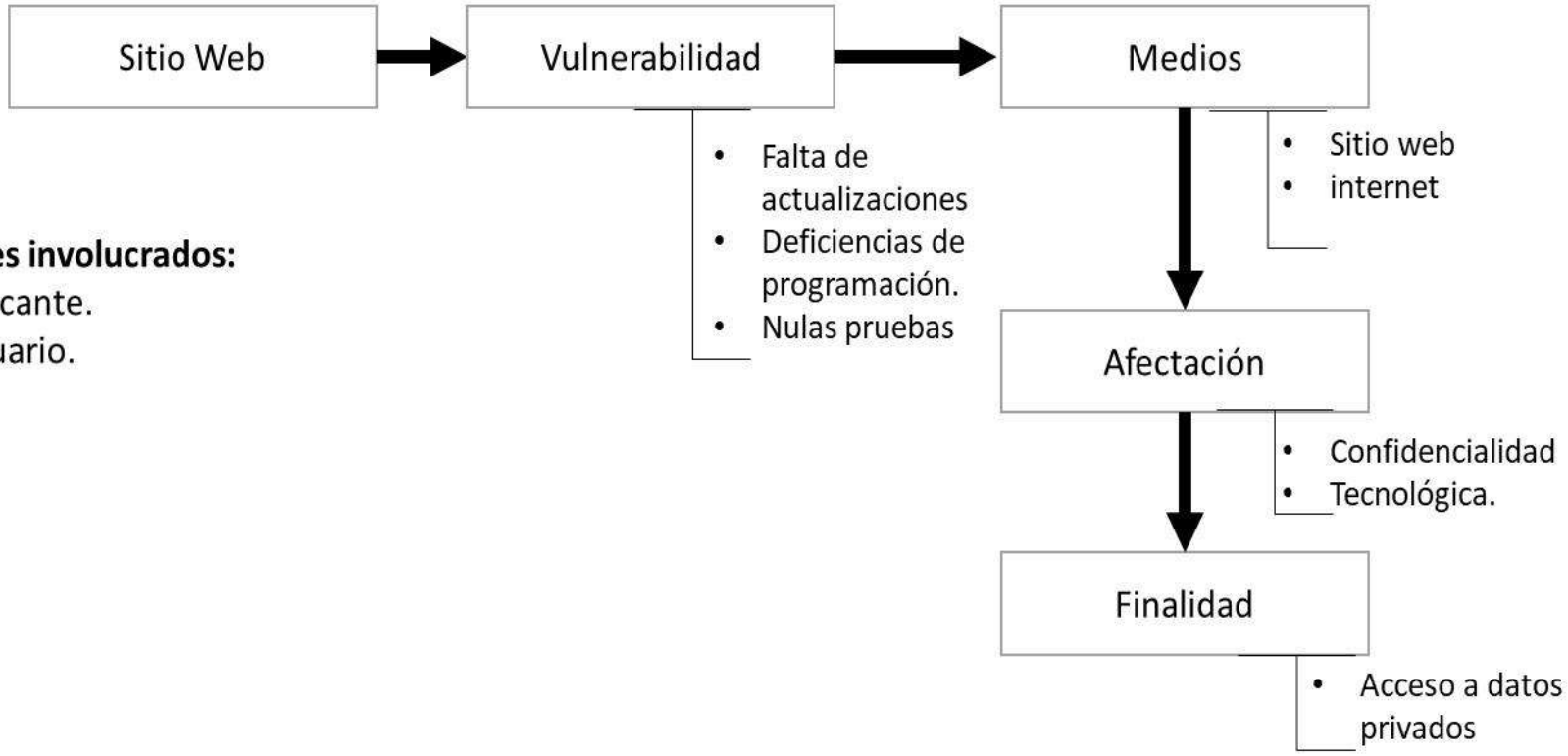
- Atacante.
- Usuario.

Ficha 14, vector de ataque:

Inyección de código SQL

Objetivo: lograr burlar los métodos de autentificación de una pagina web

Tic´s ⟹ sentencias de lenguaje SQL.



Actores involucrados:

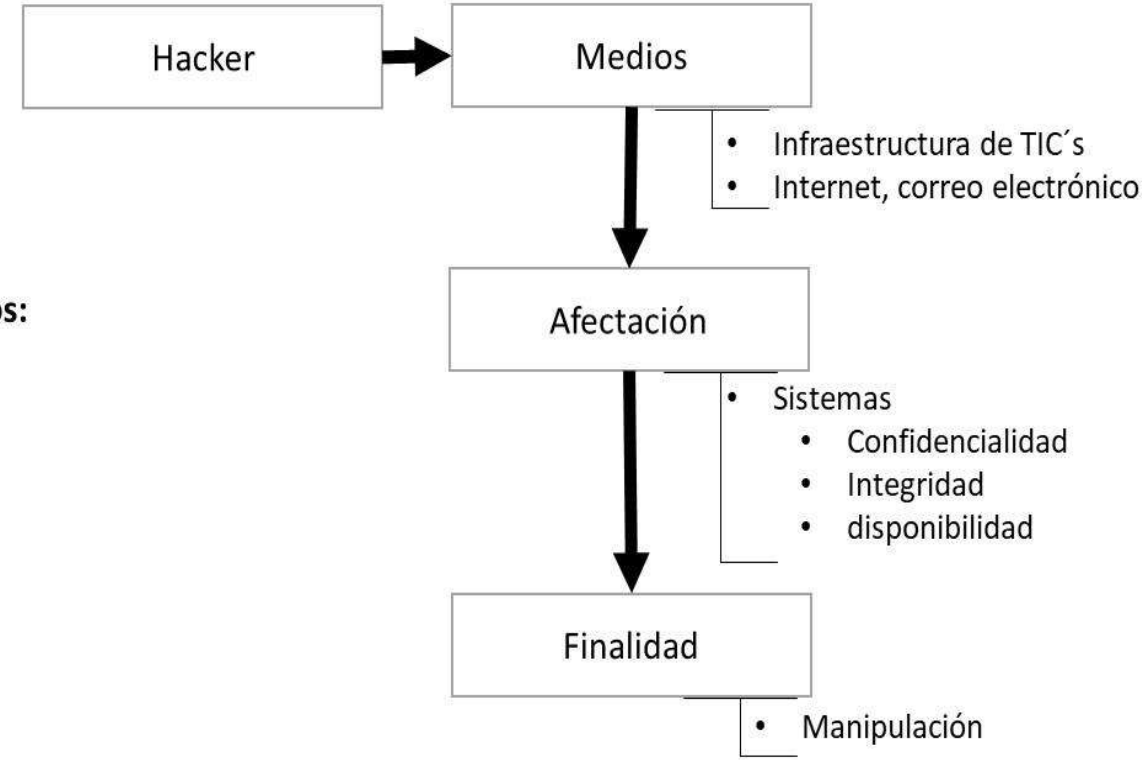
- Atacante.
- Usuario.

Ficha 15, vector de ataque:

Man-in-the-Middle

Objetivo: obtener información de los canales de comunicación no cifrados

Hacker → persona dedicada a revisar la información que es transferida por los canales de comunicación



Actores involucrados:

- Atacante.
- Usuarios
- Empresas