

## INVESTIGACIÓN SOBRE ETF DE GLOBAL X

# La ciberseguridad en Israel: Cómo fortalecer las defensas digitales en medio de riesgos elevados

Autor:  
Equipo de Investigación de  
Global X

Fecha: 3 de junio de  
2022

Israel está en el centro del ecosistema global de ciberseguridad. Con el impulso de fondos récord en 2021, consideramos que la ciberseguridad israelí está bien posicionada para ser una solución a la que las empresas y los organismos gubernamentales de todo el mundo recurran para obtener apoyo. Una serie de ataques de alto perfil ha puesto la ciberseguridad en el centro de la atención mundial en los últimos años, y **no se espera que la tendencia disminuya en 2022**. La invasión de Rusia a Ucrania es el último ejemplo de la creciente importancia de la ciberseguridad y su relación intrínseca con la geopolítica. En este artículo, examinaremos la presencia de Israel en la industria y tres empresas de dicho país que se han adaptado a la creciente amenaza de la actividad cibernética maliciosa.

### Conclusiones clave

- Las empresas israelíes tienen una posición clave en el ecosistema global de ciberseguridad. El crecimiento de la industria ha convertido a Israel en uno de los centros de innovación en ciberseguridad más grandes del mundo.
- El aumento de las vulnerabilidades durante la pandemia ayudó a impulsar el financiamiento a las empresas emergentes de ciberseguridad israelíes a un máximo histórico de 8.800 millones de USD en 2021.<sup>1</sup> Aproximadamente un tercio de los unicornios en ciberseguridad de todo el mundo tuvieron sede en Israel en 2021.<sup>2</sup>
- Si bien las tendencias potenciales a largo plazo, como **el aumento de las informática en la nube**, están actuando como vientos de cola para la ciberseguridad, los hechos ocurridos en 2022 están colocando al riesgo geopolítico como una preocupación principal para los gobiernos y las empresas por igual. La creciente conciencia de la necesidad de cooperación e inversión en el campo de la ciberseguridad debería crear oportunidades para las principales empresas israelíes.

### Identificar el centro de ciberseguridad israelí

A nivel mundial, tres regiones geográficas se destacan como los centros más grandes de innovación en ciberseguridad al tener en cuenta factores como el financiamiento de capital de riesgo, la cantidad de empresas líderes, el capital humano y los efectos de traspaso de conocimientos: el Área de la Bahía de San Francisco, el área metropolitana de Washington D.C. e Israel. El término centro se refiere a una "densidad concentrada de empresas dentro de una región geográfica" que típicamente disfrutan de los beneficios de altas concentraciones de capital humano, conocimiento compartido y apoyo institucional.<sup>3</sup> En el contexto de la ciberseguridad u otros campos que dependen en gran medida de la innovación, la formación de centros puede tener un efecto decisivamente positivo.

De estos centros, Israel ocupa el segundo lugar en términos de financiamiento de capital de riesgo con 4.000 millones de USD y el 32 % de las 150 principales empresas de ciberseguridad innovadoras (según compila la revista *Cybercrime Magazine*), lo que destaca la reputación de Israel como una nación "de empresas emergentes".<sup>4</sup> Tel Aviv es el corazón de la ciberseguridad y de la industria tecnológica en general en Israel. Sin embargo, Be'er Sheva, una ciudad al interior, es una presencia de rápido crecimiento en la ciberseguridad, en gran parte debido a un esfuerzo deliberado de políticas para trasladar las unidades cibernéticas nacionales allí.<sup>5</sup>

El rápido ascenso de la ciberseguridad israelí puede explicarse en parte por el enfoque del país en la defensa nacional y los esfuerzos del gobierno para promover la industria. En 2017, Israel fundó un centro nacional de cibereducación,

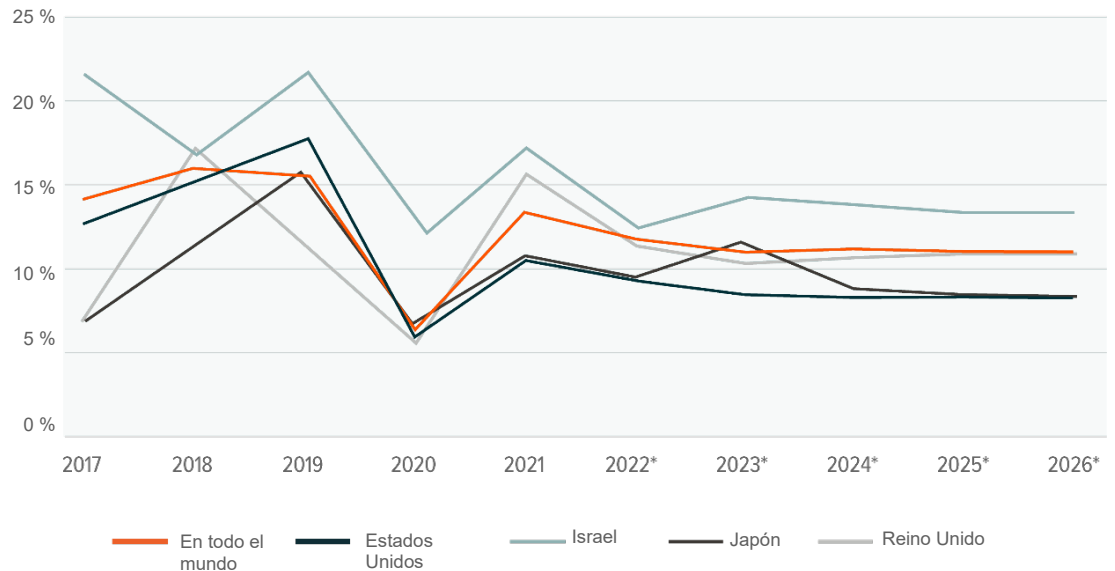


que ahora cuenta con 80 centros de aprendizaje en todo el país y 330 miembros del personal.<sup>6,7</sup> Entre 2011 y 2021, la cantidad de empresas de ciberseguridad activas en Israel se multiplicó: pasó de 162 a 459.<sup>8</sup> Estas empresas incluyen a Check Point y CyberArk, dos gigantes de ciberseguridad globales con una capitalización de mercado combinada de más de 20.000 millones de USD a abril de 2022.<sup>9</sup>

Como indica el siguiente cuadro, el compromiso nacional con la ciberseguridad hace que las empresas cibernéticas israelíes estén posicionadas para mantener un mayor nivel de crecimiento de los ingresos en comparación con otros países importantes, como los Estados Unidos, Japón y el Reino Unido.

### CAMBIO DE INGRESOS EN EL MERCADO DE CIBERSEGURIDAD POR PAÍS

Fuentes: Global X ETFs con información derivada de: Statista. (Marzo de 2022). Mercados tecnológicos: Ciberseguridad.  
\* Indica el pronóstico.



Notas: Los datos que se muestran utilizan los tipos de cambio actuales a marzo de 2022. Los datos que se muestran aún no reflejan los impactos en el mercado de la guerra entre Rusia y Ucrania; estamos trabajando en una actualización.

### Aumentan los incidentes: el 2021 marca un año récord para financiamiento cibernético en Israel

Desde que la pandemia de COVID dejó a las empresas sin otra opción que aceptar la nueva normalidad del trabajo desde casa, las vulnerabilidades recientemente expuestas y las mejores prácticas de ciberseguridad a menudo desatendidas se convirtieron en una fuente de consternación en todo el mundo. Esa consternación persistió en 2021 a medida que las variantes Delta y Ómicron se volvieron obstáculos para la reapertura de las economías. Al mismo tiempo, varios ciberataques de alto perfil llamaron la atención del mundo, incluido el ataque de ransomware a Colonial Pipeline en los Estados Unidos. Israel tampoco se libró de ello, ya que se identificaron múltiples incidentes cibernéticos.

En marzo de 2021, los autores de la campaña de phishing de diciembre de 2020 dirigida a investigadores médicos israelíes y estadounidenses fueron identificados como TA453, con sede en Irán.<sup>10</sup> En octubre de 2021, un ataque de ransomware al Centro Médico Hillel Yaffe en Hadera, Israel, puso los sistemas del hospital fuera de línea, lo que obligó a los médicos a usar bolígrafo y papel para llevar registros durante más de un día.<sup>11,12</sup> Además, la empresa de ciberseguridad con sede en Israel NSO Group se convirtió en objeto de escrutinio global. Varios gobiernos autoritarios de todo el mundo utilizaron el software de vigilancia de empresa compañía, Pegasus, para hackear dispositivos iPhone y Android de activistas, periodistas y abogados de derechos humanos.<sup>13</sup>

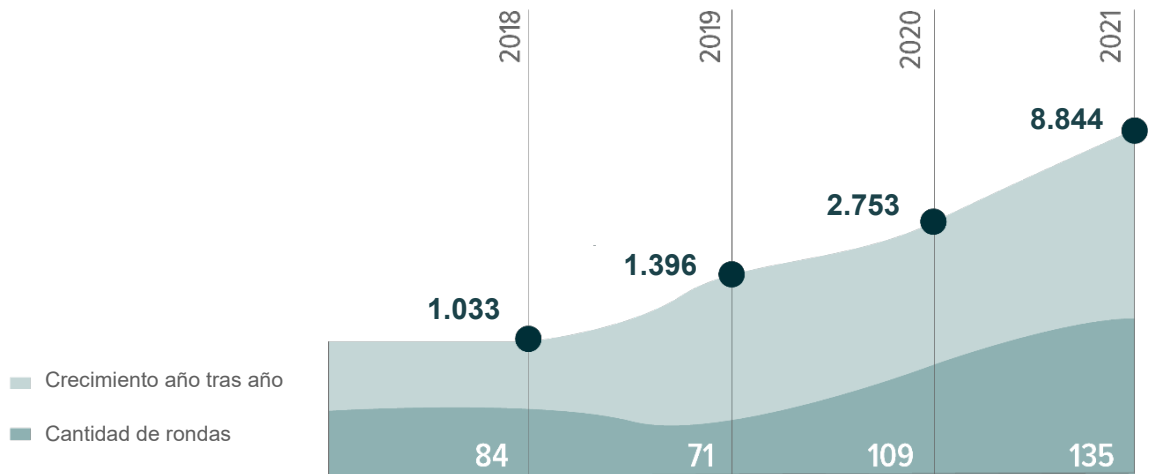
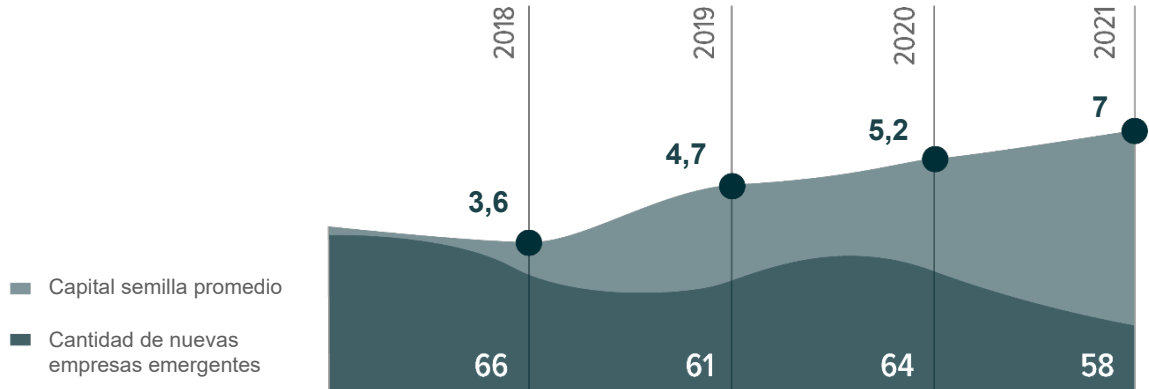
El efecto neto de estos hechos probablemente contribuyó a un año récord para el financiamiento de ciberseguridad en Israel. El sector de ciberseguridad de Israel acumuló 8.840 millones de USD en fondos durante 2021, lo que representa

un aumento del triple en comparación con los 2.750 millones de USD de 2020.<sup>14</sup> A nivel mundial, el 40 % de las inversiones privadas en rondas de financiamiento cibernético fueron a Israel en 2021, lo que es notable teniendo en cuenta el tamaño relativamente pequeño del país.<sup>15</sup>

El ingreso masivo de fondos en la ciberseguridad israelí en 2021 contribuyó al surgimiento de 11 nuevos unicornios cibernéticos, definidos como empresas emergentes con un valor de mercado de más de 1.000 millones de USD. Para poner este crecimiento en perspectiva, al 2021, el 33 % de los unicornios cibernéticos de todo el mundo estaban en Israel.<sup>16</sup>

### TENDENCIAS DE FINANCIACIÓN DE EMPRESAS EMERGENTES DE CIBERSEGURIDAD

Fuentes: Global X ETFs con información derivada de: Wiseman, Y. (4 de enero de 2022). Israel's cybersecurity startups post another record year in 2021 TechCrunch+.



### La concientización cibernética y cooperación van en aumento junto con los riesgos geopolíticos

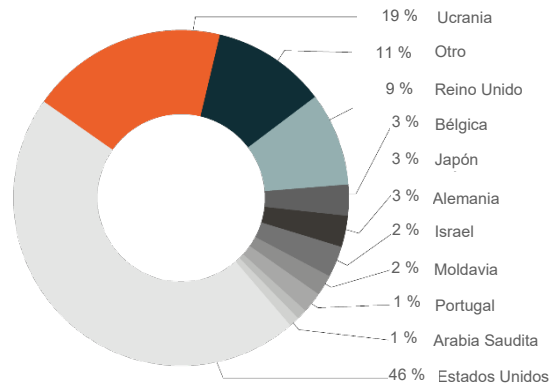
Antes de la invasión de Rusia a Ucrania en febrero, todas las señales apuntaban a más riesgos cibernéticos en 2022. La invasión estableció un tono de ansiedad para el año y destacó cómo las tensiones geopolíticas se correlacionan con el creciente miedo a los ciberataques. Ucrania fue el segundo país más afectado por los ataques cibernéticos detrás de los Estados Unidos entre julio de 2020 y junio de 2021, lo que posiblemente fue un pronóstico de la invasión en 2022.<sup>17</sup>



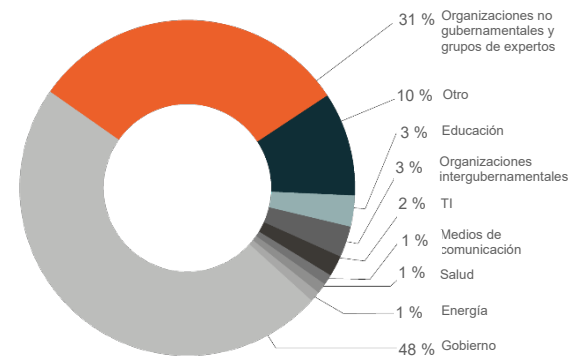
## PAÍSES Y SECTORES OBJETIVO DE ATAQUES CIBERNÉTICOS

Fuentes: Global X ETFs con información derivada de: Equipos colaboradores. (octubre de 2021). Informe de defensa digital de Microsoft. Microsoft.

Países más atacados (julio de 2020 a junio de 2021)



Sectores más atacados (julio de 2020 a junio de 2021)



Con el enfoque abrumador de los ataques cibernéticos a instituciones gubernamentales, ONG y grupos de expertos, los gobiernos están aumentando el gasto en ciberseguridad. Por ejemplo, en los Estados Unidos, la administración de Biden propone 2.500 millones de USD para la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) en 2023, un aumento de 500 millones de USD con respecto a 2022, y Australia está gastando 10.000 millones de USD para duplicar el tamaño de su Dirección de Señales.<sup>18,19</sup> Mientras tanto, Francia está trabajando para construir Campus Cyber, un centro de innovación en ciberseguridad financiado por el Estado que se modela en el centro CyberSpark de Israel en Be'er Sheva.<sup>20</sup>

Dado que las exportaciones cibernéticas de Israel alcanzaron los 11.000 millones de USD en 2021, un aumento con respecto a los 6.900 millones de USD en 2020, Israel podría beneficiarse de estos esfuerzos en todo el mundo.<sup>21</sup> Como ejemplo, para agosto de 2021, aproximadamente el 20 % de las importaciones de seguridad de TI de Australia eran de Israel.<sup>22</sup>

Quizás tan importante como el aumento del gasto por parte de gobiernos individuales es la mayor conciencia de que la ciberseguridad requiere un esfuerzo cooperativo. Como potencia en ciberseguridad, las empresas israelíes están en posición de desempeñar un papel de liderazgo en ese esfuerzo. En diciembre de 2021, el Ministerio de Finanzas de Israel promovió que el Fondo Monetario Internacional (FMI) y otros 10 países participantes realizaran una prueba de sus capacidades contra un ataque simulado al sistema financiero global en un "juego" cibernético innovador.<sup>23</sup> La firma de un acuerdo entre Israel y los Estados Unidos en marzo de 2022 para reforzar la cooperación en ciberseguridad, que incluye planes para interactuar con empresas del sector privado, es otro signo de esta tendencia.<sup>24</sup>

Además, la Conferencia Global de Cibertecnología anual en Tel Aviv es la conferencia de ciberseguridad más grande del mundo fuera de los Estados Unidos, y atrae regularmente a participantes de compañías líderes, nuevas empresas, inversores y gobiernos. La conferencia de este año, que se llevó a cabo en marzo, mostró el papel de las empresas israelíes en los esfuerzos de ciberseguridad cooperativa. El primer ministro Bennett destacó la cantidad de acuerdos cooperativos que Israel ha firmado con otros países.

### Tres empresas de ciberseguridad israelíes que responden a amenazas crecientes

La combinación de la pandemia y el incremento de los riesgos geopolíticos hace que 2022 sea un año único, mientras que los ataques continúan siendo cada vez más sofisticados. A continuación, destacaremos las principales iniciativas que tres firmas israelíes bien establecidas están tomando en 2022. Los flujos de ingresos geográficamente diversificados de estas empresas podrían convertirse en una ventaja en el entorno actual a medida que aumenta la demanda global.

### Check Point: un giro para enfocarse en los ataques de la generación V

Fundada en 1993, Check Point es una de las empresas tecnológicas más influyentes de Israel. Check Point confirmó su reputación al convertirse en una pionera en tecnología de firewalls, y para 1996 controlaba una participación del 40 % en el mercado mundial de firewalls.<sup>25</sup> A principios de este año, Check Point reveló sus planes de un cambio de estrategia en 2022. La estrategia enfatiza las crecientes amenazas que representan los ataques de la generación V, que son ataques multivectores a gran escala que pueden infectar rápidamente una gran cantidad de objetivos en todas las regiones geográficas.<sup>26</sup> Check Point considera que la tecnología de IA es una herramienta crucial para contrarrestar los ataques de la generación V y cree que su asociación con el fabricante de chips Nvidia la posiciona bien para usar tecnología de IA de vanguardia para frustrar estas amenazas.<sup>27</sup>

### CyberArk: un cambio al servicio basado en suscripción casi completo

CyberArk se fundó en 1999 con una solución para el problema de que los administradores de TI tuvieran acceso a todos los datos de una red sin una estructura sólida para supervisarlos.<sup>28</sup> El concepto de gestión de acceso privilegiado (PAM) fue la base sobre la que se construyó CyberArk, y sigue siendo integral para las operaciones de la compañía en la actualidad. Uno de los logros más notables de CyberArk fue su lanzamiento en 2016 de la Alianza C3, que ahora cuenta con más de 100 miembros, incluidos Amazon Web Services, McAfee y Check Point.<sup>29</sup> Los miembros de la alianza trabajan juntos para implementar soluciones de cuentas privilegiadas.

En los últimos años, CyberArk, una de las empresas de ciberseguridad israelíes más grandes con una capitalización de mercado de 6.400 millones de USD a abril de 2022, ha estado cambiando su modelo de negocio de licencias de software perpetuas a servicios basados en suscripción.<sup>30</sup> El modelo de servicio basado en suscripción transfiere de manera efectiva la carga de la infraestructura cibernética de los clientes a CyberArk, y esa podría ser una solución muy necesaria a medida que aumenta la demanda de servicios de ciberseguridad a pesar de la escasez de trabajadores calificados en el campo. CyberArk tiene como objetivo completar su transición a una combinación de suscripción y reservas del 85 % para el segundo trimestre de 2022.<sup>31</sup> Al final del cuarto trimestre de 2021, su combinación de suscripción y reservas fue del 71 %, en comparación con el 35 % en el cuarto trimestre de 2020.<sup>32</sup>

### Radware: las iniciativas para impulsar la seguridad en la nube comienzan a materializarse

Radware se ha convertido en un proveedor líder de seguridad para centros de datos desde su fundación en 1997. En 2022, el enfoque de Radware son las oportunidades rápidamente emergentes en la seguridad en la nube. La estrategia de la compañía incluye adquirir la empresa SecurityDAM, un proveedor de servicios de protección de denegación de servicio distribuido (DDoS). Radware también está estableciendo centros de investigación y desarrollo de seguridad en la nube en India, ampliando la capacidad de servicio en la nube de su red de entrega global y agregando centros en la nube en las principales ciudades de todo el mundo.<sup>33</sup> El lanzamiento de la plataforma de seguridad en la nube de Radware, SecurePath, también es una pieza clave de la estrategia de la empresa para 2022.<sup>34</sup>

### DESGLASE GEOGRÁFICO DE LOS INGRESOS: TRES REGIONES PRINCIPALES

Fuentes: Global X ETFs con información derivada de: Bloomberg, L.P. (n.d.) Análisis financiero (FA) de Check Point, CyberArk y Radware [Conjunto de datos]. Recuperado el 9 de mayo de 2022 de la terminal de Bloomberg de Global X.

	1	2	3
Check Point	Europa, Medio Oriente y África (EMEA): 45,3 %	América: 42,6 %	Asia Pacífico y Japón: 12,1 %
CyberArk	Estados Unidos: 50,5 %	EMEA: 23,9 %	Reino Unido: 7,1 %
Radware	América: 44,9 %	EMEA: 34,3 %	Asia Pacífico: 20,7 %



## Conclusión

La industria de la ciberseguridad de Israel obtuvo ganancias significativas en 2021, lo que aumentó su fortaleza. En nuestra opinión, la industria está bien posicionada para solidificarse y acrecentar esas ganancias en 2022. Si bien una nueva cohorte de unicornios trabaja con una cantidad récord de fondos recaudados en 2021, las empresas israelíes bien establecidas se están reajustando al panorama cambiante en 2022. Creemos que los inversionistas pueden encontrar oportunidades atractivas para capturar el crecimiento en una industria global que es fundamental para proteger la información más importante que poseen los gobiernos y las empresas. Y pueden encontrar muchas de esas oportunidades en Israel.

## Notas al pie

1. Dirección Cibernética Nacional de Israel. (20 de enero de 2022). *Israeli cyber security industry continued to grow in 2021: Record of \$8.8 billion raised*. Gov.il. [https://www.gov.il/en/departments/news/2021cyber\\_industry](https://www.gov.il/en/departments/news/2021cyber_industry)
2. Ibid.
3. Hatuka, T., y Carmel, E. (enero de 2021). *The dynamics of the largest cybersecurity industrial clusters: San Francisco Bay Area, Washington, D.C. and Israel*. Universidad de Tel Aviv. doi:10.13140/RG.2.2.11371.16169
4. Ibid.
5. Ibid.
6. Estrin, D. (4 de abril de 2017). In Israel, teaching kids cyber skills is a national mission. *AP News*. <https://apnews.com/article/e477309a4a1e407ca4ae6568d3035625>
7. Cyber Education Center. (n.d.) *About us*. Consultado el 18 de mayo de 2022 desde <https://cyber.org.il/about-us- eng/>
8. Sava, J. A. (21 de febrero de 2022). *Active cybersecurity companies in Israel 2011-2021*. Statista. <https://www.statista.com/statistics/1003442/israel-cyber-security-companies/>
9. Bloomberg, L.P. (n.d.) *Security description (DES) of CyberArk and Check Point* [Conjunto de datos]. Recuperado el 28 de abril de 2022 de la terminal de Bloomberg de Global X.
10. Miller, J., y el Equipo de Investigación de Amenazas de Proofpoint. (30 de marzo de 2021). *BadBlood: TA453 targets US and Israeli medical research personnel in credential phishing campaigns*. Proofpoint. <https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential>
11. Personal de TOI. (18 de octubre de 2021). Top cyber official: Hospital attack 'purely financial', likely by Chinese group. *The Times of Israel*. <https://www.timesofisrael.com/top-cyber-official-hospital-attack-purely-financial-likely-by-chinese-group/>
12. Center for Strategic & International Studies. (2022). *Significant cyber incidents*. <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>
13. Kirchgaessner, S., Lewis, P., Pegg, D., Cutler, S., Lakhani, N. y Safi, M. (18 de julio de 2021). Revealed: Leak uncovers global abuse of cyber-surveillance weapon. *The Guardian*. <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-vigilancia-arma-nso-grupo-pegasus>
14. Dirección Cibernética Nacional de Israel. (20 de enero de 2022). *Israeli cyber security industry continued to grow in 2021: Record of \$8.8 billion raised*. Gov.il. [https://www.gov.il/en/departments/news/2021cyber\\_industry](https://www.gov.il/en/departments/news/2021cyber_industry)
15. Ibid.



16. Wiseman, Y. (4 de enero de 2022). Israel's cybersecurity startups post another record year in 2021. *TechCrunch+*. <https://techcrunch.com/2022/01/04/israels-cybersecurity-startups-post-another-record-year-in-2021/>
17. Equipos colaboradores. (octubre de 2021). *Microsoft digital defense report*. Microsoft. <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>
18. Baksh, M. (28 de marzo de 2022). The administration expects CISA to grow by just under 300 full-time employees over the next year, for example. *Nextgov*. <https://www.nextgov.com/cybersecurity/2022/03/6-takeaways-cybersecurity-policy-presidents-fy-2023-budget/363713/>
19. Hurst, D. (29 de marzo de 2022). Redspice: Budget ushers in Australia's 'biggest ever' cybersecurity spend. *The Guardian*. <https://www.theguardian.com/australia-news/2022/mar/29/redspice-budget-ushers-in-australias-biggest-ever-cybersecurity-spend>
20. Rosemain, M. (15 de febrero de 2022). France opens new business campus to tackle cyberattacks. *Reuters*. <https://www.reuters.com/world/europe/france-opens-new-business-campus-tackle-cyberattacks-2022-02-15/>
21. Dirección Cibernética Nacional de Israel. (20 de enero de 2022). *Israeli cyber security industry continued to grow in 2021: Record of \$8.8 billion raised Gov.il*. [https://www.gov.il/en/departments/news/2021cyber\\_industry](https://www.gov.il/en/departments/news/2021cyber_industry)
22. Administración de Comercio Internacional. (16 de agosto de 2021). *Cybersecurity*. Departamento de Comercio de los EE. UU. <https://www.trade.gov/country-commercial-guides/australia-cybersecurity>
23. Reuters. (10 de diciembre de 2021). IMF and 10 countries simulate cyberattack on global financial system. *South China Morning Post*. [https://www.scmp.com/news/world/middle-east/article/3159134/imf-and-10-countries-simulate-cyberattack-global-financial?module=perpetual\\_scroll\\_0&pgtype=article&campaign=3159134](https://www.scmp.com/news/world/middle-east/article/3159134/imf-and-10-countries-simulate-cyberattack-global-financial?module=perpetual_scroll_0&pgtype=article&campaign=3159134)
24. Departamento de Seguridad Nacional de los EE. UU. (3 de marzo de 2022). *DHS to increase security cooperation with Israel through new arrangements* [Comunicado de prensa]. <https://www.dhs.gov/news/2022/03/03/dhs-increase-security-cooperation-israel-through-new-arrangements>
25. CompaniesHistory.com. (2022). *Historia, perfil y video corporativo de Check Point Software Technologies Ltd*. Consultado el 18 de mayo de 2022 desde <https://www.companieshistory.com/check-point-software/>
26. Check Point. (2022). *Gen-V cyber security: Strategic insights from past generations of threats*. <https://www.checkpoint.com/pages/gen-v-cyber-security/#>
27. Check Point. (4 de febrero de 2022). *Check Point Software introduces new strategic direction at annual CPX 360 event and unveils the world's fastest firewall* [Comunicado de prensa]. <https://www.checkpoint.com/press/2022/check-point-software-introduces-new-strategic-direction-at-annual-cpx-360-event-and-unveils-the-worlds-fastest-firewall/>
28. Kroll, S. T. (17 de junio de 2019). CyberArk: 20 years of privileged access security leadership, and counting. *Cybercrime Magazine*. <https://cybersecurityventures.com/cyberark-30-years-of-privileged-access-security-leadership-and-counting/>
29. CyberArk Software Ltd. (2022). *CyberArk C3 alliance program overview*. <https://www.cyberark.com/resources/product-datasheets/cyberark-c3-alliance-overview>
30. Bloomberg, L.P. (n.d.) *Security description (DES) of CyberArk* [Conjunto de datos]. Recuperado el 28 de abril de 2022 de la terminal de Bloomberg de Global X.
31. CyberArk. (Febrero de 2022). *Investor relations presentation*. [https://s22.q4cdn.com/395203516/files/doc\\_financials/2021/q4/CYBR-Q4-2021-Earnings-Presentation-vFinal.pdf](https://s22.q4cdn.com/395203516/files/doc_financials/2021/q4/CYBR-Q4-2021-Earnings-Presentation-vFinal.pdf)
32. Ibid.



33. Radware. (17 de febrero de 2022). *Radware announces a strategic initiative to accelerate the growth of its cloud security services business* [Comunicado de prensa]. <https://www.radware.com/newsevents/pressreleases/2022/radware-announces-strategic-initiative/>
34. Radware. (2022). Application protection as a service. <https://www.radware.com/solutions/application-protection-service/>

---

Invertir implica riesgos, incluida la posible pérdida de capital. Las inversiones internacionales pueden implicar el riesgo de pérdida de capital por fluctuaciones desfavorables en los valores de las monedas, por diferencias en los principios contables generalmente aceptados o por inestabilidad económica o política en otras naciones.

**Considere cuidadosamente los objetivos de inversión, riesgos, cargos y gastos de los fondos. Esta y otra información pueden encontrarse en los prospectos completos o resumidos de los fondos, que pueden obtenerse en [globalxetfs.com](https://globalxetfs.com). Lea el prospecto detenidamente antes de invertir.**

Global X Management Company LLC se desempeña como asesor de Global X Funds. Los fondos son distribuidos por SEI Investments Distribution Co. (SIDCO), que no está afiliada a Global X Management Company LLC ni a Mirae Asset Global Investments. Los fondos de Global X no son patrocinados, avalados, emitidos, vendidos ni promovidos por Indxx, ni Indxx realiza ninguna declaración con respecto a la conveniencia de invertir en los fondos de Global X. Ni SIDCO, ni Global X ni Mirae Asset Global Investments están afiliados a Indxx.

