Facultad de Ciencias Económicas y Empresariales
ICADE

IMPACTO ECONÓMICO DE LOS ATAQUES A AL CIBERSEGURIDAD

Autor: Carlota Uguet de Resayre Viñuales
Director: Juan Felipe Jung Lusiardo

MADRID | Abril 2025

Resumen

En un escenario de acelerada transformación digital, los ciberataques han dejado de ser una amenaza aislada para convertirse en un riesgo estructural con profundas implicaciones económicas. El presente trabajo tiene como objetivo principal estimar el impacto económico de los ciberataques mediante una combinación de análisis descriptivo y modelización econométrica, centrada en una muestra internacional de países. A partir de una función de producción de tipo Cobb-Douglas extendida, se incorpora la frecuencia de ciberataques como variable que afecta negativamente a los factores productivos.

La metodología adoptada, de carácter cuantitativo, permite identificar empíricamente los canales a través de los cuales los ciberataques erosionan la capacidad de crecimiento económico. Los resultados del modelo revelan que el capital físico no se ve significativamente afectado por este tipo de amenazas, mientras que el trabajo y, en menor medida, la infraestructura digital, presentan una disminución estadísticamente significativa en su productividad. Estos hallazgos permiten establecer que el principal canal de transmisión del impacto económico se da a través de la pérdida de eficiencia laboral.

Como consecuencia, se proponen una serie de recomendaciones estratégicas orientadas a reforzar la resiliencia económica frente a amenazas digitales, fundamentadas en la evidencia empírica obtenida. Este trabajo contribuye a la literatura actual al cuantificar el coste económico de los ciberataques y al posicionar la ciberseguridad no como un gasto, sino como una inversión esencial para la sostenibilidad del desarrollo económico en la era digital.

Palabras clave: ciberataques, economía digital, productividad, modelo econométrico, políticas públicas

Abstract

In a context of accelerated digital transformation, cyberattacks have evolved from isolated threats into structural risks with profound economic implications. This study aims to estimate the economic impact of cyberattacks through a combination of descriptive analysis and econometric modeling, using a representative sample of countries. Based on an extended Cobb-Douglas production function, the model incorporates the frequency of cyberattacks as a variable that negatively affects the performance of productive factors.

The applied quantitative methodology enables the identification of the transmission channels through which cyberattacks erode economic growth. The results show that physical capital is not significantly impacted, whereas labor productivity and, to a lesser extent, digital infrastructure, exhibit a statistically significant decline. These findings highlight labor as the most affected factor and the main economic transmission channel of cyberattack consequences.

Accordingly, this research proposes a set of strategic recommendations aimed at strengthening economic resilience to digital threats. Grounded in empirical evidence, this work contributes to the academic literature by quantifying the macroeconomic cost of cyberattacks and reframing cybersecurity not as a cost, but as a key investment for sustainable economic development in the digital era.

Keywords: cyberattacks, economic impact, productivity, cybersecurity, econometric model

Índice de contenido

Índice de Figuras

1. Introducción

Cada 39 segundos ocurre un ciberataque en el mundo, según una investigación de WatchGuard. Esto significa que, mientras lees este párrafo, al menos tres nuevos ataques han comprometido la seguridad de individuos, empresas y gobiernos. La acelerada transformación digital, que ha traído consigo innumerables beneficios, también ha abierto la puerta a una amenaza sin precedentes: la vulnerabilidad cibernética. No importa si se trata de una multinacional, un banco, un hospital o una infraestructura crítica como una red eléctrica; todos son potenciales objetivos de ataques que pueden generar pérdidas millonarias, interrupciones operativas y hasta crisis económicas a gran escala.

El impacto de los ciberataques no se limita a la pérdida de datos o el robo de información confidencial. Su alcance es mucho más profundo: pueden paralizar empresas, desestabilizar mercados financieros e incluso comprometer la seguridad nacional. En 2017, el ciberataque masivo de tipo *ransomware* conocido como *NotPetya* generó un impacto económico sin precedentes, con pérdidas globales superiores a los 10.000 millones de dólares. Empresas multinacionales de distintos sectores, como Maersk, FedEx y Saint-Gobain, se vieron gravemente afectadas. En el caso de Maersk, la magnitud del daño obligó a una reconstrucción total de su infraestructura tecnológica, lo que derivó en una interrupción operativa prolongada y un esfuerzo logístico de gran escala para restablecer sus sistemas (Weaver et al., 2022). Este no es un caso aislado, es una realidad recurrente que afecta a miles de organizaciones y gobiernos cada año.

Ante este panorama, surge una pregunta clave: ¿Cómo podemos medir el impacto económico real de los ciberataques? Este trabajo de investigación busca responder a esta cuestión a través de un análisis exhaustivo de los costos directos e indirectos de los ciberataques, evaluando su impacto en distintos niveles:

- Empresas e individuos: ¿Cómo afectan los ciberataques a la estabilidad financiera, la reputación y las operaciones de las compañías y personas?
- Sectores estratégicos: ¿Cuáles son las industrias más vulnerables y qué consecuencias económicas han enfrentado tras sufrir ataques?
- Economía global: ¿Hasta qué punto el cibercrimen puede impactar el crecimiento económico y la estabilidad de los mercados internacionales?

Para ello, este estudio aplicará modelos de estimación y análisis de datos en una muestra de países e industrias, con el objetivo de identificar patrones, cuantificar pérdidas y proponer estrategias para mitigar los efectos de los ataques.

El cibercrimen no es solo un problema tecnológico, es un desafío económico que crece a un ritmo alarmante. Se estima que las pérdidas mundiales por ciberataques alcanzan los 575.000 millones de dólares anuales (Dieye et al., 2020), lo que afecta el crecimiento económico y la confianza en el ecosistema digital. En un mundo donde la economía digital es el motor del desarrollo, ignorar el impacto de los ciberataques no es una opción. Con este estudio, buscamos aportar una visión clara y fundamentada sobre cómo estos ataques afectan la economía y qué estrategias pueden adoptarse para minimizar su impacto. En la era digital, la ciberseguridad no es un lujo, sino una necesidad urgente.

2. Revisión de literatura

2.1. Naturaleza de los ciberataques

Los ciberataques han ido evolucionando hasta convertirse en un peligro constante y progresivo que impacta tanto a personas, entidades como los propios gobiernos. Estas amenazas van allá de pérdida económicas, la estabilidad de sistemas críticos, confianza de usuarios, y llegando hasta situaciones extremas como la seguridad del país. Cada tipo de ciberataque cuenta con distintos atributos y objetivos que varían en términos de complejidad y alcance. Debido a la interdependencia de los sectores y su creciente dependencia tecnología, los ciberataques suponen un reto para la economía mundial.

En las siguientes secciones, se examinarán los tipos de ciberataques más relevantes, detallando sus características, métodos de ejecución y sus repercusiones en los sectores. Este análisis exhaustivo permitirá entender tanto la variedad como los efectos de estos ataques en un ambiente cada vez más digital y vulnerable. (Biju et al, 2019)

2.1.1. Tipos de Ciberataques

En el contexto de la naturaleza de los ciberataques, es imprescindible comprender los diferentes tipos existentes, dado que cada uno posee atributos, técnicas y metas distintivas. Estos ataques constituyen un peligro crucial para la seguridad y privacidad de personas, empresas y gobiernos, impactando no solo en la integridad de los datos, sino también en la estabilidad financiera y funcional de las organizaciones. Conforme se amplían los sistemas de información y las redes, también se incrementan las posibilidades de que los atacantes descubran vulnerabilidades y exploten fallos de seguridad. Los efectos de estos ataques puede ser devastadores, provocando pérdidas económicas,

perjuicios en el prestigio, en ciertas situaciones, poniendo en peligro la seguridad nacional. Dado el extenso abanico de técnicas y procedimientos empleados, es crucial la categorización y análisis exhaustivo de las variedades de ciberataques para comprender las amenazas presentes y diseñar estrategias eficaces de prevención y respuesta Entre los más habituales se hallan los ataques de denegación de servicio (DoS), que intentan saturar los recursos de un sistema para alterar su operatividad habitual. Ponen en riesgo la disponibilidad de los servicios y sistemas, impidiendo que los usuarios puedan utilizarlos. Esto puede detener páginas web, aplicaciones esenciales y servicios en línea. Por otro lado, los ataques de hombre en el medio (MitM) posibilitan que los atacantes intercepten y manipulen las comunicaciones entre dos partes, lo cual pone en riesgo la privacidad de los datos enviados. Estos resultan particularmente arriesgados en operaciones financieras o en transferencia de datos delicados, donde pueden sustraer información personal o alterar las instrucciones de transferencia. El siguiente tipo, los ataques phishing, emplean emails fraudulentos para confundir a los usuarios y así poder adquirir sus datos personales. Esta información puede utilizarse posteriormente con el fin de realizar fraudes o suplantación de identidad. Otros tipos son las descargas no deseadas (*drive-by downloads*), donde los usuarios se infectan al acceder a páginas web comprometidas. Estos ataques pueden provocar la desaparición o robo de datos para facilitar el ingreso no permitido en el sistema. Los ataques a contraseñas son otro tipo que pone en riesgo directamente la privacidad y acceso a los sistemas, dado que buscan adquirir o descifrar estas contraseñar para tener acceso a datos o recursos privados. La revelación de estas contraseñas podría provocar la pérdida de control sobre cuentas delicadas y divulgación de información confidencial. (Biju et al, 2019)

También existen los ataques de inyección SQL, que manipulan bases de datos para conseguir acceso no permitido a información sensible, lo que podría poner en riesgo información privadas de los clientes y datos vitales de la entidad. Los ataques de scripting entre sitios (XSS), que introducen un código malicioso en páginas web para afecte a los usuarios que las visitan, y de esta forma poder robar cookies, interceptar sesiones o redirigir a los usuarios a paginas engañosas. Adicionalmente, se pueden encontrar ataques de escucha (*eavesdropping*), que interceptan comunicaciones en redes poco seguras. Esto resulta particularmente peligroso en relación con la información personal, contraseñas e información económicas. Otro tipo son los ataques de cumpleaños, se basan en una modalidad de ataque cifrado que impacta en la integridad de los mensajes y autenticación

en sistemas que emplean funciones hash, la cual que convierte información de cualquier magnitud en una serie constante de caracteres, para corroborar información. Este ataque aprovecha la posibilidad de valores *hash*, lo que permite generar al atacante mensajes engañosos con el mismo hash. (Biju et al, 2019)

Por último, los ataques de *malware* abarcan una variedad de programas malintencionados, tales como virus, gusanos, troyanos, *ransomware* y *spyware*, que buscan dañar, espiar o extorsionar a los usuarios. Entender estos tipos de ataques y sus efectos particulares es esencial para la creación de estrategias eficaces de ciberseguridad que salvaguarden la integridad de los sistemas de información en un ambiente digital cada vez más vulnerable. (Biju et al, 2019)

2.1.2. Tipos de Cibercriminales

Para conseguir entender mejor los ciberataques, es esencial comprender los distintos tipos de cibercriminales existentes. Debido a que sus motivaciones y técnicas suelen verse reflejadas en los tipos y magnitudes de los ataques. A continuación, se muestran algunos de los tipos de cibercriminales más comunes:

1) Hackers

Este grupo está impulsado por la curiosidad técnica, y el aprendizaje a la hora de perfeccionar sus capacidades técnicas como por la aspiración de ser reconocidos en la comunidad de ciberseguridad. Tal como explican Saini et al. (2022), numerosos individuos se sienten motivados por el reto intelectual de descubrir vulnerabilidades en sistemas complejos. Por su parte, Varswani (2021) señala que otros hackers actúan por razones ideológicas, promoviendo causas políticas o sociales, como sucede con los denominados "hacktivistas". Dentro de esta categoría, se distinguen subgrupos como los "*white-hat*" o hackers éticos, que colaboran con organizaciones para fortalecer su ciberseguridad, y los "*black-hat*", que emplean sus conocimientos para infiltrarse sin autorización en sistemas, a menudo con fines destructivos o lucrativos.

2) Crackers

Estos cibercriminales tienen como finalidad principal causar daño o lograr un beneficio propio mediante la alteración deliberada de sistemas de seguridad. Según Saini et al. (2022), a diferencia de los hackers éticos, los crackers actúan con una motivación claramente maliciosa y están dispuestos a violar la ley para alcanzar sus

fines. Tal como señala Varswani (2021), sus objetivos pueden ir desde el lucro financiero hasta la venganza personal o la desestabilización de sistemas concretos. Las técnicas que emplean incluyen el uso de *malware* o software malicioso, virus y ataques de fuerza bruta destinados a romper contraseñas y obtener acceso no autorizado a información sensible. Estas acciones, orientadas muchas veces a la venta o manipulación de datos, representan una amenaza considerable tanto para empresas como para individuos.

3) Criminales Financieros

El objetivo de este grupo es, principalmente, el beneficio económico. Según Saini et al. (2022), estos actores se enfocan en el robo de información financiera, estafas bancarias y ataques de coacción como el phishing y el ransomware. Vaswani (2021) explica que el phishing se basa en suplantar la identidad de una entidad legítima para engañar a la víctima, mientras que el ransomware bloquea el acceso a archivos o sistemas a cambio de un rescate. De acuerdo con Gulyas y Kiss (2023), estos delincuentes suelen operar en redes organizadas e incluso infiltran instituciones financieras o acceden a información de clientes para explotar datos sensibles, lo que compromete directamente la economía y estabilidad financiera de sus víctimas.

4) Espías Corporativos

Este tipo de cibercriminales buscan obtener secretos comerciales y propiedad intelectual con el fin de beneficiar a una organización rival. Según Saini et al. (2012), estos ataques se impulsan por la ventaja competitiva que puede derivarse del acceso ilícito a información estratégica del mercado. Tal como explica Vaswani (2021), las técnicas utilizadas incluyen el hurto de datos sobre desarrollo de productos, tácticas comerciales o bases de datos de clientes, mediante infiltraciones en redes corporativas o a través de empleados internos. La pérdida de información sensible representa un riesgo significativo para las empresas, no solo por el debilitamiento de su posición competitiva, sino también por el daño reputacional frente a clientes, socios e inversores.

5) Terroristas Cibernéticos

Lis y Mendel (2019) destacan que este tipo de actores tienen como objetivo generar miedo, desestabilización o daños estructurales a través de ataques a infraestructuras

críticas, movidos por motivaciones ideológicas, religiosas o políticas. A diferencia de otros cibercriminales, no buscan un beneficio económico, sino la interrupción de servicios fundamentales como redes eléctricas, sistemas de transporte o instalaciones hospitalarias. Estos ataques suelen contar con respaldo estatal o de grupos extremistas, lo que incrementa su peligrosidad al poder afectar directamente a la seguridad nacional y al bienestar de la población civil (Venkatachary et al, 2017).

6) Empleados o Exempleados descontentos

Según Vaswani (2021), las personas con acceso legítimo a los sistemas y datos de una organización representan una de las amenazas más críticas en materia de ciberseguridad. Estos ataques suelen estar motivados por resentimiento personal o deseo de beneficio económico. Como señalan Saini, Rao y Panda (2012), el conocimiento profundo que estos individuos tienen sobre los sistemas internos les permite llevar a cabo acciones encubiertas difíciles de detectar, y en muchos casos, vender o filtrar datos sensibles a competidores o actores externos.

7) Ciber-mercenarios

Son individuos que actúan como profesionales a sueldo, llevando a cabo ciberataques dirigidos contra objetivos específicos a cambio de una compensación económica. Según Lis y Mendel (2019), estos actores poseen un alto grado de especialización en técnicas complejas de ciberseguridad, lo que les permite adaptar sus métodos a las necesidades de sus clientes. Como destaca Venkatachary et al. (2017), sus actividades pueden abarcar desde el espionaje industrial hasta la infiltración en infraestructuras críticas. El anonimato con el que operan, así como su flexibilidad para cambiar de cliente y evadir rastreo, los convierte en una amenaza significativa dentro del entorno digital.

Los diversos tipos de cibercriminales constituyen un extenso espectro de amenazas que demandan métodos específicos de prevención y reacción. Desde hackers y crackers, que investigan y aprovechan vulnerabilidades por curiosidad o propósitos malicioso, hasta delincuentes financieros y espías empresariales, impulsados por el beneficio económico y ventaja competitiva, cada perfil se comporta con objetivos y técnicas particulares.

2.2. El impacto económico de los ciberataques

2.2.1. Nivel Micro: Impacto en Empresas e Individuos

Los ciberataques pueden suponer un gasto directo para las compañías al perjudicar sus operaciones, ganancias y prestigio. Un caso ilustrativo es el de Saint-Gobain, que experimentó pérdidas que superaron mil millones de euros después del ataque NotPetya. Este ataque no solo paralizó sus actividades, sino que forzó a numerosos trabajadores a trabajar de manera manual, afectando a la eficiencia y productividad de la compañía (Weaver et al, 2022). Otro caso relevante fue el de TJX, una cadena comercial que sufrió pérdidas de 118 M$, como resultado de una brecha de datos que puso en riesgo 100 millones de registros. Esto hizo que tuvieran que incurrir en costos jurídicos y de asesoría de seguridad (Lis & Mendel, 2019).

Los ataques también tienen ciertas repercusiones en los individuos, en particular robando identidad y perdiendo privacidad. En Estados Unidos, el hurto de identidad impacta cerca del 10% de la población, llegando a pérdidas medias de 5.000$ por individuo. Este tipo de ataque no solo tienen una repercusión económica, sino también una carga considerable en cuanto a tiempo y recursos requeridos para solucionar estos daños (Lis & Mendel, 2019).

2.2.2. Nivel Sectorial: Impacto en Infraestructuras Críticas

En lo que respecta a los sectores, los ciberataques causan impactos significativos en sectores esenciales que dependen de infraestructuras críticas, impactando de esta manera la seguridad y estabilidad de servicios fundamentales. Por ejemplo, el ataque ruso a la red eléctrica de Ucrania en 2015 llevado a cabo por el grupo de amenazas persistentes avanzadas Sandowrm, dejó a más de 200.000 personas sin electricidad y impactó la estabilidad del sistema de energético. Estos sucesos en infraestructuras vitales pueden generar un efecto en cadena, impactando a otros sectores e incluso elevando los costes a causa de las interrupciones en la cadena de abastecimiento. (Lis & Mendel, 2019)

En el sector financiero, los ataques representan una amenaza significativa. Un caso ilustrativo es el Crelan Bank, que sufrió una pérdida de 75,8M$ a causa de un ataque de phishing que puso en riesgo las cuentas de correo electrónico de ejecutivos de alto nivel, facilitando a los atacantes desviar fondos. (Zorz, 2018)

2.2.3. Nivel Macroeconómico: Impacto a Nivel Nacional y Global

A nivel macroeconómico, los ataques afectan al producto interior bruto (PIB) del país. Se calcula que las pérdidas mundiales relacionadas con el cibercrimen llegan a 575 mil millones de dólares al año, lo que supone una "fuga" de valor económico que afecta a la innovación, desarrollo y competitividad a nivel global. Adicionalmente, ciertas investigaciones sugieren que un ciberataque que consiga perjudicar o impactar de manera significativa al sector de la tecnología de la información en Estados Unidos podría llegar a provocar una disminución económica de hasta el 3.4% del PIB. Este porcentaje muestra el potencial efecto de un ataque que deje paralizado al 40% del sector TIC, provocando además efectos secundarios en diversos sectores de la economía. (Dieye et al, 2020)

La pérdida de confianza en el comercial digital y operaciones online también repercute a nivel macroeconómico. Actualmente, con los mercados interconectados, una interrupción en los sistemas financiero en una región puede causar efectos secundarios en otros lugares, provocando pérdidas extra y perjudicando el desarrollo económico. (Venkatachary et al, 2017)

Los ciberataques provocan impactos económicos relevantes a distintos niveles, afectando tanto a la estabilidad económica de las compañías como a la economía global. Los costes asociados comprenden tanto pérdidas directas, como extracción de datos e interrupción de operaciones, como la disminución de la confianza de sus consumidores y el aumento en las inversiones en ciberseguridad.

2.3. Acciones para mitigar el problema

El continuo crecimiento de ciberataques constituye un peligro para la economía mundial y la protección de infraestructuras esenciales. Tanto gobiernos como corporaciones han puesto en marcha varias acciones para conseguir reducir estos riesgos. Incluyen medidas tales como políticas gubernamentales, regulaciones particulares, inversiones en tecnología de ciberseguridad y cooperación entre distintas áreas para poder hacer frente a estos riesgos. A continuación, se detallan algunas de las tácticas más utilizaras por economías líderes y el sector privado para enfrenar este reto. (Watkins, 2014)

Los gobiernos están continuamente buscando distintas estrategias para conseguir reducir los riesgos de ciberataques, las cuales se centran en proteger infraestructuras imprescindibles y garantizar la protección de información confidencial. Dentro de estas acciones destacan:

- Estrategias Nacionales de Ciberseguridad

El objetivo de países como Estados Unidos y la Unión Europea es desarrollar programas nacionales de ciberseguridad para poder prevenir y responder ante posibles ciberataques. El objetivo es definir estrategias específicas para cooperar entre entidad gubernamentales y corporaciones, y así fortalecer la seguridad a escala nacional (Watkins, 2014).

- Protección de Datos

Dentro de la Unión Europea, el Reglamento General de Protección de Datos (GDPR) establece que las empresas reporten los incidentes que han tenido y establezcan medidas para proteger los datos (Watkins, 2014).

- Colaboración Internacional

Un ejemplo es en 2014 la UE y EE. UU. Fortalecieron su cooperación en la Cumbre de Bruselas, en el que se comprometían a intercambiar más información sobre amenazas, implementar normas jurídicas internacionales y estables fuertes alianzas entre los sectores público y privado (Watkins, 2014).

- Normativas de Ciberseguridad para Infraestructuras Críticas

Determinadas industrias, como la energética, necesitan una protección especial dado su relevancia para la seguridad del país. Los gobiernos han impulsado regulaciones especiales para estos sectores. Por ejemplo, en la industria de la energía, hay que priorizar la protección de las redes eléctricas, ya que si reciben un ataque pueden causar interrupciones masivas con repercusiones con efectos en cascada sobre otras infraestructuras (Venkatachary et al, 2017).

- Inversión en Seguridad y Capacitación

Una encuesta de Dell extrajo que el 74% de los líderes en TIC, tienen intención de incrementar la inversión en ciberseguridad y en formar a sus trabajadores los siguientes años (Watkins, 2014)

Estas medidas son una muestra del compromiso por parte de los gobiernos para poder hacer frente a las amenazas digitales y proteger tanto a los ciudadanos como a las infraestructuras de entidades, compañías e instituciones gubernamentales.

3. Análisis descriptivo

3.1. Variables consideradas y fuentes de información

Para comprender las consecuencias económicas de los ciberataques, se ha recopilado información procedente de diversas fuentes, siendo el informe de *Netscout Threat Intelligence Report – Country Analysis* la principal referencia para los datos relativos a la frecuencia y duración de los ataques. Esta base de datos se ha enriquecido con indicadores económicos y demográficos que permiten contextualizar y medir el impacto potencial de estos incidentes en distintos países.

Partimos, por tanto, con una selección de variables clave para un análisis descriptivo preliminar que sirva como base para el posterior desarrollo econométrico. Las variables consideradas incluyen:

- Country: el país analizado.
- Semester y Year: periodo temporal del análisis.
- MBB (Mobile Broadband Penetration): nivel de penetración de la banda ancha móvil, un indicador clave de digitalización.
- Attack Frequency: frecuencia de ciberataques reportados en el país.
- Average Duration (minutes): duración promedio de los ciberataques en minutos.
- GDP_USD: Producto Interno Bruto (PIB) del país en dólares estadounidenses.
- Population: población total del país.
- Attack Frequency per capita: frecuencia de ataques ajustada por población.
- Population (M): población expresada en millones.
- Attack Frequency per capita (M): frecuencia de ataques ajustada a la escala de millones de habitantes.
- GDP_USD per capita: PIB per cápita, que permite medir el impacto económico de los ciberataques en función del nivel de desarrollo del país.

A partir de estas variables se lleva a cabo un análisis exploratorio que permite identificar patrones iniciales entre la infraestructura digital, la exposición a ciberataques

y el nivel de desarrollo económico. Estos resultados descriptivos, que incluyen representaciones gráficas de las relaciones entre variables como empleo, formación bruta de capital o penetración digital frente a ataques, ofrecen una primera aproximación visual y estadística del fenómeno.

Este enfoque permite fundamentar la selección de variables y anticipar posibles efectos que se estimarán en los siguientes apartados mediante un modelo econométrico diseñado para capturar el impacto específico de los ciberataques sobre la actividad económica.

3.2. Ranking de países por número de ciberataques

El impacto de los ciberataques no se distribuye de manera uniforme en el mundo. Existen países que, debido a su alto nivel de digitalización, desarrollo económico o importancia geopolítica, se convierten en objetivos prioritarios para los ciberdelincuentes. Otros, en cambio, registran un menor número de ataques, ya sea por contar con una infraestructura de seguridad más robusta, una menor digitalización o simplemente por no ser considerados objetivos estratégicos.

Para comprender mejor esta distribución global, en esta sección se analiza el ranking de países según la cantidad total de ciberataques anuales registrados. El objetivo es identificar tendencias y correlaciones que permitan entender qué factores influyen en la concentración de estos incidentes en ciertos territorios.

3.2.1. Países con mayor número absoluto de ciberataques

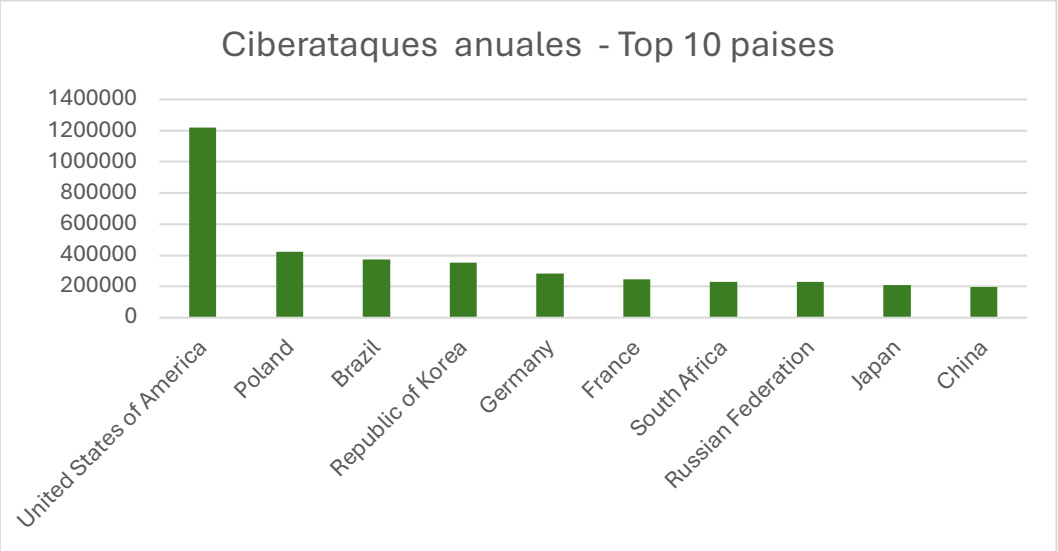


Figura 1 - Top 10 países con mayor número de ciberataques totales

i) Principales observaciones

Estados Unidos se encuentra muy por encima del resto, con más de 1.2 millones de ciberataques anuales. Esto refuerza su posición como un objetivo clave debido a su desarrollo tecnológico, economía y alta dependencia digital.

Polonia, Brasil, Corea del Sur y Alemania se posicionan en un segundo nivel, con cifras entre 300,000 y 400,000 ataques.

Francia, Sudáfrica, Rusia, Japón y China tienen un número menor de ataques, entre 200,000 y 300,000 anuales, pero siguen estando entre los países más afectados.

ii) Posibles factores que explican la distribución

- Tamaño de la economía y digitalización: Países con mayor digitalización tienden a ser más atacados, ya que hay más sistemas interconectados y, por tanto, más oportunidades para los atacantes.
- Infraestructura de ciberseguridad: Algunos países pueden tener medidas de seguridad más débiles, lo que los convierte en objetivos más fáciles.
- Atractivo económico: Empresas de tecnología, instituciones financieras y bases de datos gubernamentales pueden ser objetivos clave.
- Geopolítica y conflictos internacionales: Rusia y China tienen cifras relativamente bajas, lo que podría deberse a una falta de transparencia en la publicación de ataques o a estrategias ofensivas en lugar de defensivas.

3.2.2. Países con mayor número de ciberataques per cápita

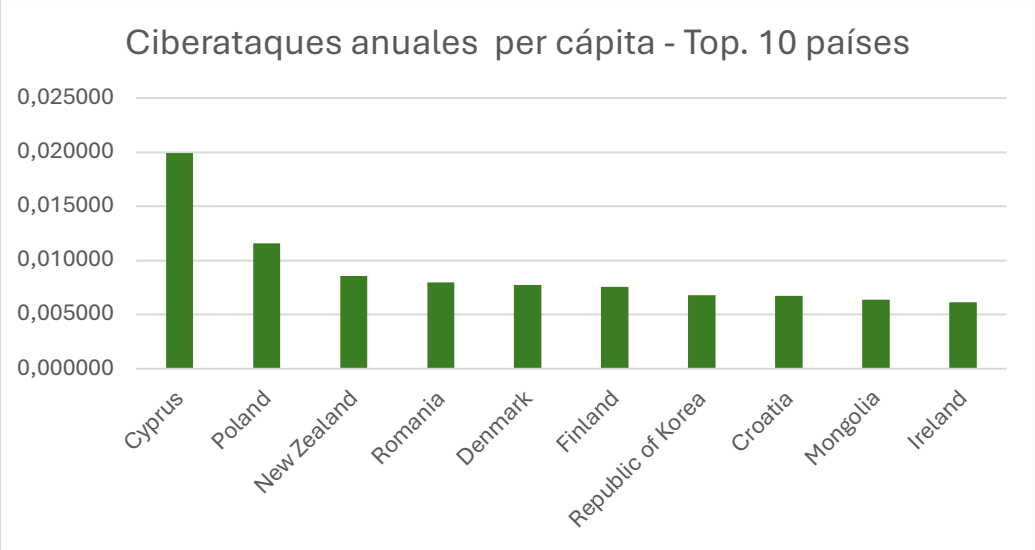


Figura 2 - Top 10 países con mayor número de ciberataques per cápita

i) Principales observaciones

Chipre lidera la lista con la mayor cantidad de ciberataques per cápita, superando a todos los demás países por un margen significativo. Esto sugiere que, aunque su población es pequeña, es un objetivo muy frecuente de ataques cibernéticos. Este alto número de ataques podría explicarse por la significativa exposición del sistema financiero chipriota, históricamente vinculado a su papel como paraíso fiscal y centro bancario internacional, lo que lo convierte en un objetivo atractivo para los ciberdelincuentes (*La UE Rescata Al Paraíso Fiscal de Chipre*, s. f.).

Polonia y Nueva Zelanda también muestran niveles elevados de ciberataques per cápita, lo que indica una gran exposición digital en relación con su población.

Rumanía, Dinamarca, Finlandia, Corea del Sur, Croacia, Mongolia e Irlanda tienen tasas de ataque per cápita similares, aunque menores que las de los líderes.

ii) Factores que pueden influir en la alta tasa per cápita

- Tamaño de la población: Países con poblaciones pequeñas pero una alta actividad digital puede registrar tasas de ataque per cápita más elevadas.
- Infraestructura tecnológica y digitalización: Una gran presencia de servicios digitales, infraestructuras críticas en línea y empresas tecnológicas puede hacer que ciertos países sean más atractivos para los atacantes.

- Política de ciberseguridad y transparencia: En algunos países, los datos sobre ciberataques se reportan con más detalle, lo que puede aumentar las cifras registradas.
- Geolocalización y acceso a redes internacionales: Países estratégicamente ubicados en términos de infraestructura de redes pueden ser más susceptibles a ataques que buscan aprovechar vulnerabilidades en puntos clave de conexión.

3.2.3. Países con menor número absoluto de ciberataques

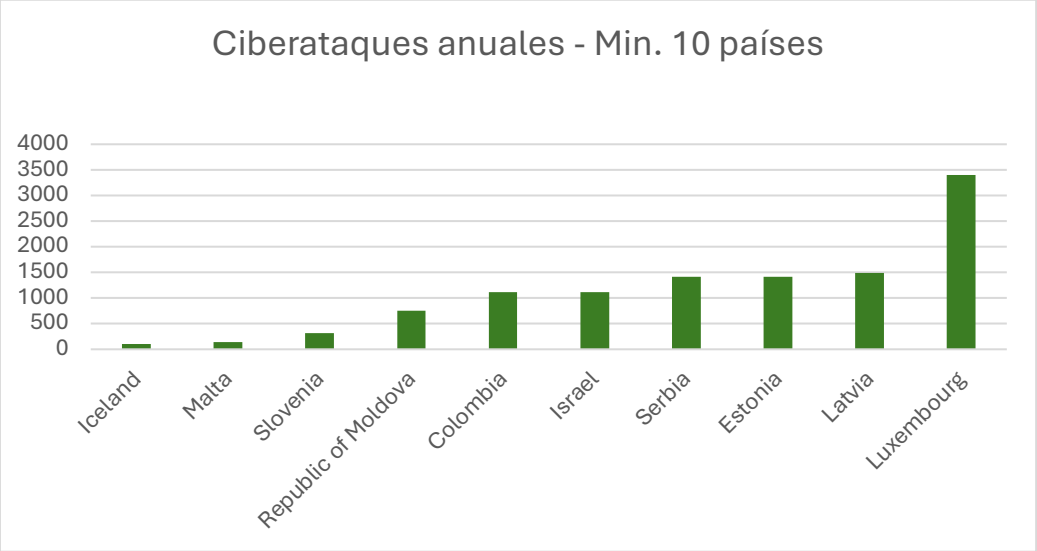


Figura 3 - Top 10 países con menor número de ciberataques totales

i) Observaciones clave

Los 10 países con menor número absoluto de ciberataques anuales en la figura 3, muestran que Islandia y Malta tienen las cifras más bajas, con menos de 100 ataques registrados anualmente.

Luxemburgo tiene el mayor número de ataques dentro de este grupo, superando los 3,500 ciberataques anuales, lo que sigue siendo bajo en comparación con los países más atacados.

Países como Eslovenia, Moldavia, Colombia, Israel, Serbia, Estonia y Letonia presentan cifras moderadas, con un rango entre 300 y 1,500 ciberataques anuales.

ii) Posibles razones de la baja cantidad de ataques

- Tamaño y población reducida: Muchos de estos países tienen poblaciones pequeñas y menor número de objetivos digitales para los atacantes.

- Menor relevancia en infraestructura tecnológica: A diferencia de grandes economías como EE. UU. o Alemania, estos países pueden no ser un foco de interés para cibercriminales.
- Estrategias de ciberseguridad eficaces: Algunos de estos países pueden contar con buenas prácticas y regulaciones que minimizan su vulnerabilidad.
- Menor transparencia en el reporte de ciberataques: En algunos casos, la baja cantidad de ataques podría estar relacionada con la falta de datos o reportes oficiales.

3.2.4. Países con menor número de ciberataques per cápita

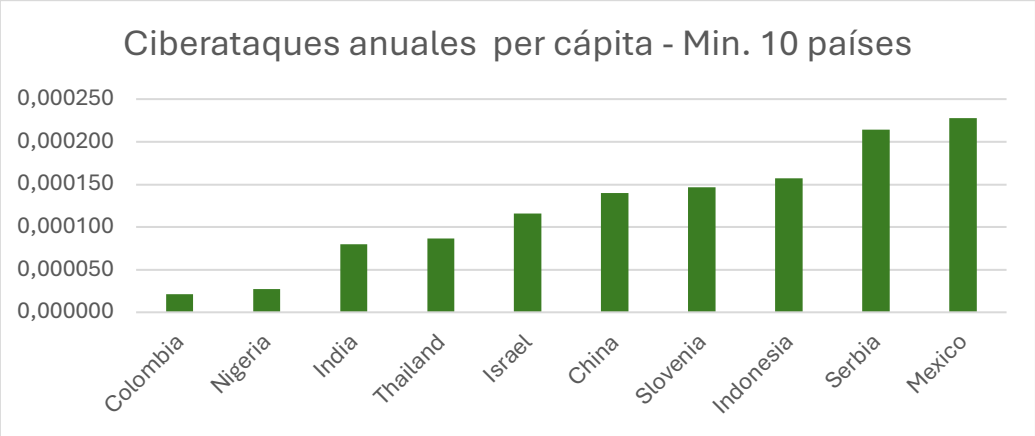


Figura 4 - Top 10 países con menor número de ciberataques per cápita

i) Observaciones

Analizando la figura 4, se muestra los 10 países con menor cantidad de ciberataques per cápita, es decir, donde los ataques son proporcionalmente menos frecuentes en relación con la población.

Colombia y Nigeria tienen las tasas más bajas, lo que sugiere que son de los países menos afectados por ataques en relación con su población. Por otro lado, países como India, Tailandia, Israel y China muestran un ligero aumento en la tasa de ataques per cápita, pero aún se encuentran en la parte baja del ranking global.

México y Serbia, aunque en la parte alta de esta lista, siguen teniendo niveles de ataque per cápita considerablemente menores en comparación con los países más atacados.

ii) Posibles razones de la baja incidencia de ataques

- Poblaciones grandes: Países como India, China y México tienen enormes poblaciones, lo que diluye la tasa de ataques per cápita, incluso si el número total de ataques es alto.
- Menor digitalización: En algunos de estos países, aunque haya un crecimiento en el acceso a Internet, el nivel de digitalización en sectores estratégicos puede ser menor que en economías avanzadas.
- Enfoque en otros tipos de ataques: Algunos países pueden tener más ataques de fraude digital, suplantación de identidad o ataques locales que no se contabilizan en estas estadísticas globales.
- Baja infraestructura tecnológica como objetivo: En países en desarrollo, muchas empresas aún no han migrado completamente a la digitalización, reduciendo su exposición a amenazas avanzadas.

3.3. Análisis gráfico de relaciones económicas y digitales

3.3.1. Ciberataques totales vs. PIB

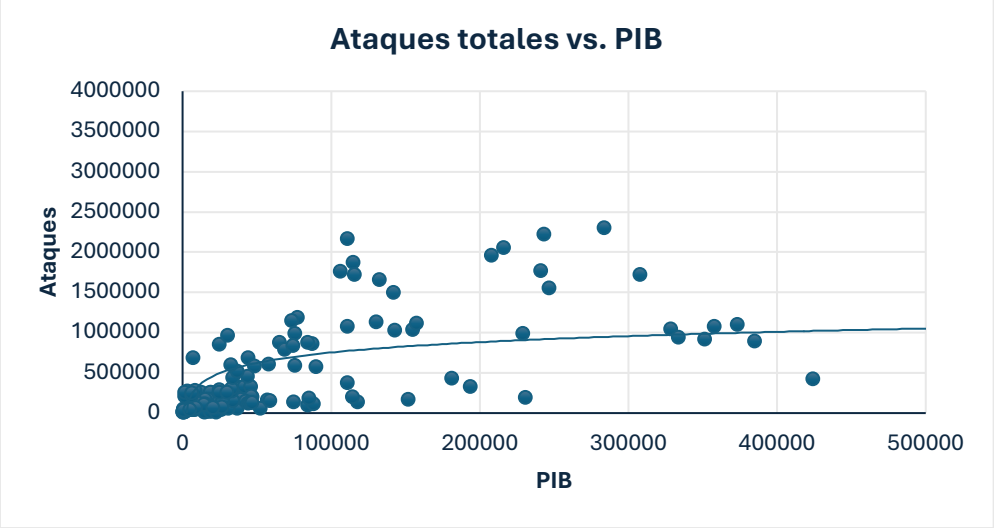


Figura 5 - Gráfico de dispersión: ataques totales vs. PIB

La figura 5 muestra la relación entre el número total de ciberataques y el Producto Interior Bruto (PIB) de distintos países. Se observa una elevada concentración de puntos en los valores más bajos del PIB, lo que señala que una amplia variedad de países con economías más pequeñas sufre una gran variabilidad en la cantidad de ataques. A medida que el PIB aumenta, la dispersión de los datos sigue siendo notable, aunque se percibe una ligera tendencia creciente en la curva. No obstante, la relación no parece ser estrictamente lineal

ni uniforme, lo que sugiere que otros factores pueden estar influyendo en la distribución de los ataques cibernéticos.

El análisis estadístico de la figura 5 confirma esta observación, con un coeficiente de correlación de -0.034, lo que sugiere una relación prácticamente nula entre PIB y ciberataques. Algunos países con economías pequeñas experimentan niveles de ataques similares a los de grandes potencias económicas, mientras que otros con alto PIB presentan una cantidad relativamente baja de ataques. Esto sugiere que existen factores adicionales más relevantes, como el nivel de digitalización, la inversión en ciberseguridad y la capacidad de detección y reporte de incidentes.

Dado que el PIB no explica por sí solo los ataques, sería interesante realizar un análisis más profundo segmentando los datos por niveles de PIB, aplicando modelos no lineales y considerando variables como pueden ser la inversión en ciberseguridad y el grado de digitalización. Esto permitiría identificar patrones más precisos y comprender mejor qué factores realmente influyen en la vulnerabilidad de un país frente a ciberataques.

3.3.2. Ciberataques totales vs. PIB per cápita

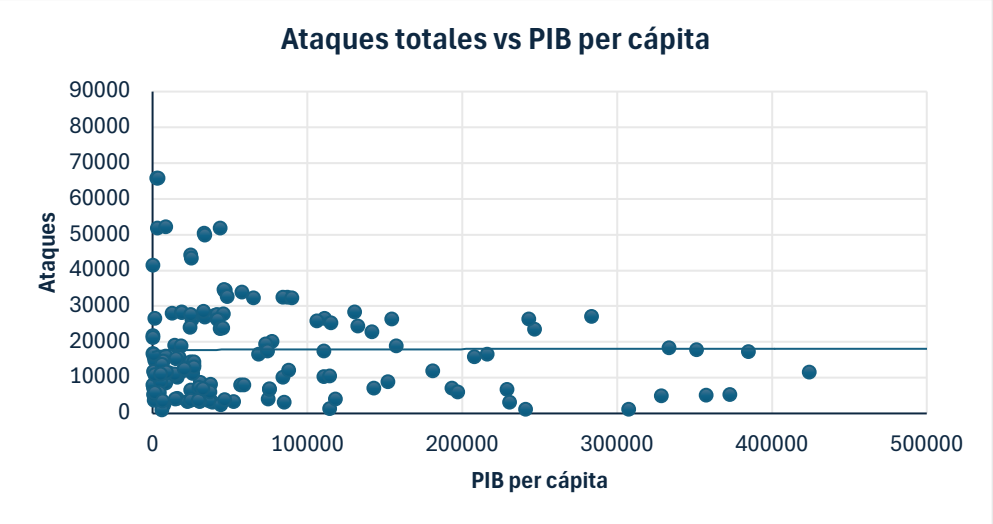


Figura 6 - Gráfico de dispersión: ataques totales vs. PIB per cápita

El análisis muestra que en la figura 6 no existe una relación clara entre el PIB per cápita y la cantidad de ciberataques. A pesar de que algunos países con menor PIB per cápita presentan más ataques, la dispersión de los datos indica que el nivel de riqueza individual no es un factor determinante en la exposición a amenazas cibernéticas. La línea de

tendencia plana refuerza esta idea, mostrando que los ataques no aumentan ni disminuyen de forma consistente con el ingreso per cápita.

Este resultado sugiere que otros factores influyen más en la cantidad de ciberataques. Podrían estar influyendo más directamente elementos como la digitalización, la inversión en ciberseguridad y la capacidad de detección y reporte en la cantidad de ciberataques. Los países con un rápido desarrollo digital, pero sin una infraestructura de seguridad adecuada pueden ser más vulnerables a ciberataques, mientras que las economías más avanzadas pueden reducir su impacto gracias a mejores sistemas de defensa. Para obtener una conclusión más precisa, sería necesario analizar estas hipótesis en mayor profundidad. Para comprender mejor este fenómeno, sería útil segmentar los datos por niveles de desarrollo o analizar modelos no lineales. Además, incluir variables como el gasto en ciberseguridad o el grado de digitalización ayudaría a identificar patrones más precisos sobre los factores que realmente afectan la frecuencia de los ciberataques.

3.3.3. Ciberataques totales vs. MBB

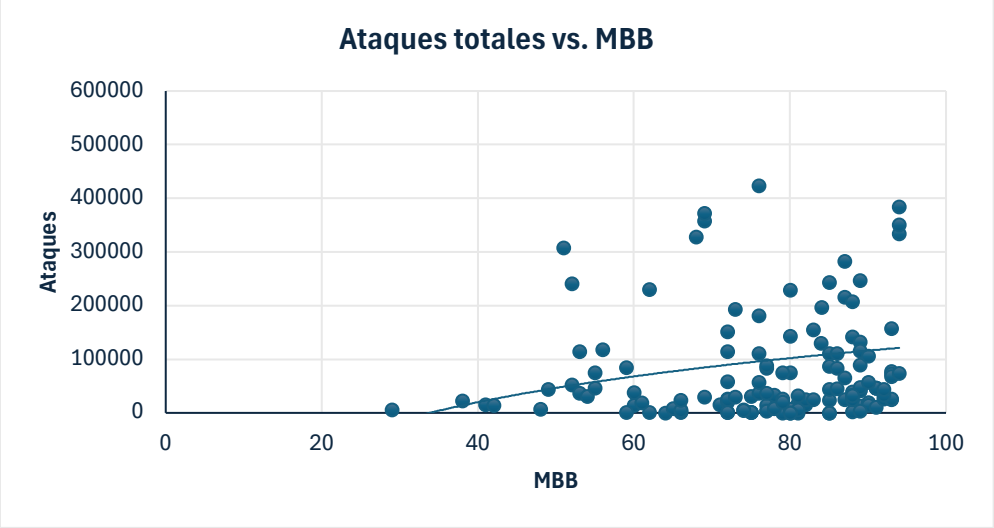


Figura 7 - Gráfico de dispersión: ataques totales vs. MBB

El gráfico 7 muestra una relación entre banda ancha móvil (MBB) y la cantidad de ciberataques, con una tendencia ascendente moderada. A medida que el MBB aumenta, se observa una mayor incidencia de ataques, aunque con una alta dispersión en los datos.

En los valores más bajos de MBB, los ataques son relativamente escasos, mientras que en niveles más altos la cantidad de incidentes varía significativamente, con algunos países experimentando un gran volumen de ataques. Esto sugiere que un mayor MBB puede

estar asociado con una mayor exposición a amenazas cibernéticas, aunque con diferencias notables entre países. A pesar de la tendencia general al alza, la dispersión de los datos indica que otros factores pueden estar influyendo en la vulnerabilidad a los ataques. La seguridad digital, la infraestructura tecnológica y la capacidad de respuesta pueden explicar por qué algunos países con MBB alto presentan menos ataques que otros en el mismo rango.

3.3.4. Ciberataques per cápita vs. PIB

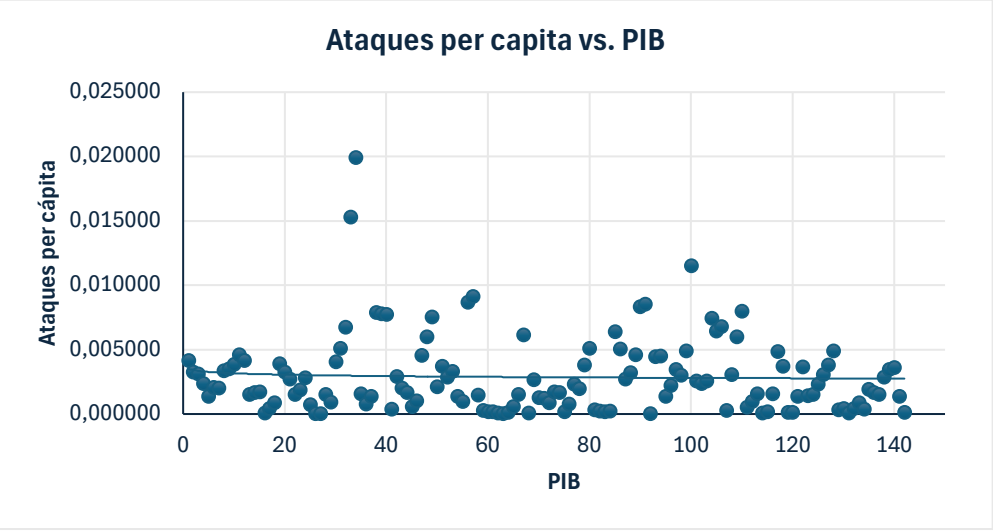


Figura 8 - Gráfico de dispersión: ataques per cápita vs. PIB

El gráfico 8 sugiere que el PIB no tiene una relación clara con la cantidad de ataques cibernéticos per cápita, lo que desafía la idea de que los países más ricos sean automáticamente más vulnerables a los ciberataques debido a su mayor digitalización. La línea de tendencia plana confirma que el tamaño de la economía no explica de manera directa la incidencia de ataques en relación con la población.

Sin embargo, la dispersión de los datos indica que en ciertos países los ataques per cápita son notablemente más altos. Esto puede deberse a brechas en ciberseguridad, donde economías con crecimiento tecnológico acelerado no han desarrollado infraestructuras de protección adecuadas. También podría estar influenciado por diferencias en la regulación y en la capacidad de monitoreo, lo que afectaría el número de ataques registrados más que la cantidad real de incidentes.

Otro punto relevante en la figura 8 es que algunos países con PIB más bajo presentan niveles altos de ataques per cápita, lo que sugiere que los ciberdelincuentes no solo buscan

objetivos económicamente atractivos, sino también infraestructuras más vulnerables. Esto refuerza la idea de que el nivel de exposición a ciberataques depende más de factores como la conectividad, la inversión en seguridad y la capacidad de respuesta, que del PIB en sí mismo.

3.3.5. Ciberataques per cápita vs. PIB

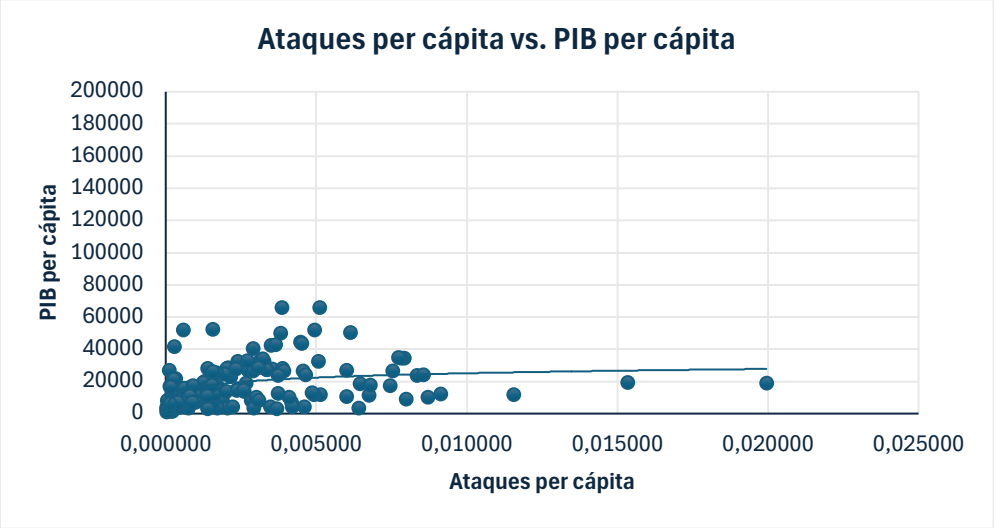


Figura 9 - Gráfico de dispersión: ataques per cápita vs. PIB per cápita

Se puede observar en la figura 9 que la riqueza individual de un país no determina su nivel de exposición a ciberataques, ya que no se observa una relación clara entre el PIB per cápita y los ataques per cápita. La mayoría de los países parecen agruparse en niveles bajos de ambas variables, sin un patrón evidente que indique que los países más ricos o pobres sean sistemáticamente más atacados.

Sin embargo, algunos países con bajo PIB per cápita destacan con niveles de ataques per cápita elevados, lo que podría deberse a fallos en la infraestructura de ciberseguridad, menor inversión en protección digital o incluso el uso de estos territorios como plataformas para lanzar ataques. Esto sugiere que la vulnerabilidad a los ciberataques no está solo vinculada a la riqueza, sino a cómo se gestiona la seguridad digital en cada país.

En países con PIB per cápita más alto, los ataques per cápita no aumentan de manera proporcional, lo que refuerza la idea de que la ciberseguridad y la capacidad de respuesta juegan un papel más importante que el desarrollo económico. Esto indica que, más allá del tamaño de la economía o del nivel de ingresos, la preparación y las estrategias de defensa cibernética son clave para determinar la incidencia de los ataques.

3.3.6. Ciberataques per cápita vs. MBB

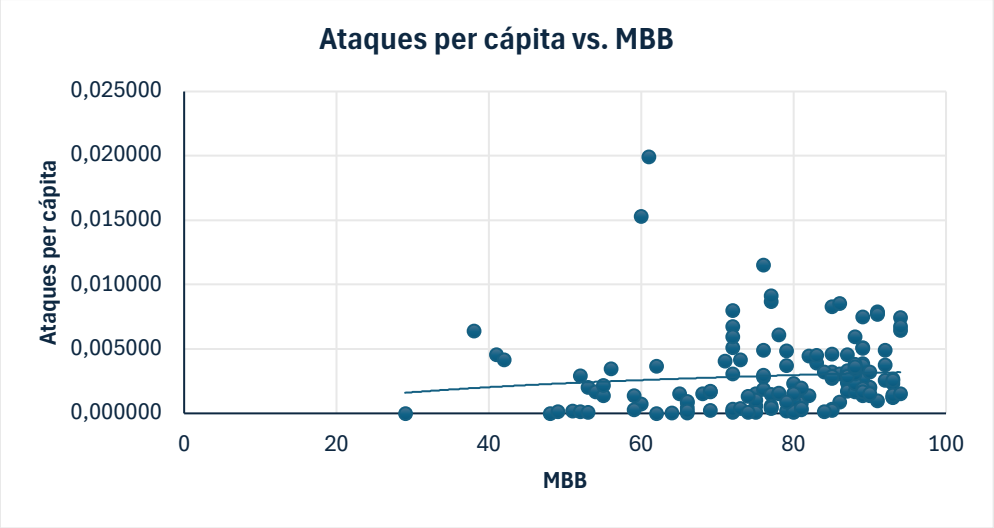


Figura 10 - Gráfico de dispersión: ataques per cápita vs. MBB

Analizando la figura 10 observamos una pequeña relación entre MBB y los ataques per cápita, mostrando una leve tendencia creciente. A medida que el MBB aumenta, los ataques per cápita parecen incrementarse en algunos casos, aunque con una gran dispersión de los datos.

Se observa que en niveles bajos de MBB la cantidad de ataques es reducida, pero en niveles más altos la variabilidad crece. Esto sugiere que una mayor penetración MBB puede estar asociada con una mayor exposición a ciberataques, posiblemente porque un mayor acceso digital amplía la superficie de ataque. Sin embargo, la dispersión indica que el impacto del MBB no es uniforme. En algunos países con alto MBB, la incidencia de ataques per cápita sigue siendo baja, lo que podría deberse a mejores estrategias de ciberseguridad, educación digital o infraestructura de protección. Esto refuerza la idea de que no es solo el nivel de conectividad lo que influye, sino cómo se gestiona la seguridad digital dentro de cada país.

4. Estimación del impacto económico de los ciberataques para una muestra de países.

4.1. Preparación del *dataset* y descripción de variables

Después del análisis descriptivo inicial, se han tratado y ajustado las variables con el objetivo de mejorar su aplicación en la futura modelización econométrica del efecto económico de los ciberataques. Este proceso de tratamiento previo ha facilitado la mejora de la coherencia interna del dataset, ha permitido una mejor comparación entre observaciones y ha asegurado el uso correcto de técnicas estadísticas. Como parte de este proceso, se eliminaron las observaciones que contenían valores nulos (NaNs). Tras esta depuración, el conjunto de datos final quedó reducido a 141 países y 18 variables, que son las que se utilizarán para el análisis y la estimación posterior.

Las variables utilizadas se detallan a continuación:

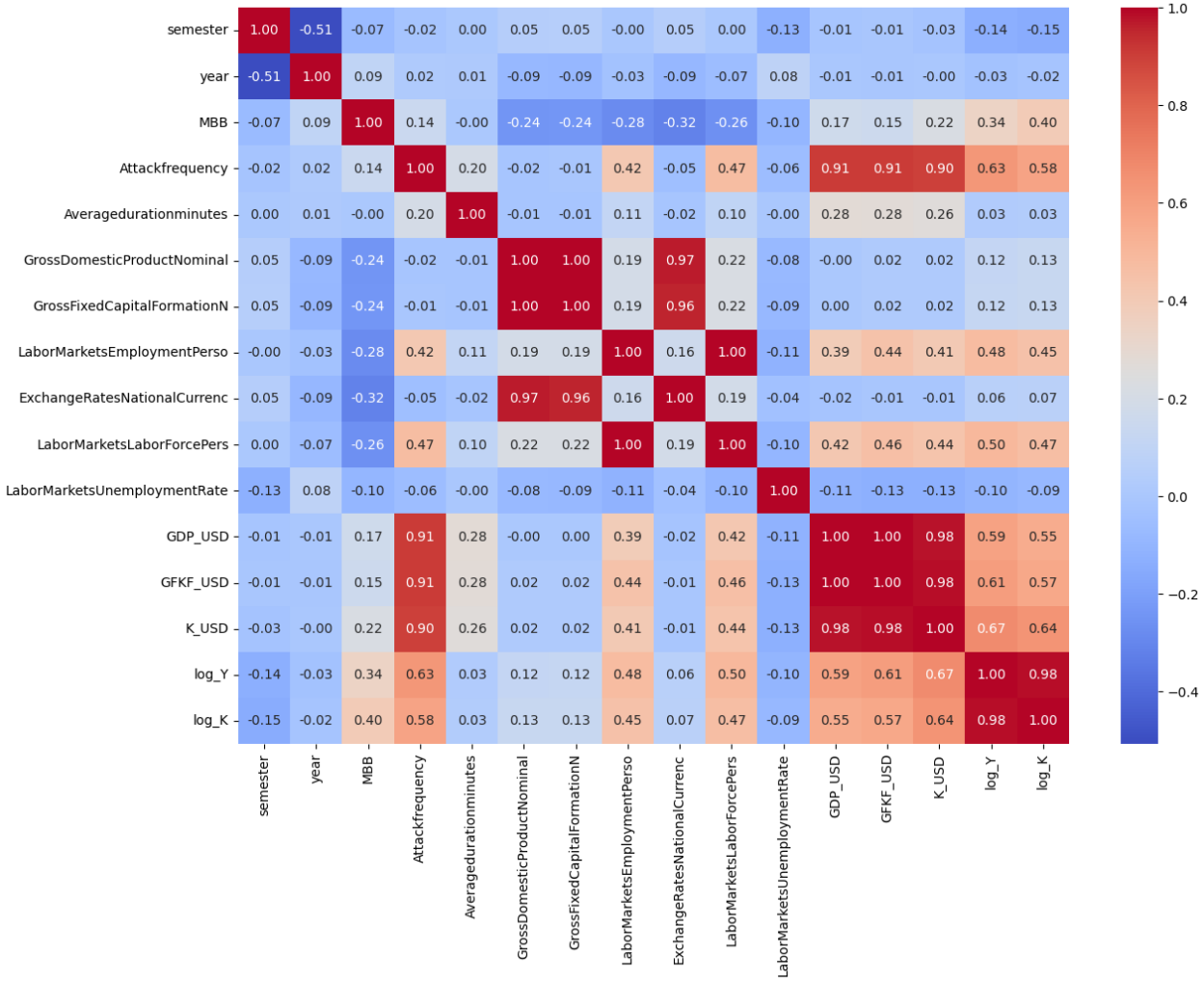
- Country: país objeto de análisis.
- semester y year: periodo temporal de referencia.
- MBB (Mobile Broadband Penetration): indicador del grado de digitalización, representado por la penetración de la banda ancha móvil.
- Attackfreq: número absoluto de ciberataques reportados en el país durante el periodo.
- Averagedu: duración promedio de los ataques, en minutos.
- GrossDom: PIB nominal del país en su moneda local.
- GrossFixed: formación bruta de capital fijo, como aproximación de la inversión nacional.
- LaborMark: número de personas empleadas.
- Exchange1: tipo de cambio de la moneda nacional frente al dólar estadounidense.
- LaborMark (fuerza laboral) y LaborMark M (tasa de desempleo): indicadores del mercado laboral.
- GDP_USD, GFKF_USD y LK_USD: PIB, inversión y capital total expresados en dólares estadounidenses, permitiendo comparabilidad internacional.
- log_Y y log_K: transformaciones logarítmicas del PIB y capital, utilizadas en los modelos econométricos para garantizar linealidad y homocedasticidad.

Este conjunto de variables constituye la base analítica sobre la cual se construyen los modelos que permitirán cuantificar el efecto económico de los ciberataques a nivel país y periodo.

4.2. Análisis exploratorio previo a modelización

Antes de comenzar a estimar el impacto económico de los ciberataques, analizaremos unas las variables contenidas en la base de datos con el objetivo de detectar vínculos relevantes entre estas. La figura 11 muestra la matriz de correlación de Pearson entre las variables principales del análisis.

Figura 11 - Correlación entre variables a estudiar



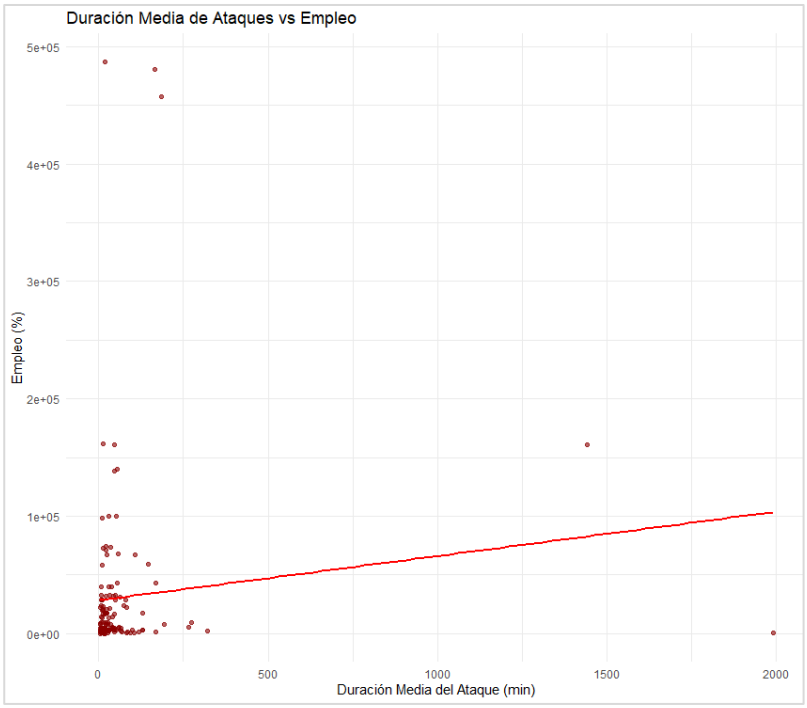
Este análisis permite detectar patrones de asociación entre indicadores clave, lo cual resulta útil tanto para la interpretación preliminar del fenómeno como para evitar problemas de multicolinealidad en las regresiones posteriores. Se observan, por ejemplo, correlaciones positivas fuertes entre variables

como GDP_USD, GFKF_USD y LK_USD, lo cual es coherente al tratarse de magnitudes económicas relacionadas con el tamaño y la inversión en cada país.

Asimismo, destaca la relación positiva entre la frecuencia de ciberataques (Attackfreq) y el PIB, lo que sugiere que los países con mayor nivel de desarrollo económico pueden ser más propensos a sufrir ataques, posiblemente por su mayor digitalización e interconectividad. También se observa una correlación moderada entre la penetración de banda ancha móvil (MBB) y el logaritmo del PIB (log_Y), reforzando la idea de que el desarrollo tecnológico está vinculado al nivel económico del país.

Estos resultados respaldan la relevancia de las variables seleccionadas y justifican su inclusión en los modelos de estimación que se desarrollarán en los siguientes apartados, donde se analizará en profundidad el impacto económico de los ciberataques a partir de modelos econométricos.

Figura 12 - Duración Media de Ataques vs. Empleo



Este gráfico, figura 12, muestra una relación entre la duración media de los ciberataques (en minutos) y el número de personas empleadas en cada país. Se observa una fuerte dispersión, con muchos países concentrados en duraciones cortas (<200 min). Existen *outliers* tanto en duración como en nivel de empleo, que distorsionan la relación. La pendiente positiva sugiere que, en promedio, una mayor duración de ataques podría asociarse con mayor nivel de empleo, aunque esta relación puede ser espuria o reflejar el

tamaño del país. Se recomienda normalizar o aplicar transformaciones para evitar sesgos por escalas distintas.

Estos análisis visuales preliminares permiten identificar patrones de relación entre los ciberataques y variables económicas clave, como el empleo, la infraestructura digital o la inversión en capital. Aunque los gráficos muestran ciertas tendencias (en general positivas), también ponen de manifiesto la existencia de dispersión, *outliers* y posibles relaciones no lineales, lo que refuerza la necesidad de aplicar técnicas econométricas más robustas que permitan aislar y cuantificar el efecto específico de los ciberataques sobre el desempeño económico.

Por tanto, y con base en estas evidencias, se justifica la inclusión de estas variables en los modelos de estimación que se desarrollarán en los siguientes apartados, donde se analizará en profundidad el impacto económico de los ciberataques a partir de un marco de análisis formal.

4.3. Especificación del modelo econométrico

Una vez realizado el análisis descriptivo y exploratorio de las variables, el siguiente paso consiste en estimar el efecto de los ciberataques sobre la actividad económica mediante un modelo econométrico. Para ello, se parte de una función de producción basada en la formulación clásica de tipo *Cobb-Douglas*, ampliamente utilizada en economía para representar la relación entre los factores productivos (capital, trabajo y tecnología) y el output agregado (PIB).

Sin embargo, este estudio introduce una extensión del modelo tradicional, incorporando explícitamente los ciberataques como un factor que erosiona la eficacia de los inputs productivos. Es decir, se plantea que la frecuencia de ataques puede disminuir la productividad del capital, la tecnología digital y el trabajo. El modelo base que interesa estimar es el siguiente:

$$Y = A(K - \delta_K CYBER)^{\alpha} + (MBB - \delta_{MBB} CYBER)^{\gamma} + (L - \delta_L CYBER)^{\beta}$$

Donde:

- Y representa el Producto Interior Bruto (PIB),
- K, MBB y L son los factores productivos: capital físico, tecnología digital (medida por la penetración de banda ancha móvil) y trabajo respectivamente.

- CYBER representa la frecuencia de ciberataques,
- δ_K, δ_{MBB}, $\delta_L$son los parámetros que capturan el efecto de los ciberataques sobre cada uno de los factores.
- ´A´ es productividad total de los factores
- α, β, γ : elasticidades de cada input

¿Por qué elegir utilizar un modelo de regresión no lineal para esta estimación?

El análisis exploratorio reveló que las relaciones entre las variables clave (como PIB, capital, trabajo, inversión o frecuencia de ciberataques) no son estrictamente lineales. Se observó una alta dispersión, patrones curvilíneos y relaciones que varían según el nivel de desarrollo o digitalización de los países. Ante este contexto, el uso de un modelo lineal clásico podría resultar insuficiente o incluso inadecuado.

Por ello, se opta por un modelo de regresión no lineal con transformación logarítmica, por las siguientes razones:

- Captura elasticidades: La forma logarítmica permite interpretar directamente los coeficientes como elasticidades, lo que facilita la comparación entre países y contextos económicos distintos.
- Mejora la estabilidad del modelo: Ayuda a corregir problemas comunes como la heterocedasticidad (variabilidad desigual de los residuos), mejorando la robustez estadística.
- Refleja mejor la realidad económica: Las relaciones entre *inputs* y *output* en macroeconomía suelen ser multiplicativas, no aditivas. La especificación log-log se ajusta mejor a este comportamiento.
- Evita sobreestimaciones en contextos extremos: En países con niveles muy altos de ataques o inversión, el modelo no lineal ofrece una representación más realista y moderada del impacto.

Para facilitar la estimación empírica del modelo y permitir la interpretación directa de elasticidades, se aplica logaritmación a la expresión anterior, obteniendo la siguiente versión:

$$\log(Y) = \log(A) + \alpha \log(K - \delta_K CYBER) + \gamma \log(MBB - \delta_{MBB} CYBER) + \\ + \beta \log(L - \delta_L CYBER)$$

Esta formulación permite analizar de forma diferenciada el efecto de los ciberataques sobre cada factor productivo, e identificar si afectan significativamente su capacidad de

contribuir al crecimiento económico. A partir de esta especificación, se plantean las siguientes hipótesis de trabajo:

- Si $\delta_K > 0$, entonces los ciberataques dañan al capital físico y reducen su contribución económica.
- Si $\delta_{MBB} > 0$, entonces los ciberataques disminuyen la contribución económica de las tecnologías digitales.
- Si $\delta_L > 0$, entonces los ciberataques reducen su contribución económica de los trabajadores dado que éstos tienen que dedicarse a reparar los sistemas ante los daños.

En la siguiente sección se presentan los resultados de la estimación realizada con R Commander, donde se contrastan empíricamente estas hipótesis. Este análisis permite identificar qué factor productivo es más vulnerable a los ciberataques, aportando información clave para la formulación de políticas públicas y estrategias empresariales orientadas a mitigar sus efectos en la economía.

4.4. Resultados obtenidos

Una vez aplicado el modelo econométrico descrito anteriormente, se estimaron los coeficientes mediante una regresión no lineal utilizando la frecuencia de ciberataques como variable que ajusta negativamente cada uno de los factores productivos. La especificación estimada toma la siguiente forma:

```
Formula: log_Y ~ c + alpha * log(pmax(K_USD - delta_k * Attackfrequency, 1e-06)) +
        gamma * log(pmax(MBB - delta_mbb * Attackfrequency, 1e-06)) +
        beta * log(pmax(LaborMarketsEmploymentPerso - delta_l * Attackfrequency, 1e-06))
```

La inclusión de la función *max* asegura que el argumento dentro del logaritmo no sea negativo ni cero, lo cual podría invalidar la estimación. Los resultados de la estimación se presentan a continuación:

Tabla 1 - Resultados Modelo Econométrico Ciberataques

Término	Estimación	Error estándar	Estadístico t	p-valor	Significación
c	-1.500	0.292	-5.15	9.15e-07	***** (p < 0.001)**
alpha	0.918	0.0296	31.0	5.04e-63	***** (p < 0.001)**
gamma	0.0109	0.00469	2.32	2.17e-02	*** (p < 0.05)**
beta	0.0820	0.0234	3.51	6.13e-04	***** (p < 0.001)**
delta_k	0.000	0.641	0.00	1.00e+00	**-**
delta_mbb	0.00949	0.00421	2.26	2.57e-02	*** (p < 0.05)**
delta_l	0.0260	0.00105	24.7	1.12e-51	***** (p < 0.001)**

Contrastamos los resultados con las hipótesis previas:

A partir de los resultados obtenidos en la estimación del modelo, se procede a contrastar empíricamente las tres hipótesis planteadas respecto al impacto de los ciberataques sobre los factores productivos:

1. Hipótesis 1 $\delta_K > 0$: Esta hipótesis sugiere que los ciberataques dañan el capital físico y, en consecuencia, reducen su contribución al crecimiento económico. Sin embargo, el coeficiente estimado para δ_K es igual a 0 y presenta un p-valor de 1.00, lo cual indica ausencia total de evidencia estadística que respalde esta afirmación. Por tanto, esta hipótesis no puede ser aceptada, y se concluye que los ciberataques no tienen un impacto significativo sobre la productividad del capital físico en el contexto analizado.
2. Hipótesis 2 $\delta_{MBB} > 0$: Esta hipótesis plantea que los ciberataques afectan negativamente la eficacia de las tecnologías digitales, como la banda ancha móvil (MBB). El valor estimado de δ_{MBB} es positivo (0.00949) y significativo al 5% (p-valor = 0.0257), lo que proporciona evidencia empírica suficiente para aceptar esta hipótesis. Esto sugiere que los ciberataques comprometen el rendimiento o disponibilidad de los recursos digitales, reduciendo su capacidad de contribuir al PIB. Este resultado pone de manifiesto la vulnerabilidad de la infraestructura tecnológica frente a los ciberataques.
3. Hipótesis 3 $\delta_L > 0$: Esta hipótesis sostiene que los ciberataques reducen la contribución económica del trabajo, dado que los empleados deben redirigir esfuerzos a reparar los sistemas en lugar de realizar actividades productivas. El coeficiente estimado para δ_L es positivo (0.0260) y altamente significativo (p-valor $\approx$ 0.000, con ***). Se trata del coeficiente con mayor significación del modelo, lo que confirma de manera robusta esta hipótesis. Por tanto, se concluye

que los ciberataques generan un efecto negativo sobre la productividad laboral, convirtiéndose en la principal vía de impacto económico detectada en este estudio.

Los resultados del modelo econométrico confirman que los ciberataques tienen un impacto negativo y estadísticamente significativo sobre algunos factores productivos, particularmente sobre el trabajo y, en menor medida, sobre la infraestructura digital. En cambio, no se ha encontrado evidencia de que los ciberataques afecten al capital físico.

Estos hallazgos permiten concluir que el principal canal de transmisión económica del impacto cibernético es la pérdida de productividad laboral, ya que los trabajadores deben destinar tiempo y recursos a mitigar los efectos de los ataques, en lugar de contribuir a la producción. Asimismo, el efecto negativo sobre la tecnología digital refleja una creciente vulnerabilidad del ecosistema económico a los riesgos cibernéticos.

A la luz de estos resultados, se hace evidente la necesidad de diseñar estrategias de mitigación eficaces que reduzcan la exposición y el impacto de los ciberataques, especialmente en los ámbitos laboral y tecnológico. En el siguiente capítulo se presentan una serie de recomendaciones prácticas y políticas públicas orientadas a fortalecer la resiliencia económica frente a estas amenazas digitales.

5. Recomendaciones para abordar el problema

Tras haber considerado previamente algunas medidas generales para mitigar los efectos de los ciberataques, este apartado se centra en aquellas recomendaciones que, a la luz del análisis cuantitativo desarrollado, se consideran más eficaces. Los resultados del modelo econométrico evidencian que los ciberataques afectan especialmente a la productividad laboral y a la infraestructura digital. Por ello, se proponen a continuación una serie de políticas públicas y acciones estratégicas que, más allá de las iniciativas ya existentes, podrían representar un enfoque más eficiente y focalizado para reducir el impacto económico de estas amenazas.

5.1. Desarrollo de Estrategias Nacionales de Ciberseguridad

La Unión Europea ha puesto en marcha la estrategia *ProtectEU* como respuesta integral ante la creciente amenaza del crimen organizado, el terrorismo y, de forma destacada, el cibercrimen. Esta estrategia no se limita a reforzar la capacidad de actuación de agencias

como *Europol* y *Frontex*, sino que persigue una transformación estructural de la arquitectura de seguridad interna europea. En concreto, *ProtectEU* plantea un enfoque coordinado que involucra a gobiernos nacionales, organismos comunitarios, empresas privadas y sociedad civil. La estrategia también aboga por la protección de infraestructuras críticas frente a ataques cibernéticos, entendiendo que estas representan un activo económico y social esencial cuya vulnerabilidad puede desencadenar efectos sistémicos. (Ayuso, 2025)

5.2. Creación de Centros Nacionales de Ciberseguridad

En consonancia con las directrices europeas, el Gobierno de España ha aprobado el anteproyecto de la Ley de Coordinación y Gobernanza de la Ciberseguridad. Esta norma contempla como eje central la creación de un Centro Nacional de Ciberseguridad, concebido como la entidad responsable de articular la protección de redes y sistemas frente a ciber amenazas. Este centro aspira a convertirse en una referencia estatal en materia de prevención, análisis y respuesta ante ataques digitales, permitiendo la coordinación de capacidades técnicas e institucionales en todo el territorio. La creación de este organismo también contribuirá a mejorar la gobernanza digital del país, fortaleciendo la resiliencia tecnológica y alineando los esfuerzos regionales con las exigencias del entorno europeo. (Efe, 2025)

5.3. Inversión en Defensa y Ciberseguridad

El refuerzo de la ciberseguridad también se ha convertido en una prioridad presupuestaria para el Gobierno de España. La vicepresidenta primera y ministra de Hacienda, María Jesús Montero, ha confirmado una ampliación del gasto en defensa mediante una modificación presupuestaria de 2.000 millones de euros. Esta inversión no solo está orientada a la defensa convencional, sino que pone un foco especial en ámbitos como la ciberseguridad y el ciberterrorismo. Esta decisión se enmarca en el compromiso del Ejecutivo con la seguridad europea y refleja el reconocimiento de que las amenazas digitales requieren una respuesta estructural y sostenida en el tiempo, capaz de proteger tanto los intereses estratégicos como la actividad económica del país. (HuffPost, 2025)

5.4. Reducción de la Dependencia Tecnológica Extranjera

Expertos en ciberseguridad han advertido que la elevada dependencia tecnológica de países europeos respecto a proveedores estadounidenses constituye una vulnerabilidad

crítica. Un ejemplo citado en medios daneses sugiere que, en un escenario extremo, Estados Unidos podría dejar paralizado digitalmente a países como Dinamarca si suspendiera el acceso a sus servicios. Este tipo de advertencias subraya la necesidad de avanzar hacia una mayor soberanía tecnológica. Para ello, es crucial fomentar el desarrollo de infraestructuras digitales propias, incentivar la innovación tecnológica nacional y diversificar las fuentes de servicios estratégicos. Esta independencia no solo mejora la seguridad nacional, sino que también favorece la competitividad económica a largo plazo. (Sanjuan, 2025)

5.5. Implementación de Normativas de Ciberseguridad

El año 2025 ha traído consigo nuevas normativas de ciberseguridad en España, que están impactando de forma directa a las empresas, especialmente a las pequeñas y medianas. Estas regulaciones buscan elevar el nivel de protección digital, exigiendo a las compañías la adopción de medidas mínimas de seguridad como el cifrado de datos, la gestión de accesos o la planificación ante incidentes. Si bien estas normativas suponen un reto operativo y económico para muchas organizaciones, especialmente para aquellas con menor madurez digital, también representan una oportunidad para mejorar su resiliencia frente a ciberataques. Además, ayudan a fortalecer la confianza de los clientes y del ecosistema económico en su conjunto. (Schenk, 2025)

5.6. Fortalecimiento de la Ciberseguridad Empresarial

El refuerzo de la ciberseguridad empresarial ha sido expresamente defendido por el ministro para la Transformación Digital y de la Función Pública, Óscar López, como una prioridad estratégica del Gobierno. En sus declaraciones oficiales, ha remarcado que este objetivo es esencial para consolidar la transformación digital del tejido productivo español, especialmente en sectores donde la digitalización avanza rápidamente, pero los niveles de protección no siempre están al mismo nivel. Las pequeñas y medianas empresas son uno de los focos de esta estrategia, ya que representan el grueso del tejido empresarial español y, al mismo tiempo, suelen ser las más vulnerables a ataques. El apoyo institucional a estas iniciativas se traduce tanto en medidas legislativas como en programas de asesoramiento y financiación para mejorar las capacidades defensivas de las empresas. (Óscar López..., s. f.)

5.7. Desarrollo de Talento en Ciberseguridad

El déficit de profesionales en ciberseguridad representa una amenaza estructural para la protección económica de los países. Según datos recientes, en países como Brasil la demanda de estos perfiles ha aumentado un 76% en tan solo un año, lo que refleja una tendencia global. La escasez de personal cualificado no solo limita la capacidad de respuesta ante ataques, sino que también retrasa la adopción de estrategias de prevención más robustas. Ante esta situación, gobiernos y empresas deben priorizar la formación y captación de talento especializado, tanto en entornos técnicos como en áreas de gestión del riesgo y cumplimiento normativo. La educación en ciberseguridad se ha convertido, así, en una inversión estratégica para la sostenibilidad económica en la era digital. (News Center Microsoft Latinoamérica, 2023)

5.8. Creación de Agencias Especializadas

Japón ha establecido el *Centro de Ciberseguridad del Gabinete (NISC)* como una agencia centralizada para coordinar la respuesta a incidentes cibernéticos y proteger infraestructuras críticas. Sin embargo, este mismo organismo fue objeto de un ciberataque en 2024, lo que pone de manifiesto que incluso las entidades más avanzadas están expuestas a amenazas sofisticadas. Este incidente no solo resalta la necesidad de vigilancia constante, sino que también justifica una revisión continua de los protocolos de seguridad y la actualización de los sistemas. La experiencia japonesa ilustra que la creación de agencias especializadas es necesaria, pero no suficiente, si no va acompañada de capacidades técnicas sólidas, protocolos ágiles de respuesta y colaboración internacional. (Sanjuan, 2025a)

5.9. Inversión en Infraestructuras de Alta Seguridad

El sector privado también está jugando un papel clave en el fortalecimiento del ecosistema de ciberseguridad. Un ejemplo notable es la apertura por parte de la empresa Fortinet de un nuevo centro de datos de alta seguridad en Torija (Guadalajara). Esta instalación no solo incrementa la capacidad de almacenamiento y procesamiento de datos bajo estándares de seguridad avanzados, sino que también actúa como un apoyo estratégico para empresas que desean proteger sus sistemas ante posibles ataques. Este tipo de inversiones refleja cómo el sector tecnológico está asumiendo una mayor responsabilidad en la defensa digital colectiva, reforzando la resiliencia económica en sectores clave. (Orozco, 2025)

5.10. Promoción de la Ciberseguridad en el Ámbito rural

El Gobierno de España ha puesto en marcha un plan para extender la cobertura 5G a municipios de menos de 10.000 habitantes. Esta medida, además de facilitar el acceso digital en zonas tradicionalmente marginadas, incluye una perspectiva de ciberseguridad al favorecer la creación de entornos digitales más protegidos y controlables. Al reducir la brecha digital entre áreas urbanas y rurales, esta iniciativa no solo impulsa la inclusión tecnológica, sino que también favorece la reindustrialización y la atracción de nuevas inversiones, dotando a estos territorios de condiciones similares a las de los grandes centros urbanos. Así, la promoción de la ciberseguridad en zonas rurales se convierte también en una herramienta para el desarrollo económico equilibrado. (Ser, 2025)

Las medidas descritas en este capítulo reflejan una creciente conciencia institucional sobre la amenaza que representan los ciberataques para la estabilidad económica, la productividad laboral y la seguridad digital de los países. Desde estrategias nacionales y centros especializados hasta inversiones en talento e infraestructuras seguras, las acciones emprendidas muestran un enfoque cada vez más multidimensional para abordar el riesgo cibernético. No obstante, los resultados obtenidos en este trabajo empírico evidencian que los ciberataques continúan teniendo un impacto significativo sobre factores productivos clave, especialmente el trabajo y la tecnología, lo que sugiere que aún queda un importante margen de mejora en la efectividad de las políticas actuales. En este sentido, los hallazgos del modelo econométrico refuerzan la urgencia de seguir fortaleciendo la ciber resiliencia desde un enfoque integral, coordinado y sostenido en el tiempo. A continuación, se presentan las principales conclusiones del estudio, así como sus implicaciones para la formulación de políticas públicas y futuras líneas de investigación.

6. Conclusiones

En un escenario de digitalización a nivel mundial creciente, los ciberataques se han transformado en un peligro estructural para la economía, impactando tanto a negocios e individuos como a sectores estratégicos y a la estabilidad macroeconómica. Este estudio ha intentado medir el efecto económico de los ciberataques mediante una perspectiva multidimensional, complementando la revisión teórica con un estudio econométrico aplicado a un grupo de países e industrias.

Los resultados obtenidos permiten extraer varias conclusiones clave:

1) El modelo econométrico desarrollado ha demostrado que los ciberataques no impactan de forma homogénea en los factores productivos. De las tres hipótesis planteadas, se rechaza la que atribuía un efecto negativo al capital físico, al no encontrarse evidencia estadísticamente significativa. En cambio, se confirma con solidez el impacto adverso de los ciberataques sobre la productividad del trabajo, que se perfila como el canal principal de transmisión económica. Asimismo, se evidencia un efecto negativo sobre la infraestructura digital, aunque en menor medida.
2) Estos descubrimientos indican que el verdadero coste de los ciberataques trasciende las pérdidas directas. Influencian la eficacia del sistema económico al redirigir recursos humanos y tecnológicos hacia labores de recuperación y defensa, disminuyendo de esta manera la capacidad de expansión de las economías, en particular las más digitalizadas.
3) Los análisis descriptivos han facilitado la detección de patrones significativos. Nacionalidades con una gran penetración digital y un fuerte peso en el sector financiero, como Chipre, exhiben tasas de ciberataques per cápita significativamente más elevadas. Esto respalda la noción de que la vulnerabilidad al riesgo cibernético está fuertemente vinculada al modelo económico y al nivel de interconectividad de cada país.
4) Las recomendaciones formuladas en este trabajo no solo responden a tendencias generales previamente abordadas en la literatura, sino que están fundamentadas en evidencia empírica. A partir de los resultados del modelo, se proponen medidas más focalizadas y eficaces, orientadas principalmente a reforzar la ciberseguridad laboral, digital y organizativa.

En conclusión, los ciberataques no son solo un problema técnico, sino también un desafío económico y social de gran magnitud. Este análisis proporciona una perspectiva cuantitativa y pragmática para entender de manera más efectiva sus impactos y orientar la toma de decisiones en la creación de políticas públicas y estrategias de negocio. La ciberseguridad debe dejar de ser considerada un gasto extra y transformarse en una inversión esencial para la continuidad del desarrollo económico en la era digital.

7. Declaración de Uso de IA

1) *Brainstorming* de ideas de investigación: Utilizado para idear y esbozar posibles áreas de investigación.
2) Referencias: Usado conjuntamente con otras herramientas, para identificar referencias preliminares que luego he contrastado y validado.
3) Interpretador de código: Para realizar análisis de datos preliminares.
4) Estudios multidisciplinares: Para comprender perspectivas de otras comunidades sobre temas de naturaleza multidisciplinar.
5) Constructor de plantillas: Para diseñar formatos específicos para secciones del trabajo.
6) Corrector de estilo literario y de lenguaje: Para mejorar la calidad lingüística y estilística del texto.
7) Sintetizador y divulgador de libros complicados: Para resumir y comprender literatura compleja.
8) Traductor: Para traducir textos de un lenguaje a otro.
9) Revisor: Para recibir sugerencias sobre cómo mejorar y perfeccionar el trabajo con diferentes niveles de exigencia.

8. Referencias

Ayuso, S. (2025, 1 abril). Bruselas impulsa una respuesta reforzada ante amenazas como el terrorismo o el crimen organizado. *El País*. Recuperado de https://elpais.com/internacional/2025-04-01/bruselas-impulsa-una-respuesta-reforzada-ante-amenazas-como-el-terrorismo-o-el-crimen-organizado.html

Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber attacks and its different types. *International Research Journal of Engineering and Technology*, *6*(3), 4849-4852.

Dieye, R., Bounfour, A., Ozaygen, A., & Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks. *Risk Management and Insurance Review*, *23*(2), 183-208.

Efe. (2025, 14 enero). El Gobierno impulsa una ley que creará un Centro Nacional de Ciberseguridad. *RTVE.es*. Recuperado de https://www.rtve.es/noticias/20250114/gobierno-impulsa-ley-creara-centro-nacional-ciberseguridad/16406428.shtml

Gulyas, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, *219*, 84-90.

HuffPost, R. (2025, 5 abril). Montero confirma que el Gobierno aprobará una modificación presupuestaria para aumentar el gasto en defensa. *ElHuffPost*. Recuperado de https://www.huffingtonpost.es/politica/montero-confirma-gobierno-aprobara-modificacion-presupuestaria-aumentar-gasto-defensabr.html

Künzler, F. (2023). *Real Cyber Value at Risk: An Approach to Estimate Economic Impacts of Cyberattacks on Businesses*(Master's thesis, University of Zurich).

La UE rescata al paraíso fiscal de Chipre. (s. f.). Alternativas Económicas. Recuperado de https://alternativaseconomicas.coop/articulo/el-tema-del-mes/la-ue-rescata-al-paraiso-fiscal-de-chipre

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics and Business Review*, *5*(2), 24-47

News Center Microsoft Latinoamérica. (2023, 19 abril). *El mundo necesita expertos en seguridad cibernética*. News Center Latinoamérica. Recuperado de https://news.microsoft.com/es-xl/el-mundo-necesita-expertos-en-seguridad-cibernetica/

Orozco, J. B. (2025, 30 enero). Cadena SER. *Cadena SER*. Recuperado de https://cadenaser.com/castillalamancha/2025/01/30/fortinet-abre-en-torija-guadalajara-un-centro-de-datos-de-alta-seguridad-ser-guadalajara/

Óscar López subraya el compromiso del Gobierno en el refuerzo de la ciberseguridad empresarial. (s. f.). Recuperado de https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/transformacion-digital-y-funcion-publica/paginas/2025/310125-refuerzo-ciberseguridad-empresarial.aspx

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

Sanjuan, L. M. (2025, 5 abril). Aviso de un experto en seguridad: el país europeo que EEUU podría desconectar en una hora. *Diario AS*. Recuperado de https://as.com/actualidad/politica/aviso-de-un-experto-en-seguridad-el-pais-europeo-que-eeuu-podria-desconectar-en-una-hora-n/

Sanjuan, L. M. (2025a, marzo 9). Lanzan una agencia de ciberseguridad para proteger al país y descubren que han sido hackeados gracias a un chi. *Diario AS*. Recuperado

de https://as.com/actualidad/sociedad/lanzan-una-agencia-de-ciberseguridad-para-proteger-al-pais-y-descubren-que-han-sido-hackeados-gracias-a-un-chivatazo-n/

Schenk, M. (2025, 13 marzo). *¿Qué medidas de ciberseguridad exige el gobierno español a las empresas en 2025 y cómo cumplirlas sin morir en el intento? - Startups Españolas*. Startups Españolas. Recuperado de https://www.startups-espanolas.es/2025/03/11/que-medidas-de-ciberseguridad-exige-el-gobierno-espanol-a-las-empresas-en-2025-y-como-cumplirlas-sin-morir-en-el-intento/

Ser, C. (2025, 2 abril). Cadena SER. *Cadena SER*. Recuperado de https://cadenaser.com/aragon/2025/04/02/oscar-lopez-afirma-en-binefar-que-apostamos-por-una-reindustrializacion-que-cierre-la-brecha-entre-el-mundo-rural-y-el-urbano-ser-aragon-oriental/

There was a cyberattack every 39 seconds in 2023. (2024, 8 enero). WatchGuard Technologies. Recuperado de https://www.watchguard.com/wgrd-news/blog/there-was-cyberattack-every-39-seconds-2023

Vaswani, N. (2021). Cyber Attacks: An Economic Impact. *Supremo Amicus*, *23*, 297.

Venkatachary, S. K., Prasad, J., & Samikannu, R. (2017). Economic impacts of cyber security in energy sector: A review. *International Journal of Energy Economics and Policy*, *7*(5), 250-262

Watkins, B. (2014). The impact of cyber attacks on the private sector. *Briefing Paper, Association for International Affair*, *12*, 1-11.

Weaver, G. A., Feddersen, B., Marla, L., Wei, D., Rose, A., & Van Moer, M. (2022). Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. *Transportation Research Part C: Emerging Technologies*, *137*, 103423.

Zorz, Z. (2018, 15 octubre). *Belgian bank Crelan loses €70 million to BEC scammers - Help Net Security*. Help Net Security. Recuperado de https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/