INVESTIGACIÓN DE GLOBAL X ETFs

Se prevé que la pandemia de ciberseguridad continúe en 2022

Autores:

Pedro Palandrani y Alec Lucas

Fecha: 24 de enero de 2022
Tema: Temática

Esperamos que el juego del gato y el ratón entre las organizaciones, los consumidores y los ciberdelincuentes que codician sus datos se intensifique este año. La última preocupación es una vulnerabilidad en el software de Internet conocido como Log4j, que podría poner en riesgo cientos de millones de sistemas en todo el mundo. Esta amenaza se suma a otras múltiples filtraciones de datos de alto perfil ocurridos en 2021, incluido el ataque de *ransomware* que puso en riesgo la distribución de combustible de Colonial Pipeline en el este de los EE. UU. Este tipo de ciberataques son cada vez más frecuentes y costosos, especialmente los ataques a infraestructuras y cadenas de suministro críticas. Y el nivel de amenaza no hará más que intensificarse a medida que la economía mundial siga transformándose en una economía en línea y se pongan en riesgo los datos sensibles. Como resultado, es previsible que haya una mayor concientización y un mayor gasto en ciberseguridad para crear vientos de cola a largo plazo para la ciberseguridad.

Aspectos clave:

- En 2021 hubo muchos y costosos ciberataques, una tendencia que probablemente se mantenga en 2022. El costo medio de una filtración de datos pasó de 3,86 millones de USD en 2020 a 4,24 millones de USD en 2021, lo que supone el costo total más alto en los 17 años que IBM ha publicado su *Cost of a Data Breach Report 2021* (Informe 2021 del costo de filtración de datos).[i]

- Las empresas, el Gobierno y los consumidores están aumentando sus compromisos en ciberseguridad, mientras que los consumidores también están tomando medidas para protegerse. Por ejemplo, se prevé que las empresas gasten 172.000 millones de USD en 2022.[ii]

- La seguridad de identidades, la red y los puntos de conexión (*endpoint*) sigue siendo un foco de atención para los esfuerzos de ciberseguridad; se prevé que la seguridad tenga el mayor crecimiento: 24 % entre 2021 y 2026.[iii]

El mundo digital muestra sus vulnerabilidades en 2021

El mundo ahora crea unos 2,5 quintillones de bytes de datos cada día, es decir, 2,5 seguidos de 18 ceros.[iv] Como resultado, los hackers tienen más puntos de entrada que nunca a datos sensibles, y tendrán muchas más oportunidades a medida que el mundo siga digitalizándose y los volúmenes de datos sigan en aumento. En particular, los dispositivos del Internet de las cosas (IdC o IoT) serán un importante contribuyente al conjunto de datos. A finales de 2021, había 14.600 millones de dispositivos conectados.[v] En 2022, esa cifra podría crecer casi un 18 % y más que duplicarse para 2027.[vi]

El giro de la economía hacia el trabajo remoto también crea importantes oportunidades para los ciberdelincuentes. Los confinamientos inducidos por la pandemia se redujeron en EE. UU. en 2021, pero hasta un 45 % de los empleados a tiempo completo siguieron trabajando en forma remota al menos parcialmente.[vii] Ya sea debido a las nuevas variantes o a la preferencia de los empleados, es probable que las iniciativas para el trabajo remoto sigan intactas, lo que da lugar a vulnerabilidades de datos para el futuro previsible. Según un informe de IBM, el trabajo remoto fue un factor en el 17,5 % de las filtraciones de datos notificadas en 2021.[viii] El costo promedio de estas filtraciones también fue un 16,6 % superior al de las filtraciones en las que el trabajo remoto no fue un factor.[ix]

En 2021, varias empresas de alto perfil fueron víctimas de costosos ciberataques. El ataque de *ransomware* a Colonial Pipeline terminó en un pago de 4 millones de USD a sus atacantes.[x] CNA Financial pagó a los hackers de *ransomware* 40 millones de USD para descifrar partes de su infraestructura digital de la que bloquearon a la empresa.[xi] Y JBS, el mayor productor de carne del mundo, cerró varias de sus plantas debido a un ciberataque.[xii] Estos son solo algunos ejemplos de los principales ataques que sufrieron las empresas el año pasado, lo que a veces terminó en pérdidas multimillonarias.

Principales ciberataques de 2021	Sector	Fecha	Millones de USD pagados o exigidos
Microsoft Exchange	Tecnología	5-ene-21	50*
Kia Motors	Automotriz	13-feb-21	20*
Bombardier	Fabricación (aviación)	23-feb-21	
CNA Financial	Servicios financieros	21-mar-21	40
Harris Federation	Educación	29-mar-21	8*
Colonial Pipeline	Energía	7-may-21	4,4
Brenntag	Productos químicos	11-may-21	4,4
JBS	Alimentos	30-may-21	11
Kaseya	Tecnología de la información	2-jul-21	70*
Accenture	Tecnología	12-ago-21	50*
Acer	Tecnología	5-oct-21	50*

**Exigido pero no pagado en su totalidad.*

Los ataques recientes impulsan el gasto en ciberseguridad

Incluso las soluciones más sofisticadas pueden no ser capaces de eliminar todas las vulnerabilidades, pero pueden obstaculizar muchas amenazas y proteger contra los peores desenlaces. En 2021, las empresas, el Gobierno de EE. UU. y los consumidores demostraron haber tomado mayor conciencia de las ciberamenazas y compromiso con las medidas preventivas.

- **Empresas:** Las víctimas de ataques de *ransomware*, sus proveedores, clientes y competidores son conscientes de lo que pueden ocasionar las filtraciones de seguridad. El costo de los daños a menudo supera el costo de la inversión en soluciones adecuadas. Las grandes empresas normalmente gastan entre 2 y 5 millones de USD en ciberseguridad al año, mientras que una sola filtración de *ransomware* cuesta a las empresas 4,62 millones de USD en promedio.[xiii,xiv] Ese costo es una de los motivos por los que, en una encuesta reciente realizada a más de 3000 ejecutivos, el 69 % de los encuestados previeron un incremento del gasto en ciberseguridad para 2022.[xv] Según una estimación, el gasto en protección de datos y gestión de riesgos podría llegar a 172 millones de USD en 2022, lo que supone un aumento del 11 % con respecto al gasto de 2021.[xvi]

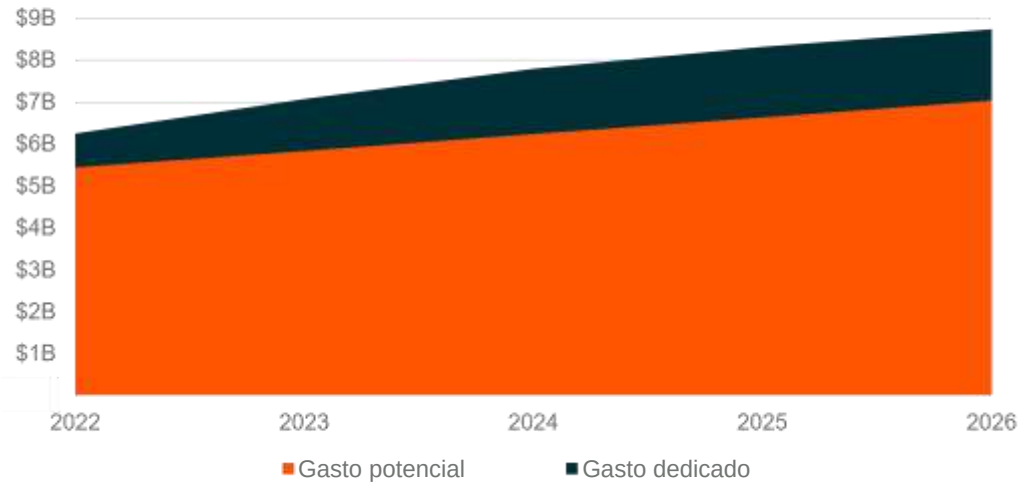
- **Gobiernos:** En mayo de 2021, el presidente Biden firmó una orden ejecutiva que tiene como objetivo modernizar las capacidades de ciberseguridad federal, estandarizar las estrategias de respuesta a los ciberataques y aumentar los requisitos de intercambio de información para los contratistas gubernamentales. En julio, Biden firmó un memorando de seguridad nacional cuyo objetivo es prevenir los ciberataques en infraestructuras críticas, especialmente en electricidad, agua y transporte. Estas medidas se tradujeron en dólares reales en la Ley de Inversión y Empleos en Infraestructura, que destina 1700 millones de USD en gastos dedicados y alrededor de 7000 millones en gastos potenciales para mejorar la ciberseguridad del país.[xvii]

  Además, el año pasado, el Senado confirmó unánimemente al primer director nacional en materia de ciberseguridad de la Casa Blanca. El Congreso creó este cargo en el marco de la Ley de Autorización de Defensa Nacional de 2021, lo que señala un mayor énfasis en la ciberseguridad en las administraciones futuras.

  .

EN VIRTUD DEL RECIENTE PROYECTO DE LEY DE INFRAESTRUCTURA DE EE. UU. SE PODRÁN DESTINAR CASI 9000 MILLONES DE USD A LA CIBERSEGURIDAD

GASTO DEDICADO Y POTENCIAL EN CIBERSEGURIDAD AUTORIZADO POR LA LEY



Fuente: 117.º Congreso (2021-2022), "H.R. 3684 – Infrastructure Investment and Jobs Act", junio de 2021.; Global X Analysis.

- **Consumidores:** Una pequeña pero creciente porción del gasto en ciberseguridad proviene de los consumidores. Alrededor del 53 % de los consumidores son víctimas de al menos un ciberdelito, lo que incita a muchos a tomar precauciones como VPN personales, autenticación de dos factores y servicios de protección frente al robo de identidad.[xviii] La pandemia intensificó las amenazas, ya que los estafadores envalentonados se aprovecharon de la cantidad de tiempo que los consumidores se pasaban en Internet. Los estadounidenses perdieron 586 millones de USD en fraudes relacionados con la COVID en octubre de 2021.[xix] Sin embargo, los consumidores son conscientes de la creciente amenaza. El año pasado, casi el 40 % de los adultos tomaron medidas para salvaguardar su actividad en Internet como resultado directo de la pandemia.[xx] Los hábitos de protección digital aprendidos durante la pandemia podrían acelerar la adopción de servicios de ciberseguridad por parte de los consumidores.

Principales áreas de ciberseguridad a proteger

- **Seguridad de identidad:** Con la explosión del trabajo remoto, proteger quién accede a los datos, recursos y aplicaciones críticos es imprescindible para las organizaciones. Dentro de este segmento, los subsegmentos de ciberseguridad incluyen la gestión de las identidades y el acceso (*Identity and Access Management*, IAM), la gestión de las cuentas privilegiadas (*Privileged Account Management*, PAM) y la gobernanza y administración de las identidades (*Identity Governance & Administration*, IGA). Se prevé que estos subsegmentos crezcan a una tasa de crecimiento anual compuesta (TCAC) promedio del 19 % entre 2021 y 2026.[xxi]

- **Seguridad de la red:** Las empresas en este mercado vertical son responsables de proteger la integridad, confidencialidad y accesibilidad de una red frente a usos indebidos o filtraciones. Las redes excesivamente permisivas pueden hacer que los ciberataques se muevan horizontalmente (es decir, de un usuario a otro) una vez que una persona se ha visto comprometida. Zero Trust Networks, por ejemplo, proporciona a los usuarios acceso a aplicaciones internas, sin necesidad de conectarse a la red de una empresa o exponer a esos usuarios a Internet. Dentro de este segmento, los subsegmentos de ciberseguridad incluyen las redes de confianza cero (*Zero Trust Network Access*, ZTNA), redes de área extensa definida por software (*Software-Defined Wide Area Network*, SD-WAN), detección y respuesta de los puntos finales (*Network Detection and Response*, NDR), los cortafuegos (Firewall/NGFW), la gestión unificada de amenazas (*Unified Threat Management*, UTM) y las arquitecturas *Secure Access Secure Edge* (SASE). Se prevé que estos subsegmentos crezcan a una TCAC promedio del 24 % entre 2021 y 2026.[xxii]

- **Seguridad de los puntos de conexión:** La multiplicidad de dispositivos conectados a Internet presenta nuevos puntos de entrada para los *hackers*, lo que añade desafíos y complejidad para gestionar de forma eficaz la seguridad de las empresas y las personas. Las implementaciones exitosas del IdC requerirán seguridad multicapa y de extremo a extremo que van desde requisitos de seguridad incorporados de ante mano hasta la administración y protección continua de datos confidenciales generados automáticamente. Dentro de este segmento, los subsegmentos de ciberseguridad incluyen las plataformas de protección de los puntos de conexión (*Endpoint Protection Platform, EPP*), la detección y respuesta de puntos de entrada (*Endpoint Protection and Response, EDR*) y la prevención de pérdida de datos (*Data Loss Prevention, DLP*). En general, se prevé que el segmento de la seguridad de los puntos de conexión crezca un 8 % de TCAC entre 2021 y 2026.[xxiii]

Más allá de estas áreas clave, las empresas de ciberseguridad están buscando cada vez más consolidarse. Normalmente, los proveedores de ciberseguridad se especializan en una selección limitada de productos, lo que obliga a los clientes a proteger sus datos por medio de un abanico de diferentes proveedores. Esta dinámica conduce a costosos retrasos y otras ineficiencias potencialmente dañinas; de hecho, la filtración de datos promedio tardó 287 días en identificarse y contenerse en 2021.[xxiv] En un esfuerzo por mejorar las capacidades de protección de extremo a extremo, varios proveedores de ciberseguridad destacados participaron en fusiones y adquisiciones en 2021. La actividad destacable incluyó la adquisición por parte de CrowdStrike Holdings de 352 millones de USD de Humio y la adquisición por parte de Rapid7 de 335 millones de USD de IntSights, lo que permitió a la empresa ofrecer un producto integrado de detección y corrección de amenazas.[xxv, xxvi] Este aumento en la actividad de consolidación probablemente continúe en 2022, con los proveedores de antivirus y servicios VPN Norton y Avast dispuestos a fusionarse en un acuerdo valuado en más de 8000 millones de USD.[xxvii]

Conclusión

En 2021 fuimos testigo de algunas de las ciberintrusiones más impactantes de las que se tenga recuerdo, y la constante transformación digital del mundo no hace más que aumentar la

probabilidad de ataques comparables en el futuro. No obstante, creemos que las lecciones aprendidas durante este tiempo podrían acelerar aún más la adopción de servicios de ciberseguridad. En nuestra opinión, los recientes compromisos financieros para frustrar a los ciberdelincuentes pueden ser factores favorables para las empresas de ciberseguridad en 2022 y fortalecer el argumento a favor de invertir a largo plazo en el tema de la ciberseguridad en general.

[i] IBM, ""Cost of a Data Breach Report 2021", julio de 2021.
[ii] Soffid, "Cybersecurity Trends for 2022, December 29", 2021.
[iii] Indicador calculado a partir de las TCAC promedio de las siguientes fuentes: Markets and Markets, "Zero Trust Security Market by Solution Type (Data Security, Endpoint Security, API Security, Security Analytics, Security Policy Management), Deployment Type, Authentication Type, Organization Size, Vertical, and Region - Global Forecast to 2026", febrero de 2021; Research and Markets, "SD-WAN - Global Market Trajectory & Analytics", abril de 2021; Market Growth Reports, "Global Network Detection and Response (NDR) Market Growth (Status and Outlook) 2021-2026", julio de 2021; Expert Market Research, "Global Unified Threat Management Market: By Component: Hardware, Software, Virtual; By Service: Consulting, Support & Maintenance, Managed UTM; By Deployment Mode; By Company Size; Regional Analysis; Historical Market and Forecast (2017-2027); Market Dynamics; Competitive Landscape; Industry Events and Developments", 2021; Markets and Markets, "Secure Access Service Edge (SASE) Market with COVID-19 Impact Analysis, by Offering (Network as a Service and Security as a Service), Organization Size (SMEs and Large Enterprises), Vertical, and Region - Global Forecast to 2026", agosto de 2021; Global X Analysis.
[iv] CloudTweaks, "Infographic: How Much Data is Produced Every Day?", consultado el 15 de noviembre de 2021.
[v] Ericsson Mobility Visualizer, "Connected Devices", consultado el 15 de noviembre de 2021.
[vi]. Ibid.
[vii] Gallup, "Remote Work Persisting and Trending Permanent", 13 de octubre de 2021.
[viii] IBM, (n1).
[ix] IBM, (n1).
[x] CNBC, "Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate", 8 de junio de 2021.
[xi] Bloomberg, "CNA Financial Paid $40 Million in Ransom After March Cyberattack", 20 de mayo de 2021.
[xii] CNBC, "Meat supplier JBS paid ransomware hackers $11 million", 9 de junio de 2021.
[xiii] PCH Technologies, "Cost of Cyber Attacks vs. Cost of Cyber Security in 2021", 7 de julio de 2021.
https://pchtechnologies.com/cost-of-cyber-attacks-vs-cost-of-cyber-security-in-2021/
[xiv] IBM, "Cost of a Data Breach Report 2021", julio de 2021.
[xv] PwC, "Global Digital Trust Insights 2022", octubre de 2021.
https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html#findings
[xvi] Gartner, "Gartner IT Symposium/Xpo Americas", octubre de 2021.
https://www.soffid.com/cybersecurity-trends-for-2022/
[xvii] Infrastructure Investment and Jobs Act, H.R. 3684, 117th Cong. 2021.

[xviii] Norton, “2021 Norton Cyber Safety Insights Report Global Results”, mayo de 2021.
[xix] CNBC, “Covid-related scams have bilked Americans out of $586 million”, 18 de octubre de 2021.
[xx] Norton, “2021 Norton Cyber Safety Insights Report Global Results”, mayo de 2021.
[xxi] Indicador calculado a partir de las TCAC promedio de las siguientes fuentes: Technavio, “Privileged Access Management Solutions Market by Deployment and Geography - Forecast and Analysis 2022-2026”, enero de 2022; Mordor Intelligence, “Identity Governance And Administration Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027)”, enero de 2022; Technavio, “Consumer Identity and Access Management (IAM) Market by Deployment and Geography - Forecast and Analysis 2022-2026”, diciembre de 2021.
[xxii] Indicador calculado a partir de las TCAC promedio de las siguientes fuentes: Markets and Markets, “Zero Trust Security Market by Solution Type (Data Security, Endpoint Security, API Security, Security Analytics, Security Policy Management), Deployment Type, Authentication Type, Organization Size, Vertical, and Region - Global Forecast to 2026”, febrero de 2021; Research and Markets, “SD-WAN - Global Market Trajectory & Analytics”, abril de 2021; Market Growth Reports, “Global Network Detection and Response (NDR) Market Growth (Status and Outlook) 2021-2026”, julio de 2021; Expert Market Research, “Global Unified Threat Management Market: By Component: Hardware, Software, Virtual; By Service: Consulting, Support & Maintenance, Managed UTM; By Deployment Mode; By Company Size; Regional Analysis; Historical Market and Forecast (2017-2027); Market Dynamics; Competitive Landscape; Industry Events and Developments”, 2021; Markets and Markets, “Secure Access Service Edge (SASE) Market with COVID-19 Impact Analysis, by Offering (Network as a Service and Security as a Service), Organization Size (SMEs and Large Enterprises), Vertical, and Region - Global Forecast to 2026”, agosto de 2021; Global X Analysis.
[xxiii] Mordor Intelligence, “Endpoint Security Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027)”, enero de 2022.
[xxiv] IBM, (n1).
[xxv] Crowdstrike, “CrowdStrike Completes Acquisition of Humio”, 5 de marzo de 2021.
[xxvi] VentureBeat, “Rapid7 acquires threat intelligence platform IntSights for $335M”, 19 de julio de 2021.
[xxvii] Norton, “NortonLifeLock and Avast to Merge to Lead the Transformation of Consumer Cyber Safety”, 10 de agosto de 2021.