PANORAMA GENERAL

ECONOMÍA DE LA CIBERSEGURIDAD PARA LOS MERCADOS EMERGENTES

Estefania Vergara Cobos

GRUPO BANCO MUNDIAL

Panorama general

ECONOMÍA DE LA CIBERSEGURIDAD PARA LOS MERCADOS EMERGENTES

Estefanía Vergara Cobos

GRUPO BANCO MUNDIAL

Este cuadernillo contiene el panorama general y el prólogo de la publicación *Cybersecurity Economics for Emerging Markets*, doi:10.1596/978-1-4648-2120-2. El libro completo en versión en PDF está disponible en https://openknowledge.worldbank.org/, y se pueden solicitar copias impresas en http://Amazon.com. Sírvase utilizar la versión final para citar, reproducir o adaptar el contenido de esta obra.

Diseño de la portada: Bill Pragluski, Critical Stages, LLC

Índice

GRÁFICOS

Prólogo

En un contexto global en el que existen alrededor de 5450 millones de personas (cerca del 67 % de la población mundial) conectadas a internet y unos 18 000 millones de dispositivos de internet de las cosas, las economías, las sociedades, las organizaciones y las personas se han vuelto altamente dependientes del buen funcionamiento de los sistemas en línea. A pesar de que la digitalización trae enormes beneficios económicos y sociales, nuestra creciente dependencia de las tecnologías digitales también conlleva importantes riesgos. Este es el caso también para los países en desarrollo, donde el ritmo de la digitalización suele superar a las inversiones necesarias y a la atención requerida para crear resiliencia cibernética, una situación que conlleva consecuencias potencialmente perjudiciales.

Mediante un abordaje innovador en el que se aplicaron herramientas avanzadas de inteligencia artificial para analizar millones de artículos en línea, escritos en 98 idiomas, el equipo de investigación digital creó una base de datos única de los incidentes cibernéticos (ciberincidentes divulgados) ocurridos durante la última década, abordando así uno de los desafíos a los que se enfrenta la investigación en este campo: la falta de datos completos y disponibles al público. Las conclusiones revelaron una realidad alarmante: a una tasa de crecimiento anual del 21 %, los ciberincidentes divulgados están en aumento en todo el mundo. Esta aceleración es más intensa en América Latina y el Caribe, y en todos los países de ingreso mediano alto. Esto podría ser solo la punta del iceberg, ya que más del 40 % de los ciberincidentes no suelen denunciarse.

Estas tendencias tienen una importante repercusión económica en los países en desarrollo. En 2022, Costa Rica experimentó un masivo ataque de *ransomware* que paralizó a más de 20 organismos gubernamentales, incluido el Ministerio de Hacienda y Seguridad Social. Este incidente, que duró casi dos meses, dio lugar a la primera declaración de emergencia nacional en la historia a causa de un incidente cibernético, que dejó inactivos sistemas clave y representó un costo económico estimado del 2,4 % del producto interno bruto (PIB) anual del país. Al no contar con los recursos financieros y humanos necesarios para proteger la seguridad de los entornos digitales ni con los servicios de ciberseguridad para contextos específicos, otros países en desarrollo corren el riesgo de experimentar costosos incidentes similares en el futuro.

Además de ser desgastantes para las economías, los ciberincidentes también ponen en peligro la seguridad humana. Cada año, más de la mitad de los países en desarrollo experimentan al menos un ciberincidente divulgado dirigido hacia la infraestructura crítica del país. Como consecuencia de estos incidentes, millones de personas se han visto afectadas por cortes de energía, interrupciones en los servicios médicos, escasez de combustible y el cierre de los puertos, entre otros inconvenientes. Los datos sobre los ciberincidentes divulgados indican que los sectores más afectados a nivel mundial son las finanzas, los servicios de atención médica, la información y las comunicaciones, y los servicios públicos.

La mitigación del riesgo informático es crucial para impulsar el crecimiento económico y el desarrollo sostenible e inclusivo. En este estudio, se demuestra que, en un país en desarrollo donde se reduce la cantidad de ciberincidentes divulgados desde el cuartil superior hasta el cuartil inferior de la distribución (una reducción de 50 a 7 incidentes, aproximadamente, durante el período de estudio) se podría aumentar el PIB per cápita en un 1,5 %. De igual importancia, un ciberespacio más seguro promueve la confianza en la economía digital y protege a las personas más vulnerables, lo que incluye a aquellas que se encuentran en la fracción más baja de la distribución del ingreso y a las pequeñas y medianas empresas.

Si bien no es posible eliminar el riesgo cibernético, sí podemos tratar de gestionarlo y mitigarlo. Con ese fin, debemos colaborar para comprender y evaluar el panorama de amenazas e identificar soluciones eficientes y adaptadas a las capacidades, tanto de los países desarrollados como de aquellos en desarrollo. Un componente esencial de esta iniciativa es la recopilación de datos estandarizada y de rutina sobre los ciberincidentes. Esto será esencial para orientar futuras investigaciones e intervenciones, lo que incluye comprender la magnitud del problema, desplegar recursos financieros y humanos limitados para mejorar la resiliencia cibernética de manera tal de generar el mayor impacto posible, y proporcionar un medio para evaluar mejor la efectividad de estas intervenciones.

Proteger la seguridad de nuestro futuro digital depende del compromiso que asumamos para promover una ciberseguridad eficiente. No es una opción. Es un imperativo vital.

Christine Zhenwei Qiang
Directora global
Departamento Global de Transformación Digital
Banco Mundial

Stephane Straub
Economista en jefe
Vicepresidencia de Infraestructura
Banco Mundial

Panorama general

Introducción

En un mundo cada vez más interconectado gracias a la rápida adopción de las tecnologías digitales y los sistemas en línea, no debe subestimarse el papel fundamental que desempeña la ciberseguridad. A medida que las sociedades pretenden aprovechar el poder de la tecnología para impulsar el crecimiento económico, mejorar los servicios públicos y aumentar el nivel de calidad de vida, se enfrentan a mayores riesgos asociados a las amenazas cibernéticas. En ese contexto, esta obra demuestra que la ciberseguridad es esencial para el progreso socioeconómico de las naciones.

A pesar de que existe una mayor conciencia acerca de la ciberseguridad, aún persisten importantes brechas, que se deben, en gran medida, a la falta de una comprensión profunda de los ciberincidentes y sus consecuencias. Se trata de un problema que plantea importantes obstáculos a la hora de movilizar recursos para la ciberseguridad, sobre todo en los países en desarrollo que presentan limitaciones presupuestarias y necesidades sociales apremiantes. En respuesta a estos desafíos, en esta obra, se ofrece un análisis pionero que 1) describe los elementos clave del panorama de amenazas para la ciberseguridad a nivel mundial; 2) vincula estas amenazas con los medios a través de los que repercuten sobre las economías; 3) identifica problemas de eficiencia dentro de los mercados de la ciberseguridad, y 4) propone estrategias de adaptación, políticas flexibles e iniciativas de gestión institucional descentralizadas para promover la innovación y la sostenibilidad en un marco de cambios continuos e incertidumbre.

El panorama de amenazas

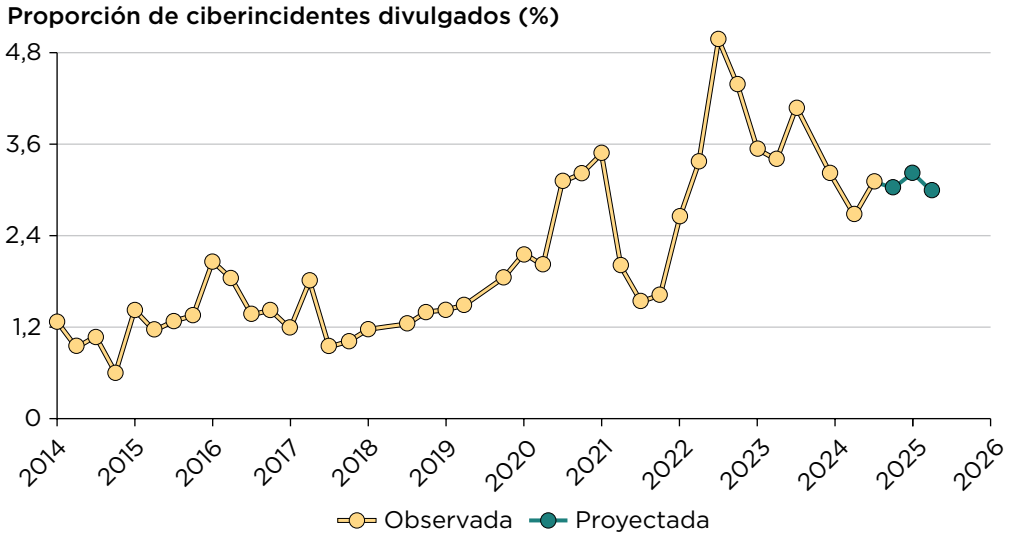
Generar conocimientos sistémicos en torno al panorama de la ciberseguridad supone un reto, dada la escasez de datos sobre los ciberincidentes a nivel mundial, en particular, en los países en desarrollo. A fin de abordar esta brecha, los investigadores del Banco Mundial aplicaron herramientas avanzadas de inteligencia artificial (IA) para analizar millones de artículos acerca de la ciberseguridad en 98 idiomas, publicados en internet durante la última década, a partir de los que se identificaron más de 30 000 ciberincidentes divulgados. Al combinarse con datos del Centro de Estudios Internacionales y de Seguridad de Maryland, se creó una base de datos completa que abarca alrededor de 190 países

y 21 industrias. Las conclusiones revelan una realidad alarmante, que probablemente no pueda explicarse únicamente por cambios en la divulgación de ciberincidentes.

En el auge de la era digital, el mundo se encuentra atrapado en una red de ciberincidentes que está aumentando en tamaño y complejidad. De 2014 a 2023, los ciberincidentes divulgados en todo el mundo crecieron a una tasa anual promedio del 21 %, con un aumento más pronunciado en los países de ingreso mediano alto, que presentaron una tasa de crecimiento del 37 % (gráfico R.1)[1]. Por su parte, los países de ingreso alto (PIA) y los países de ingreso mediano bajo presentaron tasas de crecimiento del 22 % y del 17 %, respectivamente. La tendencia en aumento de los ciberincidentes divulgados durante la última década se vio impulsada, principalmente, por la pandemia de COVID-19 y la guerra entre la Federación de Rusia y Ucrania.

Si bien es cierto que las tecnologías digitales mejoran la resiliencia social y económica frente a una amplia gama de amenazas, también es necesario proteger a las sociedades contra estas. Por ejemplo, la pandemia de COVID-19 dio lugar a una transición rápida hacia la infraestructura digital a fin de facilitar la mejora

GRÁFICO R.1 Evolución mundial de los ciberincidentes divulgados, por trimestre, 2014-25



Fuente: Gráfico original de esta obra, basado en los datos del Centro de Estudios Internacionales y de Seguridad de Maryland y el Banco Mundial sobre los ciberincidentes divulgados.

de los servicios en línea en el ámbito de la salud, la educación, la protección social, el comercio electrónico, el teletrabajo y la productividad. Aunque estas tecnologías proporcionaron importantes beneficios durante un período crítico, introdujeron, al mismo tiempo, graves dificultades para la ciberseguridad. Tal es el caso que, de 2019 a 2020, los ciberincidentes divulgados a nivel mundial aumentaron en un 62 %, con consecuencias, en mayor medida, para los sectores de la administración pública, la atención de la salud y la educación.

Casi dos años después del inicio de la pandemia de COVID-19 y con el telón de fondo de las tensiones geopolíticas, estalló la invasión terrestre a Ucrania, que empañó el ámbito digital. El período posterior a la invasión fue testigo de un incremento extraordinario del 80 % en ciberincidentes divulgados de 2021 a 2022, que repercutieron, en particular, sobre los países de Europa y Asia central, como Italia, Lituania y Polonia, y en sectores críticos como los servicios públicos y la información y las comunicaciones. La guerra entre Rusia y Ucrania es un ejemplo de cómo los ciberincidentes se han convertido en parte integral de los conflictos modernos, poniendo de manifiesto la necesidad urgente de diseñar infraestructuras digitales que refuercen la resiliencia en tiempos de conflictos.

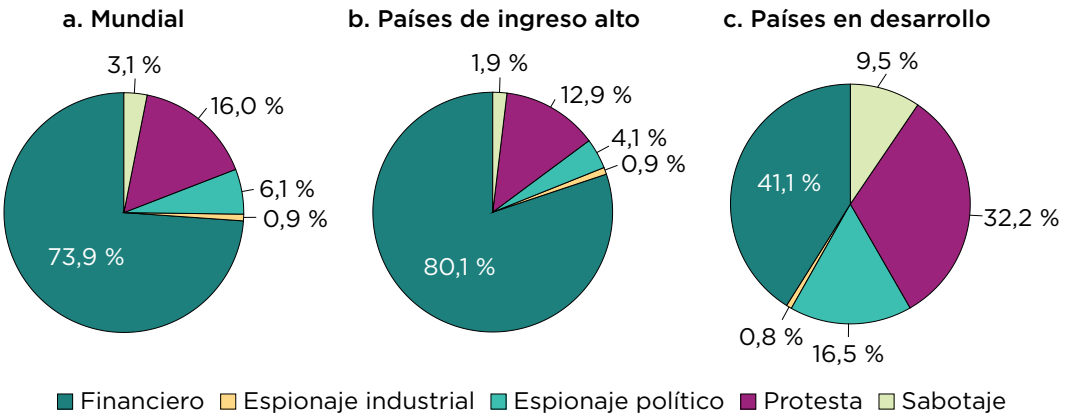
Los países en desarrollo representan aproximadamente el 30 % de los incidentes cibernéticos divulgados en el mundo[2]. No obstante, el aumento y el impacto de los ciberincidentes podría ser más grave en estos países debido a su rápido proceso de digitalización, los menores niveles de inversión en ciberseguridad y la inestabilidad política y económica. Cabe destacar que América Latina y el Caribe (ALC) es la región del mundo que presenta el aumento más rápido de ciberincidentes divulgados, con una tasa de crecimiento anual del 25 % de 2014 a 2023. Este importante aumento en ALC se asoció a un incremento del 145 % de dispositivos de internet de las cosas, un aumento del 280 % en el volumen del comercio electrónico y una mayor adopción de las herramientas de gobierno electrónico en el período posterior a la pandemia de COVID-19 en la región.

El panorama mundial de ciberincidentes divulgados durante la última década muestra un conjunto complejo y diverso de incidentes conformado por distintos factores interconectados (Harry y Gallagher, 2018). Alrededor del 61 % de estos incidentes a nivel mundial fueron de naturaleza explotadora, al igual que el 63 % de los ciberincidentes en los PIA y el 49 % en los países en desarrollo. Los ciberincidentes restantes fueron de carácter disruptivo[3], caracterizados por una tendencia altamente estocástica, lo que añade un factor de incertidumbre.

El panorama de los ciberincidentes divulgados está dominado por motivos financieros, que representan el 74 % de los ciberincidentes a nivel mundial y el 80 % en los PIA. En marcado contraste, solo el 41 % de los ciberincidentes divulgados en los países en desarrollo respondieron principalmente a motivos financieros (gráfico R.2). Las proporciones restantes de los ciberincidentes divulgados (el 20 % en los PIA y el 59 % en los países en desarrollo) mostraron que se fundamentan en motivos políticos que abarcan desde protestas hasta el espionaje político. Estas diferencias persisten a nivel sectorial: la mayor proporción de los incidentes divulgados en los PIA se produjo en el sector de la atención de la salud, mientras que en los países en desarrollo la mayoría de los ciberincidentes divulgados, cerca del 30 %, ocurrieron en la administración pública (gráfico R.3). Este hallazgo coincide con los niveles generalmente más bajos de estabilidad política registrados en los países en desarrollo. No obstante, también plantea una preocupación acerca de la falta de requisitos de divulgación de ciberincidentes para el sector privado en estos países.

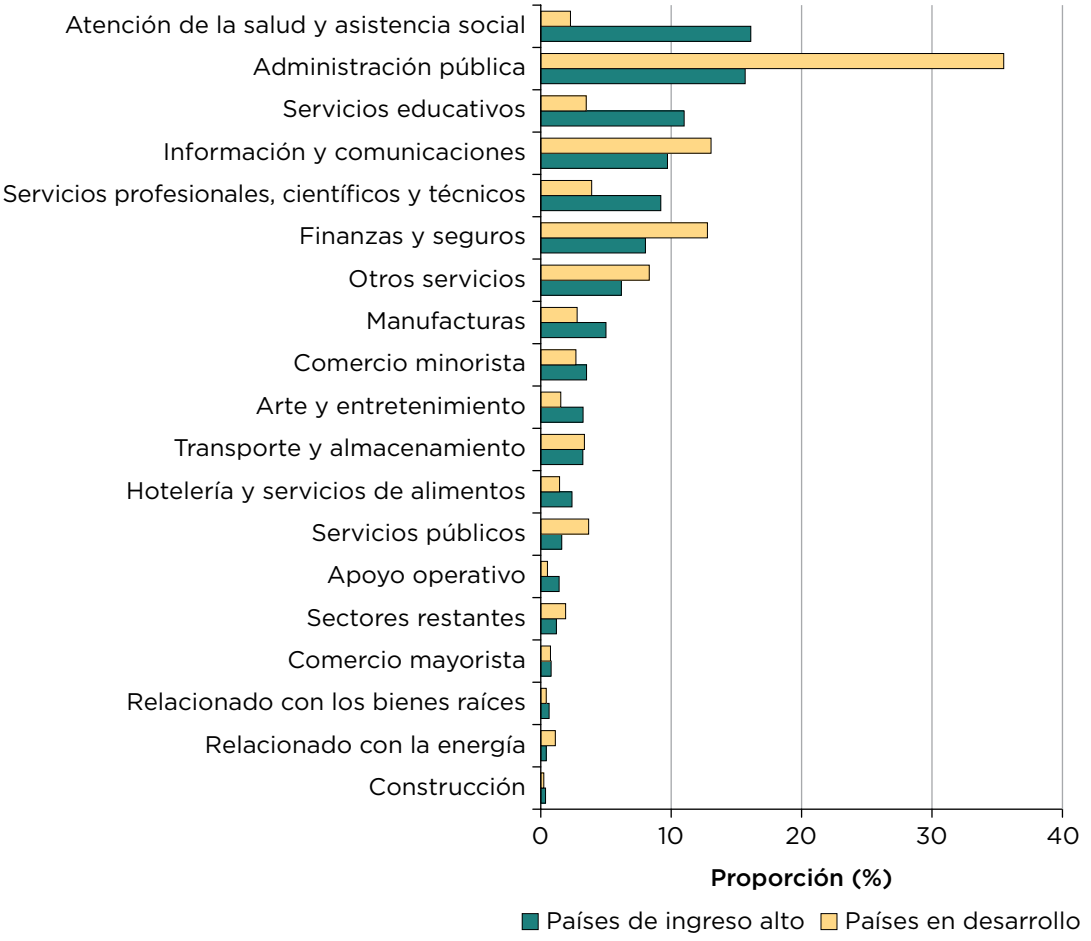
A nivel mundial, los riesgos cibernéticos varían en gran medida (gráfico R.4), con países que enfrentan distintos niveles de exposición a las amenazas cibernéticas y diversos grados de compromisos con la ciberseguridad. Los PIA, como los Estados Unidos y el Reino Unido, son los que más exposición presentan a las amenazas cibernéticas. No obstante, diversos países de ingreso mediano podrían enfrentarse a niveles más elevados de riesgo cibernético debido a que presentan niveles de exposición a amenazas por encima de la mediana global y niveles de

GRÁFICO R.2 Distribución de los ciberincidentes divulgados, por motivo y grupo de ingresos, 2014-23



Fuente: Gráfico original de esta obra, basado en los datos del Centro de Estudios Internacionales y de Seguridad de Maryland sobre los ciberincidentes divulgados.

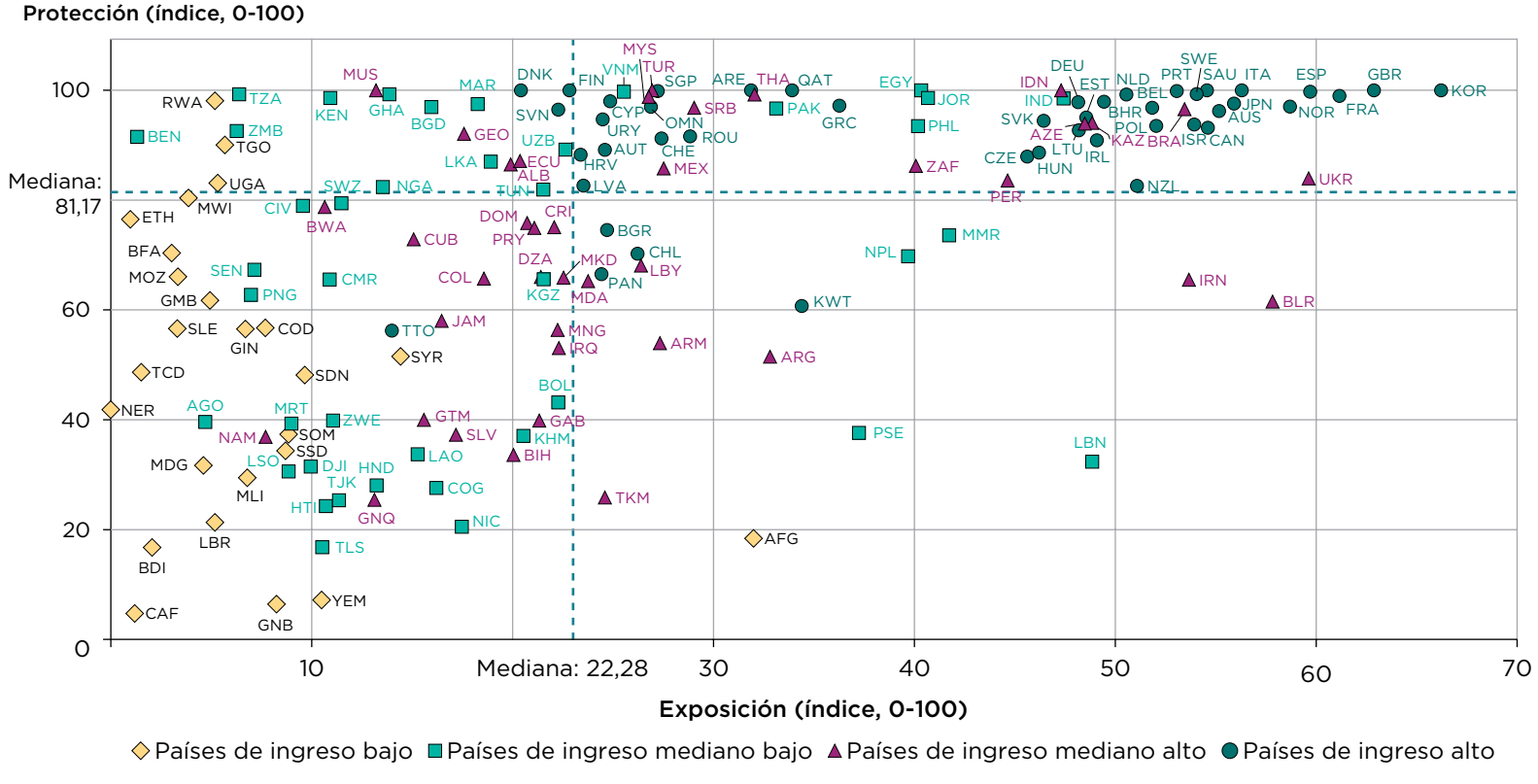
GRÁFICO R.3 Porcentaje de los ciberincidentes divulgados, por sector y grupo de ingresos, 2014-23



Fuente: Gráfico original de esta obra, basado en los datos del Centro de Estudios Internacionales y de Seguridad de Maryland sobre los ciberincidentes divulgados.

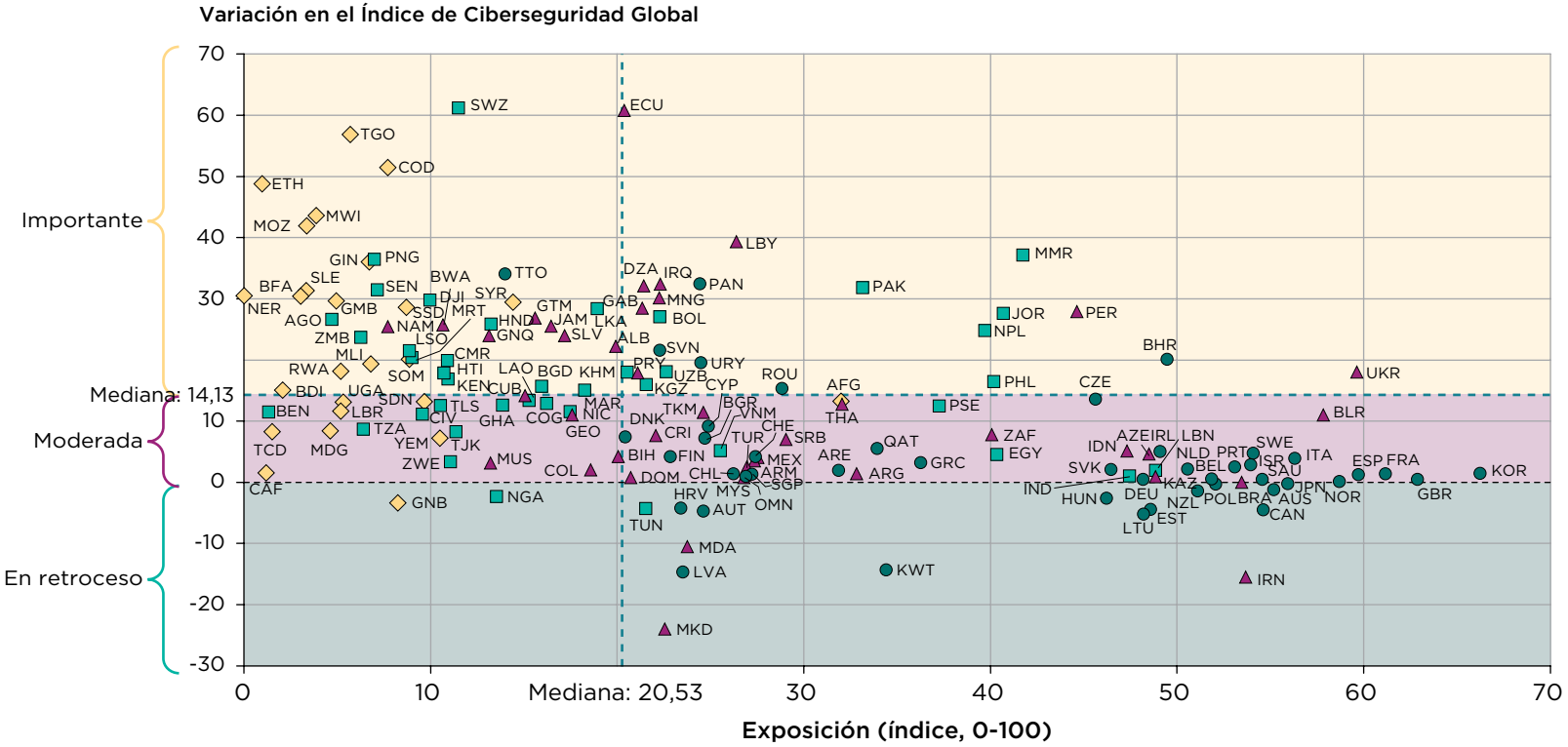
protección por debajo de la mediana global. Los compromisos con la ciberseguridad, que reflejan el nivel de protección, son fundamentales para la mitigación del riesgo. De hecho, entre 2014 y 2023, el promedio anual de ciberincidentes divulgados se triplicó en los países con bajos niveles iniciales de compromiso con la ciberseguridad y se duplicó en aquellos con altos niveles de compromiso. No obstante, entre 2020 y 2024 los países de ingreso bajo han logrado grandes avances en sus niveles de compromiso con la ciberseguridad (gráfico R.5).

GRÁFICO R.4 Grupos de riesgo cibernético establecidos según los niveles relativos de exposición y protección de las economías



Fuente: Gráfico original de esta obra, basado en los datos de la Unión Internacional de Telecomunicaciones.
Nota: Los datos sobre la protección (eje Y) son para 2024. Los años de los datos sobre la exposición (eje X) varían. Para consultas sobre las abreviaciones de países, visite la página web de la Organización Internacional de Normalización, https://www.iso.org/obp/ui/es/#search.

GRÁFICO R.5 Cambios en las calificaciones del compromiso con la ciberseguridad y la exposición relativa, 2020-24



Fuente: Gráfico original de esta obra, basado en los datos del Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones.
Nota: El gráfico no incluye China, la Federación de Rusia y los Estados Unidos por tener valores atípicos. Los datos sobre la protección (eje Y) reflejan el cambio en el ICG de 2020 a 2024. Los años de los datos sobre la exposición (eje X) varían. Para consultas sobre las abreviaciones de países, visite la página web de la Organización Internacional de Normalización, https://www.iso.org/obp/ui/es/#search.

El costo económico de los ciberincidentes

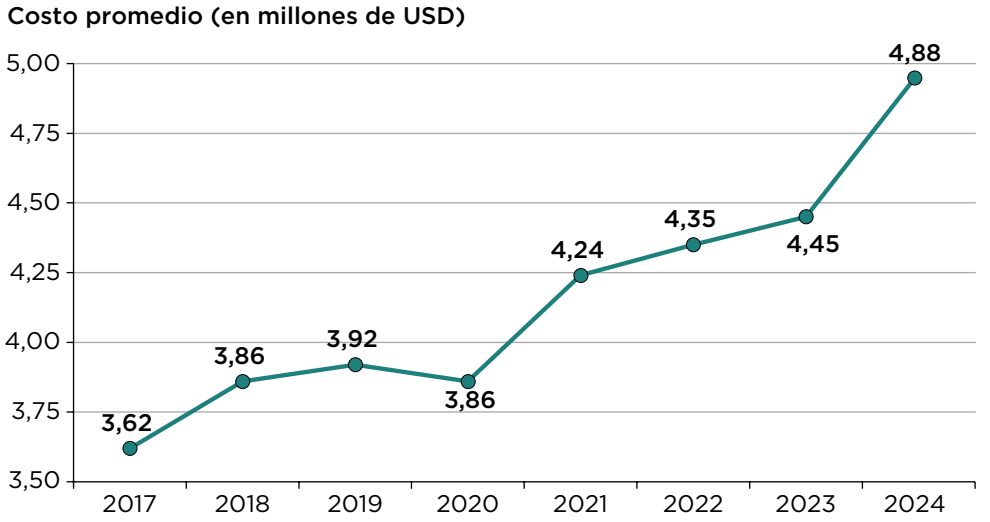
La frecuencia y los costos en aumento de los ciberincidentes que se producen en todo el mundo son alarmantes y conllevan riesgos reales para la estabilidad macroeconómica, en particular para los países en desarrollo. Asimismo, dado que muchos ciberincidentes no se divulgan, lo que sabemos podría representar solo la punta del iceberg. Las repercusiones económicas de los ciberincidentes son incluso potencialmente más graves en los países en desarrollo, donde los cálculos señalan que el incidente cibernético divulgado promedio tiene un mayor impacto que en los PIA.

Para lograr un desarrollo inclusivo y sostenible, así como un crecimiento económico, es necesario reducir la frecuencia de los ciberincidentes importantes. Según una investigación reciente de Vergara Cobos y otros (de próxima publicación), un país en desarrollo que reduce la cantidad de ciberincidentes importantes divulgados, desde el cuartil superior de la distribución (cerca de 50 ciberincidentes divulgados) hasta el cuartil inferior (cerca de 7 ciberincidentes divulgados) en una década podría experimentar un aumento en el producto interno bruto (PIB) per cápita de aproximadamente el 1,5 %. Esto excede las ganancias que se espera obtener con la adopción de la IA en una década (Acemoglu, 2024). De forma similar, los compromisos más sólidos con la ciberseguridad a nivel nacional tienen repercusiones positivas, y hay estimaciones que muestran que, si todo lo demás se mantiene constante, las industrias más digitalizadas tienen un mejor desempeño en los países con niveles más altos de compromisos con la ciberseguridad que en aquellos donde estos niveles son más bajos.

El inicio de la pandemia de COVID-19 amplificó tanto la frecuencia como las repercusiones de los ciberincidentes, con importantes aumentos en los costos unitarios promedio. Por ejemplo, de 2022 a 2023, el costo promedio de un ataque de *ransomware* subió en un 13 % y, durante el año siguiente, el costo promedio de los incidentes de filtraciones de datos treparon casi un 10 % (gráfico R.6). Estos aumentos afectan de forma desproporcionada a las pequeñas y medianas empresas (pymes) a nivel mundial, mientras que las grandes organizaciones (con más de 10 000 empleados) experimentan disminuciones en los costos unitarios de los incidentes de filtraciones de datos (IBM, 2023, 2024).

La naturaleza sistémica del riesgo cibernético implica que incluso un solo incidente puede desencadenar perturbaciones generalizadas. Tal fue el caso del ciberataque NotPetya de 2017, que ocasionó pérdidas de USD 7300 millones para los consumidores, cifra cuatro veces mayor que la caída inicial en las ganancias reportadas por las empresas que se vieron afectadas directamente

GRÁFICO R.6 Costo promedio mundial de una filtración de datos, 2017-24



Fuente: Gráfico original de esta obra, basado en los datos de IBM (2023, 2024).

(Crosignani, Macchiavelli y Silva, 2023). La naturaleza sistémica del riesgo cibernético podría conducir a escenarios peligrosos, como las "corridas cibernéticas" (*cyber runs*), que ponen en riesgo de forma rápida y a gran escala la estabilidad financiera y operativa del sector bancario; hasta el momento, estos escenarios se han prevenido gracias a las medidas proactivas que han adoptado ciertos bancos y entidades reguladoras.

A medida que aumentan las amenazas cibernéticas, las consecuencias se extienden más allá de las meras pérdidas económicas y abarcan preocupaciones de seguridad más amplias a nivel nacional y la protección de los derechos de las personas, lo que incluye la privacidad y el acceso a los servicios esenciales. Esta cuestión destaca la necesidad urgente de aplicar medidas eficientes en materia de ciberseguridad para salvaguardar la estabilidad económica y el bienestar social.

El mercado de la ciberseguridad

Hoy en día, el mercado de la ciberseguridad experimenta un crecimiento y una transformación excepcionales, gracias al impulso de factores como la adopción generalizada de las tecnologías en la nube y el surgimiento de nuevos desafíos para la seguridad, tales como los relacionados con los avances en los modelos de lenguaje de gran tamaño y otras herramientas de la IA. Estas dinámicas están reconfigurando la manera en la que las organizaciones abordan la seguridad de sus

activos digitales y su información confidencial, y cómo invierten en ellos. En 2024, se prevé un aumento del gasto mundial en la seguridad de la información y en la gestión de los riesgos de un 14 % en comparación con 2023 (Gartner, 2024), una cifra que alcanzará casi el 0,2 % del PIB mundial. Esta tasa de crecimiento estimada notablemente alta del gasto global en seguridad es casi el doble de la del gasto en tecnologías de la información y casi cuatro veces superior al crecimiento proyectado de la economía global para 2024 (Gartner, 2024; FMI, 2024). Las áreas que experimentan las tasas más elevadas de crecimiento incluyen la seguridad en la nube y la privacidad de los datos. No obstante, los servicios de seguridad, como los de consultoría y tercerización, continúan dominando el gasto en ciberseguridad, lo que pone de manifiesto el papel crítico que desempeña el apoyo de los expertos en materia de ciberseguridad.

A pesar del crecimiento, la industria enfrenta obstáculos importantes, que incluyen una baja inversión en investigación y desarrollo (IyD), indispensable para afrontar las amenazas nuevas y avanzadas, y una escasez generalizada a nivel mundial de profesionales capacitados en ciberseguridad, con más de 4 millones de puestos vacantes en el área en 2023 (Consorcio Internacional de Certificación de Seguridad de Sistemas de Información [ISC2], 2023). La escasez en la fuerza laboral especializada en ciberseguridad afecta, en particular, a los sectores públicos no militares, a las pymes y a las naciones en desarrollo.

Asimismo, a medida que las sociedades avanzan en la era digital, puede que las variaciones en la accesibilidad a los mercados de ciberseguridad estén otorgando ventajas comparativas a los PIA y a las organizaciones más grandes. América del Norte domina más del 50 % del mercado mundial; con una demanda 16 veces superior a la de todos los países de ALC en conjunto. La demanda sesgada del mercado también es evidente a nivel gubernamental: el gasto público per cápita en ciberseguridad en los PIA (como Canadá y Estados Unidos) supera los USD 30, en comparación con menos de USD 1 en países en desarrollo altamente afectados por ciberincidentes, como India y México. En el mundo de los negocios, las grandes empresas encabezan el gasto en ciberseguridad. Mientras tanto, los principales proveedores de ciberseguridad informan una disminución en las ventas a las pymes, un fenómeno que se debe, principalmente, a la falta de recursos.

Los desafíos mencionados anteriormente podrían verse aún más agravados por varias fuentes de ineficiencia del mercado:

- *Riesgo informático de terceros no internalizado.* Las organizaciones que experimentan un incidente cibernético a menudo están expuestas debido a un tercero. Sin embargo, esto no conduce a un aumento de la inversión en la gestión ampliada del riesgo.

- *Rendimientos de la inversión poco claros.* A diferencia de otras inversiones que ahorran costos, los beneficios económicos de la ciberseguridad no están claros e incluso son imposibles de cuantificar mediante el enfoque habitual de costo-beneficio, lo que obstaculiza la asignación eficiente de los recursos.
- *Riesgo moral.* La mayoría de las empresas comprometidas trasladan las pérdidas derivadas de los ciberincidentes a los consumidores mediante aumentos de precios, mientras que los accionistas sufren las caídas del valor de mercado.
- *Incentivos que no están alineados con las necesidades.* Los ciberincidentes no divulgados, junto con la baja conciencia pública y un mercado tecnológico altamente competitivo, generan incentivos que no están alineados con las necesidades para producir tecnologías digitales resilientes.
- *Asimetrías de información.* La población general está rezagada en cuanto a los conocimientos y la conciencia sobre la ciberseguridad. Además, es prácticamente inviable evaluar el nivel de riesgo informático o la eficacia de los productos de ciberseguridad antes de un ciberataque.

Las ineficiencias del mercado podrían ser más pronunciadas en los países en desarrollo, dada la influencia de los Gobiernos de los PIA sobre la dinámica del mercado mundial a través de sus grandes adquisiciones y sus regulaciones y estándares operativos. Los Gobiernos podrían abordar estos desafíos, por ejemplo, dando prioridad a los programas de concientización y capacitación, y coordinando un plan de IyD adaptado a las necesidades del país.

Conclusiones y recomendaciones sobre políticas

La ciberseguridad es una responsabilidad colectiva que deben compartir todos los actores económicos. En esta obra, se profundiza acerca de los aspectos fundamentales de la ciberseguridad, lo que incluye el panorama de amenazas y sus costos asociados, las deficiencias del mercado y los papeles críticos que desempeñan los Gobiernos. Al proporcionar nuevas evidencias sobre las repercusiones socioeconómicas de los ciberincidentes, la obra sostiene que un ciberespacio seguro es clave para liberar todo el potencial de las tecnologías digitales y allanar el camino hacia un desarrollo inclusivo y sostenible en la era digital.

Las naciones en desarrollo, en particular, enfrentan la doble tarea de fomentar la digitalización y protegerse contra las amenazas cibernéticas. Las recomendaciones para estas naciones incluyen la implementación de prácticas estandarizadas y seguras de recopilación de datos para respaldar el diseño de

políticas basadas en evidencia; la promoción del desarrollo de una industria nacional de ciberseguridad; la elaboración de planes de acción que involucren a diferentes sectores y partes interesadas; la priorización de la resiliencia en sectores críticos, y el apoyo a los programas de capacitación y concientización sobre ciberseguridad. Las sugerencias acerca de las políticas enfatizan la importancia de proteger los sectores altamente interconectados a nivel tecnológico, operativo y financiero, como las finanzas y las comunicaciones, y también en sectores de gran atractivo, como la atención de la salud y la administración pública (gráfico R.7). Dado que el 90 % de la investigación global en ciberseguridad se centra únicamente en el contexto de Estados Unidos,

GRÁFICO R.7 Estrategias de ciberseguridad para los sectores clave

Finanzas: Concentrarse en dos prácticas que funcionan bien en los países de ingreso alto.

- Un *abordaje de mercado* en el que se fomente un mercado de ciberseguridad competitivo a nivel nacional para los productos y servicios de ciberseguridad adaptados a las necesidades de las instituciones locales.
  - Apoyar a las *startups* o empresas emergentes.
- Un *abordaje regulatorio* en el que se establezcan organismos reguladores sólidos que realicen un seguimiento continuo de la seguridad y la estabilidad.
  - Mantenerse alerta ante posibles "corridas cibernéticas".

Atención de la salud: El panorama en los países de ingreso alto sirve como advertencia para el sector de la salud en proceso de digitalización de los países en desarrollo.

- Reconocer que este sector representa un gran atractivo para los actores maliciosos.
- Establecer organismos reguladores sólidos con la autoridad para supervisar y dar seguimiento a las actividades.
- Asegurar que las leyes de protección de datos altamente confidenciales estén actualizadas y sean efectivas.

Administración pública: Una prioridad continua para todos los países.

- Implementar medidas preventivas de forma permanente.
- Promover las auditorías cibernéticas y las iniciativas para la detección de amenazas continuas.
- Priorizar los esfuerzos en favor de la resiliencia durante los períodos de mayor actividad política.
- Garantizar la protección efectiva de los datos de la población contra las amenazas emergentes.

Servicios públicos, energía, transporte, tecnología de la información y las comunicaciones

- Reconocer a la ciberseguridad en estos sectores como esencial para salvaguardar los servicios que se vinculan de manera estrecha con la protección de los derechos humanos.
- Enfocarse en el diseño de infraestructura digital resiliente, sobre todo en los países con un riesgo geopolítico elevado.
- Colaborar de manera estrecha con el sector privado y la comunidad internacional para garantizar una protección sólida de los sistemas compartidos.

Fuente: Gráfico original elaborado para esta obra.

también se recomienda promover iniciativas de investigación inclusivas en los ámbitos de la ciberseguridad y la economía de la ciberseguridad, y seguir de cerca los impactos económicos de los ciberincidentes a corto y a largo plazo. Asimismo, se hace hincapié en respaldar un plan de IyD estratégico y personalizado; abogar por disposiciones de ciberseguridad asequibles para las pymes, y marcos regulatorios dinámicos y actualizados; fomentar la colaboración internacional y las asociaciones público-privadas, así como realizar un seguimiento del desarrollo y de la adopción de las tecnologías emergentes, como la computación en la nube y la IA avanzada. Por último, las sugerencias sobre políticas están también dirigidas a proteger la infraestructura crítica y los servicios esenciales, aprendiendo de sectores resilientes como el sector financiero de Estados Unidos y de naciones en desarrollo que registran fuertes mejoras en compromisos y resultados en ciberseguridad.

Notas

1. Un *incidente cibernético* es un evento o el resultado final de cualquier acción única y no autorizada que se realiza mediante el uso de un sistema de información (por ejemplo, la tecnología informática) o una red, que da como resultado un efecto adverso, real o potencial, que es relevante a nivel nacional en cualquiera de las tres capas que constituyen el ciberespacio: los sistemas de información, las redes y la información que reside en ellas (Harry y Gallagher, 2018; Instituto Nacional de Normas y Tecnología [NIST], s. f.).
2. El término *países en desarrollo* se utiliza para referirse a las naciones que no están clasificadas como países de ingreso alto.
3. El Centro de Estudios Internacionales y de Seguridad de Maryland define dos tipos principales de ciberincidentes: "disruptivos" y "de explotación". Un *incidente disruptivo* impide llevar a cabo las operaciones habituales de la organización afectada, y un *incidente de explotación* es aquel que de forma ilícita accede a información confidencial o la extrae, como información de identificación personal, información clasificada o datos financieros.

Bibliografía

Acemoglu, D. 2024. "The Simple Macroeconomics of AI." Working Paper 32487, National Bureau of Economic Research, Cambridge, MA.

Crosignani, M., M. Macchiavelli, and A. F. Silva. 2023. "Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains." *Journal of Financial Economics* 147 (2): 432–48.

Gartner. 2024. "Planning for GenAI Initiatives Is Helping to Drive IT Spending in 2024 and Beyond." Gartner, San Francisco, CA (accessed July 21, 2024), https://www.gartner.com/en/newsroom/press-releases/2024-04-16-gartner-forecast-worldwide-it-spending-to-grow-8-percent-in-2024#:~:text=Worldwide%20IT%20spending%20is%20expected,the%20end%20of%20the%20decade.

Harry, C., and N. Gallagher. 2018. “Classifying Cyber Events.” *Journal of Information Warfare* 17 (3): 17–31.

IBM. 2023. “2023 Cost of a Data Breach.” IBM, Armonk, NY.

IBM. 2024. “2024 Cost of a Data Breach.” IBM, Armonk, NY.

IMF (International Monetary Fund). 2024. *Global Financial Stability Report*. Washington, DC: IMF.

ISC2 (International Information System Security Certification Consortium). 2023. “How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce.” ISC2, Alexandria, VA.

NIST (National Institute of Standards and Technology). n.d. “NIST Glossary.” Definition of Cyberspace. NIST, Gaithersburg, MD. https://csrc.nist.gov/glossary/term/cyberspace.

Vergara Cobos, E., S. Cakir, H. Mei-Zahav, and B. Barakcin. Forthcoming. “The Role of Cybersecurity in Economic Performance.” World Bank, Washington, DC.

En nuestro mundo cada vez más interconectado, donde las tecnologías digitales transforman con rapidez múltiples aspectos de la vida cotidiana, no se puede subestimar el papel fundamental de la ciberseguridad, sobre todo en los países en desarrollo. A medida que estos países se esfuerzan por aprovechar el poder de la tecnología moderna para impulsar el crecimiento económico, mejorar los servicios públicos y elevar los niveles de vida, se enfrentan, de forma simultánea, a mayores riesgos asociados a las amenazas cibernéticas. A menudo, la creciente exposición de los países en desarrollo a los ciberincidentes se ve agravada por varios factores, como la escasez de recursos, la infraestructura inadecuada, la agitación política, las ineficiencias en los mercados de la ciberseguridad y la tecnología, la escasez de profesionales capacitados en ciberseguridad, los vacíos legislativos y las elevadas tasas de adopción digital.

Economía de la ciberseguridad para los mercados emergentes es una obra de investigación pionera que profundiza en los factores que impulsan los ciberincidentes en todo el mundo y sus profundas consecuencias. Desde reveses económicos que pueden desestabilizar economías enteras hasta interrupciones de servicios vitales e impedimentos para el desarrollo social y económico, las repercusiones de los ciberincidentes tienen un enorme alcance.

En esta obra, se analizan cientos de trabajos académicos y miles de ciberincidentes de divulgación pública que ocurrieron durante la última década en unos 190 países. Se explican las características y las tendencias de estos incidentes, así como los roles que pueden asumir los actores del mercado privado y los Gobiernos para salvaguardar la infraestructura en el ciberespacio de manera efectiva. En la obra, se presentan sugerencias prácticas y recomendaciones de políticas públicas basadas en evidencia, que incluyen iniciativas para fortalecer la resiliencia de los sectores más esenciales e interconectados. Se aboga por reforzar las industrias nacionales de ciberseguridad, diseñar estrategias de investigación y desarrollo de ciberseguridad, abordar las deficiencias del mercado a través de programas de capacitación y concientización sobre la ciberseguridad, y tomar medidas proactivas para reducir y controlar los efectos de contagio de los ciberincidentes.

Al revelar dimensiones empíricas y teóricas cruciales de la economía de la ciberseguridad, esta obra proporciona ideas que podrían funcionar como fundamento para la creación de inversiones efectivas en materia de ciberseguridad, con un enfoque en los países en desarrollo. Estas conclusiones son invaluables para los responsables de formular políticas y las partes interesadas comprometidas con fortalecer el ecosistema digital frente al panorama en constante evolución de las amenazas cibernéticas.

GRUPO BANCO MUNDIAL

SKU 33747