UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE ECONOMÍA

TEMA:

Determinación de las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe

AUTOR (ES):

Massuh Villamar Vanessa Amira

Trabajo de titulación previo a la obtención del título de ECONOMISTA

TUTOR:

Econ. Pacheco Bruque Marlon Estuardo, Mgs

Guayaquil, Ecuador

1 de septiembre del 2023

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE ECONOMÍA

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Massuh Villamar Vanessa Amira** como requerimiento para la obtención del título de Economista.

TUTOR

f._____

Econ. Pacheco Bruque Marlon Estuardo, Mgs

DIRECTOR DE CARRERA

f._____

Econ. Erwin José Guillen Franco, Mgs

Guayaquil, día 1 del mes de septiembre del año 2023.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE ECONOMÍA

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Massuh Villamar Vanessa Amira**

DECLARO QUE:

El Trabajo de Titulación: **Determinación de las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe.** Previo a la obtención del título de **Economista,** ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a el 1er día del mes de septiembre del año 2023

AUTORES

f. _____

Massuh Villamar Vanessa Amira

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE ECONOMÍA

AUTORIZACIÓN

Yo, **Massuh Villamar Vanessa Amira**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación: **Determinación de las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe,** cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, 1 día del mes de septiembre del año 2023

AUTORES

f._____

Massuh Villamar Vanessa Amira

REPORTE COMPILATIO


CERTIFICADO DE ANÁLISIS
magister

yap

< 1% Similitudes

< 1% Texto entre comillas
0% similitudes entre comillas

2% Idioma no reconocido

Nombre del documento: tesisplagio.docx
ID del documento: 891688c2b2c4e60f7c033db450e211ecd35edd86
Tamaño del documento original: 820,47 kB
Autor: van nessa

Depositante: van nessa
Fecha de depósito: 27/8/2023
Tipo de carga: url_submission
fecha de fin de análisis: 27/8/2023

Número de palabras: 12.335
Número de caracteres: 81.802

Ubicación de las similitudes en el documento:

TUTOR:

Firmado electrónicamente por:
MARLON ESTUARDO PACHECO BRUQUE

f._____

Econ. Pacheco Bruque Marlon Estuardo.Mgs.

AUTOR

f._____

Massuh Villamar Vanessa Amira

AGRADECIMIENTOS

A Dios.

A mi tutor por la paciencia, seguridad y firmeza.

A mis profesores por confiar en mí.

A mis padres y hermanos por el apoyo incondicional.

Mi más profundo agradecimiento.

DEDICATORIA

A Dios, mi familia, mi tutor, mis amigos, profesores y directivos de la Universidad Católica Santiago de Guayaquil. Un pedacito de cada uno está en esta tesis.

Muchas Gracias.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE ECONOMÍA

TRIBUNAL DE SUSTENTACIÓN

f. _____

Econ. Erwin Jose Guillen Franco, Mgs.

DECANO O DIRECTOR DE CARRERA

f. _____

Ing. Freddy Ronalde Camacho Villagómez, Ph.D.

DOCENTE COORDINADOR DE ÁREA

f. _____

Econ. Delgado Salazar Jorge Luis. Ph.D.

DOCENTE OPONENTE

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ECONOMÍA Y EMPRESA

CARRERA DE ECONOMÍA

CALIFICACIÓN

TUTOR:

f. _____

Econ. Pacheco Bruque Marlon Estuardo.Mgs.

AUTOR

f._____

Massuh Villamar Vanessa Amira

INDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El objetivo de esta investigación es determinar las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe, para aquello se buscó establecer bases teóricas sólidas, aplicar el mejor modelo econométrico para la estimación de las variables y brindar conclusiones pertinentes al contexto de estudio. Así mismo se planteó cinco hipótesis de; factor económico, social, político, tecnológico y de ciberseguridad. En representación de la sección del continente, se tomaron datos de 31 países representativos con características económicas y sociales con un comportamiento similar. El modelo econométrico utilizado en esta investigación fue regresión lineal múltiple. Como fuente de información se utilizaron las bases de datos del Banco Mundial, Global Data Lab y las listas de IP de Firehol, Indice Global de Ciberseguridad (GCI) e Índice nacional de ciberseguridad (NSCI). Del mismo modo de las diecinueve variables planteadas por el marco teórico solo las variables ingresos per cápita, calidad reguladora, control de corrupción, servidores seguros de internet, personas que utilizan internet, las suscripciones de banda ancha fija, índice nacional de ciberseguridad y nivel de desarrollo digital fueron significativas, destacando que del factor social ninguna entro a esta lista. Para futuras investigaciones se espera encontrar mayor información de variables explicadas por ausencia de registros y de registros actualizados de números de ciberataques de los últimos años.

Palabras clave: ciberdelincuencia, ciberseguridad, socioeconómico, tecnológico, político

ABSTRACT

The objective of this research is to determine the driving forces of cybercrime in Latin America and the Caribbean, for which we sought to establish solid theoretical foundations, apply the best econometric model for estimating the variables and provide conclusions relevant to the context of the study. Five hypotheses were proposed: economic, social, political, technological and cybersecurity factors. In representation of the section of the continent, data were taken from 31 representative countries with similar economic and social characteristics. The econometric model used in this research was multiple linear regression. As a source of information, the databases of the World Bank, Global Data Lab and Firehol's IP lists, Global Cybersecurity Index (GCI) and National Cybersecurity Index (NSCI) were used. Similarly, of the nineteen variables proposed by the theoretical framework, only the variables per capita income, regulatory quality, corruption control, secure Internet servers, people using the Internet, fixed broadband subscriptions, national cybersecurity index and level of digital development were significant, highlighting that none of the social factor entered this list. For future research it is expected to find more information on variables explained by the absence of records and updated records of the number of cyber-attacks in recent years.

Keywords: cybercrime, cybersecurity, socioeconomic, technological, political.

1 CAPITULO I

1.1 Introducción

En primer término la ciberdelincuencia se la reconoce como un delito relativamente nuevo que de manera exclusiva ha sido posible con la aparición de Internet y evolución de las tecnologías digitales avanzada, la ciberdelincuencia se representa como cualquier delito que involucre un ordenador y una red (Luppicini, 2014).

En este contexto los ciberdelitos actuales preocupan ya que son complejos de detectar y perseguir en comparación a los delitos tradicionales (Butkovic et al., 2019). En virtud de esta explicación numerosos factores, como las características y rasgos sociodemográficas aportan a la ciberdelincuencia (Shan-A-Khuda & Schreuders, 2020). Inclusive Pravdiuk et al. (2021) expresaron que garantizar la seguridad nacional en el ciberespacio es una materia cada vez más sustancial debido al creciente número de estos delitos en respuesta a la adaptación a las emergentes tecnologías de seguridad y protección.

En los últimos años el reconocimiento de la ciberdelincuencia basada en el contenido se ha convertido en un tema atractivo para los investigadores, surgiendo como una industria promovida por el dinero con fines maliciosos hacia los mercados y espacios en línea, como resultado los ciberdelincuentes manipulan las zonas indefensas del ciberespacio jugando con el entendimiento humano y alcanzando beneficios (Singh & Kaur, 2020). En virtud de esto, los usuarios particulares de Internet con frecuencia suelen considerarse los eslabones más frágiles de la cadena de ciberseguridad (De Kimpe et al., 2022).

A partir de estas explicaciones, las amenazas contra la seguridad afectan directamente la economía digital en el contexto de la expansión de la ciberdelincuencia, se explica claramente en el uso de las tecnologías digitales en cuanto a un espacio único de información que de manera exclusiva no sólo proporciona las oportunidades para la mejora constante de los negocios, la unificación de los flujos de información, el intercambio de conocimientos y la interacción con nuevas tecnologías, sino que también abre las puertas a convertirse en una plataforma para actos ilegales, tales como un intermediario de comisión de delitos (Makhalin & Makhalina, 2018). En este sentido, la economía digital que se basa en los procesos y progresos de la tecnología informática además de las telecomunicaciones de la información añadiendo que expande sus confines en indivisibles áreas de la actividad económica, financiera, industrial, comercial y de forma complementaria la esfera de la administración pública, estará en constante exposición a diversos delitos criminales, requiriendo la mejora de nuevos mecanismos y el desarrollo de los existentes para la asegurar la información de los sistemas y tecnologías digitales globales (Klimovich & Molokov, 2019).

Bajo esta explicación el trabajo presente busca explicar los determinantes de la ciberdelincuencia y sus efectos económicos en América Latina y el Caribe. Al respecto, los cibercrímenes han evolucionado en los últimos años en respuesta de tecnologías emergentes dirigidas a las industrias productivas a nivel internacional. Con esta finalidad, surge la interrogante de ¿Cuáles son las causas socioeconómicas y de desarrollo tecnológico asociadas con la ciberdelincuencia en América Latina y el Caribe? Para su desarrollo y por consiguiente resolución se analizan las diferentes teorías en las dimensiones de estudio que respalden su comportamiento además de su vínculo con la

ciberdelincuencia entre ella encontramos el factor social, económico, político, tecnológico y en materia seguridad informática

En la primera parte del estudio se presenta la introducción, planteamiento del problema, justificación objetivos, pregunta e hipótesis. En la segunda parte se ostenta el marco teórico seguido por metodología. Adicionalmente, encontramos análisis de datos y resultados finalizando con un capítulo que contiene conclusiones y recomendaciones.

1.2 Planteamiento del problema

Como aspecto importante los ciberataques amenazan de manera constante con la usurpación de datos personales y llegan a influir tanto en el funcionamiento de las organizaciones comerciales y financieras, al igual que la economía del estado en su conjunto (Borisova & Belousov, 2019). No obstante, es valioso reconocer que la ciberdelincuencia y los ciberataques simbolizan actividades de eminente beneficio e imperceptible costo para quienes los ejecutan y, por tanto, los costos económicos que sufren las organizaciones, personas e instituciones públicas llegan a ser elevados y de igual manera se evidencian costos sociales de gran impacto (Fonfría & Duch-Brown, 2020).

Tal es el caso, cuanto al estudio de la ciberdelincuencia, investigadores argumentaron que una mejor perspectiva y comprensión del delito cibernético son una condición indispensable para desarrollar respuestas legales y políticas apropiadas que busquen detener al delito cibernético (Donalds & Osei-Bryson, 2019). Desde esta perspectiva dentro de los delitos cibernéticos se reconoce al delito formal como el acto de alguien que entra en el computador de otra persona sin su consentimiento, y el delito material donde se causa un impacto negativo a otras personas mediante el uso de tecnología dando lugar a la existencia de la ciberdelincuencia que autores reconocen como una amenaza para la estabilidad ya que se torna complicado para el gobierno equilibrar e identificar los delitos de tecnología informática, especialmente en la red que conocemos como Internet (Rais & Songkarn, 2022).

En el año 2015, los gastos a nivel mundial relacionados con la ciberdelincuencia fueron evaluados en 3 trillones de dólares, y para el año 2021, según información

proporcionada por Cybersecurity Ventures, esta cifra se incrementó en un 100%, de acuerdo con el CEO de Cisco, Chuck Robbins, si consideramos la ciberdelincuencia como medimos el Producto Interno Bruto (PIB) de naciones, su magnitud equivaldría a la tercera economía más grande del planeta, superando únicamente a Estados Unidos y China, con daños globales estimados en 6 trillones de dólares (Forbes, 2022).

En consecuencia, la ciberdelincuencia tiene un efecto destructivo a gran escala inclusive llegando a generar daños materiales, tal es el caso como es reportado *el mayor ciberdelito de la historia*, la propagación del peligroso virus WannaCrypt en 2017, los creadores atracaron un gran número de ordenadores al mismo tiempo que exigieron un rescate por los datos, causando así enormes pérdidas económicas a muchas grandes empresas de todo el mundo (Atnashev & Yakheeva, 2019).

Otro componente para entender la magnitud del impacto de este fenómeno en la actualidad es la *brecha de datos*, reconocido como un acceso no autorizado a información ultra sensible por una persona o grupo ciberdelincuentes, siendo su único objetivo explotar esta información con fines ilegítimos y beneficios monetarios (Fenoy Illacer, 2023). Poniendo cifras totales, los costos de una brecha de datos promedio para corporaciones y empresas registraron un aumento de 3,86 millones de dólares según la publicación del informe del año 2020 a 4,24 millones de dólares que representa un aumento del 9% en 2021, por otro lado para las brechas más grandes con bases que poseen entre 50 y 65 millones de registros el costo promedio fue de 401 millones en 2021 un aumento, que se lo puede llamas más modesto, del 2% con referencia a los 392 millones de dólares en el periodo de 2020 («IBM», 2021).

1.3 Justificación

En referencia al problema planteado, el presente trabajo de investigación es de gran importancia y a su vez innovador, debido a que la ciberdelincuencia dado por los cambios tecnológicos y la migración de empresas a medios digitales han formado parte del desarrollo de la economía. En el aspecto económico se investiga medidas de tendencia en la ciberdelincuencia y sus efectos en las economías de América Latina y el Caribe lo que permitiría analizar y proponer recomendaciones para mitigar el impacto de los ciberataques. Por otro lado, en lo social, muestra el interés en el comportamiento de quienes provocan los ciberataques en el análisis geográfico y otros factores socioeconómicos lo que permitiría a los países generar políticas o acciones que mejoren inclusive la calidad de vida para evitar este efecto negativo en otras economías y en las propias.

Es bueno enfatizar en el aspecto académico, el estudio de modelos econométrico en el análisis de datos, el impacto de variables sobre el tema de estudio, análisis de políticas tanto en el sector público y privado aseguran un tema de gran notabilidad y relevancia a la academia. Por otro lado, en el aspecto profesional permite desarrollar habilidades de investigación y especializarnos en el tema como es la ciber-economía que se encuentra en auge.

1.4 Objetivos

1.4.1 Objetivo general

Determinar las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe periodo 2021.

1.4.2 Objetivos específicos

- Investigar las teorías sociales, económicas, tecnológicas y de ciberseguridad relacionadas con la ciberdelincuencia.
- Estimar mediante un modelo econométrico los factores determinantes de la ciberdelincuencia en América Latina y el Caribe periodo 2021.
- Brindar conclusiones y recomendaciones que busquen amortiguar los efectos negativos de ciberdelincuencia en las economías de América Latina y el Caribe.

1.4.3 Pregunta de investigación

¿Cuáles son las causas socioeconómicas y los factores tecnológico asociadas a la ciberdelincuencia en América Latina y el Caribe?

1.5 Hipótesis

A partir de la interrogante planteada y los diversos aspectos que se toman cuenta en este estudio se plantearan las hipótesis por cada factor de estudio:

Factor económico

H_1: Los ingresos, ingresos per cápita, tasa bruta de natalidad y tasa bruta de mortalidad se asocia positivamente con la ciberdelincuencia.

Factor social

H_2: El índice de educación e índice de desarrollo humano se asocia positivamente con la ciberdelincuencia.

Factor político

H_3: El control de corrupción, eficiencia del gobierno, restado de derecho, estabilidad política y ausencia de violencia/terrorismo, voz y rendición de cuentas, calidad reguladora, se asocian negativamente con la ciberdelincuencia.

Factor tecnológico

H_4: Servidores seguros de Internet, personas que utilizan Internet, las suscripciones de banda ancha fija, Infraestructura de internet y nivel de desarrollo digital están positivamente asociados a la ciberdelincuencia.

Factor de ciberseguridad

H_5: El índice global de ciberseguridad y el índice nacional de ciberseguridad están asociados negativamente con la ciberdelincuencia.

1.6 Limitaciones

En esta investigación durante su desarrollo se presentaron las siguientes limitaciones:

- Exclusión de países de América Latina y el Caribe por inexistencia de información además de falta de representación socioeconómica y política para la interpretación de los resultados.
- Carencia de información actualizada a 2021 de las siguientes variables; nivel de desarrollo digital, índice mundial de ciberseguridad, índice nacional de ciberseguridad y servidores seguros de internet, por tanto, se procedió a utilizar los valores de 2020.
- Omisión de variables por ausencia de información en 2020 y 2021.

1.7 Delimitaciones

El contexto de la investigación una vez que se reconocen las limitaciones se da en los países de América Latina y el Caribe en el periodo 2021 tomando en cuenta los siguientes países; Antigua, Argentina, Bahamas, Barbados, Belice, Bolivia, Brasil, Colombia, Costa Rica, Chile, Dominica, Ecuador, El Salvador, Grenada, Guatemala, Guayana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay , Perú, República Dominicana , San Cristóbal y Nieves, San Vicente y la Granadinas, Santa Lucia, Surinam, Trinidad & Tobago y Uruguay.

2 CAPITULO II

Marco Teórico

2.1 Teorías económicas

2.1.1 La economía de la teoría de la información

En primera medida la teoría de la información es desarrollada por el investigador Claude Shannon en la década de 1940, precisamente se basa en encontrar una respuesta a cómo procesar señales de la forma más eficiente, por ejemplo, la compresión de datos para su almacenamiento o la comunicación a través de una red (Shannon, 1948; citado en Miner et al., 2012). Bajo este contexto ya para la década de 1980 la "economía de la información" era definida como la economía de la búsqueda, Stigler por su parte estudia y modifica en aquel entonces la teoría competitiva y señala al precio como una variable aleatoria con una función de distribución acumulativa determinada, de este modo, amplió la teoría para reconocer que incluir la actividad de *búsqueda* era necesaria para obtener información, en otras palabras *economía de búsqueda* (Lippman & McCall, 2001).

Esta teoría evoluciona con el autor Stigler (1961) ilustrando la importancia de someter la información al análisis económico, tomando en cuenta cómo definir y cuantificar esta información lo más preciso posible (Ibe, 2014). Sin embargo, esta teoría comienza a evolucionar con los años presentando nuevos aspectos.

Otros autores comenzaron a centrarse en una nueva perspectiva donde la información al ser imperfecta puede dar lugar a problemas de elección adversa y conflicto moral que repercute en las toma de decisiones (Cumming et al., 2021). De este modo los

ataques informáticos añaden apertura a la economía de la información y es posible que el papel desempeñado es de gran importancia en el éxito de la economía informática, quizás tan relevante como los avances tecnológicos (Elsner et al., 2015). Por tanto, a partir de los hallazgos de Ruan (2019) es que se comienza a estudiar el factor *economía de la seguridad de la información* que analiza, destaca y considera la relación de aspectos como los desafíos para la optimización de costos de la gestión del ciber riesgo, retos para ponderar costos de seguridad, retos para establecer el nivel óptimo de inversión en seguridad y riesgo, y la teoría de juegos en la inversión en seguridad.

2.1.2 Teoría de los efectos de red

Convencionalmente, Yu Peng Lin y Camara (2020) definieron el efecto de red como el valor que un usuario adicional de un producto tiene sobre el valor de ese producto para los demás y que las empresas deberían ser pioneras en considerar el posible papel de la red en el establecimiento de una ventaja competitiva, sin embargo también se propone que el sector público en paralelo con el estado considere esta figura. En virtud de las investigaciones de McIntyre y Srinivasan (2017), enfatizaron que los efectos de red brindan oportunidades productivas y lucrativas a las empresas que aprovechan específicamente esta dinámica para establecer plataformas tecnológicas dominantes.

Agbo y Zabsonré (2022) consideraron efecto de red directo el existente para el producto o servicio por el cual su valor crece a medida que aumenta el número de usuarios, por otra parte en su literatura, el efecto de red indirecto describe una situación en la que la adopción y adaptación de una tecnología se hace significativamente más valiosa a medida que esa tecnología se vuelve más disponible en términos de variedad y la disponibilidad crece entonces en medida que aumenta el número de usuarios de la

tecnología. Estos mismos autores en su revisión de estudios destacaron que los efectos de red contribuyen a acelerar la adopción del dinero móvil, lo que ha logrado con exito en varios países. Por su parte Haftor et al. (2021) destaca que la empresas están tomando en cuenta los efectos directos e indirectos de la red donde el tamaño de la red es un factor clave y sustancial para la creación y apropiación de valor.

Bajo este ángulo se enfatiza que los efectos de red pueden ser negativos o positivos así mismo, cuando los usuarios pueden identificarse y reconocer la pertenencia a grupos distintos en una plataforma es de gran utilidad distinguir entre los efectos de red que surgen dentro de un grupo determinado de usuarios (efectos de red dentro de un grupo) y los que un usuario de un grupo ejerce sobre los usuarios de otro grupo (efectos de red entre grupos) (Peitz & Belleflamme, 2021).

Como aspecto importante Carroll y Wang (2023) en su literatura más reciente utiliza las herramientas de la "teoría de redes" para estudiar modelos en los que los puntos localizados en las conexiones son personas y las redes que los unen son vínculos sociales. Mas aun Jaeger et al. (2005) reconocieron que el estudio y la medición de los comportamientos informativos mediante el uso de la teoría de redes sociales y metodologías etnográficas ayudaron a analizar fenómenos de comportamiento observados.

2.1.3 Teoría de la Economía de plataforma

Es definida como los fenómenos económicos únicos de mercados específicos de dos caras en la economía de mercado tradicional estudiado tecnologías digitales impulsadas por Internet, la nube, los macrodatos y el Internet de las cosas que diseñan e

implementan un conjunto completo de plataformas, consumidores y proveedores de servicios, a su vez estas influyen en las empresas para minimizar costos de transacción dentro de las normas de organización y los servicios para permitir un nuevo tipo de integración económica en la que los recursos tecnológicos están inmersamente integrados con las industrias tradicionales (Xue et al., 2020).

Es importante agregar que Peitz y Belleflamme (2021) definieron las plataformas como la entidad que junta a diversos agentes económicos esto daría paso a gestionar activamente los efectos de red entre ellos, así mismo recalcaron que una entidad es responsable de facilitar la interacción entre usuarios vinculados por alguna forma de efectos de red.

2.2 Teorías del comportamiento social

2.2.1 Teoría del actor red

Callon (2001) explico en primer término la teoría de los actores en red haciendo un contraste por cómo se combinan dos palabras que pueden considerarse opuestas: actor y red que para el autor representan conflictos tradicionales de las ciencias sociales, como la agencia y estructura o entre microanálisis y microanálisis; en segundo término la teoría intenta facilitar herramientas analíticas para explicar el proceso por el cual la sociedad se reconfigura de manera constante y su explicación se enfoca en la sociedad en construcción, donde la ciencia y la tecnología desempeñan un papel clave.

Dankert (2012) concuerda que la teoría del actor-red tiene sus raíces en los estudios con base en ciencia y tecnología centrándose en las conexiones que se establecen y

rehacen entre instituciones humanas y no humanas que forman parte de la problemática en cuestión, a manera de ilustración cuando se adentra en contextos o en lo que conocemos como estructuras subyacentes el rastreo de las conexiones puede hacerse mediante entrevistas profundas, observaciones y análisis.

Thór Jóhannesson y Bærenholdt (2020) declararon dos aspectos importantes a tomar en cuenta: como primera instancia la teoría propuso una comprensión alternativa de los actores, las redes y la teoría provocado críticas que argumentaron que era débil a la hora de estudiar imaginarios culturales, relaciones de poder y la escala; sin embargo en su segunda observación señalaron que durante la última década los defensores de la teoría cubrieron explícitamente lo político reubicándose a varios subcampos de geografía humana, como la geografía económica, la naturaleza y el Antropoceno, el turismo y la experiencia, así también los ensamblajes urbanos y diseño.

2.2.2 Teoría de la aceptación de la tecnología

La teoría pretende explicar el problema de la aceptación de la tecnología a partir de varios factores impulsores que incentivan la aceptación del comercio electrónico; que dimensión tecnológica es un factor relevante en la aceptación de la tecnología, que los cambios en el comercio electrónico impactan en los factores que promueven su aceptación, que la confianza se concilia en un factor de suma importancia al principio de la fase de introducción del comercio electrónico y que por tanto, la experiencia del usuario como agregado de la dimensión tecnológica se vuelve en un factor de gran relevancia al momento de estimar el comercio electrónico en función de su mercado (Haryanti & Subriadi, 2020).

Alazab et al. (2021) en su investigación demostró que el impacto social indica el límite hasta cuando somos responsables de comprender el valor de que las personas digan o no que debería adoptar tecnologías en la cadena de suministros como el blockchain, en el análisis de teorías destacaron que a nivel individual la influencia social se ve afectada por las acciones y creencias de compañeros para la introducción de nuevos sistemas, concluyendo que la realización de mayores efectos de red podría dar lugar a un mayor uso intencionado de aquellas tecnologías.

2.2.3 Teoría del aprendizaje social

Esta teoría se centra principalmente en el reconocimiento de las interacciones que las personas sostienen con otras de su grupo de iguales por lo que de parte de los supuestos planteados por Sutherland en 1947 se destaca (Akers & Jennings, 2015);

> (a) La conducta delictiva es aprendida, (b) la conducta delictiva se aprende en la interacción con otras personas en un proceso de comunicación, (c) la dirección específica de los motivos e impulsos se aprende de las definiciones de los códigos legales como favorables o desfavorables, (d) una persona se convierte en delincuente debido a un exceso de definiciones favorables a la violación de la ley sobre las definiciones desfavorables a la violación de la ley (p. 231).

Además, Lucas (2022) enfatiza que el comportamiento poco ético se encuentra relacionado con el aprendizaje social e indica como el comportamiento poco ético es más contagioso que el comportamiento ético.

En la misma medida, los autores Akers y Jennings (2015) recalcaron el apoyo de las bases sólidas de la teoría del aprendizaje social en paralelo con la explicación de la

delincuencia y la desviación, reconociendo y revisando pruebas empíricas referentes a la aplicabilidad transcultural en esta teoría es así como los investigadores propusieron que cualquier teoría general sobre delincuencia y la desviación debería ser capaz de explicar la delincuencia y la desviación mediante contextos geográficos/culturales.

2.3 Teorías de la globalización

2.3.1 La teoría económica de la localización

Es reconocida como una teoría básica en el área de estudio común de la geografía económica (Fengru & Guitang, 2019). Sin embargo se destacan varios puntos importantes sobre esta teoría que presentan Ottaviano & Thisse (2004):

> (a)el espacio económico es el resultado de un compromiso entre diversas formas de rendimientos crecientes y distintos tipos de costes de movilidad; (b)la competencia de precios, los elevados costes de transporte y el uso del suelo fomentan la dispersión de la producción y el consumo; por lo tanto (c)es probable que las empresas se agrupen en grandes áreas metropolitanas cuando venden productos diferenciados y los costes de transporte son bajos; (d) las ciudades ofrecen una amplia gama de bienes finales y mercados laborales especializados que las hacen atractivas para los consumidores/trabajadores; y (e)las aglomeraciones son el resultado de procesos acumulativos en los que intervienen tanto la oferta como la demanda (p. 2571).

Gorter & Nijkamp (2001) consideraron que esta teoría es en esencia el “corazón de la geografía económica y la economía regional”, además esta se encontraría vinculada

a distintas organizaciones industriales y la teoría del comercio, tal es el contexto del actual proceso de globalización que da lugar a cuantiosas respuestas rápidas y ajustes de conducta de las empresas dado los acelerados cambios tecnológicos (incluidas las TIC).

2.3.2 Teoría de la globalización

Reyes (2001) como primera instancia reconoce la globalización como una teoría que tiene propósito de interpretar los eventos que actualmente se desarrolla en áreas como el desarrollo, economía, escenarios sociales y las influencias culturales y políticas. Bodemer (1998) de su parte en aquella época se mencionaba a la globalización como la intensificadora de las transacciones transversales que hasta la actualidad se incluyen en la llamada internacionalización

Vargas-Hernández (2008) concuerda que la teoría de la globalización enfatiza las transacciones económicas y sus lazos políticos y financieros realizados de la mano del desarrollo de la tecnología de la información y la comunicación. Así mismo, la globalización se reconoce como un significado de realidad doble; por un lado la internacionalización de bienes, servicios y los factores de producción, por el otro lado las empresas industriales emergentes scon capaces de estableces su desarrollo en escala mundial y con ellos producir estrategias globales de que mejoran la producción, comercialización y gestión (Cohen, 1995, pp. 62; citado en Vargas-Hernández, 2008).

2.4 Teorías del desarrollo

2.4.1 Desarrollo económico

En relación a este sustento teórico Lin (2017) explico como el desarrollo económico es un proceso de transformación estructural que va de la mano con la innovación tecnológica continua y modernización industrial, a su vez reconoce el aumento de la productividad laboral y mejoras acompañadas en infraestructuras e instituciones, todo aquello para que se reduzcan los costos de transacción.

Al respecto Stockwell (1962) estableció las mediciones del desarrollo económico de un país son guiadas por las tendencias de su producción per cápita o en su ingreso per cápita, sin embargo en su investigación expresa la amplia disponibilidad de la herramienta de estadística demográfica para establecer índices indirectos del desarrollo económico como: a) la mortalidad infantil que demostró tener la más correlación del ingreso anual per cápita, b) tasa bruta de natalidad y c) tasa bruta de mortalidad. Otro autor denota y recalca la importancia de comprender la diferencia entre el crecimiento y la distribución para esclarecer el termino de desarrollo económico, ya que es posible que crezca la producción y la masa de la población se empobrezca, así mismo, la producción puede aumentar y el consumo disminuir (Lewis, 1957).

Kuznets (1958) por su parte explicó el desarrollo económico de un país caracterizado por un crecimiento sostenido en su representación como unidad económica. Otros autores comparten que la interacción entre los actores y estatales conlleva una revolución por la tecnología está conectada al surgimiento de una nueva dimensión conocida como ciberespacio, dichas interacciones afectan las bases fundamentales de la

economía ya que el internet se ha constituido como un elemento clave para el desarrollo y un recurso crítico para sectores productivos y económicos de las cuales obedecen a operaciones bancarias/financieras nacionales e internacionales, infraestructuras y medios de movilización, el sector energía y el sanitario (Machín & Gazapo, 2016). Investigaciones han llegado a sostener que el desarrollo económico cada vez se encuentra acercado a la ciencia y la tecnología a nivel internacional, explican como la conexión ciencia-industria pasa primordialmente al centro estratégico de desarrollo económico ya que progresivamente las organizaciones creadoras de conocimiento se convierten en creadoras y benefactoras de nuevas industrias (Etzkowitz, 2001).

2.4.2 Desarrollo tecnológico

Según Moreno Posada & Darío (1986) el concepto desarrollo tecnológico es entendido como la infraestructura que es conformada por instituciones y personas que producen conocimientos, estos pueden ser integrados por universidades, organizaciones públicas y privadas las cuales buscan control, calidad y productividad. Por su parte Vega Centeno (1993) reconoció al desarrollo tecnológico como el acrecentamiento de la capacidad de elegir, de adecuar y de generar tecnología; y, que al hacerse en el país, puede mantener la referencia y preocupación por sus posibilidades y exigencias propias.

En la teoría económica clásica el desarrollo tecnológico se lo considera como una determinante del crecimiento sostenido en el largo plazo, asi mismo autores reconocen que el desarrollo tecnológico también es conocido como la productividad total de los factores, mientras que la visión convencional es presentada como el factor de crecimiento

al cual constantemente varía la tecnología (Quiroz & Correa, 2012; Delfín Ortega & Navarro Chávez, 2015; Enríquez Pérez, 2016; Acero & Hue, 2019)

2.4.3 Desarrollo social

El desarrollo social es comprendido como un proceso que abre la posibilidad a que la población tenga una mejora en su condición de vida, en los ámbitos más destacables encontramos: salarios, empleo, vivienda, salud, vulnerabilidad, educación, y más, que va en paralelo de un proceso dinámico que ayudaría a su propio crecimiento económico y social tanto así que los estados se desplazan a un papel decisivo como promotor y su fin elemental es el bienestar de las personas dentro de una sociedad (Anaya Laime & Jhony Abel, 2022). Por otro lado Alaminos y López Monsalve (2009) propusieron una medición para el índice de desarrollo social de la siguiente manera:

Tabla 1

Variables de desarrollo social

Variable	Componente	Indicador
Índice de desarrollo humano	Vida larga y saludable	Esperanza de vida al nacer
	Educación	1. Tasa de alfabetización de adultos
		2. Tasa Bruta de matriculación
	Nivel de vida digno	PIB per. cápita

Índice de desarrollo humano relativo al género	Esperanza de vida	1. Esperanza de vida de las mujeres
		2. Esperanza de vida de los de hombres
	Educación	1. Tasa de alfabetización de mujeres
		2. Tasa de alfabetización de hombres
	Nivel de vida digno	1. Cálculo de ingresos percibidos por mujeres
		2. Cálculo de ingresos percibidos por hombres
Índice de pobreza humana 1	Vida larga y saludable	1. Probabilidad al nacer de no vivir hasta los 40 años
	Educación	1. Tasa de analfabetismo de adultos
	Nivel de vida digno	1. Porcentaje de la población sin acceso sostenible a fuente de agua
		2. Porcentaje de niños con peso insuficiente para su edad
Otras variables	**Cálculo**	
Índice de progreso genuino	Consumo comercial doméstico ajustado en función de la desigualdad económica + Servicios de trabajo doméstico y comunitario + Gastos públicos - Gastos privados y públicos “defensivos” - Gastos de degradación del medio ambiente - Desvalorización del capital natural	

Índice del planeta feliz	Esperanza de vida x Satisfacción en la vida/ Huella ecológica

Nota: Los indicadores de la tabla son presentados por Alaminos y López Monsalve (2009)

2.5 Marco conceptual

2.5.1 Industria 4.0

El término Industria 4.0 representa la cuarta revolución industrial que se define como un nuevo nivel de organización y control sobre toda la cadena de valor del ciclo de vida de los productos; está orientado a las necesidades cada vez más individualizadas de los clientes (Vaidya et al., 2018). Las nueve tecnologías pilares que mencionan estos autores, por ejemplo, los robots autónomos, el análisis de Big Data, la realidad aumentada, el internet industrial de las cosas y la ciberseguridad, tecnologías que requieren de los servicios de diseño de software, mantenimiento, gestión, asesoría y consultoría (Rüßmann et al., 2016).

2.5.2 Ciberdelincuencia

La necesidad de una taxonomía de la ciberdelincuencia se deriva de la falta de una definición y de normas para medir y gestionar la ciberdelincuencia, de acuerdo con Chandra y Snowe (2020) explican la ciberdelincuencia por niveles; en el primer nivel se encuentra un delito tradicional (offline) o un ciberdelito (online) mientras que en el segundo nivel está el crimen a) puramente tecnológico delictivo que tiene como objetivo o víctima el ecosistema de la tecnología informática y el servicio de red, o b) ciberdelincuencia avanzada es un acto delictivo que utiliza la tecnología informática para atacar o victimizar a personas físicas, gobiernos, entidades empresariales o bienes distintos del ecosistema de la tecnología informática.

Ibrahim (2016) propone que los ciberdelitos están motivados de tres formas diferentes: socioeconómica, psicosocial y geopolítica, además los impactos negativos

según el tipo de delito pueden repercutir en las pérdidas económicas, las psicológicas que afectan directamente en la persona y las geopolíticas que inciden en las entidades o país bajo su contexto en la pérdida de influencia política, alianzas e inclusive sobre control de regiones estratégicas. Preocupa, ya que varios autores concuerdan que las tecnologías y su naturaleza impulsan a la interacción abierta entre billones de dispositivos, sin embargo son estas dependencias a tecnologías inalámbricas las que generan estos problemas para empezar (Yaqoob et al., 2019), por consiguiente es necesario analizar estas amenazas desde su desarrollo primario.

Es por supuesto entender por estas definiciones que varias investigaciones no dejarían de lado la comprensión sobre cómo se debe analizar la ciberseguridad, de manera que los autores Gupta Bhol et al. (2023) propusieron cinco principales componentes de análisis para proteger las entidades o gobiernos de la ciberdelincuencia; vulnerabilidades, mecanismos de protección, amenazas, los usuarios y los encuentros de situación que es donde se analizan los resultados de un ciberataque directo al usuario.

Así mismo Cascavilla et al. (2021) explicaron el ciclo de vida de la inteligencia sobre amenazas de Pokorny con el propósito de comprender los ciberataques desde su primer acercamiento; la **dirección** es la fase en la que se establecen los objetivos de la inteligencia sobre amenazas como interrupción del proceso empresariales o de activos informáticos, la **recopilación** de información como escaneo de fuentes abiertas e infiltración en fuentes cerradas, el p**rocesamiento** de información falsa o redundante y se ponen a disposición de la organización (por ejemplo, extracción de direcciones IP y creación de un archivo de informes CSV), tal como en el **análisis** por proceso humano para la toma de decisiones, por ultimo recopilar **información de retorno** utilizable.

2.5.3 Ciberseguridad

Se ofrece una definición amplia de la ciberseguridad como un medio no sólo de proteger y defender la sociedad y sus infraestructuras de información esenciales, sino también una forma de llevar a cabo políticas nacionales e internacionales a través de medios informáticos (Stevens, T. citado en Dunn Cavelty & Wenger, 2020).

2.5.4 Variables de estudio

Convencionalmente es importante destacar el significado de las variables que se usaran en el modelo con el propósito de comprender mejor la relación entre la teoría, la interpretación y la recopilación de datos abordando efectivamente el tema, dichas definiciones son presentadas por el Banco Mundial (2023):

Control de la corrupción capta la percepción de hasta qué punto se ejerce el poder público en beneficio privado, incluyendo todas las formas de corrupción y los intereses privados. La estimación proporciona la calificación del país en el índice compuesto, expresada en términos de una distribución normal estándar, variando aproximadamente entre -2.5 y 2.5 unidades.

Eficacia del gobierno capta la percepción de la calidad de los servicios públicos, la calidad de la función pública y su grado de independencia de las presiones políticas, la calidad de la formulación y aplicación de las políticas y la credibilidad del compromiso del gobierno con dichas políticas. La estimación proporciona la calificación del país en el índice compuesto, expresada en términos de una distribución normal estándar, variando aproximadamente entre -2.5 y 2.5 unidades.

El **Estado de Derecho** recoge la percepción de hasta qué punto los agentes confían en las reglas de la sociedad y las acatan, y en particular Los derechos de propiedad, la calidad del cumplimiento de los contratos, la policía y los tribunales, así como la probabilidad de que se produzcan delitos y violencia. La estimación da la puntuación del país en el indicador agregado, en unidades de una distribución normal estándar, es decir, oscilando aproximadamente entre -2,5 y 2,5.

Estabilidad política y ausencia de violencia/terrorismo mide la percepción de la probabilidad de inestabilidad política y/o violencia por motivos políticos, incluido el terrorismo. La estimación da la puntuación del país en el indicador agregado, en unidades de una distribución normal estándar, es decir, oscilando aproximadamente entre -2,5 y 2,5.

Voz y rendición de cuentas recoge la percepción del grado en que los ciudadanos de un país pueden Tomar parte en la elección de su gobierno, así como tener la libertad de manifestar opiniones, la libertad de unirse a grupos y la libertad de los medios de comunicación. La estimación proporciona la calificación del país en el índice compuesto, expresada en términos de una distribución normal estándar, variando aproximadamente entre -2.5 y 2.5 unidades.

La tasa bruta de natalidad indica el número de nacidos vivos ocurridos durante el año, por cada 1.000 habitantes estimados a mitad de año. Restando la tasa bruta de mortalidad de la tasa bruta de natalidad se obtiene la tasa de crecimiento natural, que es igual a la tasa de variación de la población en ausencia de migraciones.

La tasa de mortalidad infantil es el número de niños que mueren antes de cumplir un año por cada 1.000 nacidos vivos en un año determinado.

Servidores seguros de Internet son el número de certificados TLS/SSL distintos y de confianza pública encontrados en la Encuesta de servidores seguros de Netcraft.

Personas que utilizan Internet (% de la población).

Las suscripciones de banda ancha fija se refieren a las suscripciones fijas al acceso de alta velocidad a la Internet pública (una conexión TCP/IP), a velocidades de bajada iguales o superiores a 256 kbit/s. Esto incluye módem por cable, DSL, fibra hasta el hogar/edificio, otras suscripciones de banda ancha fija (por cable), banda ancha por satélite y banda ancha inalámbrica fija terrestre.

La **Calidad Reguladora** capta la percepción de la habilidad gubernamental para crear y implementar políticas y regulaciones robustas que faciliten y fomenten el crecimiento del ámbito privado. La estimación proporciona la calificación del país en el índice compuesto, expresada en términos de una distribución normal estándar, variando aproximadamente entre -2.5 y 2.5 unidades.

Ingreso per cápita está en la paridad del poder adquisitivo (PPA). El PIB PPA es el producto interior bruto convertido a dólares internacionales utilizando los tipos de paridad del poder adquisitivo, Se determina sin considerar la disminución en el valor de los activos manufacturados ni la disminución y deterioro de los recursos naturales, y de esta manera los valores se presentan en dólares internacionales ajustados a los del año 2017

También encontramos el resto de variables como:

Índice de desarrollo humano que es un indicador compuesto que condensa los logros promedio de una nación en tres dimensiones fundamentales del desarrollo humano:

bienestar de la salud, adquisición de conocimientos y nivel de vida, el promedio de cada dimensión entre 0 y 1 (World Health Organization, 2023).

Índice nacional de ciberseguridad es una medida global activo que evalúa la capacidad de las naciones para prevenir amenazas cibernéticas y manejar incidentes en línea, doce indicadores que representan un porcentaje (NCSI, 2021).

Nivel de desarrollo digital se calcula en función del Índice de Desarrollo de las TIC (IDI) y del Índice de Preparación para las Redes, es el porcentaje medio que el país recibió del valor máximo de ambos índices (NCSI, 2021).

Indice global de ciberseguridad es una referencia fiable que mide el compromiso de los países con la ciberseguridad a nivel mundial, para concienciar sobre la importancia y las diferentes dimensiones de esta cuestión, se evalúa a lo largo de cinco pilares; medidas legales, medidas técnicas, medidas organizativas, desarrollo de capacidades, y cooperación, asi se agrega en una puntuación global expresada en porcentaje (ITU, 2022).

Índice de educación es la media de años de escolarización y años de escolarización previstos presentados en un promedio entre 0 y 1 (Smits & Permanyer, 2019).

2.6 Marco referencial

En su publicación Hall et al. (2021) estudiaron la comprensión de las geografías de las actividades económicas ilegales, la ciberdelincuencia, en concreto el fraude en línea con ánimo de lucro, a través de la lente de la geografía económica, los autores reconocen una literatura que rastrea las formas en que lo legal y lo ilegal, lo lícito y lo ilícito se entrelazan dentro de las regiones y a través de prácticas y movilidades sociales, económicas y políticas.

Así mismo, los ataques distribuidos de denegación de servicio son un tipo de ciberdelincuencia frecuente con costes potencialmente elevados para la economía real, los autores Overvest & Straathof (2015) desarrollaron un modelo econométrico que utiliza variables de carácter económico y tecnológico para analizar y dar razón a los patrones observados en los ataques de denegación de servicio distribuido, su enfoque se inspira en modelos que se encuentran en la literatura de comercio internacional, que explican cómo se producen los patrones de comercio, en este caso, descubrieron que las relaciones comerciales están estrechamente vinculadas con los ataques, mientras que factores económicos como el Producto Interno Bruto (PIB) per cápita no parecen tener una influencia significativa.

Según los autores Park et al. (2019) que investigaron si realmente el internet se asocia a los delitos cibernéticos encontraron que las actividades ciber delictivas dependen de factores socioeconómicos y de la velocidad de conexión, es probable que unos ingresos más elevados, un mayor nivel educativo, un menor índice de pobreza y una mayor desigualdad hagan que la penetración de Internet esté más positivamente relacionada con

los autores de ciberdelitos, que son realmente diferentes de las condiciones de la delincuencia terrestre en el mundo real.

La ciberdelincuencia, los ciberataques, la ciberguerra son el resultado de la formación de una civilización de la información que no sólo permite construir una sociedad más eficiente y exitosa, sino que también forma nuevas amenazas a la seguridad nacional; el estado debería proporcionar la definición terminológica; promover la formación de la coordinación adecuada de las actividades de diversos departamentos de información relacionados con las oportunidades del ciberespacio; crear un sistema eficaz de formación para las unidades cibernéticas estructurales especiales; cooperar con los organismos internacionales que tratan de proporcionar la seguridad cibernética en el mundo (Shimchenko, 2019).

Gañán et al. (2017) articularon y midieron las diversas formas en que la ciberdelincuencia repercute en la sociedad en general, siguieron una metodología mixta top-down/bottom-up para identificar sistemáticamente los impactos a corto y largo plazo de la ciberdelincuencia tanto a nivel de agente como de sociedad. Este marco sirve de base para evaluar las consecuencias económicas de la ciberdelincuencia más allá de los costes monetarios, centrándose en el impacto sobre el crecimiento económico.

Watters et al. (2012) por su parte en sus estudios etnográficos sobre ciberataques construyeron un modelo utilizando variables sociales y económicas independientes o predictivas de varios países de Europa del Este y compara indicadores de ciberdelincuencia dentro del sistema australiano de servicios financiero, encontraron un vínculo muy fuerte entre la corrupción percibida y el PIB en dos grupos distintos de países; los resultados del análisis de regresión sugieren que una mano de obra altamente

cualificada, móvil y que trabaja en un entorno de elevada corrupción percibida en los países objetivo está relacionada con el aumento de la ciberdelincuencia.

Chen et al. (2023) consideraron la ciberdelincuencia como un fenómeno social y construyeron un marco teórico que integra los factores sociales, económicos, políticos, tecnológicos y de ciberseguridad que influyen en la ciberdelincuencia; utilizaron modelos lineales generalizados (MLG) para identificar los principales factores que influyen en la ciberdelincuencia, y modelos de ecuaciones estructurales (MEE) para estimar los efectos directos e indirectos de los distintos factores en la ciberdelincuencia, los resultados del MLG sugieren que la inclusión de un amplio conjunto de factores socioeconómicos puede mejorar significativamente el poder explicativo del modelo, y que la ciberdelincuencia está estrechamente asociada al desarrollo socioeconómico, mientras que sus efectos sobre la ciberdelincuencia difieren según el nivel de renta. Además, los resultados del SEM revelan aún más las relaciones causales entre la ciberdelincuencia y numerosos factores contextuales, demostrando que los factores tecnológicos sirven como mediadores entre las condiciones socioeconómicas y la ciberdelincuencia (Chen et al., 2023).

Los autores Schiks et al. (2022) exploraron la relación entre los puntajes de las pruebas CITO (sistemas de prueba y monitoreo de clase mundial para completar programas educativos) y el delito cibernético en los Países Bajos, aplicando mínimos cuadrados ordinarios se utilizó análisis de regresión para comparar las puntuaciones de las pruebas CITO entre ciberdelincuentes, delincuentes tradicionales y no delincuentes, además de hermanos discordantes para controlar la confusión no medida por factores familiares. Los hallazgos revelaron que los ciberdelincuentes tienen puntajes de prueba CITO significativamente más altos en comparación con los delincuentes tradicionales y

puntajes de prueba CITO significativamente más bajos en comparación con los no delincuentes.

Por su parte Tao et al. (2019) estudiaron el análisis desde una perspectiva económica de la protección de la seguridad y la privacidad de los macrodatos donde los datos comprometidos a menudo se ven favorecidos por los posibles beneficios financieros (por ejemplo, chantaje, fraude, información falsa, robos de propiedad intelectual, competencia empresarial) concluyendo que un factor importante para las inversiones económicas actuales y futuras se debe a la motivación de las actividades de ciberdelincuencia. En este documento, analizamos en primer lugar una cuestión sobre nuestro esfuerzo en materia de seguridad y privacidad en términos de perspectivas económicas.

Los autores Ilievski & Bernik (2016) estudiaron la ciberdelincuencia y examinaron la posible relación entre un desarrollo económico débil y la escalada de los niveles de ciberdelincuencia, encontraron que a partir de la revisión bibliográfica, los estudios comparativos y la síntesis de los resultados las teorías sociológicas y los resultados de la investigación empírica, comprobamos que los factores socioeconómicos, como el PIB per cápita, el desempleo y la educación, están estrechamente relacionados con la incidencia de la ciberdelincuencia en los distintos países, esto les permitió concluir que el desarrollo económico relativamente pobre es una de las razones que contribuyen a una mayor incidencia de la ciberdelincuencia en los países de Europa del Este.

Asi mismo Ibrahim (2016) en su artículo logró establecer las particularidades de la ciberdelincuencia en Nigeria basándose en teorías motivacionales para ofrecer un marco conceptual tripartito para agrupar los nexos de la ciberdelincuencia encontrando

que los ciberdelitos están motivados por factores interrelacionados: los factores sociales, económicos, políticos, tecnológicos y de ciberseguridad.

Por otro lado, Srivastava et al. (2020) investigaron sobre como los ciberdelitos repercuten negativamente en la reputación y la economía de una nación, estos factores se agruparon en tres categorías: capital económico, capital tecnológico y preparación en materia de ciberseguridad donde de 124 países se desprende que el capital económico y el capital tecnológico son los principales factores que influyen en la frecuencia de los ciberdelitos que se originan en él además el capital tecnológico también media parcialmente en la relación entre el capital económico y la frecuencia de la ciberdelincuencia originada en la nación, por último la preparación en materia de ciberseguridad modera negativamente la relación entre el capital tecnológico y la frecuencia de la ciberdelincuencia que se origina en ella. Conectando con lo anterior, se utilizo un modelo de mínimos cuadrados parciales junto al modelo de ecuaciones estructurales.

Srivastava et al. (2020) estudiaron los diversos factores externos del ámbito sociocultural y político de Bangladesh que fomentan la ciberdelincuencia, también exploraron la relación entre la ciberdelincuencia y el ámbito del comercio electrónico encontrando que la debilidad económica de la nación empuja a los jóvenes a dedicarse a actividades ilegales utilizando su destreza tecnológica siendo los factores mencionados el motivo de este comportamiento, además, se demostró que los incidentes de ciberdelincuencia y el temor a ser víctima de tales actos delictivos han obstaculizado considerablemente el crecimiento y el desarrollo del sector del comercio electrónico en el país.

La ciberdelincuencia y la amenaza que genera están creciendo en su alcance, de acuerdo con un crecimiento similar de la tecnología de la información, Kigerl (2012) tomo una muestra de 132 países y descubrió que las naciones más ricas y con más usuarios de Internet per cápita tenían una mayor actividad de ciberdelincuencia y a su vez observó que el desempleo interactuaba con los usuarios de Internet, de modo que el efecto de la proporción de usuarios de Internet sobre el spam era mayor en los países con mayor desempleo.

Chen et al. (2021) demostraron la alta incidencia de delitos de en ciberespacio y como estaba estrechamente asociada a una gran población no agrícola, una elevada proporción de la industria terciaria en el PIB, un gran número de estudiantes universitarios en general, una mayor longitud del cable y un gran número de usuarios de Internet.

Por ultimo Casais Solano & Reinoso (2017) estudiaron los factores socio económicos en el cibercrimen de la siguiente manera:

Tabla 2

Variables agrupadas en factores

Factor	**Variables**
Económico	PIB (nominal, constante, per cápita y PPA), inflación, exportaciones de tecnología, índice de innovación, población activa, gasto en I+D y tasa de desempleo.
Politico	Libertades civiles, libertad política, libertad de prensa, nivel de corrupción, eficacia del gobierno, Estado de

	Derecho, riesgo político, riesgo de guerra y estabilidad política.
Social	Desarrollo humano, tasa de encarcelamiento, acceso a Internet de banda ancha, población, usuarios de Internet, esperanza de vida, tasa de escolarización primaria, tasa de escolarización secundaria, tasa de escolarización universitaria, tasa de robos y tasa de hurtos.

Nota: Los indicadores económicos, políticos y sociales de la tabla son presentados por Casais Solano & Reinoso (2017)

2.7 Marco legal

Convenio de Budapest sobre la Ciberdelincuencia

El Convenio del Consejo de Europa sobre la Ciberdelincuencia, conocido como Convenio de Budapest sobre la Ciberdelincuencia, se ha difundido a escala mundial y está sirviendo de referencia o "ley modelo" para la elaboración de legislación nacional en materia de ciberdelincuencia en muchos países de todo el mundo (Nguyen & Golman, 2021).

Dentro de los países de América Latina se encuentran Argentina, Brasil, Chile, Colombia, Costa Rica, Paraguay, Perú, República Dominicana y otros países que conforman 81 estados, además, Ecuador, Fiyi, Guatemala, México, Nueva Zelanda, Níger, Trinidad y Tobago, Uruguay y otros 11 países se encuentran como signatarios e invitados a adherirse (COE, 2022).

Asimismo, diversas organizaciones internacionales se han adherido a él, tales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Organización de los Estados Americanos (OEA), la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), y la Unión Internacional de Telecomunicaciones (UIT) (Cordero Ruiz, 2021).

En su marco establecido el convenio presenta los siguientes dos aspectos a tomar en cuenta cada estado participante:

> Delitos informáticos
>
> Artículo 7 – Falsificación informática
>
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal. (COE, 2022, pág. 10)
>
> Artículo 8 – Fraude informático
>
> Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:
>
> a. la introducción, alteración, borrado o supresión de datos informáticos;
> b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo

o para otra persona (COE, 2022, pág. 10).

Por su parte Isom (2022) explica los tratados y leyes aplicadas en forma internacional divida en dos grandes grupos;

Tabla 3

TRATADO DE LAS NACIONES UNIDAD

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (2000)	Este tratado, también conocido como la Convención de Palermo, obliga a los Estados parte a promulgar delitos penales nacionales dirigidos contra los grupos delictivos organizados y a adoptar nuevos marcos para la extradición, la asistencia jurídica mutua y la cooperación policial. Aunque el tratado no aborda explícitamente la ciberdelincuencia, sus disposiciones son muy pertinentes.
Convención sobre los Derechos del Niño (1989)	El artículo 34 de esta Convención obliga a los Estados Partes a proteger a los niños de todas las formas de explotación y abuso sexuales.
Protocolo Facultativo de la Convención sobre los Derechos del Niño (2001)	Este protocolo de la Convención de 1989 aborda la venta de niños, la prostitución infantil y la pornografía infantil. El artículo 3(1)(c) prohíbe la producción, distribución, difusión, venta y posesión de pornografía infantil; el preámbulo menciona Internet como medio de distribución.

	La definición de pornografía infantil establecida en el Artículo 2(3) es lo suficientemente amplia como para abarcar las imágenes virtuales de niños.

Nota: El autor de la información sobre los convenios es Isom (2022)

Tabla 4

TRATADOS EUROPEOS

Convenio sobre la Ciberdelincuencia (2001)	También conocido como Convenio de Budapest, es el primer acuerdo internacional destinado a reducir la delincuencia informática mediante la armonización de las legislaciones nacionales, aumento de la cooperación internacional y la mejora de las técnicas de investigación.
Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de naturaleza racista o xenófoba cometidos por medio de sistemas informáticos (2003)	Los Estados Partes que han ratificado este protocolo de la Convención de Budapest están obligados a promulgar leyes que penalicen los actos racistas o xenófobos que se expresen o comuniquen de otro modo en línea.

Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (2022)	Este protocolo se abrió a la firma el 12 de mayo de 2022 y no había entrado en vigor hasta diciembre de 2022.
Convenio sobre la protección de los niños contra la explotación y el abuso sexual (2007)	Este tratado prohíbe expresamente el uso de "tecnologías de la información y la informática (TIC)" para acceder a pornografía infantil (Artículo 21(1)(f)), distribuir pornografía infantil (Artículo 30(5)) o solicitar niños con fines sexuales (Artículo 23).

Nota: El autor de la información sobre los convenios es Isom (2022)

3 CAPITULO III

3.1 Metodología de la investigación

3.1.1 Enfoque de la investigación

El enfoque de esta investigación es cuantitativa ya que ocupa la recopilación y análisis de datos estructurados y que pueden representarse numéricamente, permitiendo conocer mejor la demografía de una población, medir cuántos usuarios utilizan un servicio o producto, examinar actitudes y comportamientos, documentar tendencias o explicar lo que se sabe anecdóticamente (Goertzen, 2017). Para los autores Kitchel y Ball (2014) una delimitación clara del uso de la teoría en la investigación cuantitativa puede servir a la profesión para centrarse más claramente en la investigación de problemas de calidad, en profundidad y comunicables a contextos más amplios.

3.1.2 Alcance

En primera medida esta investigación posee un alcance explicativo ya que pretende describir las influencias de una o varias variables sobre otras variables a partir de datos secundarios (Mangesti Rahayu, 2019). Además la investigación explicativa pretende examinar la causalidad entre variables que explican un fenómeno en varios campos de estudio (Mujianto, 2019).

Por otro lado, también cuenta con un alcance correlacional dado que se examina la relación entre una variable y otra u otras variables (Ikhsan & Tanjung, 2020). También existen otro autores que concuerdan en que los resultados de la investigación correlacional pueden utilizarse para determinar la prevalencia y las relaciones entre variables, así como

para prever acontecimientos a partir de los datos y conocimientos actuales (Curtis et al., 2016).

Así mismo usaremos un análisis descriptivo, de acuerdo con los autores Lalanne & Mesbah (2017) el enfoque descriptivo es estrictamente univariante, lo que constituye el requisito previo para cualquier enfoque estadístico. De acuerdo con Alvo et al. (2014) este análisis debe ser considerado por los investigadores antes de cualquier análisis sofisticado de datos, de forma que proporcionan un resumen y una dirección para analizar los datos de clasificación.

3.1.3 Diseño de la investigación

El propósito de la investigación es reconocer los factores determinantes de la ciberdelincuencia en América Latina y el Caribe, es así como se planteó un diseño de estudio no experimental. Los diseños no experimentales también pueden utilizarse para investigar las relaciones causa-efecto entre variables independientes y dependientes, pero hay una serie de características definitorias que marcan la verdadera investigación experimental como la manipulación de datos de la variables que se estudian (Rogers & Revesz, 2019). Como nos comenta Arias Gonzáles y Covinos Gallardo (2021) las variables de estudio no son sujetas a estímulos ni condiciones experimentales, sino que se evalúan en su entorno natural sin modificar ninguna circunstancia.

3.1.4 Población/Muestra

Si bien lo que se desea es estudiar la ciberdelincuencia mediate el uso de direcciones IP donde surgen los ataques, los autores Chen et al. (2023) comenzaron su estudio con la población global que contaba con mas de 600 millones de IP únicas además

que se excluyeron en sus bases aquellas que eran anónimas o que utilizaban algún proveedor de VPN ya que esto entorpece la geolocalización de donde proviene realmente el ataque, de esta forma se decide trabajar con la base tratada que representa la población de América Latina y El Caribe siempre y cuando se comprenda que estas IP junto a las herramientas de búsqueda poseen un 98% de precisión a nivel país y un 60% en lo que es ciudad tal cual lo explican los autores por lo que el análisis de hace a nivel sub región de cada país (por ejemplo Ecuador: costa, sierra y oriente)

3.1.5 Recolección de datos

Recolección de datos de fuentes secundarias se basará en diversas fuentes de recopilación de información; los datos de las listas de IP de FireHOL, Global Data Lab, Banco Mundial, Índice Global de Ciberseguridad (GCI) e Índice nacional de ciberseguridad (NSCI)

3.1.6 Método y tipo de Investigación

El método de esta investigación es deductivo puesto que las hipótesis son planteadas a partir de teorías y métodos científicos (Dahl, 2017). El tipo de investigación es trasversal dado que nuestro análisis se hará en un solo periodo.

3.2 Análisis de datos

En esta sección se presenta los el modelo que se va a utilizar en la investigación, las variables para el análisis y las herramientas de apoyo estadístico.

3.2.1 Modelo aplicado en la investigación- regresión lineal múltiple

La regresión lineal múltiple constituye un valioso enfoque estadístico para comprender el efecto de varios predictores de manera simultánea en una variable dependiente de naturaleza continua, sin embargo, su aplicación está condicionada por la necesidad de satisfacer ciertos supuestos rigurosos (Jankovic, 2022). Los supuestos que plantean en esta regresión para poder hacer un análisis pertinente son distribución normal, linealidad, ausencia de valores extremos y ausencia de vínculos múltiples entre las variables independientes (Uyanık & Güler, 2013).

En la explicación de la variación de los datos Y, es común la influencia de múltiples factores dando lugar a la regresión múltiple con más de una variable X, en la siguiente ecuación general de regresión lineal con n variables explicativas (X) se reconoce este modelo (Pinder, 2017):

$$\hat{Y} = \hat{\beta}_0 + \hat{\beta}_1 x_1 + \cdots + \hat{\beta}_n x_n + \hat{\varepsilon}$$

Donde

Y= Variable dependiente

β_0= Coeficiente de regresión de la variable dependiente

β_1= Coeficiente de regresión de la variable independiente

X_1 = Variable de independiente

βn= N numero de coeficientes de regresión de variables independientes

Xn= N número de variables independientes

ε= Error por cada variable, error aleatorio, error.

3.3 Variables del modelo

Tabla 5

Propuesta de variables para el modelo de acuerdo a la revisión de literatura.

Factor	Variable	Autores
Económico	Ingresos, ingresos per cápita, tasa bruta de natalidad y tasa bruta de mortalidad	Alaminos y López Monsalve (2009), Overvest & Straathof (2015), Ilievski & Bernik (2016), Casais Solano & Reinoso (2017).
Social	Índice de educación e índice de desarrollo humano.	Ilievski & Bernik (2016), Casais Solano & Reinoso (2017), Schiks et al. (2022).
Político	Control de corrupción, eficiencia del gobierno, restado de derecho, estabilidad política y ausencia de violencia/terrorismo, voz y rendición de cuentas y calidad reguladora.	Casais Solano & Reinoso (2017), Srivastava et al. (2020), Chen et al. (2023).
Tecnológico	Servidores seguros de Internet, personas que utilizan Internet, las suscripciones de	Kigerl (2012), Chen et al. (2023).

	banda ancha fija, Infraestructura de interne y nivel de desarrollo digital.	
Ciberseguridad	Índice global de ciberseguridad y el índice nacional de ciberseguridad	Chen et al. (2023) y el autor

Nota: Cada autor es representado por el aporte de la literatura investigada, el autor solo presenta la distribución por factor

3.4 Herramientas de análisis

El presente proyecto de investigación se implementará el uso de programas estadísticos como Microsoft Excel, el cual se utilizará para el tratamiento de la data y el software estadístico RStudio el cual servirá para aplicar el modelo de regresión múltiple además que nos ayudará para estimar los efectos directos e indirectos de diversos factores sobre la ciberdelincuencia.

4 CAPITULO IV

4.1 Resultados

En este capítulo presentaremos los resultados de la investigación planteada además que se caracteriza el sector estudiado para comprender los problemas que subyacen de la ciberdelincuencia comprendiendo su comportamiento mundial para lograr enfocarnos en los países perjudicados en América Latina y el Caribe.

4.2 Caracterización del sector

Figura 1: **Costo mundial de los daños causados por la ciberdelincuencia**

Nota: La información de esta imagen fue obtenida de Muggah y Margolis (2023) publicada en el Foro Económico Mundial

En el 2023 el Foro Económico Mundial publicó un artículo que hablaba expresamente de los costos mundiales producidos por el cibercrimen, el monto total estimado en el 2021 fue de $ 6 Trillones USD al año es traducido de la siguiente manera; $ 500 billones al mes, $115.4 billones a la semana, $ 16.4 billones al día, es decir $ 684.9 millones la hora, $ 11.4 millones el

minuto y $ 190 000 el segundo (Muggah & Margolis, 2023). En este articulo establecen la conexión no solo económica, sino que influye en la confianza de los usuarios cibernéticos además de que perjudican la reputación de instituciones públicas como privadas por lo que se debate sobre la falta de normas, estándares y reglas mundiales para anticipar y mitigar la ciberdelincuencia ya que se espera que para el 2025 los costos por daños de $10.5 Trillones USD. En concordancia la compañía PwC (2022) considera que para alcanzar el objetivo de combatir las amenazas cibernéticas hacia las compañías y sus usuarios es necesario añadir leyes enfocadas en ciberdelincuencia.

Sin embargo, se considera necesario analizar esta cifra con economías mundiales para observar a lo que nos estamos enfrentando.

País	2021	2022	2023*	2024*	2025*
Estados Unidos	$ 23.31	$ 25.46	$ 26.85	$ 27.74	$ 28.76
China	$ 17.82	$ 18.10	$ 19.37	$ 20.88	$ 22.40
Japón	$ 5.00	$ 4.23	$ 4.40	$ 4.52	$ 4.73
Alemania	$ 4.25	$ 4.07	$ 4.30	$ 4.44	$ 4.63
India	$ 3.15	$ 3.38	$ 3.73	$ 4.06	$ 4.40

Figura 2: **Países con mayor producto interior bruto (PIB) estimado de 2021 a 2025 (en trillones de dólares)**

Nota: Cifras estimadas fueron publicadas por el Fondo Monetario Internacional (2023).

El banco mundial hasta el 2021 presento los resultados del PIB de las economías más fuertes colocando a Estados Unidos como líder en el ranking con un total de $23.31 trillones de dólares, seguido de China con $ 17.82 trillones de dólares, colocando después a Japón con $ 5.00 trillones de dólares (The World Bank, 2023). Es decir que en el 2021 los costos de daños

causados por la ciberdelincuencia se encontrarían en el tercer puesto si es comparado con las economías más fuertes del mundo. Por otro lado las estimaciones del Fondo Monetario Internacional establecerían un crecimiento sostenible de las economías, a 2025 Estados Unidos habrá aumentado de $ 23 trillones a $28 trillones de dólares mientras que China habrá pasado dde $ 17 trillones a $ 22 trillones de dólares en 2025 (FMI, 2023), de acuerdo con las estimaciones ofrecidas por el Foro Económico Mundial los costos de daños causados por la ciberdelincuencia estarían estimados a $ 10 trillones de dólares por lo que mantendría su tercer puesto en comparación a las economías mundiales ya que si observamos el comportamiento de Japón es una estimación negativa ya que pasa de $ 5 trillones a $ 4,7 trillones en 2025.

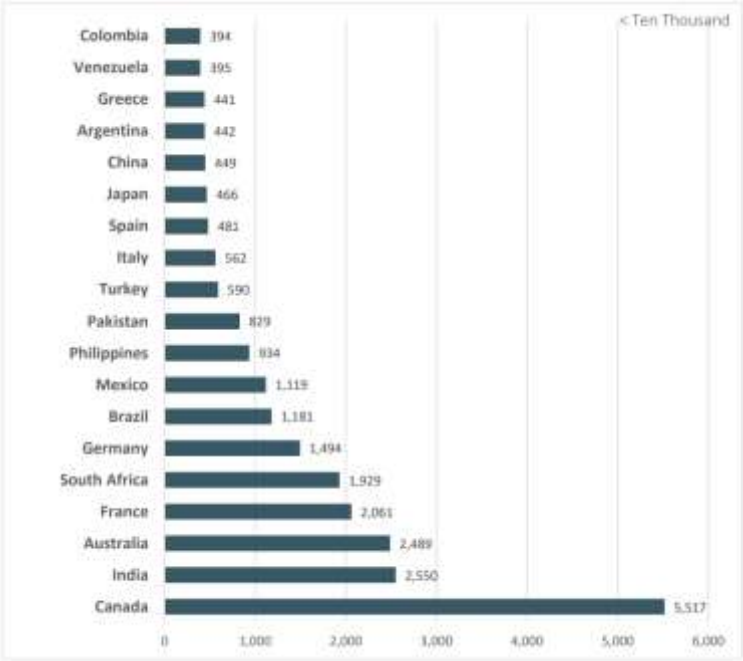


Figura 3: **Los 20 paises internacionales con más víctimas. FBI-2022.**

Nota: Los autores de esta imagen son FBI y la subdivisión Internet Crime Complaint Center (2023)

En el 2023 el FBI emitió un *Reporte sobre delitos en Internet 2022* en conjunto con IC3 (Internet Crime Complaint Center- Centro de Denuncias de Delitos por Internet), reportando los 20 países, fuera de Estados Unidos y Reino Unido, con el mayor número de víctimas por los Cibercrimen (FBI & IC3, 2023). En esta lista se destaca Colombia con el puesto veinte, Venezuela en el puesto diecinueve, Argentina en diecisiete, entrando en el top 10 encontramos a México en octavo y Brasil en séptimo puesto. Estableciendo los crímenes mas comunes como violación de datos personales, impago/no entrega, extorsión, soporte técnico, inversión, usurpación de identidad, fraude con tarjetas de crédito/cheques e inmobiliaria. De acuerdo con este reporte al final de 2022, contrastando con la información ofrecida por el Foro Económico Mundial, la cifra total de perdidas monetarias por delitos cibernéticos fue de $ 10,3 trillones de dólares, es decir la predicción de que anualmente se esperaba por las perdidas monetarias esta por igualarse.

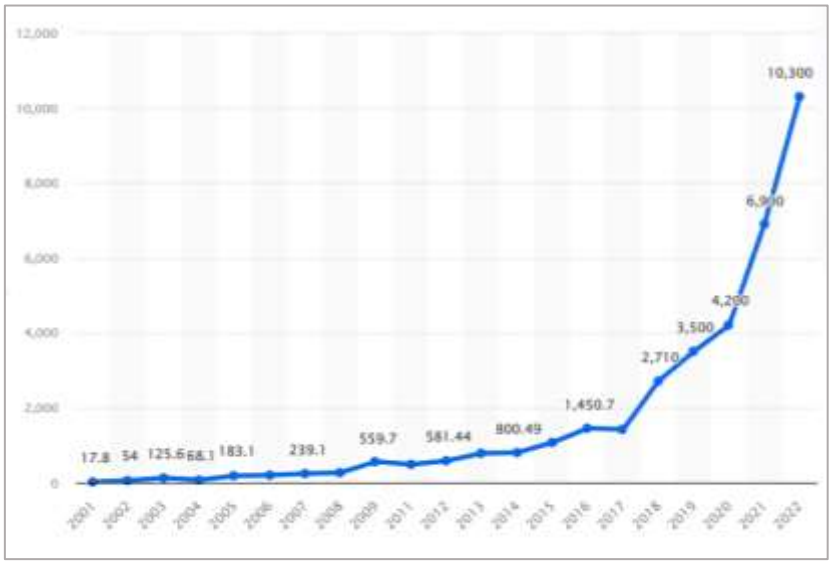


Figura 4: **Costos globales por ciberataque 2001-2022**

Nota: La autora de esta imagen es Petrosyan (2023), su fuente de información es Internet Crime Complaint Center y publica este grafico en la plataforma S*tatista*.

Por este lado observamos que a partir del año 2018 se disparan las cifras por pérdidas monetarias dadas por los ciberataques, de acuerdo con varios autores el Covid-19 fue uno de los factores que impulsaron los niveles altos ciberataque por lo que el fenómeno obligó en gran medida a empresas y usuarios a adaptarse a los cambios en las prácticas laborales y la socialización haciendo que se pase cada vez más tiempo en línea (Pranggono & Arabo, 2021; Lallie et al., 2021; Jhanjhi et al., 2022; Alsmadi & Tawalbeh, 2022).

4.3 Modelo de regresión lineal múltiple

Como primer aspecto, tomamos en cuenta la amplitud de la distribución de los valores en el número de ataques, nuestra matriz de correlación demostró que planteando el valor total registrado en nuestra base de datos puede identificar la significancia con otras variables, es tal que para evitar una correlación clara entre la población y el número de ciberataques se optó por juntar estas variables y crear la variable dependiente de *número de ciberataques por cada mil personas* (ATT1000). Recordando además que los ciberataques registrados engloban la gama amplia (tipos y categorías) de la ciberdelincuencia en el 2021.

Como variable independiente está el índice de desarrollo humano (IDH), ingresos (INC), ingresos per cápita (INCPERCAP), índice de educación (EDU), tasa bruta de natalidad (BRATE), tasa bruta de mortalidad (MRATE), como Indicadores Mundiales de Gobernanza (IAG) tenemos control de corrupción (CONTCORR), eficiencia del gobierno (GOVEFF), restado de derecho (RULELAW), estabilidad política y ausencia de violencia/terrorismo (POLISTAB), voz y rendición de cuentas (VOICACCO), calidad reguladora (REGQUA), por otro lado, los servidores seguros de internet (SECINTSERV), personas que utilizan internet

(INDUSINT), las suscripciones de banda ancha fija (FIXBROSUBS), infraestructura de internet (INTINFRA), índice global de ciberseguridad (GLOBCYBINDEX), índice nacional de ciberseguridad (NATCYBINDEX) y nivel de desarrollo digital (DIGDEVELEV).

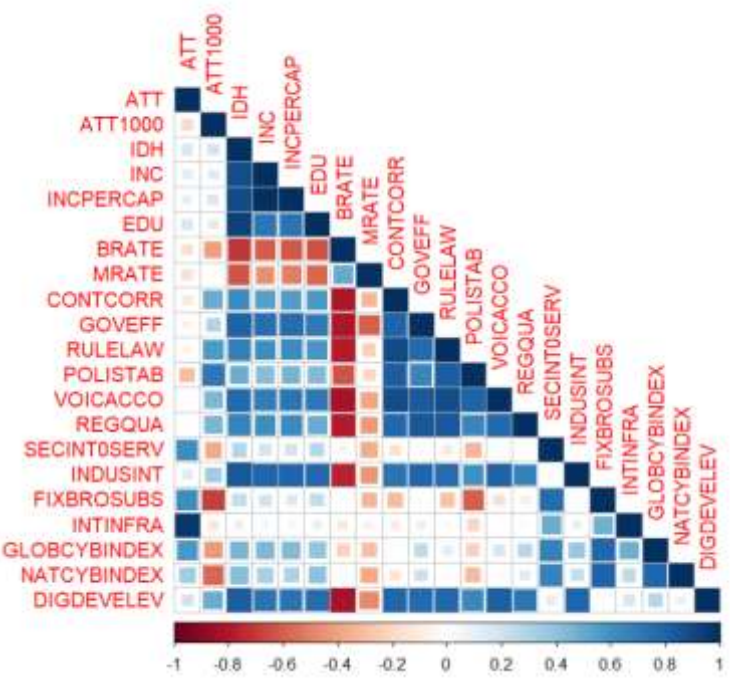


Figura 5: **Matriz de correlación variables de estudio**

Nota: La matriz de correlación presentada es el primer modelo planteado de acuerdo a la revisión de la literatura, con un total de diecinueve variables.

Como demostración, se observa el número de ciberataques dado en cifras totales, este no correspondió a un modelo elocuente por lo que muchas variables no responden al comportamiento de la variable dependiente. Así mismo podremos entender que las variables de la dimensión política demuestran estar altamente correlacionadas lo cual se debe tomar en cuenta cuando planteemos el modelo final y evitar problemas de multicolinealidad. Buscamos una respuesta positiva, pero no altamente correlacionadas, es así que al plantear una variable

dependiente para disminuir la alta dispersión de datos y mejorar la normalidad podemos reconocer un modelo mayormente variable significativas capaces de explicar el modelo. Cabe destacar que los ingresos per cápita, las subscripciones de banda ancha fija y los servidores seguros de internet se les aplicaron logaritmo natural para mejorar la normalidad de los residuos al aplicar las pruebas pertinentes.

```
Call:
lm(formula = ATT1000 ~ IDH + INC + INCPERCAP + EDU + BRATE +
    MRATE + CONTCORR + GOVEFF + RULELAW + POLISTAB + VOICACCO +
    REGQUA + SECINTOSERV + INDUSINT + FIXBROSUBS + INTINFRA +
    GLOBCYBINDEX + NATCYBINDEX + DIGDEVELEV)

Residuals:
      Min        1Q    Median        3Q       Max
-0.133432 -0.019794  0.005033  0.032910  0.116966

Coefficients:
              Estimate Std. Error t value Pr(>|t|)
(Intercept) -1.4906030  3.1580245  -0.472  0.64615
IDH          0.1793862  2.3285142   0.077  0.93998
INC         -2.5156748  3.3886793  -0.742  0.47341
INCPERCAP    0.4422855  1.2193019   0.363  0.72368
EDU         -0.0756270  0.9629891  -0.079  0.93881
BRATE        0.0086331  0.0134554   0.642  0.53427
MRATE        0.0046077  0.0054522   0.845  0.41606
CONTCORR    -0.2556625  0.0818863  -3.122  0.00971 **
GOVEFF      -0.0541593  0.1353664  -0.400  0.69675
RULELAW      0.0594971  0.1073461   0.554  0.59049
POLISTAB     0.0953347  0.0924779   1.031  0.32473
VOICACCO    -0.1081017  0.1373094  -0.787  0.44775
REGQUA       0.2945115  0.1151053   2.559  0.02658 *
SECINTOSERV  0.0698606  0.0334505   2.088  0.06080 .
INDUSINT     0.0120757  0.0038617   3.127  0.00963 **
FIXBROSUBS  -0.0561208  0.0997897  -0.562  0.58513
INTINFRA    -0.0004474  0.0008618  -0.519  0.61396
GLOBCYBINDEX -0.0035582  0.0024974  -1.425  0.18197
NATCYBINDEX -0.0045620  0.0025912  -1.761  0.10605
DIGDEVELEV   0.0167587  0.0044468   3.769  0.00311 **
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.09933 on 11 degrees of freedom
Multiple R-squared:  0.9417,    Adjusted R-squared:  0.841
F-statistic: 9.353 on 19 and 11 DF,  p-value: 0.0002689
```

Figura 6: **Modelo regresión lineal múltiple**

Nota: El primer modelo de regresión lineal múltiple planteado es presentado para hacer el análisis de las variables estadísticamente significativas.

En el primer modelo al que aplicamos una regresión lineal múltiple de las diecinueve variables independientes solo **control de corrupción, calidad regadora, servidores seguros de internet, personas que utilizan internet y nivel de desarrollo digital** fueron estadísticamente significativas, sin embargo la variable servidores seguros de internet se

encuentra con un p-value por encima de 0.05, esto da un indicio de que eliminado variables tanto el modelo como la variable pueden tener un mejor ajuste. que se analizará la matriz de correlación procediendo a escoger las variables que mejor respondan al modelo.

```
Call:
lm(formula = ATT1000 ~ INCPERCAP + REGQUA + CONTCORR + SECINTSERV +
    INDUSINT + FIXBROSUBS + NATCYBINDEX + DIGDEVELEV)

Residuals:
      Min        1Q    Median        3Q       Max
-0.170231 -0.050868  0.008004  0.052147  0.128289

Coefficients:
              Estimate Std. Error t value Pr(>|t|)
(Intercept)  1.719462   0.413242   4.161 0.000407 ***
INCPERCAP   -0.487069   0.123244  -3.959 0.000666 ***
REGQUA       0.234461   0.051927   4.515 0.000171 ***
CONTCORR    -0.270022   0.046993  -5.746 8.84e-06 ***
SECINTSERV   0.065988   0.022247   2.966 0.007132 **
INDUSINT     0.008868   0.002513   3.528 0.001892 **
FIXBROSUBS  -0.208407   0.034500  -6.041 4.43e-06 ***
NATCYBINDEX -0.004149   0.001497  -2.772 0.011124 *
DIGDEVELEV   0.016978   0.003057   5.554 1.39e-05 ***
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.08444 on 22 degrees of freedom
Multiple R-squared:  0.9157,    Adjusted R-squared:  0.8851
F-statistic: 29.89 on 8 and 22 DF,  p-value: 4.344e-10
```

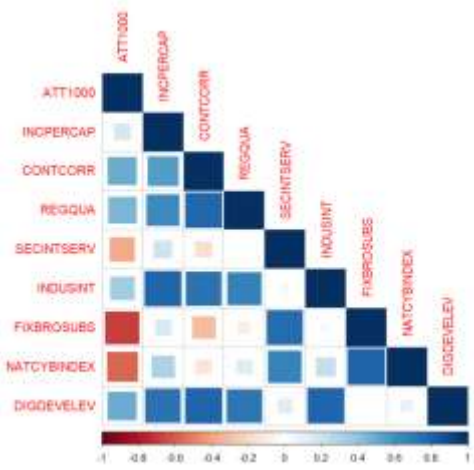


Figura 7: Segundo modelo regresión lineal múltiple y su matriz de correlación.

Nota: El segundo modelo planteado con las ocho variables significativas del modelo junto a su matriz de correlación son presentadas para el análisis descriptivo

Analizando la nueva matriz de correlación con las mejores variables predictoras lo primero que se observa es; a) las variables ingresos per cápita, calidad reguladora, control de corrupción, servidores seguros de internet, personas que utilizan internet, las suscripciones de banda ancha fija, índice nacional de ciberseguridad y nivel de desarrollo digital cumplen con un p-value menor a 0.05, b) el ingresos per cápita, control de corrupción, las suscripciones de banda ancha fija y desarrollo digital poseen un efecto negativo es decir en medida que disminuyan en su unidad de análisis el número de ciberataques aumentará, y c) en la matriz de correlación se observa que calidad reguladora y control de corrupción están altamente correlacionadas, entendible ya que pertenecen a las dimensiones de IAG, el ingreso per cápita y personas que

utilizan internet altamente correlacionadas al igual que nivel de desarrollo digital con control de corrupción y personas que utilizan internet.

Antes de aceptar el modelo planteado y analizar el ajuste del modelo es necesario aplicar las pruebas pertinentes para determinar si el modelo cumple con normalidad, cumple con el principio de homocedasticidad y no existe autocorrelación.

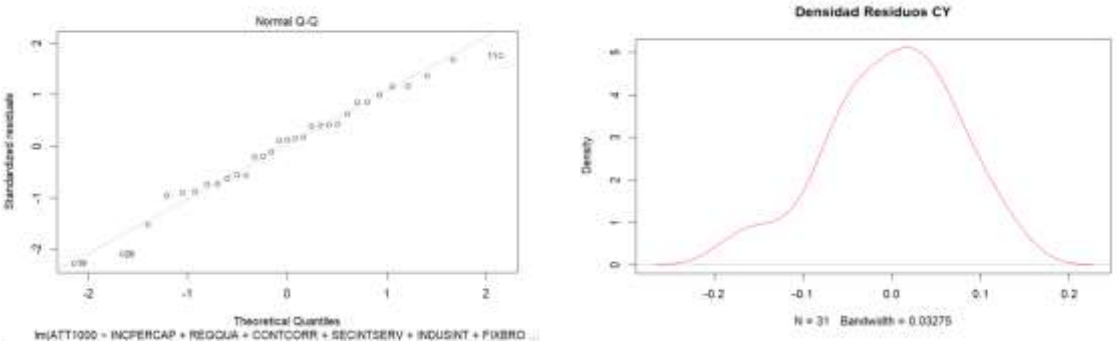


Figura 8: Grafico Q-Q y distribución de los residuos.

Nota: Las ilustraciones son presentadas como apoyo del análisis del segundo modelo planteado para la evaluación de los residuos.

En el grafico Q-Q como prueba para evaluar la distribución de los residuos podemos observar que siguen una distribución normal ya que los puntos están próximos a la recta, en el lado izquierdo del grafico se puede reconocer una cola larga es por eso que se conforma con el grafico de Densidad de Residuos. Bajo este esquema se confirma la propuesta lo que nos quiere decir que se observa una retribución normal con cola larga

4.4 Pruebas de diagnóstico para la regresión lineal múltiple

4.4.1 Normalidad

En la prueba de normalidad se toma como referencia un nivel de significancia de $\propto$ =0.05, para el test se plantean las siguientes hipótesis

Ho: Los datos demuestran una distribución normal

H1: Los datos no demuestran una distribución normal

```
        Pearson chi-square normality test

data:  ResiduosCY
P = 3.3226, p-value = 0.6504
```

Figura 9: Prueba de normalidad Prearson chi-square

Nota: Las ilustraciones presenta el test Prearson chi-square del segundo modelo planteado

La prueba se destaca exitosamente ya que el resultado del p-value es mayor, siendo 0.6504 esto nos dice que los datos demuestran una distribución normal. Siendo así se puede perseguir con las pruebas de enfermedades.

4.4.2 Heterocedasticidad

En la prueba de heterocedasticidad se trabajó con una significación de $\propto$ =0.05, las hipótesis planteadas son:

Ho: Homocedasticidad

H1: Heteroscedasticidad

```
        studentized Breusch-Pagan test

data:  data2
BP = 5.2112, df = 8, p-value = 0.7348
```

Figura 10: Prueba de Homocedasticidad de Breush-Pagan

Nota: Las ilustraciones presenta el test de Breush-Pagan del segundo modelo planteado

El éxito de la prueba Breusch Pagan resulto en un p-value de 0.7348, por tanto, es mayor a 0.05, es así como no se rechaza la hipótesis nula dado que los datos poseen homocedasticidad

4.4.3 Autocorrelación

Así mismo con esta prueba se trabajó con un nivel de significancia de $\propto$ =0.05, establecido con las siguientes hipótesis:

Ho: No existe autocorrelación

H1: Existe autocorrelación

```
        Durbin-Watson test

data:  data2
DW = 1.8714, p-value = 0.2916
alternative hypothesis: true autocorrelation is greater than 0
```

Figura 11: Prueba de autocorrelación Durbin Watson

Nota: Las ilustraciones presenta el test de Durbin Watson del segundo modelo planteado

Los resultados de la prueba determino un p value de 0.2916 lo que significa que al ser mayor a 0.05 se rechaza la hipótesis alternativa, en el modelo no cuenta con problemas de autocorrelación

4.4.4 Multicolinealidad

```
#Multicolinealidad
#Prueba VIF
#Criterio VIF > 10 existe multicolinealidad problematica
vif(data2)
INCPERCAP      REGQUA    CONTCORR  SECINTSERV    INDUSINT FIXBROSUBS NATCYBINDEX  DIGDEVELEV
 3.486650    3.399648    6.004131    2.716974    4.910789    4.769736    3.928805    5.060953
```

Figura 12: Prueba de multicolinealidad mediante el cálculo del VIF

Nota: Las ilustraciones presenta el cálculo del VIF (Factor de Inflación de la Varianza) del segundo modelo planteado por cada variable para su análisis de multicolinealidad.

Por último, se ha aplicado la prueba de multicolinealidad, en esta prueba se si el VIF es mayor a diez la variable presenta un grave problema de multicolinealidad, si se encuentra entre uno y cinco no deberíamos preocuparnos por la multicolinealidad. Sin embargo, es destacable que se ha decidido mantener en el modelo nivel de desarrollo digital y control de corrupción en el modelo, la decisión se toma a partir de que las pruebas denotan un buen ajuste del modelo; no cuenta con enfermedades y cumple con normalidad. Además de haber realizado las pruebas de manera individual y sus resultados no inciden en la creación de enfermedades del modelo, ya que en conjunto estas variables son capaces de explicar muy bien el modelo (anexos).

Otra prueba que hicimos para determinar que estas variables aportan al modelo fue efectivamente correr el modelo sin variable control corrupción, otro modelo sin nivel de desarrollo digital y un último modelo sin ambas variables. Se demostró que una o más variables perdían su significancia por lo que son necesarias para explicar el comportamiento de las otras variables por como influyen sobre la ciberdelincuencia

4.5 Planteamiento del modelo de regresión lineal múltiple

A continuación, se plantea la ecuación de modelo de regresión:

$$1)\ \hat{Y} = \hat{\beta}_0 + \hat{\beta}_1 x_1 + \hat{\beta}_2 x_2 + \hat{\beta}_3 x_3 + \hat{\beta}_4 x_4 + \hat{\beta}_5 x_5 + \hat{\beta}_6 x_6 + \hat{\beta}_7 x_7 + \hat{\beta}_8 x_8 + \hat{\mu}$$

$$2)\ Y = 1.719 - 0.488\, x_1 + 0.234\, x_2 - 0.270\, x_3 + 0.066\, x_4 + 0.009\, x_5 - 0.208\, x_6 - 0.004\, x_7 + 0.017\, x_8 + \mu$$

Es decir que; cada que disminuya el 0.488 dólares del ingreso per cápita (x_1) aumentara 1 ciberataque por cada mil habitantes, por cada 0.234 puntos porcentuales que aumente la calidad reguladora(x_2) del país aumentará 1 ciberataque por cada mil habitantes, por cada que disminuya los 0.270 puntos porcentuales del control de corrupción (x_3) aumentara 1 ciberataque por cada mil habitantes, por cada 0.066 de subscripciones a servidores seguros de internet (x_4) aumentara 1 ciberataque por cada mil habitantes en el país, por cada 0.009 puntos porcentuales que aumente de personas que utilizan internet (x_5) aumentara 1 ciberataque por cada mil habitantes, por cada que disminuya 0.208 número de suscripciones de banda ancha fija (x_6) aumentará 1 ciberataque por cada mil habitantes , por cada 0.004 puntos porcentuales que disminuya el índice nacional de ciberseguridad(x_7) aumentará 1 ciberataque por cada mil habitantes, por último, por cada 0.017 puntos porcentuales que aumente el nivel de desarrollo digital(x_8) aumentará 1 ciberataque por cada mil habitantes en el país.

El de igual manera muy importante reconocer que el r cuadrado ajustado del modelo tiene un muy buen ajuste, r^2 =0.8851. Esto nos indica que con éxito el 88.51% de la variabilidad del número de ciberataques puede ser predicha por el modelo de regresión lineal múltiple planteado.

5 CAPITULO V

5.1 Discusión

De acuerdo con Butkovic et al. (2019) están más que claro que elaborar perfiles geográficos de la ciberdelincuencia permite asimilar una importante diferenciación entre el comportamiento socioeconómico, tecnológicos y políticos. Chandra y Snowe (2020) agregan a este aspecto que el objetivo es identificar técnicas y políticas pertinentes para recopilación de información con el fin de simplificar y apoyar la actividad de los profesionales de la lucha contra la ciberdelincuencia. De esta forma se ha establecido una ventaja sobre el estudio de esta categoría de la delincuencia, poder observar un comportamiento desde diferentes factores en el nacimiento de la ciberdelincuencia permitirá crear políticas en torno a las variables significativas, el buen ajuste del segundo modelo planteado por tanto nos acerca a la realidad de los factores que influyen en las economías de América Latina y el Caribe con el propósito de evitar perjuicios a entidades públicas y privadas.

Se establece con estas explicaciones que el comportamiento de las variables en otros países (Overvest & Straathof, 2015; Kigerl, 2012; Ibrahim, 2016; Shimchenko, 2019; Hall et al., 2021; Chen et al., 2023) dependerán mucho del contexto geopolítico, socioeconómico y tecnológico. Es decir que en esta medida se esperaba que en el aspecto social el índice de desarrollo humano como la educación jugaran un papel importante en la asociación de la ciberdelincuencia, sin embargo, las pruebas demostraron lo contrario. Por otro lado, en el aspecto tecnológico la infraestructura de internet fue otras de las variables que el modelo rechazo, es decir que el contexto de América Latina y el Caribe no es necesario reconocer el nivel de educación o las estructuras de internet para que el cibercrimen se establezca.

5.2 Conclusiones

- En el factor económico solo el ingreso per cápita se asoció negativamente con la ciberdelincuencia
- En el factor social ni el índice de educación, ni el índice de desarrollo humano demostraron ser significativas para el modelo
- En el factor político la calidad reguladora se asoció positivamente mientras que el control de la corrupción se asoció negativamente con la ciberdelincuencia
- En el factor tecnológico los servidores seguros de internet (métrica en número de subscripciones) y personas que utilizan internet (métrica porcentaje de la población) se asoció positivamente con la ciberdelincuencia mientras que las subscripciones de banda ancha fija se asociaron negativamente con la ciberdelincuencia. Por otro lado, el nivel de desarrollo digital se asoció positivamente con la ciberdelincuencia.
- En el factor de ciberseguridad el índice nacional de ciberseguridad se asoció negativamente con la ciberdelincuencia
- Se concluye que los altos costos por efecto de la ciberdelincuencia son motivaciones para estudiar el fenómeno en los diferentes factores con el propósito de promover políticas apegadas a la regulación de esta nueva categoría de crimen en América Latina y El Caribe.
- Se concluye el ajuste del modelo y las variables ingresos per cápita, calidad reguladora, control de corrupción, servidores seguros de internet, personas que utilizan internet, las suscripciones de banda ancha fija, índice nacional de ciberseguridad y nivel de desarrollo

digital explican en un 88.51% la variabilidad de numero de ciberataques en América Latina y El Caribe en 2021

5.3 Recomendaciones

- Se recomienda para futuras investigaciones tomar en cuenta al menos otro año para la base de datos ya que podría percibir el comportamiento de las variables en el tiempo.
- Se recomienda iniciar investigaciones sobre la ciberdelincuencia de manera regional con el propósito de generar una base de datos que nos permita comparar entre las naciones de América Latina y el Caribe, permitiendo establecer un nuevo marco legal en la región.
- Se recomienda para futuras investigaciones reconocer más variables para el modelo econométrico dado que no se han registrado actualizaciones de otras variables de estudio.

6 Referencias Bibliográficas

Acero, A., & Hue, T. (2019). *Efecto de los bienes no transables en el proceso productivo de los bienes transables Período 1990-2015*. http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAU2212.pdf

Agbo, M., & Zabsonré, A. (2022). *Mobile Phone Communication and Mobile Money Adoption in Burkina Faso: A Direct and Indirect Network Effects Analysis* (SSRN Scholarly Paper 4063995). https://doi.org/10.2139/ssrn.4063995

Akers, R. L., & Jennings, W. G. (2015). Social Learning Theory. En *The Handbook of Criminological Theory* (pp. 230-240). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781118512449.ch12

Alaminos, A., & López Monsalve, B. (2009). *La medición del desarrollo social*. https://doi.org/10.14198/OBETS2009.4.02

Alazab, M., Alhyari, S., Awajan, A., & Abdallah, A. B. (2021). Blockchain technology in supply chain management: An empirical study of the factors affecting user adoption/acceptance. *Cluster Computing*, *24*(1), 83-101. https://doi.org/10.1007/s10586-020-03200-4

Alsmadi, I., & Tawalbeh, L. (2022). New Waves of Cyber Attacks in the Time of COVID19. En P. Nicopolitidis, S. Misra, L. T. Yang, B. Zeigler, & Z. Ning (Eds.), *Advances in Computing, Informatics, Networking and Cybersecurity: A Book Honoring Professor Mohammad S. Obaidat's Significant Scientific Contributions* (pp. 617-630). Springer International Publishing. https://doi.org/10.1007/978-3-030-87049-2_21

Alvo, M., Yu, P. L. H., Alvo, M., & Yu, P. L. H. (2014). *Exploratory Analysis of Ranking Data*. 7-21. https://doi.org/10.1007/978-1-4939-1471-5_2

Anaya Laime, & Jhony Abel. (2022). La ciberdelincuencia y su influencia en el desarrollo económico-social en el distrito de Ayacucho, 2021. *Repositorio Institucional - UCV*. https://repositorio.ucv.edu.pe/handle/20.500.12692/101768

Arias Gonzáles, J. L., & Covinos Gallardo, M. (2021). *Diseño y metodología de la investigación*. Enfoques Consulting EIRL. http://repositorio.concytec.gob.pe/handle/20.500.12390/2260

Atnashev, V. R., & Yakheeva, S. N. (2019). International Cooperation on Cybercrime and Cyberterrorism. *Евразийская Интеграция: Экономика, Право, Политика*, *0*(3), 37-42.

Bodemer, K. (1998). La globalización. Un concepto y sus problemas. *Nueva sociedad*, *156*, 54-69.

Borisova, E. S., & Belousov, A. L. (2019). Innovations as a tool for providing cyber security and increasing the efficiency of banking system. *Russian Journal of Economics and Law*, *13*(3), 1330-1342. https://doi.org/10.21202/1993-047X.13.2019.3.1330-1342

Butkovic, A., Mrdovic, S., Uludag, S., & Tanovic, A. (2019). Geographic profiling for serial cybercrime investigation. *Digital Investigation*, *28*, 176-182. https://doi.org/10.1016/j.diin.2018.12.001

Callon, M. (2001). Actor Network Theory. En N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 62-66). Pergamon. https://doi.org/10.1016/B0-08-043076-7/03168-5

Carroll, C., & Wang, T. (2023). Chapter 25—Epidemiological expectations. *Handbook of Economic Expectations* (pp. 779-806). Academic Press. https://doi.org/10.1016/B978-0-12-822927-9.00034-3

Casais Solano, P., & Reinoso, A. (2017). *Socio-economic factors in cybercrime: Statistical study of the relation between socio-economic factors and cybercrime*. 1-4. https://doi.org/10.1109/CyberSA.2017.8073392

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W.-J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security, 105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Chandra, A., & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, *38*, 100467. https://doi.org/10.1016/j.accinf.2020.100467

Chen, S., Gao, C., Jiang, D., Hao, M., Ding, F., Ma, T., Zhang, S., & Li, S. (2021). The Spatiotemporal Pattern and Driving Factors of Cyber Fraud Crime in China. *ISPRS International Journal of Geo-Information*, *10*(12), Article 12. https://doi.org/10.3390/ijgi10120802

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1), Article 1. https://doi.org/10.1057/s41599-023-01560-x

COE. (2022). *The Budapest Convention (ETS No. 185) and its Protocols*. Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Cordero Ruiz, N. F. (2021). *La ciberdelincuencia*. https://ebuah.uah.es/dspace/handle/10017/49563

Cumming, D. J., Vanacker, T., & Zahra, S. A. (2021). Equity Crowdfunding and Governance: Toward an Integrative Model and Research Agenda. *Academy of Management Perspectives*, *35*(1), 69-95. https://doi.org/10.5465/amp.2017.0208

Curtis, E. A., Comiskey, C., & Dempsey, O. (2016). Importance and use of correlational research. *Nurse Researcher*, *23*(6), 20-25. https://doi.org/10.7748/nr.2016.e1382

Dahl, P. (2017). Hypothetico-Deductive Method. En *Music and Knowledge: A Performer's Perspective* (pp. 51-61). Brill. https://doi.org/10.1163/9789463008877_008

Dankert, R. (2012). Actor–Network Theory. En S. J. Smith (Ed.), *International Encyclopedia of Housing and Home* (pp. 46-50). Elsevier. https://doi.org/10.1016/B978-0-08-047163-1.00606-8

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, *41*(8), 1796-1808. https://doi.org/10.1080/0144929X.2021.1905066

Delfín Ortega, O. V., & Navarro Chávez, J. C. L. (2015). Productividad total de los factores en las terminales de contenedores en los puertos de México: Una medición a través del índice Malmquist. *Contaduría y Administración*, *60*(3), 663-685. https://doi.org/10.1016/j.cya.2015.05.011

Donalds, C., & Osei-Bryson, K.-M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*, 403-418. https://doi.org/10.1016/j.chb.2018.11.039

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32. https://doi.org/10.1080/13523260.2019.1678855

Elsner, W., Heinrich, T., & Schwardt, H. (2015). *The Information Economy and the Open-Source Principle* (pp. 451-471). https://doi.org/10.1016/B978-0-12-411585-9.00015-4

Enríquez Pérez, I. (2016). Las teorías del crecimiento económico: Notas críticas para incursionar en un debate inconcluso. *Revista Latinoamericana de Desarrollo Económico*, *25*, 73-125.

Etzkowitz, H. (2001). Science and Industry. En N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 13610-13614). Pergamon. https://doi.org/10.1016/B0-08-043076-7/03171-5

FBI, & IC3. (2023). *Internet Crime Complaint Center(IC3) Report*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Fengru, C., & Guitang, L. (2019). Chapter 3—Analytical Framework of Microcosmic GPN Studies. En C. Fengru & L. Guitang (Eds.), *Global Value Chains and Production Networks* (pp. 41-68). Academic Press. https://doi.org/10.1016/B978-0-12-814847-1.00003-8

Fenoy Illacer, D. R. (2023). *Implantación de un sistema DLP en una clínica dental*. https://openaccess.uoc.edu/handle/10609/147303

FMI. (2023). *World Economic Outlook (April 2023)—GDP per capita, current prices*. https://www.imf.org/external/datamapper/NGDPDPC@WEO

Fonfría, A., & Duch-Brown, N. (2020). *Ciberseguridad económica*.

Forbes. (2022). *El negocio de la ciberdelincuencia podría convertirse en la tercera economía mundial*. Forbes Ecuador. https://www.forbes.com.ec/negocios/el-negocio-ciberdelincuencia-podria-convertirse-tercera-economia-mundial-n14526

Gañán, C. H., Ciere, M., & van Eeten, M. (2017). Beyond the pretty penny: The Economic Impact of Cybercrime. *Proceedings of the 2017 New Security Paradigms Workshop*, 35-45. https://doi.org/10.1145/3171533.3171535

Goertzen, M. J. (2017). Chapter 3. Introduction to Quantitative Research and Data. *Library Technology Reports*, *53*(4), Article 4.

Gorter, C., & Nijkamp, P. (2001). Location Theory. En N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (pp. 9013-9019). Pergamon. https://doi.org/10.1016/B0-08-043076-7/02490-6

Gupta Bhol, S., Mohanty, J., & Kumar Pattnaik, P. (2023). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings, 80*, 2274-2279. https://doi.org/10.1016/j.matpr.2021.06.228

Haftor, D. M., Costa Climent, R., & Lundström, J. E. (2021). How machine learning activates data network effects in business models: Theory advancement through an industrial case of promoting ecological sustainability. *Journal of Business Research, 131*, 196-205. https://doi.org/10.1016/j.jbusres.2021.04.015

Hall, T., Sanders, B., Bah, M., King, O., & Wigley, E. (2021). Economic geographies of the illegal: The multiscalar production of cybercrime. *Trends in Organized Crime*, *24*(2), 282-307. https://doi.org/10.1007/s12117-020-09392-w

Haryanti, T., & Subriadi, A. P. (2020). Factors and Theories for E-Commerce Adoption: A Literature Review. *International Journal of Electronic Commerce Studies*, *11*(2), Article 2. https://doi.org/10.7903/ijecs.1910

Ibe, O. C. (2014). Chapter 1—Basic Probability Concepts. En O. C. Ibe (Ed.), *Fundamentals of Applied Probability and Random Processes (Second Edition)* (pp. 1-55). Academic Press. https://doi.org/10.1016/B978-0-12-800852-2.00001-8

IBM: Cost of a Data Breach Report. (2021). *Computer Fraud & Security*, *2021*(8), 4. https://doi.org/10.1016/S1361-3723(21)00082-8

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44-57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Ikhsan, M., & Tanjung, M. S. B. (2020). Pengaruh Budaya Organisasi dan Gaya Kepemimpinan Terhadap Kinerja Pegawai Dinas Pemberdayaan Masyarakat dan Desa Kota Sungai Penuh. *OSF Preprints*, Article zn96h. https://ideas.repec.org//p/osf/osfxxx/zn96h.html

Ilievski, A., & Bernik, I. (2016). SOCIAL-ECONOMIC ASPECTS OF CYBERCRIME. *Innovative Issues and Approaches in Social Sciences*, *9*(3). https://doi.org/10.12959/issn.1855-0541.IIASS-2016-no3-art1

Isom, D. (s. f.). *Guides: International and Foreign Cyberspace Law Research Guide: Treaties & International Agreements*. Recuperado 14 de julio de 2023, de https://guides.ll.georgetown.edu/cyberspace/cyber-crime-treaties

ITU. (2022). *Global Cybersecurity Index*. ITU. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Jaeger, P. T., Thompson, K. M., & McClure, C. R. (2005). Information Management. En K. Kempf-Leonard (Ed.), *Encyclopedia of Social Measurement* (pp. 277-282). Elsevier. https://doi.org/10.1016/B0-12-369398-5/00531-4

Jankovic, S. (2022). The Multivariate Statistical Analysis – Multiple Linear Regression. *International Journal on Biomedicine and Healthcare*, *10*(4), 173. https://doi.org/10.5455/ijbh.2022.10.173-175

Jhanjhi, N. Z., Ahmad, M., Khan, M. A., & Hussain, M. (2022). The Impact of Cyber Attacks on E-Governance During the COVID-19 Pandemic. En *Cybersecurity Measures for E-Government Frameworks* (pp. 123-140). IGI Global. https://doi.org/10.4018/978-1-7998-9624-1.ch008

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, *30*, 470-486. https://doi.org/10.1177/0894439311422689

Kitchel, T., & Ball, A. L. (2014). Quantitative Theoretical and Conceptual Framework Use in Agricultural Education Research. *Journal of Agricultural Education*, *55*(1), 186-199.

Klimovich, L. P., & Molokov, V. V. (2019). Cybercrime in the Conditions of the Digital Economy and the New Tendencies in the Forensic Enquiry Development. *Вестник Национальной Академии Наук Республики Казахстан*, *5*. https://doi.org/10.32014/2019.2518-1467.117

Kuznets, S. (1958). Medición Del Desarrollo Económico. *El Trimestre Económico*, *25*(97(1)), 72-96.

Lalanne, C., & Mesbah, M. (2017). Introduction. En C. Lalanne & M. Mesbah (Eds.), *Biostatistics and Computer-based Analysis of Health Data using SAS* (pp. ix-xiii). Elsevier. https://doi.org/10.1016/B978-1-78548-111-6.50009-5

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and

analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Lewis, W. A. (1957). Teoría Del Desarrollo Económico. *El Trimestre Económico*, *24*(96(4)), 454-467.

Lin, J. Y. (2017). Chapter 8—New Structural Economics and Industrial Policies for Catching-Up Economies. En S. Radosevic, A. Curaj, R. Gheorghiu, L. Andreescu, & I. Wade (Eds.), *Advances in the Theory and Practice of Smart Specialization* (pp. 183-199). Academic Press. https://doi.org/10.1016/B978-0-12-804137-6.00008-5

Lippman, S. S., & McCall, J. (2001). Economics of Information. En *International Encyclopedia of the Social & Behavioral Sciences* (pp. 7480-7486). https://doi.org/10.1016/B0-08-043076-7/02244-0

Lucas, A. (2022). Nonequilibrium phase transitions in competitive markets caused by network effects. *Proceedings of the National Academy of Sciences*, *119*(40), e2206702119. https://doi.org/10.1073/pnas.2206702119

Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal, Canadian Edition*, *7*, 35-49.

Machín, N., & Gazapo, M. (2016). La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea. *Revista UNISCI*, *0*(42), 47-67. https://doi.org/10.5209/RUNI.53786

Makhalin, V. N., & Makhalina, O. M. (2018). Management of calls and threats in digital economy of Russia. *UPRAVLENIE*, *6*, 57-60. https://doi.org/10.26425/2309-3633-2018-2-57-60

Mangesti Rahayu, S. (2019). Mediation effects financial performance toward influences of corporate growth and assets utilization. *International Journal of Productivity and Performance Management*, *68*(5), 981-996. https://doi.org/10.1108/IJPPM-05-2018-0199

McIntyre, D. P., & Srinivasan, A. (2017). Networks, platforms, and strategy: Emerging views and next steps. *Strategic Management Journal*, *38*(1), 141-160. https://doi.org/10.1002/smj.2596

Miner, G., Delen, D., Elder, J., Fast, A., Hill, T., & Nisbet, R. A. (Eds.). (2012). Chapter 10—Feature Selection and Dimensionality Reduction. En *Practical Text Mining and Statistical Analysis for Non-structured Text Data Applications* (pp. 929-934). Academic Press. https://doi.org/10.1016/B978-0-12-386979-1.00038-4

Moreno Posada, F., & Darío, M. P. (1986). *Introducción al desarrollo tecnológico*. https://repositorio.sena.edu.co/handle/11404/3225

Muggah, R., & Margolis, M. (2023, enero 2). *Why we need global rules to crack down on cybercrime*. World Economic Forum. https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/

Mujianto, H. (2019). *PEMANFAATAN YOUTUBE SEBAGAI MEDIA AJAR DALAM MENINGKATKAN MINAT DAN MOTIVASI BELAJAR*. https://www.semanticscholar.org/paper/PEMANFAATAN-YOUTUBE-SEBAGAI-MEDIA-AJAR-DALAM-MINAT-Mujianto/9f3a15e004bc280222814ce536816d460bafab26

NCSI. (2021). *NCSI: Methodology National Cybersecuryty Index*. https://ncsi.ega.ee/methodology/

Nguyen, Dr. C. L., & Golman, Dr. W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Ottaviano, G., & Thisse, J.-F. (2004). Chapter 58—Agglomeration and Economic Geography. En J. V. Henderson & J.-F. Thisse (Eds.), *Handbook of Regional and Urban Economics* (Vol. 4, pp. 2563-2608). Elsevier. https://doi.org/10.1016/S1574-0080(04)80015-4

Overvest, B., & Straathof, B. (2015). *What drives cybercrime? Empirical evidence from DDoS attacks* (CPB Discussion Paper 306). CPB Netherlands Bureau for Economic Policy Analysis. https://econpapers.repec.org/paper/cpbdiscus/306.htm

Park, J., Cho, D., Lee, J. K., & Lee, B. (2019). The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status. *ACM Transactions on Management Information Systems*, *10*(4), 13:1-13:23. https://doi.org/10.1145/3351159

Peitz, M., & Belleflamme, P. (Eds.). (2021). Platforms: Definitions and Typology. En *The Economics of Platforms: Concepts and Strategy* (pp. 10-40). Cambridge University Press. https://doi.org/10.1017/9781108696913.003

Petrosyan, A. (2023). *Cyber crime: Reported damage to the IC3 2022*. Statista. https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

Pinder, J. P. (2017). Chapter 10—Regression. En J. P. Pinder (Ed.), *Introduction to Business Analytics using Simulation* (pp. 313-369). Academic Press. https://doi.org/10.1016/B978-0-12-810484-2.00010-4

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247. https://doi.org/10.1002/itl2.247

Pravdiuk, A., Gerasymenko, L., & Tykhonova, O. (2021). Overcoming Cybercrime in Ukraine (Cyberterrorism). *International Journal of Computer Science and Network Security*, *21*(6), 181-186. https://doi.org/10.22937/IJCSNS.2021.21.6.24

PwC. (2022). *Cyber breach reporting to be required by law for better cyber defense*. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html

Quiroz, J. T., & Correa, S. (2012). Tecnología y Sociedad: Una aproximación a los estudios sociales de la tecnología. *Revista Iberoamericana de Ciencia, Tecnología y Sociedad*. http://repository.eafit.edu.co/handle/10784/28155

Rais, M. A., & Songkarn, P. (2022). Hacker and the Treat for National Security: Challenges in Law Enforcement. *Indonesian Journal of Counter Terrorism and National Security*, *1*(1), Article 1. https://doi.org/10.15294/ijctns.v1i1.56728

Reyes, G. (2001). Teoría de la globalización: Bases fundamentales. *Tendencias*, *2*(1), 1.

Rogers, J., & Revesz, A. (2019). *Experimental and quasi-experimental designs*.

Ruan, K. (2019). Chapter 6—The Point of Diminishing Return on Cyber Risk Investment. En K. Ruan (Ed.), *Digital Asset Valuation and Cyber Risk Measurement* (pp. 99-115). Academic Press. https://doi.org/10.1016/B978-0-12-812158-0.00006-5

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. J. (2016). *Industry 4 . 0: The Future of Productivity and Growth in Manufacturing Industries April 09*. https://www.semanticscholar.org/paper/Implementation-of-Industry-4.0-

Technologies%3A-What-Maghazei-Netland/eefaeb2e6ae516ad54b4b3711ff0bdd22e34ce9e

Schiks, J. A. M., van de Weijer, S. G. A., & Leukfeldt, E. R. (2022). High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals. *Computers in Human Behavior*, *126*, 106985. https://doi.org/10.1016/j.chb.2021.106985

Shan-A-Khuda, M., & Schreuders, Z. C. (2020). *Understanding Cybercrime Victimisation: Modelling the Local Area Variations in Routinely Collected Cybercrime Police Data Using Latent Class Analysis*. https://doi.org/10.5281/zenodo.3708924

Shimchenko, L. (2019). Cyber-threats in Ukraine as a problem in conditions of geopolitical rivalry. *Економічний Вісник Університету*, *40*, 70-76. https://doi.org/10.31470/2306-546X-2019-40-70-76

Singh, A., & Kaur, M. (2020). Detection Framework for Content-Based Cybercrime in Online Social Networks Using Metaheuristic Approach. *Arabian Journal for Science and Engineering*, *45*(4), 2705-2719. https://doi.org/10.1007/s13369-019-04125-w

Smits, J., & Permanyer, I. (2019). The Subnational Human Development Database. *Scientific Data*, *6*(1), Article 1. https://doi.org/10.1038/sdata.2019.38

Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of Cybercrime Originating within a Nation: A Cross-country Study. *Journal of Global Information Technology Management*. https://www.tandfonline.com/doi/full/10.1080/1097198X.2020.1752084

Stigler, G. J. (1961). The Economics of Information. *Journal of Political Economy*, *69*(3), 213-225.

Stockwell, E. (1962). La Medición del Desarrollo Económico. *Desarrollo Económico*, *2*(2), 5-21. https://doi.org/10.2307/3465688

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, Md. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660-671. https://doi.org/10.1016/j.future.2019.03.042

The World Bank. (2023). *World Development Indicators | DataBank*. https://databank.worldbank.org/source/world-development-indicators#

Thór Jóhannesson, G., & Bærenholdt, J. O. (2020). Actor–Network Theory. En A. Kobayashi (Ed.), *International Encyclopedia of Human Geography (Second Edition)* (pp. 33-40). Elsevier. https://doi.org/10.1016/B978-0-08-102295-5.10621-3

Uyanık, G. K., & Güler, N. (2013). A Study on Multiple Linear Regression Analysis. *Procedia - Social and Behavioral Sciences*, *106*, 234-240. https://doi.org/10.1016/j.sbspro.2013.12.027

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0 – A Glimpse. *Procedia Manufacturing*, *20*, 233-238. https://doi.org/10.1016/j.promfg.2018.02.034

Vargas-Hernández, J. (2008). ANÁLISIS CRÍTICO DE LAS TEORÍAS DEL DESARROLLO ECONÓMICO. *ECONOMÍA, GESTIÓN Y DESARROLLO*.

Vega-Centeno, M. (1993). Desarrollo económico y desarrollo tecnológico. *Libros PUCP / PUCP Books*. https://ideas.repec.org//b/pcp/puclib/lde-1993-01.html

Watters, P. A., McCombie, S., Layton, R., & Pieprzyk, J. (2012). Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP). *Journal of Money Laundering Control*, *15*(4), 430-441. https://doi.org/10.1108/13685201211266015

World Health Organization. (2023). *Human development index*. https://www.who.int/data/nutrition/nlis/info/human-development-index

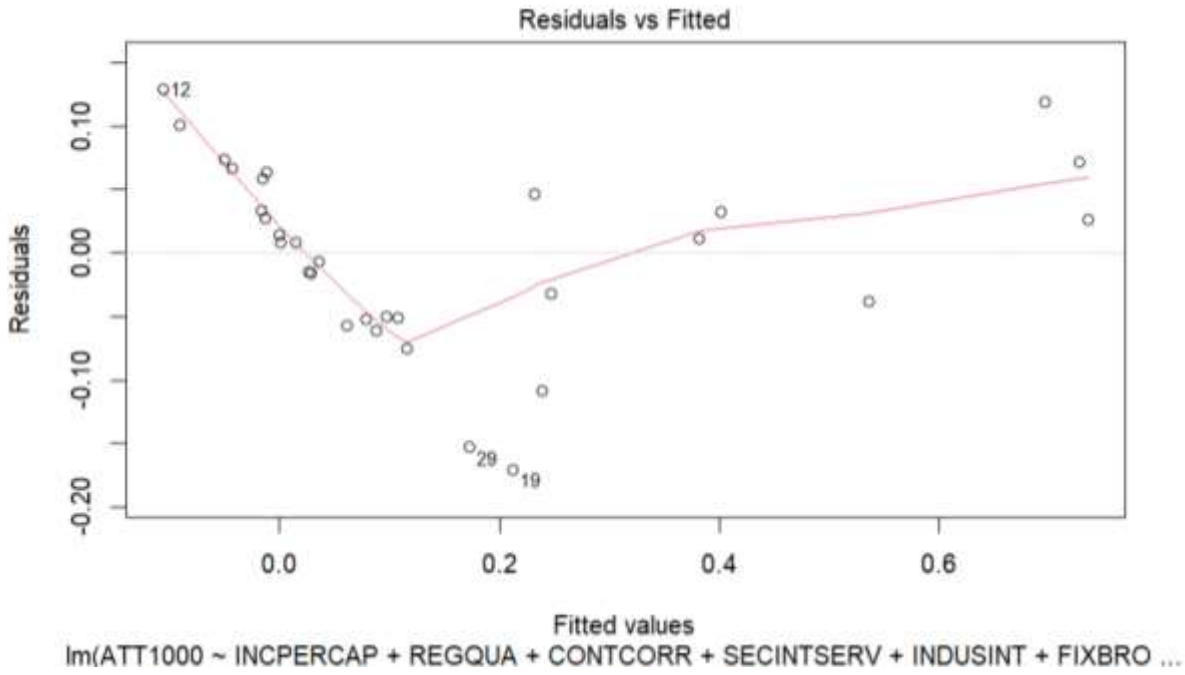
Xue, C., Tian, W., & Zhao, X. (2020). The Literature Review of Platform Economy. *Scientific Programming*, *2020*, e8877128. https://doi.org/10.1155/2020/8877128

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. M. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, *92*, 265-275. https://doi.org/10.1016/j.future.2018.09.058

Yu Peng Lin, & Camara, A. (2020). Network Effect as a Competitive Edge: What Have We Learnt From the Literature? *Journal of Strategic Innovation & Sustainability*, *15*(7), 43-52. https://doi.org/10.33423/jsis.v15i17.3702

ANEXOS

Figura 13: Residuos vs. Valores Ajustados y Q-Q Residuals



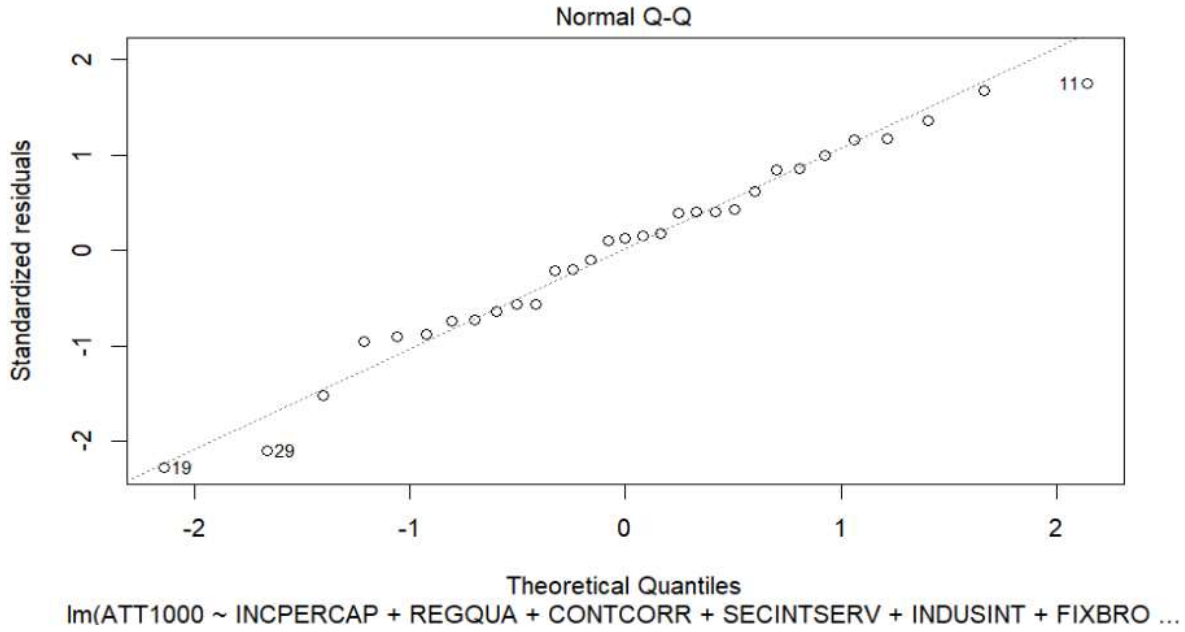
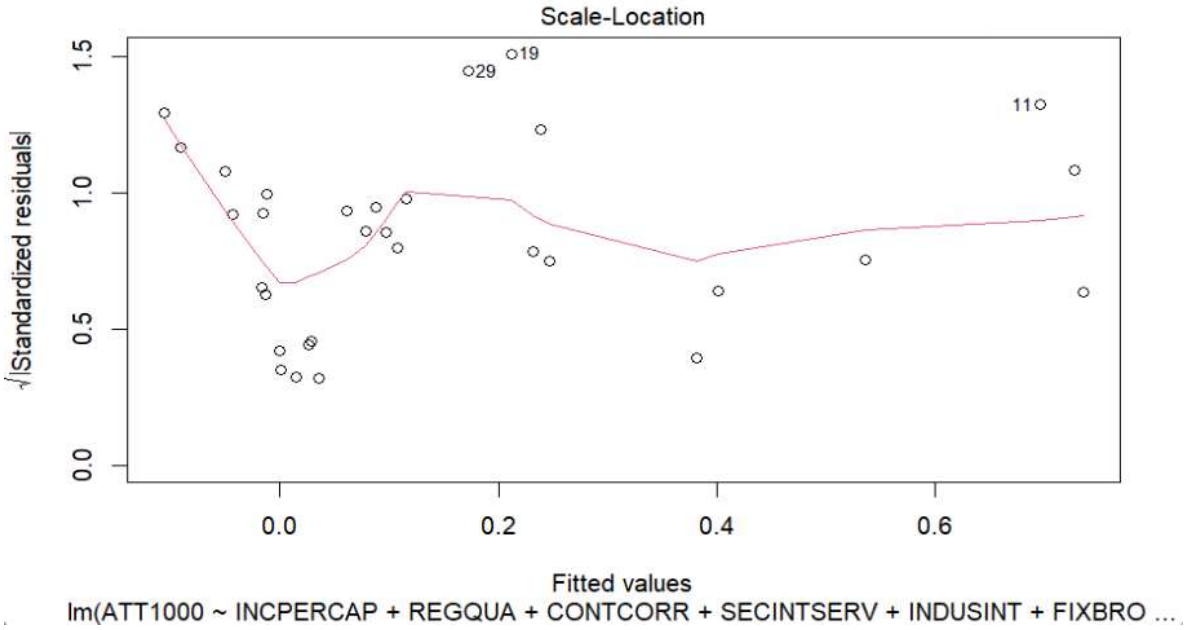


Figura 14: Scale-Location y Residuos vs. Influencia



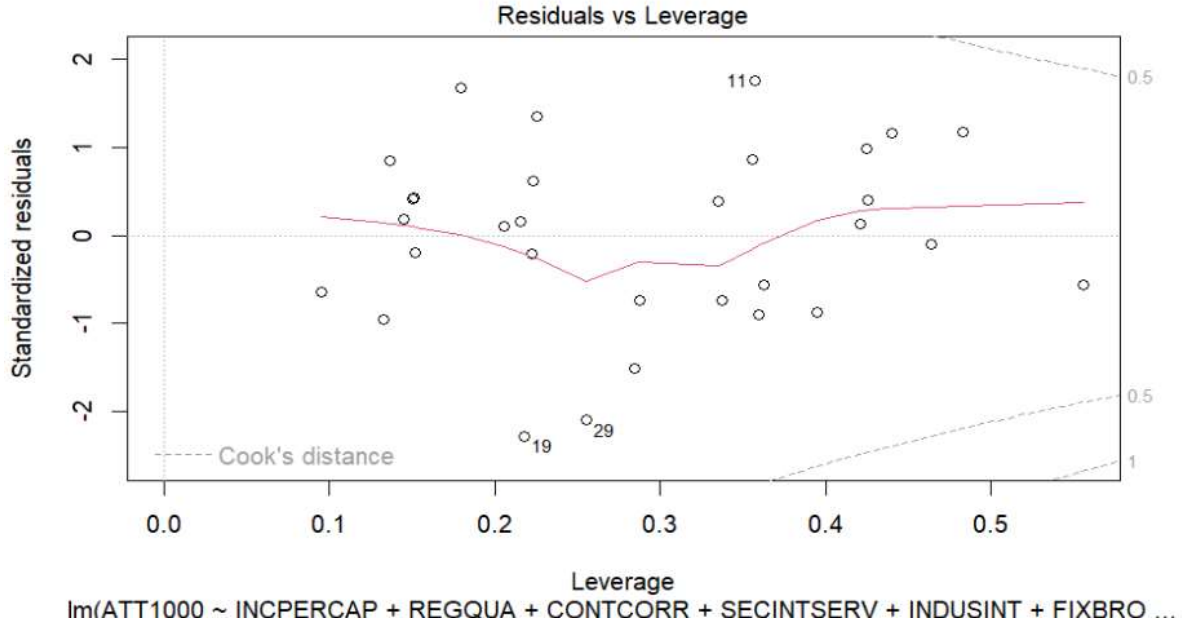


Figura 15: Histograma de residuos y Densidad de los residuos

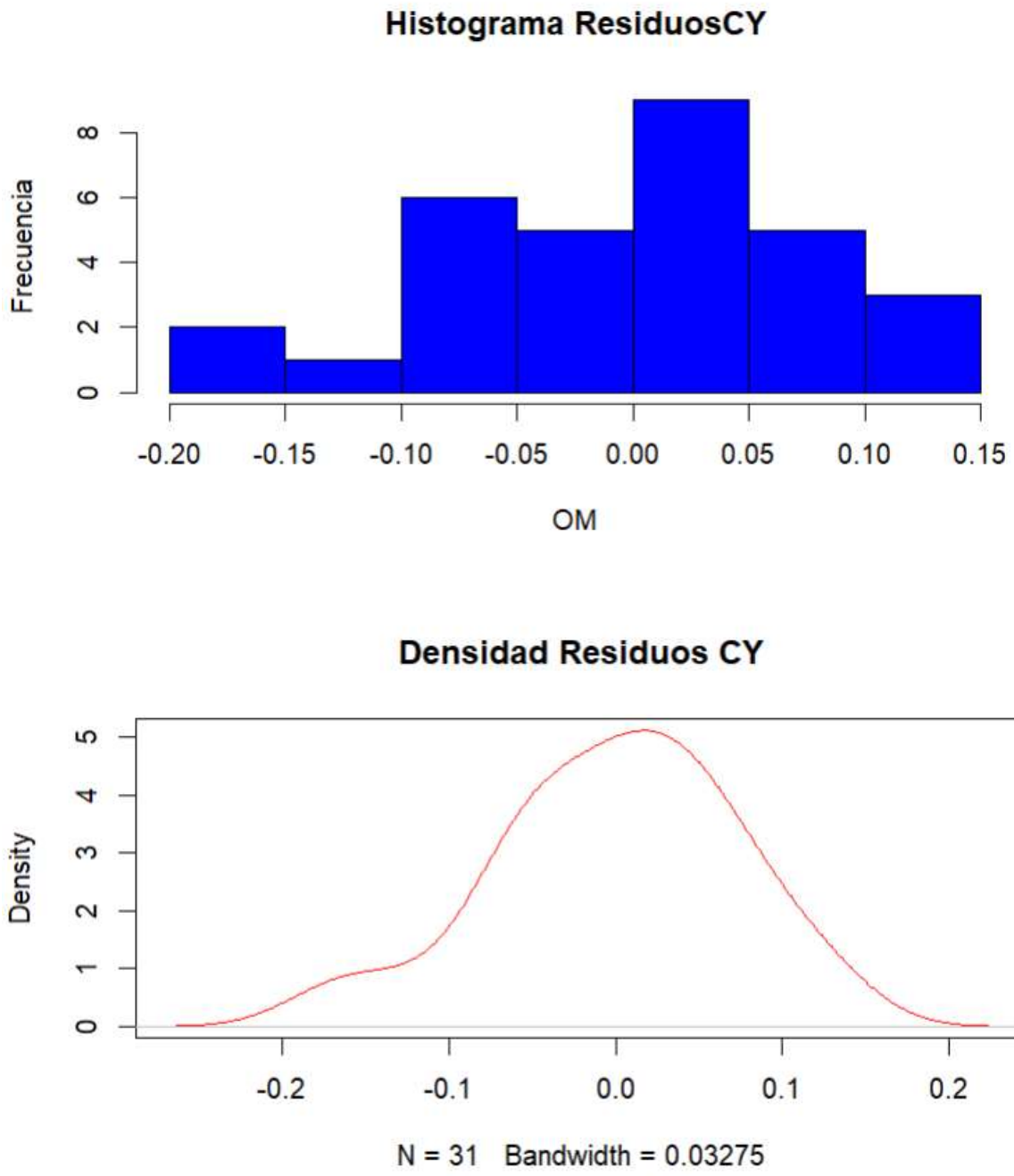


Figura 16: Segundo modelo sin variable control de corrupción

```
Call:
lm(formula = ATT1000 ~ INCPERCAP + REGQUA + SECINTSERV + INDUSINT +
    FIXBROSUBS + NATCYBINDEX + DIGDEVELEV)

Residuals:
     Min       1Q   Median       3Q      Max
-0.24726 -0.07642  0.01652  0.07089  0.22014

Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept)  1.512920   0.636705   2.376   0.0262 *
INCPERCAP   -0.301217   0.183864  -1.638   0.1150
REGQUA       0.084552   0.069440   1.218   0.2357
SECINTSERV   0.059538   0.034364   1.733   0.0966 .
INDUSINT     0.003006   0.003553   0.846   0.4062
FIXBROSUBS  -0.161907   0.051870  -3.121   0.0048 **
NATCYBINDEX -0.003120   0.002299  -1.357   0.1878
DIGDEVELEV   0.009600   0.004291   2.237   0.0352 *
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.1306 on 23 degrees of freedom
Multiple R-squared:  0.7893,    Adjusted R-squared:  0.7252
F-statistic: 12.31 on 7 and 23 DF,  p-value: 1.867e-06
```

Figura 17: Segundo modelo sin variable nivel de desarrollo digital

```
Call:
lm(formula = ATT1000 ~ INCPERCAP + REGQUA + CONTCORR + SECINTSERV +
    INDUSINT + FIXBROSUBS + NATCYBINDEX)

Residuals:
      Min        1Q    Median        3Q       Max
-0.186390 -0.061254 -0.001957  0.038319  0.300679

Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept)  1.242832   0.612735   2.028  0.05426 .
INCPERCAP   -0.272062   0.177276  -1.535  0.13850
REGQUA       0.269603   0.078125   3.451  0.00217 **
CONTCORR    -0.160396   0.064643  -2.481  0.02084 *
SECINTSERV   0.091856   0.032975   2.786  0.01051 *
INDUSINT     0.012010   0.003712   3.235  0.00366 **
FIXBROSUBS  -0.169701   0.051217  -3.313  0.00303 **
NATCYBINDEX -0.006511   0.002176  -2.993  0.00650 **
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.128 on 23 degrees of freedom
Multiple R-squared:  0.7976,    Adjusted R-squared:  0.736
F-statistic: 12.95 on 7 and 23 DF,  p-value: 1.203e-06
```

Figura 18: Segundo modelo sin variable control de corrupción y nivel de desarrollo digital

```
Call:
lm(formula = ATT1000 ~ INCPERCAP + REGQUA + SECINTSERV + INDUSINT +
    FIXBROSUBS + NATCYBINDEX)

Residuals:
     Min       1Q   Median       3Q      Max
-0.22504 -0.10090  0.02386  0.07986  0.33618

Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept)  1.243252   0.675359   1.841   0.0780 .
INCPERCAP   -0.205037   0.193112  -1.062   0.2989
REGQUA       0.150466   0.067927   2.215   0.0365 *
SECINTSERV   0.079096   0.035901   2.203   0.0374 *
INDUSINT     0.006798   0.003373   2.015   0.0552 .
FIXBROSUBS  -0.148294   0.055645  -2.665   0.0135 *
NATCYBINDEX -0.005029   0.002306  -2.181   0.0392 *
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.1411 on 24 degrees of freedom
Multiple R-squared:  0.7434,    Adjusted R-squared:  0.6793
F-statistic: 11.59 on 6 and 24 DF,  p-value: 4.313e-06
```

Guayaquil, 1 de septiembre de 2023.

Ingeniero

Freddy Camacho Villagómez

COORDINADOR UTE A-2023

ECONOMÍA

En su despacho.

De mis Consideraciones:

Economista Marlon Estuardo Pacheco Bruque, Docente de la Carrera de Economía, designado TUTOR del proyecto de grado de Massuh Villamar Vanessa Amira, cúmpleme informar a usted, señor Coordinador, que una vez que se han realizado las revisiones al 100% del avance del proyecto avaló el trabajo presentado por el estudiante, titulado **"Determinación de las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe"** por haber cumplido en mi criterio con todas las formalidades.

Este trabajo de titulación ha sido orientado al 100% de todo el proceso y se procedió a validarlo en el programa de URKUND dando como resultado un 1% de plagio.

Cabe indicar que el presente informe de cumplimiento del Proyecto de Titulación del semestre A-2023 a mi cargo, en la que me encuentra(o) designada (o) y aprobado por las diferentes instancias como es la Comisión Académica y el Consejo Directivo, dejo constancia que los únicos responsables del trabajo de titulación **Determinación de las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe** somos el Tutor Econ. Marlon Estuardo Pacheco Bruque y la Srta Massuh Villamar Vanessa Amira y eximo de toda responsabilidad a el Coordinador de Titulación y a la Dirección de Carrera.

La calificación final obtenida en el desarrollo del proyecto de titulación fue: 10/10 Diez sobre Diez.

Atentamente,

Econ. Marlon Estuardo Pacheco Bruque
ROFESOR TUTOR-REVISOR PROYECTO DE GRADUACIÓN

Massuh Villamar Vanessa Amira
AUTOR PROYECTO DE GRADUACIÓN

DECLARACIÓN Y AUTORIZACIÓN

Yo**, Vanessa Amira Massuh Villamar**, con C.C: # 0930465729 autor/a del trabajo de titulación: **Determinación de las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe** previo a la obtención del título de **Economista** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, **01** de **septiembre** de **2023.**

f. _____

Nombre: **Vanessa Amira Massuh Villamar**,

C.C: 0930465729

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TEMA Y SUBTEMA:	Determinación de las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe		
AUTOR(ES)	Massuh Villamar Vanessa Amira		
REVISOR(ES)/TUTOR(ES)	Econ. Pacheco Bruque Marlon Estuardo, Mgs.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Economía y Empresa		
CARRERA:	Economía		
TITULO OBTENIDO:	Economista		
FECHA DE PUBLICACIÓN:	1 de septiembre del 2023	**No. DE PÁGINAS:**	82
ÁREAS TEMÁTICAS:	Cibercrimen, Comportamiento social		
PALABRAS CLAVES/ KEYWORDS:	Ciberdelincuencia, ciberseguridad, socioeconómico, tecnológico, político		

RESUMEN/ABSTRACT (180 palabras): El objetivo de esta investigación es determinar las fuerzas motrices de la ciberdelincuencia en América Latina y el Caribe, para aquello se buscó establecer bases teóricas sólidas, aplicar el mejor modelo econométrico para la estimación de las variables y brindar conclusiones pertinentes al contexto de estudio. Así mismo se planteó cinco hipótesis de; factor económico, social, político, tecnológico y de ciberseguridad. En representación de la sección del continente, se tomaron datos de 31 países representativos con características económicas y sociales con un comportamiento similar. El modelo econométrico utilizado en esta investigación fue regresión lineal múltiple. Del mismo modo de las diecinueve variables planteadas por el marco teórico solo las variables ingresos per cápita, calidad reguladora, control de corrupción, servidores seguros de internet, personas que utilizan internet, las suscripciones de banda ancha fija, índice nacional de ciberseguridad y nivel de desarrollo digital fueron significativas, destacando que del factor social ninguna entro a esta lista. Para futuras investigaciones se espera encontrar mayor información de variables explicadas por ausencia de registros y de registros actualizados de números de ciberataques de los últimos años.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:**+593-995446610	E-mail: vamassuh@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	Nombre: Camacho Villagomez Freddy Ronalde	
	Teléfono: +593-4-2206953 ext 1634	
	E-mail:Freddy.camacho.villagomez@gmail.com; Freddy.camacho@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA

Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	