

El futuro es ahora: inversión en ciberseguridad

- IA generativa, tensiones geopolíticas, teletrabajo dan soporte a esta temática
- Adopción ya sugiere que es de uso básico para empresas
- Aumento costo ciberataques

La ciberseguridad es la práctica de proteger los sistemas críticos e información confidencial y sensible de los ataques cibernéticos. La creciente dependencia de la tecnología y digitalización de la sociedad en el siglo XXI hace imprescindible tomar medidas para combatir las amenazas en los sistemas y aplicaciones en la red.

Dentro de las amenazas comunes que busca frenar la ciberseguridad se encuentran:

- **Malware:** software malicioso que brinda acceso no autorizado o causa daños a una computadora.
- **Secuestro de datos (ransomware):** malware que bloquea archivos, datos o sistemas, y amenaza con destruir o hacer públicos los datos.
- **Phishing/ ingeniería social:** engaña a los usuarios para que proporcionen información de identificación personal (PII) o confidencial.

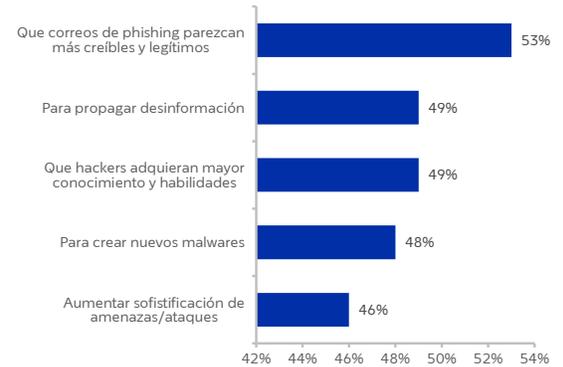
¿POR QUÉ LA CIBERSEGURIDAD AHORA?

El *boom* de la inteligencia artificial generativa ha revolucionado el mundo digital. La aparición de ChatGPT significó nuevos desafíos para la industria de ciberseguridad. Según una encuesta de Blackberry de comienzos de 2023, ChatGPT podría ser usada por hackers para mejorar sus ataques en línea. Un ejemplo de esto es que los correos de phishing parezcan más creíbles y legítimos (gráfico 1). La complejidad creciente de los ciberataques, además de ser un desafío incrementa la demanda por ciberseguridad.

El aumento de las tensiones geopolíticas ha llevado a un aumento en los ciberataques, acrecentando las necesidades por servicios de ciberseguridad. A nivel mundial el volumen de los ataques cibernéticos en 2022 creció 38% anual, no obstante, los dirigidos a los países de la OTAN se expandieron un 300% frente a 2021. Detrás de estos ataques surge como principal sospechoso Rusia, quien también sería responsable de la ola de ciberataques que ha sufrido Suecia después de solicitar unirse a la OTAN.

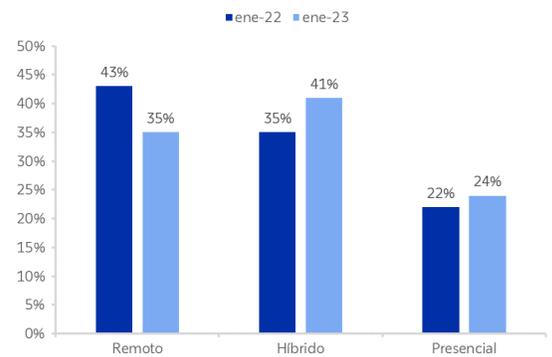
A su vez, la pandemia nos llevó a adoptar el teletrabajo de manera generalizada, de forma tal que firmas de distintas industrias han optado por seguir con una modalidad remota o híbrida (Gráfico 2). Estas modalidades permiten que la

GRÁFICO 1. POSIBLES USOS DE CHATGPT EN CIBERCRIMEN
% de encuestados



Fuente: Blackberry, enero 2023

GRÁFICO 2. EE.UU.: TRABAJADORES SEGÚN RÉGIMEN LABORAL
%



Fuente: PEW Research Center

GRÁFICO 3. CURVA S DE ADOPCIÓN



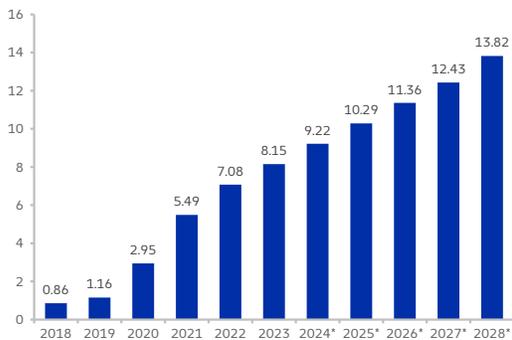
Fuente: Global X

GRÁFICO 4. TAMAÑO DE MERCADO DE CIBERSEGURIDAD GLOBAL
USD billion



Fuente: Next Move Strategy Consulting

GRÁFICO 5: COSTO ESTIMADO DEL CIBERCRIMEN
USD trillion



Fuente: Statista

conexión se realice a través de redes domésticas o públicas, aumentando la superficie de ataque para los ciberdelincuentes. Por lo tanto, esto lleva a las compañías a evaluar políticas de ciberseguridad más complejas con softwares que superen la mayor vulnerabilidad de la conexión a redes públicas.

Diversos gobiernos han instaurado medidas para mejorar el resguardo tecnológico, lo que da un soporte adicional a la industria de ciberseguridad. Un claro ejemplo es la nueva ley de ciberseguridad de la Unión Europea que refuerza a la agencia para la ciberseguridad, además de establecer un marco de certificación para productos y servicios. Otros gobiernos como el del Reino Unido y EE.UU. han impulsado medidas en pro de la ciberseguridad como CSWP 24 del NIST (criterios recomendados para el etiquetado de ciberseguridad para productos de consumo de Internet de las cosas) y *Data Protection Act* (regula el procesamiento de datos en el Reino Unido).

SERVICIO CLAVE PARA EL FUNCIONAMIENTO EMPRESARIAL

La ciberseguridad se encuentra en fase de mayoría temprana posición en la curva de adopción temática, donde existe un crecimiento absoluto alto, llegando a *peak*, pero que comienza a aplanarse (Gráfico 3). En esa fase, las perspectivas para las ventas también son positivas, ya que tienden a explotar.

Estos niveles de adopción de cierta forma aseguran que la temática no va a desaparecer, ya que la creciente sofisticación de los ciberataques ha llevado a que la contratación de servicios de ciberseguridad sea prácticamente de primera necesidad para las compañías. Así, se proyecta que el crecimiento anual compuesto de la industria a nivel global será de un 14.5% a 2030, estimando que el tamaño de mercado alcance los USD 650 mil millones a fines de esta década (Gráfico 4).

Por último, los ciberataques se han vuelto cada vez más costosos para las compañías, por lo que la demanda por servicios de ciberseguridad crece y añade desafíos adicionales a la industria. Es más, se espera que a 2028 el costo del ciberdelincuencia supere los USD 18 *trillion* (gráfico 5). La creciente demanda por servicios de ciberseguridad que supone este escenario llevaría a que las compañías de la industria alcancen economías de escala de manera de reducir los costos asociados a su implementación.

Cabe mencionar que también existen riesgos a la hora de invertir en la ciberseguridad. Uno de ellos es que las nuevas generaciones no son los grandes impulsores ni usuarios de la temática, por lo que no se ve respaldada por la megatendencia de cambios demográficos. Sin embargo, en la medida que las nuevas generaciones posean información que pueda ser blanco de costosos ciberataques, debieran avanzar en promover y usar servicios de ciberseguridad.

UNA INVERSIÓN CON POTENCIAL

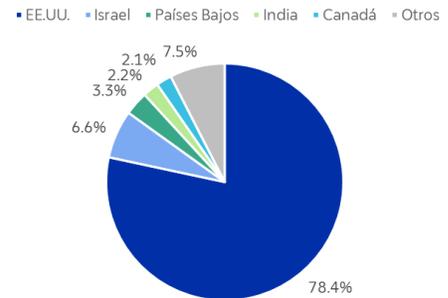
En el mercado, existen índices que agrupan empresas de la temática de ciberseguridad, que sirven de *benchmarks* para ETFs y/o fondos de inversión. Dos de ellos son el índice MSCI Cybersecurity y Nasdaq Cybersecurity. El primero de ellos tiene una exposición más global, pero aun mayoritariamente concentrado en EE.UU. (gráfico 6). Este índice agrupa las acciones de casi 90 empresas ligadas al sector, por lo que sus métricas son capaces de entregar señales respecto del atractivo de invertir en la temática.

En primer lugar, las valorizaciones se encuentran descontadas, transando media desviación estándar bajo su promedio histórico (razón Precio/Utilidad a doce meses), lo que se compara de manera similar con el descuento que muestra el índice MSCI ACWI Innovation que agrupa todas las temáticas. Es más, al comparar las valorizaciones de ciberseguridad con las de todas las temáticas, transan bajo el nivel de su promedio histórico, luciendo atractiva también en términos relativos.

Por el lado de las utilidades, para 2023 se proyecta un crecimiento de ~9% con respecto al año pasado, sobre el crecimiento proyectado para las otras temáticas. Además, esta estimación se ha venido corrigiendo al alza en el último mes, de manera más pronunciada que el resto de las temáticas. A su vez, esta temática también lidera en proyección de crecimiento de ventas para este año, que superaría el 20%. Por otro lado, si bien los flujos de inversión no muestran entradas netas en los últimos meses, el análisis técnico del índice sugiere que, hacia adelante, continuaría la tendencia positiva que ha mostrado en lo que va del año (tabla 1).

Se favorece la inversión en ciberseguridad. Acontecimientos recientes -que no se prevé se disipen en el corto plazo- dan soporte a la creciente adopción de la temática, mientras que las variables de mercado apoyan la tesis de que es un buen momento para invertir en ella.

GRÁFICO 6: COMPOSICIÓN GEOGRÁFICA
ÍNDICE MSCI
Ciberseguridad | %



Fuente: MSCI.

Tabla 1: Retornos - Var. % USD

Índice	MTD	3M	YTD	2022	2021	Volatilidad 1Y
S&P 500	1.9	9.7	18.1	-19.4	26.9	19%
MSCI ACWI Innovation	2.5	14.1	30.3	-35.9	7.1	24%
MSCI Cybersecurity	2.8	10.8	21.2	-28.6	15.9	24%
Nasdaq Cybersecurity	0.8	10.1	18.4	-26.6	19.6	24%

Fuente: Bloomberg, datos al 23 de julio de 2023

Las opiniones contenidas en el presente informe no deben considerarse como una oferta o una solicitud de compra o de venta, de suscripción o rescate, de aporte o retiro de ningún tipo de valores, sino que se publican con un propósito meramente informativo para nuestros clientes. Las proyecciones y estimaciones que se presentan han sido elaboradas por nuestro equipo de trabajo, apoyado en las mejores herramientas disponibles, no obstante, esto no garantiza que ellas se cumplan. La información contenida en este informe no corresponde a objetivos de inversión específicos, situación financiera o necesidades particulares de ningún receptor del mismo. Antes de realizar cualquier transacción de valores, los inversionistas deberán informarse sobre las condiciones de la operación, así como de los derechos, riesgos y responsabilidades implícitos en ella, por lo cual las sociedades de Compass y/o personas relacionadas ("Compass"), no asumen responsabilidad alguna, ya sea directa o indirecta, derivada del uso de las opiniones contenidas en este informe. Cualquier opinión expresada en este material, está sujeta a cambios sin previo aviso de Compass, quienes no asumen la obligación de actualizar la información contenida en él. Compass, sus personas relacionadas, ejecutivos u otros empleados, podrán hacer comentarios de mercado, orales o escritos, o transacciones que reflejen una opinión distinta a aquéllas expresadas en el presente informe.