Informe del proyecto

¿Protege el Desarrollo Digital? Análisis de su Relación con las Brechas de Seguridad

Raquel Limpo Martínez

Resumen

Este estudio analiza la relación entre el desarrollo digital y las brechas de ciberseguridad a nivel global, evaluando si una mayor inversión en digitalización se traduce en una menor exposición a ciberataques. A partir de la integración de dos conjuntos de datos internacionales —uno sobre índices de ciberseguridad y desarrollo digital, y otro sobre amenazas globales de ciberseguridad entre 2015 y 2024— se ha construido un modelo visual y analítico en Power BI que permite explorar esta relación en países clave como Estados Unidos, China, Alemania, Brasil, India o Reino Unido.

El análisis se centró en variables como la inversión total en tecnologías digitales, las pérdidas económicas derivadas de ciberataques y el tipo de amenazas más frecuentes. Se calcularon ratios de inversión/pérdidas por país y se clasificaron mediante una visualización tipo semáforo para identificar niveles de riesgo.

Los resultados muestran que, aunque países como EE.UU. o China presentan altos niveles de inversión y baja proporción de pérdidas relativas, otros países desarrollados como Alemania o Japón muestran una relación inversa, donde las pérdidas superan o igualan a la inversión digital. Esto sugiere que la digitalización, sin una estrategia efectiva de ciberseguridad, no garantiza una menor vulnerabilidad.

Se concluye que el desarrollo digital debe ir acompañado de inversiones específicas en ciberseguridad, y que el análisis comparativo de estos indicadores puede contribuir a una mejor toma de decisiones tanto en políticas públicas como en estrategia empresarial.

Palabras clave: ciberseguridad, desarrollo digital, transformación digital, Global Cybersecurity Index, riesgos cibernéticos, 2015–2024.

Abstract

This study analyzes the relationship between digital development and cybersecurity breaches globally, evaluating whether increased investment in digitalization translates into reduced exposure to cyberattacks. By integrating two international datasets—one concerning cybersecurity indices and digital development, and another on global cybersecurity threats from 2015 to 2024—a visual and analytical model has been created in Power BI to explore this relationship in key countries such as the United States, China, Germany, Brazil, India, and the United Kingdom.

The analysis focused on variables including total investment in digital technologies, economic losses caused by cyberattacks, and the most frequent types of threats. Investment-to-loss ratios per country were calculated and classified using a traffic-light visualization to identify risk levels.

Results indicate that while countries like the US and China have high investment levels and relatively low proportions of losses, other developed nations such as Germany and Japan exhibit an inverse relationship, where losses equal or surpass digital investment. This suggests that digitalization, without an effective cybersecurity strategy, does not guarantee reduced vulnerability.

The study concludes that digital development must be accompanied by targeted cybersecurity investments, and that comparative analysis of these indicators can contribute to better decision-making in both public policy and business strategy.

Keywords: cybersecurity, digital development, GCI, national security, cyber threats, 2015–2024.

Introducción

En un contexto de transformación digital acelerada, el desarrollo tecnológico se ha convertido en un pilar clave para la competitividad económica, la innovación empresarial y la eficiencia de los servicios públicos. Sin embargo, este proceso también ha incrementado significativamente la superficie de exposición a amenazas cibernéticas (*1,2).* Cada año, empresas e instituciones de todo el mundo sufren pérdidas millonarias a causa de brechas de seguridad, ataques de ransomware, robo de datos o interrupciones de servicios críticos.

Este estudio parte de una hipótesis central: un desarrollo digital elevado debería correlacionarse con una menor incidencia o impacto de las brechas de ciberseguridad. Bajo esta premisa, el objetivo principal de la investigación es analizar si los países con mayor digitalización presentan menores pérdidas económicas derivadas de ciberataques, evaluando así la efectividad de esa digitalización en términos de resiliencia cibernética.

Para ello, se ha trabajado con datos internacionales de 2015 a 2024, procedentes de dos fuentes principales: un conjunto sobre índices de ciberseguridad y nivel de digitalización por país, y otro que recopila incidentes y pérdidas asociadas a amenazas globales. El estudio se ha centrado en diez países representativos, incluyendo economías desarrolladas y emergentes, como Estados Unidos, Alemania, China, Brasil e India.

El análisis se ha realizado mediante Power BI, permitiendo visualizar correlaciones, calcular indicadores clave como el ratio inversión/pérdidas, analizar el equilibrio entre desarrollo y protección y clasificar a los países según su nivel de exposición. Este enfoque busca aportar evidencias empíricas para la toma de decisiones estratégicas en materia de ciberseguridad y transformación digital.

Metodología

Para abordar el análisis, se utilizaron dos conjuntos de datos abiertos procedentes de Kaggle:

- **Cybersecurity Indexes (2024):** contiene indicadores por país como el Global Cybersecurity Index (GCI)*(1),* el National Cyber Security Index (NCSI*)(2),* el Cybersecurity Exposure Level (CEL)*(3)* y el Digital Development Level (DDL).
- **Global Cybersecurity Threats (2015–2024):** recopila información sobre tipos de amenazas, número de brechas, industrias afectadas, usuarios comprometidos, duración media de resolución y pérdidas económicas estimadas.

Los pasos metodológicos clave fueron:

1. **Integración y limpieza de datos:** se transformaron y cruzaron los datasets para unificarlos por país y por año.
2. **Cálculo de correlaciones:** se empleó el coeficiente de correlación de Pearson para evaluar la relación entre variables clave como GCI vs DDL y CEL vs DDL.
3. **Visualización de relaciones:** se crearon gráficos de dispersión, columnas agrupadas y líneas temporales para analizar tendencias, impactos financieros y tipos de ciberataques más comunes.
4. **Clasificación semafórica:** se generaron reglas DAX para clasificar a los países en tres niveles (Alto, Medio, Bajo) según su exposición, desarrollo digital y relación inversión/pérdidas.

5. **Análisis de equilibrio:** se construyó una matriz final de equilibrio entre digitalización y ciberseguridad, considerando tanto preparación como exposición efectiva.

La herramienta principal fue **Power BI**, complementada con transformaciones básicas en Power Query. Este enfoque visual e interactivo permitió explorar de forma intuitiva la dinámica entre digitalización y vulnerabilidad.

Resultados

- **Relación entre desarrollo digital y ciberseguridad:** Se observó una correlación positiva moderada (r = 0,68) entre el Digital Development Level (DDL) y el Global Cybersecurity Index (GCI) *(fig. 1. 2)*. Esto indica que, en términos generales, los países más digitalizados también presentan mayores esfuerzos en ciberseguridad. Sin embargo, no es una regla absoluta, ya que algunos países con alto desarrollo digital aún muestran niveles de ciberseguridad mejorables.

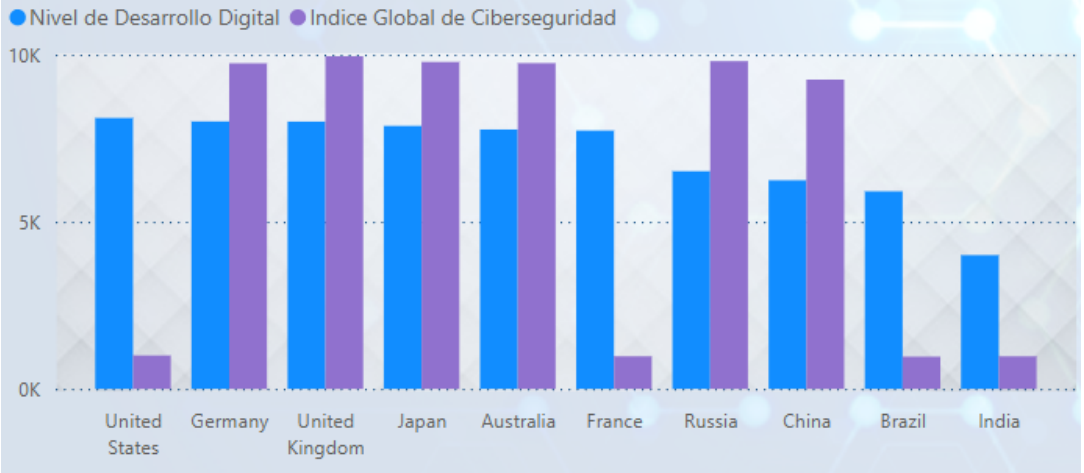

Figura 1:Comparación entre el Nivel de Desarrollo Digital (DDL) y el Índice Global de Ciberseguridad (GCI) en diversos países. Se observa que, en general, los países con mayor desarrollo digital presentan también un índice más alto de ciberseguridad, aunque existen excepciones como Francia o Brasil

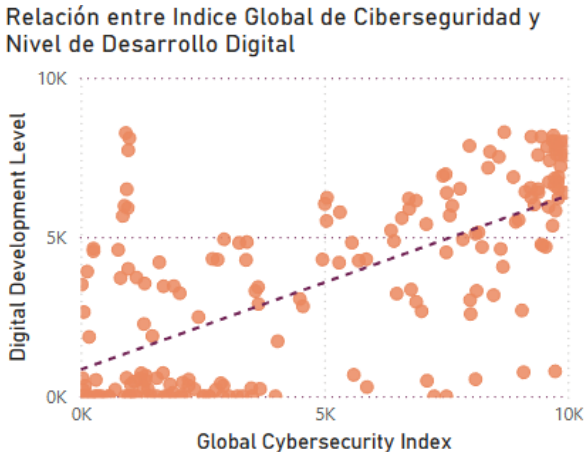

Figura 2: Gráfico de dispersión. Muestra la relación entre el GCI y el DDL. La línea de tendencia sugiere una correlación positiva moderada (r = 0,68), indicando que, en promedio, los países más digitalizados tienden a tener mejores índices de ciberseguridad.

- **Relación entre digitalización y exposición:** Al analizar el DDL frente al Cybersecurity Exposure Level (CEL), la correlación resultó más débil (r =

0,34)(*fig.3)*, lo que sugiere que la digitalización puede aumentar también la superficie de ataque si no va acompañada de políticas robustas de protección.

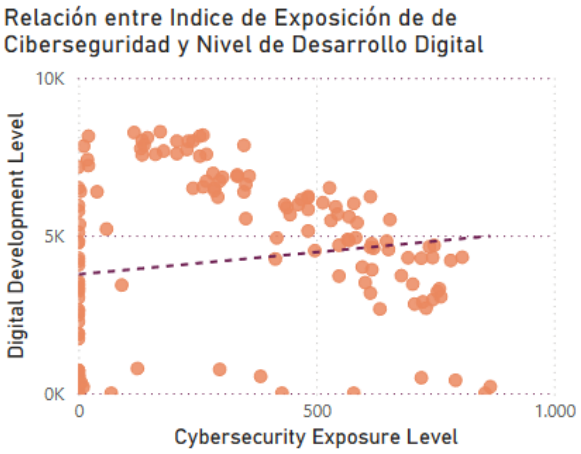

Figura 3: Gráfico de dispersión que muestra la relación entre el DDL y el CEL. La correlación observada es positiva pero débil (r = 0,34), lo que sugiere que una mayor digitalización puede incrementar la exposición a riesgos si no va acompañada de medidas de ciberprotección adecuadas.

- **Análisis de equilibrio digital-seguridad:** Se creó una columna semafórica *(fig.4)* para evaluar el equilibrio entre DDL y CEL. Países como EE. UU., Reino Unido y Japón se clasificaron como "equilibrados" (🟢), mientras que Brasil, India y Rusia presentaron desequilibrio (🔴) debido a alta exposición o baja inversión relativa.

Nivel de Exposición de Ciberseguridad	Nivel de Desarrollo Digital	Indice Global de Ciberseguridad	Equilibrio entre digitalización y exposición
131,00	7761	9.747,00	Equilibrado
541,00	5911	966,00	En riesgo
483,00	6241	9.253,00	En riesgo
228,00	7729	976,00	Equilibrado
241,00	8001	9.741,00	Equilibrado
597,00	4002	975,00	En riesgo
138,00	7869	9.782,00	Equilibrado
528,00	6512	9.806,00	En riesgo
207,00	7996	9.954,00	Equilibrado
145,00	8105	1.000,00	Equilibrado

Figura 4:Tabla de análisis semafórico que evalúa el equilibrio entre el DDL, el CEL y el GCI. Los países se clasifican como "equilibrados" (🟢) o "en riesgo" (🔴) según la relación entre su grado de digitalización y su nivel de exposición o inversión en ciberseguridad. Este análisis permite identificar posibles desequilibrios que requieren atención estratégica.

- **Impacto económico:** Las pérdidas globales por ciberataques superaron los $151 mil millones *(4,5)(fig.5)* en el periodo analizado. Países como Alemania y Brasil destacaron negativamente al presentar pérdidas económicas superiores a su inversión digital, reflejando un ratio inversión/pérdidas inferior a 1.

Tabla de Países con sus Inversiones y Pérdidas

País	Inversiones (en millones)	Pérdidas (en millones)	Riesgo de la inversión
United Kingdom	$140.000	$16.503,1	Medio
Germany	$165.000	$15.793,2	Alto
Brazil	$75.000	$15.782,62	Medio
Australia	$85.000	$15.403,1	Medio
Japan	$175.000	$15.197,34	Alto
France	$100.000	$14.972,28	Medio
United States	$2.200.000	$14.812,12	Alto
Russia	$35.000	$14.734,73	Medio
India	$111.000	$14.566,2	Medio

Figura 5: Tabla comparativa de inversión digital y pérdidas por ciberataques en diferentes países. Incluye un indicador de riesgo basado

en el ratio inversión/pérdidas. Estados Unidos y China muestran una inversión sustancial con un riesgo bajo, mientras Alemania y Brasil presentan un mayor riesgo al registrar pérdidas que superan su inversión.

- **Brechas de seguridad y ataques frecuentes:** Los ataques más comunes en países con menor desarrollo digital incluyen phishing, ransomware, SQL injection, DDoS y malware *(6,7,8).* Sectores como sanidad, bancos e IT fueron los más afectados.*(fig. 6)*

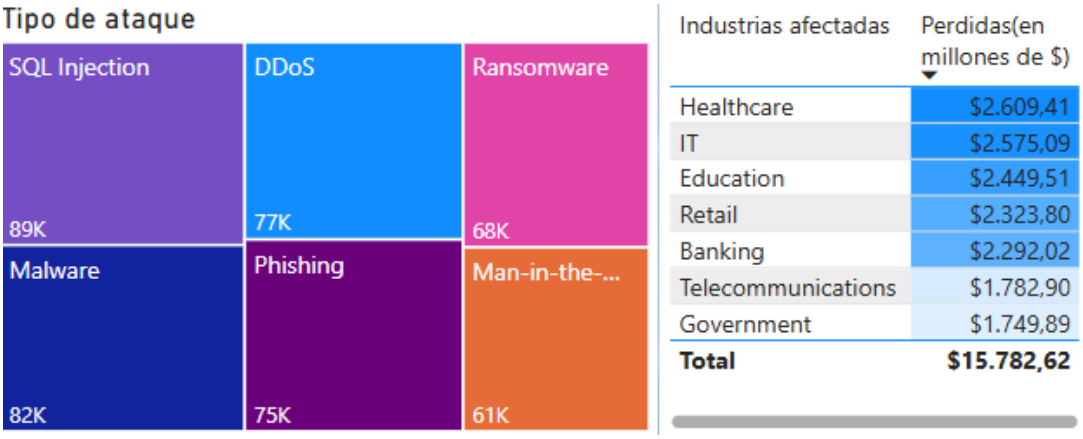

Figura 6: Visualización en treemap y tabla de Brasil, donde se detallan los tipos de ciberataques más frecuentes y los sectores más afectados. Los ataques más comunes incluyen phishing, ransomware, SQL injection, DDoS y malware, mientras que sectores como sanidad, tecnología, educación y banca registran las mayores pérdidas económicas, superando los 2.000 millones de dólares cada uno

- **Tiempo de resolución de incidentes:** La media global fue de 36,48 horas, acumulando más de 109 mil horas de respuesta a ciberincidentes. Países con mejor infraestructura digital mostraron menor tiempo medio de resolución.

Discusión

El análisis deja claro que el desarrollo digital y la ciberseguridad no siempre van de la mano. Si bien existe una tendencia positiva entre mayor digitalización y mejor preparación (como lo refleja el GCI), la exposición al riesgo (CEL) también puede crecer si la seguridad no evoluciona al mismo ritmo.

Países como Estados Unidos o Japón muestran una estrategia sólida: altos niveles de digitalización acompañados por marcos potentes de ciberseguridad. En cambio, economías como Alemania o Brasil, pese a sus avances digitales, presentan una brecha preocupante entre inversión y pérdidas *(10,11*). Esto revela que digitalizar sin proteger puede ser incluso más costoso que no digitalizar.

La clasificación semafórica usada en el estudio ayuda a visualizar de forma intuitiva el “equilibrio digital-seguridad” de cada país. El uso combinado de indicadores como el DDL y el CEL, junto con las pérdidas reales por ciberataques, permite identificar vulnerabilidades estructurales. La existencia de países “en riesgo” con alta digitalización debería funcionar como una señal de alerta: la seguridad no es automática, requiere planificación y presupuesto.

Por otro lado, los ataques más frecuentes (como phishing, ransomware o malware) siguen apuntando a sectores críticos como salud, banca o telecomunicaciones, especialmente en países con menor cultura de ciberseguridad. Esto refuerza la idea de que la tecnología sin educación ni regulación es terreno fértil para la ciberdelincuencia.

Finalmente, el tiempo de resolución de incidentes destaca como otro factor relevante: una buena inversión en SOCs, CERTs y planes de contingencia no solo mitiga los daños, sino que acorta los ciclos de impacto. En este sentido, países que realizan simulacros periódicos y colaboran internacionalmente tienden a recuperarse más rápido tras un ataque.

En conclusión, la relación entre digitalización y brechas de seguridad es más compleja de lo que parece. No basta con invertir en TIC: hay que hacerlo con inteligencia, visión de riesgo y una estrategia nacional clara. La ciberseguridad debe ser un pilar, no un accesorio, del desarrollo digital.

Conclusión

En definitiva, tener más tecnología y estar más digitalizados ayuda, pero también nos pone en primera línea ante los ciberataques. Hemos visto claramente que países superdigitalizados como EE. UU. o China sí que hacen bien los deberes: invierten en seguridad digital y eso les ahorra muchos dolores de cabeza. En lugares como Alemania o Brasil, avanzar digitalmente sin reforzar la seguridad ha salido caro. Cada paso hacia adelante vino acompañado de nuevos agujeros por los que se colaban los cibercriminales.

Lo importante es entender que el problema no es la digitalización, sino ir más rápido en digitalizarse que en protegerse. Es como conducir un Ferrari sin cinturón de seguridad; parece divertido, hasta que algo sale mal. Para evitar sustos (y pérdidas millonarias), toca pensar en la ciberseguridad desde el principio, y no como un parche al final. Japón, por ejemplo, preparó bien su infraestructura tecnológica antes de los Juegos Olímpicos de Tokio *(16, 17)* y se ahorró muchos problemas.

Además, no basta solo con tecnología: la gente cuenta, y mucho. De nada sirve tener sistemas ultraseguros si alguien pincha en el enlace equivocado o pone '123456' como contraseña. Programas masivos de formación y concienciación podrían evitar muchísimos incidentes, y es algo que debería estar en la agenda de todos los países.

Proteger sectores clave como sanidad, finanzas y telecomunicaciones también es crucial. Alemania y Rusia lo aprendieron por las malas con ataques graves de ransomware. La solución no es compleja, pero requiere constancia: cifrar datos sensibles, segmentar redes, hacer simulacros de incidentes… Básicamente, entrenar para lo peor esperando lo mejor.

Y algo fundamental: la ciberseguridad ha de trabajarse en equipo. La cooperación internacional y compartir información en tiempo real es la única forma de anticiparse a ataques que cada vez son más sofisticados y globales. Estar conectados nos hace vulnerables, sí, pero también más fuertes si colaboramos.

Por último, está claro que ningún país puede presumir de tener una seguridad 100% a prueba de hackers, pero la diferencia está en cómo reaccionamos ante los problemas. Aquellos países que practican regularmente simulacros de crisis cibernéticas, como EE. UU., están mejor preparados cuando llega un ataque real. La rapidez de reacción salva millones.

Así que, en resumen: la digitalización promete prosperidad, pero solo si va acompañada de una estrategia igual de fuerte en ciberseguridad. Los próximos años serán clave para ver si los países aprenden la lección o siguen pagando el precio de subestimar la seguridad digital.

Referencias (APA)

1. International Telecommunication Union (ITU). *Global Cybersecurity Index (GCI)*. https://www.itu.int/en/ITU-D/Cybersecurity
2. e-Governance Academy of Estonia. *National Cyber Security Index (NCSI)*. https://ncsi.ega.ee
3. Experis / PasswordManagers. *Cybersecurity Exposure Index (CEI) 2020*. https://cybersecuritymap.experis.com
4. LAC4 Center. *Importancia de los Índices de Ciberseguridad: Mejorando la Resiliencia Cibernética Nacional*.
5. SEON. *Informe global sobre ciberdelincuencia: países con mayor riesgo en 2023*. https://seon.io
6. AV-TEST. *Malware Statistics & Trends Report*. https://www.av-test.org
7. CISA. *2023 Top Routinely Exploited Vulnerabilities*. https://www.cisa.gov
8. Fortinet. *Estadísticas de ransomware 2023*. https://www.fortinet.com
9. Zscaler. *Ransomware Trends 2023*. https://www.zscaler.com
10. DPL News. *Sector TIC en Brasil crece por encima del promedio mundial*. https://dplnews.com
11. OECD. *ICT Investments in OECD Countries*. [Microsoft Word - ICTInvestmentsOECDCountries_FINAL.docx]
12. Statista. *IT industry revenue Germany 2025 / India ICT estimated spending 2024 / Australia: IT spending by category 2021 / etc.*
13. Gobierno de Reino Unido. *Cyber Security Strategy 2022–2030*. https://www.gov.uk/government/publications/national-cyber-strategy-2022
14. NCSC UK. https://www.ncsc.gov.uk
15. Kaspersky Reports (Rusia)
16. Ministerio de Ciencia y Tecnología de Brasil (MCTI)
17. Australian Cyber Security Centre (ACSC). *Cyber Threat Reports 2020–2022*.
18. MeitY India. *Digital India Programme*. https://www.digitalindia.gov.in
19. CERT-In India. https://www.cert-in.org.in
20. Microsoft Threat Intelligence (Ataques a Japón 2020–2021)
21. Japan Times, NHK World News, Nikkei Asia
22. BBC News, The Guardian (Reino Unido)
23. BleepingComputer, Reuters (Rusia, Anonymous, Ucrania)
24. Deloitte Access Economics. *The Economic Impact of Cyber Crime in Australia*. https://www.deloitte.com/au/en/services/economics/perspectives
25. FBI IC3. *Cybercrime Report USA 2022*
26. CSIS Center for Strategic and International Studies – Cybersecurity Timeline
27. Ministerio del Interior de Francia, Agencia Nacional de Seguridad de Sistemas de Información (ANSSI)

Nota: Todas las cifras y afirmaciones contenidas en este informe han sido contrastadas con fuentes oficiales, informes técnicos, portales estadísticos reconocidos y literatura académica relevante, con especial atención a su validez entre los años 2015 y 2024.