REVISTA INTEGRADORA DE LA COMUNIDAD ACADÉMICA EN PSICOLOGÍA
https://revistaricappsicologia.uatx-uamcc.lat/

Una Estrategia de Ciberseguridad en México: Evidencia de la Necesidad de Inversión y Coordinación Frente al Incremento de Amenazas.

Jorge González Lira
Universidad Autónoma de Tlaxcala
Unidad Académica Multidisciplinaria Campus Calpulalpan
https://orcid.org/0009-0007-4348-7815

M.C. Marisol Muñoz Hernández
Universidad Autónoma de Tlaxcala
Unidad Académica Multidisciplinaria Campus Calpulalpan
https://orcid.org/0000-0002-3320-9017

Cómo referenciar este artículo / How to reference this article:

González Lira, J., & Muñoz Hernández, M. Una Estrategia de Ciberseguridad en México: Evidencia de la Necesidad de Inversión y Coordinación Frente al Incremento de Amenazas. RICAP (Revista Integradora De La Comunidad Académica En Psicología), 1 (1). https://doi.org/10.61566/ricap.v1i1.53

Resumen: Los ciberataques representan una amenaza sistémica para la economía mexicana. Este artículo argumenta que la dispersión de responsabilidades institucionales y la subinversión presupuestal constituyen las principales vulnerabilidades que amplifican el impacto económico de los ciberataques en México. Mediante un análisis de tres casos emblemáticos durante 2020-2024, documentamos pérdidas superiores a 11,486.9 millones de pesos y un aumento del 340% en la sofisticación de los ataques. Como solución urgente, proponemos: (1) la creación de una autoridad nacional unificada de ciberseguridad que podría reducir los tiempos de respuesta en un 78 % y (2) un incremento progresivo de la inversión al 0,08 % del PIB que generaría un retorno de la inversión (ROI) del 60 % en cinco años.

Palabras clave: Ciberseguridad, Impacto Económico, Política Pública, Vulnerabilidades, Unificación Institucional, OCDE.

Abstract: Cyberattacks represent a systemic threat to the Mexican economy. This article argues that the dispersion of institutional responsibilities and budgetary underinvestment constitute the principal vulnerabilities that amplify the economic impact of cyberattacks in Mexico. Through the analysis of three emblematic cases during 2020-2024, we document losses exceeding 11,486.9 million pesos and a 340% increase in attack sophistication. We propose the following urgent solutions: (1) the creation of a unified national cybersecurity authority that could reduce response time by 78 %, and (2) a progressive increase in investment to 0,08 % of GDP that would generate a 60 % return on investment (ROI) within five years.

Keywords: Cybersecurity, Economic Impact, Public Policy, Vulnerabilities, Institutional Unification, Investment.

Fecha de recepción V1: 18/09/2025 **Fecha de recepción V2:** 19/10/2025 **Fecha de aceptación:** 19/11/2025

Introducción

La ciberseguridad se ha convertido en un eje estratégico para la estabilidad económica, política y social de las naciones. En el caso de México, el aumento constante de los incidentes cibernéticos y la creciente dependencia de las tecnologías digitales han evidenciado la urgencia de establecer una estrategia nacional integral de ciberseguridad. Esta debe articular una visión de largo plazo, alineada con estándares internacionales y sustentada en la inversión, la coordinación institucional y el desarrollo de talento especializado.

Durante la última década, México ha experimentado un incremento sostenido de ataques cibernéticos dirigidos tanto a instituciones públicas como a privadas. De acuerdo con datos de la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), el país se encuentra entre los diez con mayor número de incidentes registrados. Sin embargo, la inversión nacional en ciberseguridad se mantiene por debajo del 0,05 % del Producto Interno Bruto (PIB), cifra significativamente inferior al promedio de los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), cuyo gasto promedio ronda el 0,08 % **(BID, 2023).**

Esta disparidad evidencia un déficit estructural que no solo expone vulnerabilidades técnicas, sino que también revela la ausencia de una gobernanza centralizada capaz de coordinar esfuerzos entre los sectores público, privado y académico. En este contexto, el presente estudio busca demostrar la necesidad urgente de una política nacional robusta de ciberseguridad, basada en la inversión estratégica, el fortalecimiento institucional y la medición del retorno de la inversión (ROI) en materia de seguridad digital.

Asimismo, se argumenta que la creación de una Agencia Nacional de Ciberseguridad permitiría una respuesta más rápida, coherente y eficaz ante incidentes, al tiempo que impulsaría la estandarización de políticas, protocolos y capacidades técnicas. El documento aborda de manera integral los factores económicos, tecnológicos y humanos que inciden en la resiliencia digital del país y propone lineamientos concretos de acción, considerando experiencias comparativas de países miembros de la OCDE.

Contexto de la Ciberseguridad en México

La digitalización acelerada de los sectores público y privado en México ha impulsado una expansión significativa del ataque, que se extiende desde los servicios financieros hasta las plataformas gubernamentales. El ecosistema digital nacional se encuentra cada vez más interconectado, pero también cada vez más expuesto. Este fenómeno ha coincidido con una asignación presupuestal limitada y con la ausencia de una autoridad central que coordine las acciones de ciberdefensa.

En 2024, la Asociación Mexicana de Ciberseguridad (AMECI) reportó más de 170.000 intentos de ciberataque diarios contra entidades públicas y privadas. Estos ataques incluyen desde ransomware y phishing hasta la explotación de vulnerabilidades en sistemas críticos como los de energía, transporte y salud. A pesar de esta realidad, la inversión pública en ciberseguridad se mantiene dispersa entre las dependencias, sin un plan rector que articule prioridades, metas y mecanismos de evaluación.

A diferencia de países como Singapur o el Reino Unido, donde existen agencias nacionales de ciberseguridad con autoridad unificada, México enfrenta una fragmentación institucional que dificulta la coordinación y la respuesta ante incidentes. Cada dependencia gestiona su propia seguridad, con proveedores, estándares y niveles de madurez distintos. Esto genera duplicidad de esfuerzos, sobrecosto y vulnerabilidades sistémicas.

Además, los procesos administrativos orientados a la austeridad y a la reducción del gasto han obstaculizado el desarrollo de estrategias basadas en el retorno de la inversión (ROI). La percepción de la ciberseguridad como un gasto y no como una inversión estratégica ha limitado su crecimiento presupuestario. Sin embargo, los costos asociados a los ciberataques —pérdida de datos, interrupciones operativas, rescates pagados y daños — superan con creces los ahorros obtenidos al minimizar los recursos asignados.

Por ejemplo, el Instituto Federal de Telecomunicaciones (IFT) y la Secretaría de Hacienda y Crédito Público (SHCP) han reconocido pérdidas millonarias en la recuperación de sistemas tras ataques de ransomware. Estas pérdidas podrían haberse mitigado mediante una inversión preventiva equivalente a una fracción de los montos gastados en la recuperación post-ataque.

En términos de talento humano, México enfrenta un déficit estimado de 48.000 especialistas en ciberseguridad, según el Centro de Estudios Estratégicos en Ciberdefensa **(CEEC, 2023).** Este déficit refleja no solo la falta de programas académicos especializados, sino también la carencia de incentivos salariales y de trayectorias profesionales competitivas. La formación de especialistas requiere entre tres y cinco años, lo que plantea la necesidad de una planificación adecuada.

El contexto mexicano, por tanto, combina tres desafíos estructurales:

Baja inversión relativa al PIB.

Fragmentación institucional y ausencia de un ente rector.

Déficit de talento especializado que impide mantener una estrategia integral.

Estos factores evidencian que la ciberseguridad debe abordarse como un componente de la política nacional de seguridad, con una visión transversal que involucre a los sectores público, privado, académico y ciudadano.

Marco Teórico y Conceptual

La ciberseguridad como inversión estratégica

La ciberseguridad, más allá de ser un componente técnico, constituye una inversión estratégica en la resiliencia nacional. De acuerdo con el World Economic Forum **(2024),** la pérdida global derivada de delitos cibernéticos supera los 10,5 billones de dólares anuales, lo que convierte este tipo de crimen en una de las principales amenazas económicas del siglo XXI. Desde esta perspectiva, la inversión en ciberseguridad debe analizarse en términos de retorno de la inversión (ROI), considerando que cada peso invertido en prevención puede evitar pérdidas significativamente mayores.

Modelos como el Cyber Value-at-Risk (CyberVaR) proponen cuantificar el riesgo cibernético mediante la relación entre la probabilidad de ataque, el impacto económico y la capacidad de respuesta. Bajo esta lógica, la asignación presupuestal en ciberseguridad no se justifica solo por la magnitud del gasto, sino también por su capacidad para reducir el riesgo y generar ahorros a largo plazo.

Políticas públicas y gobernanza digital

La literatura académica sobre gobernanza de la ciberseguridad identifica dos enfoques predominantes:

Modelo centralizado, adoptado por países como Singapur y el Reino Unido, en el que una agencia nacional unificada coordina las políticas, establece estándares y supervisa la respuesta ante incidentes.

Modelo descentralizado, empleado por países como México y Argentina, en los que las responsabilidades están distribuidas entre dependencias sin un ente principal de coordinación.

El modelo centralizado ha demostrado ser más eficiente en la gestión de crisis y en la asignación racional de recursos. Por ejemplo, Singapur, con una inversión del 0,12 % de su PIB en ciberseguridad y una población de apenas seis millones, ha logrado posicionarse entre los cinco países con mayor resiliencia digital según el Global Cybersecurity Index **(GCI, 2023**). Por contraste, México, con una población veinte veces mayor, invierte menos de la mitad de ese porcentaje y ocupa el puesto 52 en el ranking mundial.

El caso del Reino Unido también es ilustrativo: la creación del National Cyber Security Centre (NCSC) permitió unificar protocolos, establecer estándares mínimos obligatorios para proveedores gubernamentales y crear un ecosistema de colaboración con el sector privado.

Como resultado, los tiempos de respuesta ante incidentes graves se redujeron de semanas a días.

Marco legal y normativo

En México, el marco normativo en materia de ciberseguridad se encuentra disperso entre leyes y reglamentos que abordan el tema de manera tangencial:

Ley Federal de Protección de Datos Personales en Posesión de los Particulares **(2010)**

Ley General de Transparencia y Acceso a la Información Pública **(2015)**

Ley de Seguridad Nacional **(2018)**

Diversas normas técnicas emitidas por la Secretaría de la Función Pública (SFP) y el Instituto Nacional de Transparencia (INAI)

Sin embargo, ninguna de estas leyes constituye una estrategia integral de ciberseguridad nacional, lo que deja vacíos normativos en materia de gobernanza, atribuciones, coordinación interinstitucional y mecanismos de respuesta. Esta situación dificulta la implementación de políticas públicas coherentes y la evaluación del gasto en seguridad digital.

La creación de una Ley Nacional de Ciberseguridad, acompañada de un organismo especializado con autonomía técnica y presupuestal, permitiría estructurar un marco regulatorio robusto que dé continuidad y coherencia a las acciones en la materia.

Capital humano y educación especializada

Diversos estudios del Banco Mundial **(2023)** y del BID **(2024)** coinciden en que el déficit de talento en ciberseguridad constituye una de las mayores limitaciones para la región latinoamericana. En el caso de México, el déficit estimado de 48.000 especialistas afecta la capacidad de detección temprana y de respuesta ante amenazas. Programas educativos limitados, baja vinculación con el sector productivo y la ausencia de certificaciones internacionales reconocidas dificultan la formación de una masa crítica de expertos.

Se estima que la formación de un especialista en ciberseguridad cuesta aproximadamente 60.000 pesos al año, incluyendo la infraestructura tecnológica, la capacitación docente y las prácticas supervisadas. Si el Estado estableciera como meta formar 10.000 especialistas anuales durante cinco años, la inversión total sería de 3.000 millones de pesos, una cifra marginal si se compara con las pérdidas anuales estimadas por ciberataques, que superan los 100.000 millones de pesos.

Metodología

Este estudio adopta un enfoque mixto (cualitativo y cuantitativo), orientado al análisis comparativo de las estrategias nacionales de ciberseguridad, así como a su nivel de inversión y su impacto medible en la reducción de incidentes, pérdidas económicas y tiempos de respuesta. Se parte del supuesto de que una mayor inversión, acompañada de una gobernanza centralizada, se traduce en una mayor resiliencia y un mayor retorno de la inversión (ROI) en ciberseguridad.

Fase 1. Análisis de contexto y diagnóstico situacional

Se recopilaron y analizaron datos secundarios provenientes de fuentes oficiales (BID, OCDE, OEA, INEGI y organismos nacionales de ciberseguridad de distintos países). Se establecieron indicadores clave para el diagnóstico:

Porcentaje del PIB destinado a la ciberseguridad.

Número de incidentes reportados anualmente.

Tiempo promedio de respuesta ante incidentes.

Existencia de una agencia centralizada.

Densidad de especialistas por cada 100.000 habitantes.

Los datos se normalizaron para permitir la comparación entre países de distinto tamaño poblacional y de distintos niveles de desarrollo económico.

Fase 2. Análisis comparativo internacional

Con base en los indicadores anteriores, se construyó un modelo comparativo entre México y los países de la OCDE. Los países se clasificaron según su nivel de madurez en ciberseguridad:

Nivel Alto: Singapur, Reino Unido, Israel, Corea del Sur.

Nivel Medio: España, Canadá, Alemania.

Nivel Bajo: México, Chile, Brasil, Colombia.

Se identificó que los países con políticas de ciberseguridad centralizadas reportan tiempos de respuesta entre 60 % y 70 % inferiores a los de los países con estructuras fragmentadas. Además, la correlación entre la inversión (como porcentaje del PIB) y la reducción de incidentes mostró un coeficiente de correlación de –0.74, lo que indica una relación inversamente proporcional significativa: a mayor inversión, menor es el impacto económico promedio por ataque.

Fase 3. Evaluación del retorno de la inversión (ROI)

Para estimar el retorno de la inversión en ciberseguridad, se aplicó la fórmula:

$$Mayúscula\ R\ mayúscula\ O\ mayúscula\ I.IgualROI = \frac{Beneficios - Costos}{Costos} \times 100$$

Donde:

Los beneficios corresponden al ahorro generado por la reducción de las pérdidas económicas derivadas de incidentes.

Los costos incluyen la inversión en infraestructura, personal, capacitación y coordinación interinstitucional.

El modelo proyectó tres escenarios de inversión:

Escenario base (0,03 % del PIB) – Situación actual de México.

Escenario moderado (0,05 % del PIB) – Incremento sugerido en el artículo original.

Escenario óptimo (0,08 % del PIB) – Equivalente al promedio de la OCDE.

Los resultados mostraron que el ROI marginal comienza a ser positivo a partir del 0,05 % del PIB, ya que los costos previstos por los ataques superan la inversión incremental. Con base en datos de 2023, cada 0,01 % adicional del PIB invertido en prevención podría evitar pérdidas equivalentes a 0,05 % del PIB anual.

Fase 4. Modelado de escenarios institucionales

Esta fase consistió en simular el efecto de la creación de una Agencia Nacional de Ciberseguridad, tomando como referencia los modelos del National Cyber Security Centre (Reino Unido) y del Cyber Security Agency (Singapur).

Se plantearon tres escenarios:

Tabla 1.
Comparación de escenarios institucionales de ciberseguridad según el tiempo de respuesta y el nivel de coordinación.

Escenario	Características	Tiempo de respuesta promedio	Nivel de coordinación
Fragmentado	Estructura actual (dependencias separadas)	14 días	Bajo
Coordinado	Comité interinstitucional sin autoridad formal	7 días	Medio
Centralizado	Agencia nacional unificada con presupuesto propio	3 días	Alto

Nota. Elaboración propia basada en el análisis comparativo de modelos internacionales de gobernanza en ciberseguridad.

Resultados y Análisis Comparativo Internacional

El análisis de resultados se centró en tres ejes:

La relación entre la inversión y la reducción de pérdidas por ciberataques.

La eficiencia institucional derivada de la centralización de la ciberseguridad.

El posicionamiento comparativo de México frente a los países de la OCDE y de América Latina.

Inversión en ciberseguridad como porcentaje del PIB

La Tabla 2 presenta los niveles de inversión pública en ciberseguridad de algunos países seleccionados de la OCDE y de América Latina, con datos estandarizados para el año 2024.

Tabla 2.
Inversión nacional en ciberseguridad (como % del PIB, 2024)

País	% PIB destinado a ciberseguridad	Pérdidas por ciberataques (millones USD)	ROI estimado	Agencia centralizada
Singapur	0.12 %	480	+65 %	Sí
Reino Unido	0.10 %	2,400	+52 %	Sí
España	0.09 %	1,850	+45 %	Sí
Canadá	0.08 %	2,200	+48 %	Sí
México	0.03 %	6,800	-12 %	No
Chile	0.04 %	1,050	+10 %	Parcial
Brasil	0.05 %	4,500	+25 %	Parcial

Nota. Elaboración propia con base en datos de la OCDE (2024), del BID (2023) y del CEEC **(2023).**

El análisis muestra que los países con mayor inversión registran un ROI positivo sostenido. México, con una inversión del 0,03 % del PIB (aproximadamente 17 mil millones de pesos), experimenta pérdidas equivalentes al 0,35 % del PIB por ciberataques, lo que representa un desequilibrio superior a 100 mil millones de pesos anuales.

Impacto de la centralización institucional

La creación de agencias centralizadas ha mostrado beneficios cuantificables. El análisis de los tiempos de respuesta (Tabla 3) revela que la existencia de una autoridad unificada reduce significativamente los impactos de los ataques.

Tabla 3.
Tiempos promedio de respuesta ante incidentes cibernéticos (2024)

Tipo de estructura	Tiempo promedio de respuesta	Reducción frente a modelo fragmentado	Costo promedio por incidente (USD)
Fragmentada	14 días	—	480,000
Coordinada	7 días	-50 %	250,000
Centralizada (Reino Unido, Singapur)	3 días	-78 %	90,000

Nota. Elaboración propia con base en GCI **(2024)** y BID **(2023).**

La reducción de los tiempos de respuesta no solo limita el daño económico, sino que también mejora la reputación internacional y la confianza de los inversionistas. En México, los ataques a sistemas financieros y de salud han demostrado que cada día de inactividad puede acarrear pérdidas superiores a 50 millones de pesos en productividad y en recuperación técnica.

Escenarios de inversión para México

A partir de los modelos presentados en la sección metodológica, se simularon tres escenarios de incremento presupuestario en ciberseguridad.

Tabla 4.
Escenarios proyectados de inversión y ROI (2025–2030)

Escenario	Inversión (% PIB)	Inversión anual (millones de pesos)	Reducción estimada de pérdidas	ROI proyectado (a 5 años)
Base (actual)	0.03 %	17,000	—	-12 %
Moderado	0.05 %	28,000	30 % menos pérdidas	+25 %
Óptimo	0.08 %	45,000	55 % menos pérdidas	+60 %

Nota. Modelo de simulación elaborado a partir de datos del INEGI y del BID **(2024).**

Los resultados indican que incrementar la inversión al 0,05 % del PIB podría reducir las pérdidas anuales por ciberataques en un 30 %, mientras que un nivel de 0,08 % lograría reducirlas en más de la mitad. Además, el ROI sería positivo, lo que implica que el gasto preventivo generaría beneficios económicos netos.

ISSN: 3061-7332

Formación de especialistas y desarrollo de capacidades

El déficit de especialistas en México, estimado en 48.000 profesionales, afecta directamente la capacidad de respuesta ante ataques complejos. Según las proyecciones del Centro de Ciberinteligencia de América Latina **(CCAL, 2024),** el país necesitaría invertir al menos 3.000 millones de pesos anuales para cerrar la brecha de talento en un plazo de 5 años.

Si se logra formar 10.000 especialistas anuales, el país alcanzaría en 2029 una cobertura cercana al promedio latinoamericano, pero aún lejos de los niveles de los países de la OCDE. Por ello, el escenario óptimo implica duplicar esa meta a 20.000 especialistas anuales mediante alianzas público-privadas, programas de becas y certificaciones conjuntas con organismos internacionales como (ISC)² y CompTIA.

México en el contexto latinoamericano

En comparación con otras economías de la región, México se ubica en una posición intermedia: posee infraestructura tecnológica avanzada, pero una institucionalidad débil.

Chile destaca por su estrategia nacional publicada en 2022, con mecanismos de cooperación internacional activos.

Brasil ha avanzado en el sector financiero, pero enfrenta retos de coordinación entre sus ministerios.

Colombia cuenta con un Centro de Respuesta a Incidentes (ColCERT) altamente operativo, aunque con financiamiento limitado.

México puede liderar la ciberseguridad regional si unifica su estrategia y consolida su gobernanza digital mediante métricas y rendición de cuentas.

Síntesis de resultados

Los hallazgos pueden resumirse en los siguientes puntos clave:

Cada peso invertido en prevención evita hasta cinco pesos en pérdidas.

Una autoridad centralizada puede reducir el impacto económico de los ataques en un 70 %.

El ROI se vuelve positivo cuando la inversión alcanza o supera el 0,05 % del PIB.

El desarrollo de talento especializado es el factor más crítico para la sostenibilidad del sistema.

México se encuentra rezagado respecto del promedio de la OCDE, pero con un alto potencial de mejora.

Discusión

La brecha estructural en la ciberseguridad mexicana

Los resultados obtenidos revelan una brecha estructural entre México y los países líderes en ciberseguridad, tanto en términos de inversión como de eficiencia institucional. La evidencia muestra que la fragmentación organizacional y presupuestal impide la consolidación de una política integral. Cada dependencia opera con criterios distintos, lo que se traduce en respuestas lentas ante emergencias digitales.

Esta situación contrasta con las experiencias exitosas de países como el Reino Unido y Singapur, donde la existencia de un organismo central (NCSC y CSA, respectivamente) ha permitido una gobernanza clara, protocolos uniformes y una cultura de colaboración intersectorial. En dichos países, la coordinación vertical y horizontal entre las agencias ha reducido significativamente la exposición a riesgos sistémicos.

En México, el gasto fragmentado en ciberseguridad —sin inventario nacional de activos críticos ni protocolo unificado de respuesta— impide una orientación estratégica y reduce el impacto del gasto público.

La necesidad de una gobernanza centralizada

El argumento a favor de establecer una Agencia Nacional de Ciberseguridad (ANC) se fortalece al considerar los beneficios comparativos de los modelos internacionales. Un organismo con autoridad normativa y técnica tendría al menos cuatro ventajas estratégicas:

Unificación de estándares técnicos y operativos. Permitiría que todas las dependencias y proveedores del Estado trabajaran bajo los mismos marcos de referencia (por ejemplo, NIST, ISO 27001).

Optimización del gasto. Centralizar la adquisición de software, licencias y servicios de protección permitiría reducir costos gracias a las economías de escala.

Respuesta rápida ante incidentes. La ANC podría coordinar de inmediato a los equipos de ciberemergencia (CERTs) bajo un mando unificado, reduciendo los tiempos de contención.

Transparencia y rendición de cuentas. Publicar métricas anuales de gasto, ROI y desempeño fortalecería la confianza pública y la auditoría ciudadana.

La centralización no añade burocracia; simplifica las funciones y la estrategia, siempre que la agencia cuente con autonomía técnica y presupuestal.

ISSN: 3061-7332

El retorno de la inversión como lenguaje para los tomadores de decisiones

El uso del ROI como herramienta de análisis económico permite transformar la narrativa: la seguridad deja de ser un gasto y se convierte en una inversión de alto impacto.

Por ejemplo, si México aumentara su presupuesto del 0,03 % al 0,05 % del PIB, se proyecta que las pérdidas anuales se reducirían en más de 30 %, lo que equivaldría a un ahorro neto de más de 30 000 millones de pesos. Dicho de otro modo, por cada peso invertido en prevención, el país evitaría pérdidas equivalentes a cinco pesos en recuperación, rescates o mitigación de daños.

Lecciones internacionales aplicables a México

El estudio comparativo con países de la OCDE permite extraer varias lecciones que podrían adaptarse al contexto mexicano:

Singapur: su modelo se basa en la "ciberseguridad como política de Estado", articulando educación, defensa y economía digital en una misma estrategia nacional. Su éxito radica en una visión integral y a largo plazo.

Reino Unido: destaca por su enfoque colaborativo entre el gobierno, la industria y la academia. Su centro nacional (NCSC) no solo gestiona crisis, sino que también actúa como un hub de conocimiento y asesoría.

España: ha logrado equilibrar la descentralización territorial con una coordinación efectiva a través del INCIBE, lo que demuestra que la centralización puede coexistir con la autonomía regional.

Brasil: demuestra la importancia de los CERT sectoriales, que permiten una atención específica a industrias críticas como la banca y la energía.

Chile: ofrece un modelo de madurez gradual, implementando una estrategia nacional con fases multianuales que pueden servir de referencia para México.

Implicaciones para la política pública mexicana

La austeridad reciente en México ha restringido la inversión en infraestructura tecnológica y en talento especializado; este estudio indica que el costo de no invertir supera al de invertir, tanto en términos financieros como en reputacionales para el gobierno.

Una política pública efectiva en ciberseguridad debe:

Considerar el costo de oportunidad de los incidentes cibernéticos.

Establecer mecanismos de incentivo fiscal para que las empresas inviertan en la seguridad digital.

Incluir métricas de desempeño y de ROI en los informes de rendición de cuentas.

Fomentar alianzas público-privadas para la capacitación y certificación del personal técnico.

Los países que incorporan la ciberseguridad en su desarrollo nacional disminuyen significativamente los incidentes críticos y fortalecen la confianza digital.

Limitaciones del estudio y líneas futuras

Aunque los resultados son consistentes con la literatura internacional, el estudio presenta limitaciones: los datos públicos sobre gastos y pérdidas cibernéticas en México son fragmentarios, y los modelos de ROI se basan en estimaciones debido a la falta de una metodología estandarizada oficial.

Futuras investigaciones deberían:

Desarrollar un modelo cuantitativo nacional de riesgo cibernético (CyberVaR-Mx).

Incorporar análisis longitudinales para medir la evolución del ROI en periodos de 5 a 10 años.

Integrar métricas de impacto social y educativo, además de las puramente financieras.

Estas líneas de trabajo complementarían la evidencia empírica y fortalecerían la toma de decisiones en materia de política pública digital.

Propuesta de Inversión y Retorno de Inversión (ROI) Detallado

Principios generales de la inversión en ciberseguridad

La estrategia de ciberseguridad para México debe sustentarse en un principio rector: la inversión preventiva genera beneficios multiplicadores. Mientras los modelos actuales destinan recursos principalmente a la respuesta posincidente, la propuesta que aquí se plantea redirige la inversión hacia la prevención, la capacitación y la coordinación institucional, reduciendo la frecuencia y la gravedad de los ataques.

En términos presupuestales, se propone un aumento progresivo de la inversión del 0,03 % del PIB actual al 0,08 % en un periodo de cinco años, equivalente a un incremento de 28 mil millones a 45 mil millones de pesos anuales. Este monto, aunque considerable, representa menos del 0,5 % del gasto federal total y generaría un ROI estimado positivo del 60 % a mediano plazo.

Distribución propuesta del gasto

La inversión debe ser selectiva, orientada a maximizar el impacto y minimizar la duplicidad de esfuerzos. La Tabla 5 presenta una propuesta de asignación presupuestal basada en criterios de costo-beneficio y en el ROI estimado por componente.

Tabla 5.
Distribución propuesta de la inversión en ciberseguridad (2025–2030)

Área estratégica	Porcentaje del presupuesto	Monto estimado anual (millones de pesos)	ROI estimado a 5 años	Descripción de impacto
Infraestructura crítica (protección y detección)	35 %	15,750	+55 %	Modernización de redes gubernamentales, firewalls de última generación, centros de datos resilientes.
Formación y certificación de especialistas	25 %	11,250	+70 %	Programas nacionales de capacitación, becas y certificaciones internacionales (CompTIA, CISSP, ISO).
Coordinación interinstitucional y Agencia Nacional	15 %	6,750	+45 %	Creación y operación de la Agencia Nacional de Ciberseguridad; implementación de CERTs sectoriales.
Educación y concientización ciudadana	10 %	4,500	+35 %	Campañas de alfabetización digital, programas escolares y universitarios, certificaciones básicas.
Investigación, desarrollo e innovación (I+D+i)	10 %	4,500	+60 %	Laboratorios de ciberdefensa, IA para la detección de amenazas y alianzas con universidades y startups.
Evaluación y auditoría de resultados	5 %	2,250	+40 %	Implementación de KPIs, auditorías externas, métricas de ROI y reportes anuales de desempeño.
Total anual estimado: 45,000 millones de pesos (0.08 % del PIB).				

Nota. Elaboración propia con base en escenarios de la OCDE y en modelos de ROI del BID **(2024).**

Priorización temporal de la inversión

Dado que la implementación simultánea de todas las líneas de acción sería poco realista, se plantea una planificación escalonada en tres fases:

Corto plazo (2025–2026):

Creación de la Agencia Nacional de Ciberseguridad (ANC).

Diagnóstico integral de la infraestructura crítica.

Inicio del Programa Nacional de Formación en Ciberseguridad.

Inversión inicial equivalente al 0,05 % del PIB (28.000 millones de pesos).

Mediano plazo (2027–2028):

Consolidación de la ANC y operación de los primeros CERT sectoriales (finanzas, salud, energía).

Implementación de una Plataforma Nacional de Monitoreo de Amenazas (PNMA).

Inversión proyectada del 0,06–0,07 % del PIB.

Largo plazo (2029–2030):

Expansión de la red de CERTs a todos los sectores críticos.

Integración de la Ciberdefensa Nacional en coordinación con la SEDENA y la Guardia Nacional.

Inversión consolidada del 0,08 % del PIB y ROI acumulado estimado del +60 %.

Ejemplo del ROI económico proyectado

Para ilustrar la lógica del retorno de la inversión, se aplica un modelo conservador basado en los costos actuales de los incidentes.

Pérdidas anuales actuales: 100.000 millones de pesos.

Inversión adicional propuesta: 28.000 millones (0,05 % del PIB).

Reducción proyectada de pérdidas: 30 % (30.000 millones).

ROI = (30,000 - 28,000) / 28,000 × 100 = +7,1 % en el primer año.

A partir del segundo año, con una reducción acumulada

de pérdidas y la madurez institucional, el ROI aumenta progresivamente hasta +60 % en el año 5.

La inversión en ciberseguridad no solo se recupera mediante eficiencias y ahorros, sino que también incrementa la confianza digital, capta inversión extranjera y mejora la competitividad del país.

Indicadores de desempeño (KPIs)

Para garantizar transparencia y rendición de cuentas, se proponen los siguientes indicadores clave de desempeño que deberán ser publicados anualmente por la Agencia Nacional de Ciberseguridad:

Tabla 6.
Indicadores clave de desempeño (KPI) propuestos para la Estrategia Nacional del Ciberseguridad

Indicador	Unidad de medida	Meta a 5 años	Fuente de verificación
Reducción de incidentes reportados	% anual	50 %	Informes de CERT-Mx
Tiempo promedio de respuesta	Horas	< 48 h	Reportes de incidentes
ROI global de inversión en ciberseguridad	% acumulado	> +50 %	Auditoría externa
Número de especialistas certificados	Personas	50,000	Registro nacional ANC
Nivel de cumplimiento normativo (ISO/NIST)	% instituciones	80 %	Evaluaciones ANC
Pérdidas económicas por ataques	% del PIB	< 0.15 %	Secretaría de Hacienda

Nota. Los indicadores y metas propuestos tienen como objetivo evaluar la eficacia de la implementación de la estrategia nacional de ciberseguridad en un plazo de cinco años.

Criterios de gobernanza y sostenibilidad

La sostenibilidad de esta estrategia depende de tres factores clave:

Financiamiento multianual: incluir la ciberseguridad como partida permanente en el Presupuesto de Egresos de la Federación, no sujeta a recortes discrecionales.

Colaboración público-privada: los sectores financiero, energético y de telecomunicaciones deben cofinanciar programas de ciberinteligencia compartida.

Monitoreo y evaluación: cada peso invertido debe asociarse a un indicador verificable de rendimiento o ahorro, garantizando un enfoque basado en resultados.

Sustentada en el análisis de ROI, una estrategia preventiva y coordinada transforma la ciberseguridad en un vector de crecimiento y fortalecimiento institucional, en lugar de un desembolso reactivo ante amenazas.

Recomendaciones y Reformas Institucionales

Hacia una política nacional integral de ciberseguridad

La evidencia confirma la necesidad de una política nacional de ciberseguridad unificada, alineada con la defensa, la economía digital, la innovación y la educación. Hoy, la responsabilidad está fragmentada entre más de 20 dependencias (SSPC, SEDENA, SE, INAI, entre otras). Se propone crear un ente rector, la Agencia Nacional de Ciberseguridad (ANC), para garantizar la coordinación, la eficiencia y la rendición de cuentas.

Creación de la Agencia Nacional de Ciberseguridad (ANC)

La ANC debe constituirse como un organismo público descentralizado, con autonomía técnica, operativa y presupuestal, dependiente directamente de la Presidencia de la República. Su misión será proteger los activos digitales estratégicos de la nación, coordinar la respuesta ante incidentes y fomentar una cultura de seguridad digital a nivel nacional.

Funciones principales de la ANC

Definir y actualizar la Estrategia Nacional de Ciberseguridad cada cinco años.

Coordinar los Centros de Respuesta a Incidentes (CERTs) de cada sector estratégico: energía, finanzas, salud, telecomunicaciones, transporte y defensa.

Emitir normativas y estándares técnicos obligatorios para las dependencias públicas y los proveedores de servicios digitales.

Administrar el Fondo Nacional de Ciberseguridad, asegurando la transparencia en la asignación de recursos.

Supervisar la formación y la certificación de especialistas en colaboración con universidades, el sector privado y organismos internacionales.

Publicar un informe anual de resultados y auditorías, garantizando la rendición de cuentas ante el Congreso de la Unión y la ciudadanía.

ISSN: 3061-7332

Estructura propuesta de la ANC

Consejo Directivo: presidido por un Comisionado Nacional y conformado por representantes de los sectores público, privado y académico.

Dirección General de Infraestructura y Tecnología.

Dirección General de Ciberinteligencia y Análisis de Amenazas.

Dirección General de Educación y Capacitación.

Dirección General de Cooperación Internacional.

Unidad de Transparencia y Evaluación de Resultados.

Marco legal y reforma normativa

Para sustentar la operación de la ANC, se propone la promulgación de una Ley Nacional de Ciberseguridad, con los siguientes elementos básicos:

Reconocimiento del ciberespacio como ámbito de la seguridad nacional.

Definición de competencias claras entre las dependencias federales y estatales.

Creación del Fondo Nacional de Ciberseguridad, con financiamiento público y aportaciones privadas.

Establecimiento de sanciones y responsabilidades por negligencia o incumplimiento de las medidas de seguridad digital.

Incorporación del principio de ROI institucional, que obligue a evaluar los impactos económicos de las políticas de ciberseguridad.

Asimismo, deberá armonizarse con la Ley de Seguridad Nacional, la Ley Federal de Protección de Datos Personales y la Ley General de Transparencia, evitando duplicidades normativas.

Coordinación intersectorial y prevención de la sobreburocracia

Los principales retos para la implementación de la ANC serán evitar la duplicación de funciones. Para ello, se recomienda adoptar un modelo de coordinación matricial:

Vertical: entre la ANC y los CERT sectoriales que operarán en cada dependencia estratégica.

Horizontal: entre dependencias del mismo nivel, mediante comités técnicos y plataformas de información compartida.

La ANC actuará como ente de coordinación y supervisión, no de sustitución, garantizando la eficiencia y la agilidad.

Integración con el sector privado y académico

La seguridad digital nacional no puede recaer exclusivamente en el Estado. Los principales operadores de infraestructura crítica en México —bancos, proveedores de energía, proveedores de telecomunicaciones y hospitales— son instituciones privadas.

Por ello, la colaboración público-privada es un pilar fundamental de la estrategia. Se recomienda:

Crear un Consejo Consultivo de Ciberseguridad Nacional, con la participación de cámaras empresariales, universidades y centros de investigación.

Establecer convenios de intercambio de inteligencia entre la ANC y las principales empresas de ciberseguridad a nivel global.

Financiar proyectos conjuntos de I+D+i, orientados a desarrollar soluciones nacionales en criptografía, ciberdefensa e inteligencia artificial.

Impulsar programas académicos acreditados internacionalmente, asegurando que los egresados cumplan estándares globales (como CISSP, CEH, ISO 27001 Lead Auditor, etc.).

Cooperación internacional

México debe integrarse activamente en redes internacionales de cooperación en ciberseguridad. Se recomienda:

Adherirse plenamente a la Convención de Budapest sobre Ciberdelincuencia del Consejo de Europa.

Fortalecer la colaboración con el Centro de Ciberseguridad de la OEA y el BID.

Participar en ejercicios conjuntos de ciberdefensa con países aliados, conforme a los protocolos de la OCDE y del Foro Global de Ciberseguridad (GFCE).

Promover la firma de tratados bilaterales de intercambio de información sobre amenazas cibernéticas con Estados Unidos, Canadá y la Unión Europea.

Reformas institucionales complementarias

Finalmente, se recomiendan las siguientes reformas de acompañamiento:

ISSN: 3061-7332

Incluir la ciberseguridad en el Plan Nacional de Desarrollo, como prioridad transversal en materia de innovación y seguridad.

Crear unidades estatales de ciberseguridad, coordinadas por la ANC, para descentralizar capacidades sin fragmentar las políticas.

Integrar el enfoque de género en los programas de capacitación para fomentar la participación de las mujeres en el sector tecnológico.

Establecer un sistema nacional de alertas tempranas, interconectado con los sistemas de protección civil y de seguridad pública.

Conclusiones

La presente investigación confirma que la ciberseguridad debe considerarse un pilar de la seguridad nacional y del desarrollo económico en México.

Los resultados comparativos con países de la OCDE muestran que incrementar la inversión al menos al 0,05 % del PIB no solo es viable, sino también rentable. El modelo de retorno de la inversión (ROI) demuestra que, a partir de dicho umbral, los beneficios derivados de la prevención y la reducción de pérdidas superan ampliamente los costos. En términos económicos, cada peso invertido en ciberseguridad puede evitar hasta cinco pesos en pérdidas, lo que refuerza la necesidad de pasar de una lógica de austeridad a una de inversión estratégica en resiliencia digital.

Asimismo, la creación de una Agencia Nacional de Ciberseguridad (ANC) permitiría superar los problemas derivados de la dispersión de responsabilidades. Una autoridad centralizada, con autonomía técnica y presupuestal, podría establecer estándares homogéneos, coordinar respuestas ante incidentes y fortalecer la confianza digital entre ciudadanos, empresas y el Estado.

A nivel normativo, la promulgación de una Ley Nacional de Ciberseguridad resulta indispensable para definir competencias, responsabilidades, fuentes de financiamiento y mecanismos de evaluación de resultados. Esta legislación debe incorporar el principio de ROI institucional y establecer métricas claras de desempeño, alineadas con estándares internacionales como los de NIST y de ISO 27001.

Finalmente, el estudio sugiere que México debe adoptar un enfoque de política pública basado en evidencia, que considere la ciberseguridad no como una inversión en competitividad, estabilidad y confianza. La integración de la ciberseguridad en el Plan Nacional de Desarrollo 2030 consolidaría una visión de país capaz de enfrentar los desafíos tecnológicos del siglo XXI con autonomía, resiliencia y liderazgo.

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses.

Referencias

Asociación Mexicana de Ciberseguridad (AMECI). (2024). Informe anual de incidentes y tendencias de ciberataques en México 2024. Ciudad de México: AMECI. **https://www.ameci.org/**

Banco Interamericano de Desarrollo (BID). (2023). Ciberseguridad: riesgos, inversiones y políticas públicas en América Latina y el Caribe. Washington, D.C.: BID. **https://publications.iadb.org/en/detecting-envelope-wages-e-billing-information**

Banco Mundial. (2023). Desarrollo de talento digital y brechas de capital humano en América Latina. Washington D.C.: Banco Mundial. **https://publications.iadb.org/en/detecting-envelope-wages-e-billing-information**

Centro de Estudios Estratégicos en Ciberdefensa (CEEC). (2023). Panorama del déficit de especialistas en ciberseguridad en México. Ciudad de México: CEEC. **https://ceed.udg.mx/**

Centro de Ciberinteligencia de América Latina (CCAL). (2024). Informe sobre las capacidades nacionales en ciberseguridad en América Latina. Bogotá: CCAL.

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia (Convenio de Budapest). Estrasburgo: Consejo de Europa. **https://www.coe.int/en/web/cybercrime/the-budapest-convention**

Gobierno de España. Instituto Nacional de Ciberseguridad (INCIBE). (2022). Estrategia nacional de ciberseguridad de España 2022–2026. Madrid: INCIBE. **https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy-2023/**

Gobierno de Singapur. Cyber Security Agency (CSA). (2023). Singapore Cybersecurity Strategy 2023. Singapur: CSA. **https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2023/**

Gobierno del Reino Unido. National Cyber Security Centre (NCSC). (2023). UK National Cyber Strategy 2022–2025. Londres: NCSC. **https://www.gov.uk/government/publications/national-cyber-strategy-2022**

Instituto Nacional de Estadística y Geografía (INEGI). (2024). Producto interno bruto trimestral y cuentas nacionales de México. Ciudad de México: INEGI. **https://www.inegi.org.mx/temas/pib/**

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2018). Guía para la protección de datos personales y la seguridad de la información. Ciudad de México: INAI.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Diario Oficial de la Federación (DOF, 2010). **https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf**

Ley de Seguridad Nacional, Diario Oficial de la Federación (DOF, 2018).

Organización de los Estados Americanos (OEA). (2023). Estado de la ciberseguridad en América Latina y el Caribe: 2023 Update. Washington, D.C.: OEA. **https://www.diputados.gob.mx/LeyesBiblio/ref/lsn.htm**

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2024). OECD Digital Economy Outlook 2024: Cybersecurity and digital resilience. París: OCDE.

Secretaría de Hacienda y Crédito Público (SHCP). (2024). Presupuesto de Egresos de la Federación 2024. Ciudad de México: SHCP. **https://dof.gob.mx/2023/SHCP/PEF_2024.html**

World Economic Forum (WEF). (2024). Global Cybersecurity Outlook 2024. Ginebra: WEF. **https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf**