Comentarios de Mercado
Mayo 2026

Versión en Español

El efecto Mythos: el cibercrimen como servicio

Obtenga orientación sobre inversiones y los principales factores estructurales detrás de los portfolios de sus clientes.

insigneo

Mauricio Viaud
Estratega de Inversión *Senior* y Manager de Portafolio

Andrés Salamanca
Estratega de Inversión

El efecto Mythos: el cibercrimen como servicio

El cibercrimen está transformándose en una industria escalable y automatizada, donde la IA puede identificar y explotar vulnerabilidades en segundos, poniendo un poder ofensivo sin precedentes incluso en manos de no expertos.

Las consecuencias ya no son solo digitales: los ciberataques modernos pueden detener fábricas, interrumpir infraestructura crítica y generar daños en el mundo real con grandes consecuencias económicas.

A medida que este entorno de amenazas se expande, la ciberseguridad evoluciona hacia un ecosistema completo, donde proveedores de software, hardware e infraestructura desempeñan roles críticos en la defensa de la economía digital.

Para los inversionistas, este cambio va mucho más allá de las empresas puras de ciberseguridad, abriendo oportunidades a lo largo de toda la cadena de valor, desde software y hardware de redes hasta centros de datos, infraestructura de telecomunicaciones e incluso los sistemas energéticos necesarios para impulsar todo.

¿Alguna vez has recibido en tu correo un mensaje de un "príncipe" o de un misterioso desconocido multimillonario ofreciéndote una gran herencia a cambio de casi nada? El desarrollo de la humanidad generalmente ha seguido un camino que va del *mythos* al *logos*, de la creencia a la razón. Pero en ciberseguridad, esa trayectoria ahora parece estar revirtiéndose. En este contexto, Anthropic, el principal competidor de OpenAI (creador de ChatGPT), ha presentado recientemente Claude Mythos, un modelo que está obligando a las empresas a replantear lo que antes consideraban "lógico". Considerado ampliamente como el modelo más potente de Anthropic hasta la fecha, Mythos ha demostrado en pruebas la capacidad de identificar y explotar miles de vulnerabilidades de ciberseguridad en cuestión de segundos. Si bien el daño cibernético tradicionalmente se ha asociado con estafas y otras amenazas no físicas, como exploraremos en este documento, modelos como Mythos podrían marcar un punto de inflexión para la sociedad en general.

Si bien la IA nos está obligando a enfrentar escenarios que hace solo unos años habrían parecido distópicos, también está creando oportunidades significativas para los inversionistas. Con esto en mente, este documento se divide en dos partes: la primera describe qué está ocurriendo y por qué es importante, mientras que la segunda examina las empresas que se están posicionando para beneficiarse de este nuevo entorno de "*mythos*" moderno.

Parte 1. "No es si ocurrirá, sino cuándo" – Una serie de preguntas para entender el panorama actual de la ciberseguridad

¿Qué es la ciberseguridad? Según IBM, es la práctica de proteger a las personas, los sistemas y los datos de los ciberataques mediante una combinación de tecnología, procesos y políticas. Aunque las primeras computadoras aparecieron en la década de 1940, la ciberseguridad como concepto suele remontarse al investigador Bob Thomas en 1970. Desde esos inicios, la industria ha crecido hasta convertirse en un mercado global gigante. Para 2025, el gasto en servicios profesionales de seguridad alcanzó aproximadamente USD 61.9 mil millones, mientras que los ingresos por software de ciberseguridad llegaron a cerca de USD 140 mil millones. Cabe destacar que, incluso antes de la aparición de los modelos de frontera de IA, ya se esperaba que la industria creciera a una tasa compuesta anual del 14.3% hasta 2030.

"Con la llegada de modelos avanzados de IA, los ciberataques ya no están limitados a pequeños grupos que intentan robar información, sino que se están convirtiendo en operaciones escalables, automatizadas y cada vez más autónomas."

¿Qué ha cambiado? Con la llegada de modelos avanzados de IA, los ciberataques ya no están limitados a pequeños grupos que intentan robar información, sino que se están convirtiendo en operaciones escalables, automatizadas y cada vez más autónomas. **En términos prácticos, modelos como Mythos pueden orquestar campañas globales de ciberataques.** El Internet Crime Complaint Center (IC3) del FBI recibió más de un millón de denuncias en 2025, con pérdidas reportadas que alcanzaron los USD 21 mil millones, un aumento interanual del 26%. Además, según el informe de tendencias del crimen cibernético de 2025 de SoSafe, aproximadamente el 87% de las empresas a nivel mundial experimentaron un ciberataque impulsado por IA en 2025. **No es si ocurrirá, sino cuándo.**

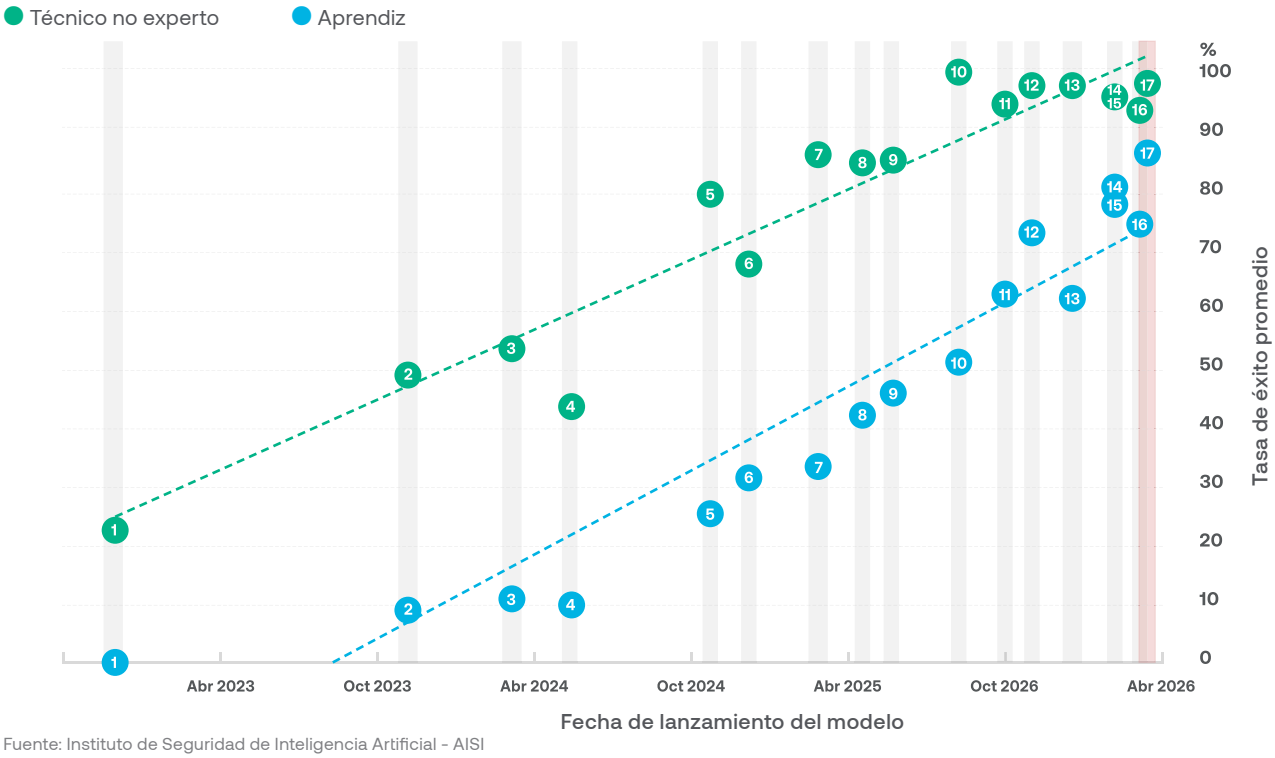
¿Cómo funciona? La IA ya no es solo un asistente de programación que ayuda a escribir o depurar código; es un sistema capaz de escanear, comprender y poner a prueba bases de código completas para descubrir debilidades explotables a gran escala. Los modelos modernos pueden identificar vulnerabilidades conocidas (*exploits*) para aprovechar fallas o identificar vulnerabilidades de día cero, que son errores que aún no han sido corregidos ni divulgados. Al combinar reconocimiento de patrones con razonamiento, estos sistemas pueden mapear superficies, encadenar múltiples debilidades y simular cómo un atacante podría moverse dentro de una red. **El resultado es que se pasó de una investigación de seguridad manual e intensiva en tiempo a un descubrimiento automatizado a gran escala.** En el contexto de modelos como Mythos, esto representa un cambio fundamental: lo

que antes requería a un humano con experiencia altamente especializada ahora puede acelerarse, replicarse y potencialmente desplegarse sobre miles de objetivos simultáneamente, transformando tanto el panorama de amenazas como las estrategias defensivas necesarias para contenerlas.

¿Qué tan bueno es Mythos? Como se muestra en el Gráfico 1, el Instituto de Seguridad de Inteligencia Artificial realizó una prueba tipo Captura la Bandera (CTF por sus siglas en inglés) diseñada para evaluar qué tan eficazmente los modelos podían identificar y explotar vulnerabilidades en un sistema objetivo. En el estudio, Mythos fue comparado con otros 16 modelos, con tareas ejecutadas tanto por aprendices como por técnicos no especializados para medir el desempeño en condiciones realistas de baja especialización. Los aprendices lograron una tasa de éxito promedio cercana al 90%, mientras que los técnicos no especializados alcanzaron casi el 100% de efectividad. En conjunto, estos resultados destacan **la capacidad inusualmente alta de Mythos para permitir la detección y explotación de vulnerabilidades, incluso en manos de usuarios inexperimentados.**

Gráfico 1: Desempeño en desafíos CTF para principiantes por modelo (presupuesto de 2.5 millones de tokens)

1. GPT-3.5 Turbo
2. GPT-4 Turbo
3. Claude 3 Opus
4. GPT-4o
5. Claude 3.5 Sonnet
6. o1
7. Claude 3.7 Sonnet
8. o3
9. Claude 4 Opus
10. GPT-5
11. Claude Sonnet 4.5
12. Claude Opus 4.5
13. Codex 5.2
14. Claude Opus 4.6
15. Codex 5.3
16. GPT-5.4
17. Mythos Preview



Fuente: Instituto de Seguridad de Inteligencia Artificial - AISI

¿Existen diferentes niveles de riesgo? Los sistemas modernos se dividen ampliamente en Tecnología de la Información (IT) y Tecnología Operacional (OT). IT abarca la infraestructura digital tradicional, incluyendo servidores, entornos en la nube, bases de datos y redes corporativas; mientras que OT se refiere a sistemas que controlan procesos físicos mediante dispositivos como Controladores Lógicos Programables (PLC) y plataformas SCADA. Por ejemplo, en una planta automotriz, los sistemas IT gestionan el inventario, la planificación de la producción y los recursos, mientras que los sistemas OT operan la planta, controlando brazos robóticos, estaciones de soldadura y sistemas de pintura.

El perfil de riesgo difiere notablemente entre ambos. Un ciberataque a sistemas IT, aunque disruptivo, a menudo puede contenerse mediante reinicios, reparaciones rápidas de código y recuperación del sistema, con un impacto limitado en la producción física. En cambio, **un ataque a sistemas OT puede detener líneas de producción completas, generando costos significativos por inactividad e incluso riesgos de seguridad para los operadores.** Siemens publicó un estudio titulado "*El verdadero costo del tiempo de inactividad*", donde reportó que el tiempo de inactividad no planificado representó aproximadamente el 11% de los ingresos de las empresas del Fortune 500 global en 2024, equivalente a cerca de USD 1.4 billones en pérdidas. Continuando con el ejemplo del sector automotriz, una sola hora de inactividad no planificada puede costar hasta USD 2.3 millones, es decir, más de USD 600 por segundo.

"la infraestructura OT sustenta sectores críticos de la sociedad, incluyendo generación de energía, exploración de petróleo y gas, plantas de tratamiento de agua, fabricación de medicamentos y sistemas de control de tráfico."

¿Por qué es tan difícil arreglar los sistemas OT? Muchos de estos sistemas tienen décadas de antigüedad y no fueron diseñados para actualizarse con frecuencia. En algunos casos, los proveedores originales ya no existen o han dejado de dar soporte, dejando a los operadores con pocas opciones viables de actualización. Al mismo tiempo, **la infraestructura OT sustenta sectores críticos de la sociedad, incluyendo generación de energía, exploración de petróleo y gas, plantas de tratamiento de agua, fabricación de medicamentos y sistemas de control de tráfico.** Un ejemplo claro de OT heredado es Windows XP: lanzado en 2001 y sin soporte desde 2014, todavía se utiliza en algunos entornos industriales debido a que muchos sistemas SCADA fueron diseñados para ejecutarse sobre él, y reemplazarlos suele requerir una transformación completa de las operaciones en lugar de un simple arreglo.

¿Qué tan grave puede ser un ciberataque? Ejemplos de ciberataques tanto en OT como en IT pueden encontrarse en la historia reciente. En OT, Stuxnet destaca como el primer gran ataque en causar daño físico: un gusano altamente sofisticado descubierto en 2010 atacó la planta nuclear de Natanz en Irán con el fin de interrumpir el enriquecimiento de uranio. Stuxnet se infiltró en sistemas de control industrial mediante múltiples vulnerabilidades de día cero, alterando de forma sutil la velocidad de las centrifugadoras de enriquecimiento al aumentar y disminuir intermitentemente su rotación más allá de

los límites seguros. Esto generó un estrés mecánico excesivo, provocando la falla de un número significativo de centrifugadoras, mientras simultáneamente mostraba lecturas normales falsas a los operadores para evitar su detección. Por el lado de IT, en 2017, el ransomware NotPetya interrumpió la infraestructura portuaria central global al deshabilitar los sistemas digitales necesarios para identificar contenedores, coordinar grúas y gestionar flujos logísticos, obligando a cerrar puertos pese a que el equipo físico seguía operativo. La transportadora Maersk reportó pérdidas de aproximadamente USD 250–300 millones tras detener operaciones portuarias a nivel global, y la Casa Blanca señaló en 2018 que el ataque causó más de USD 10 mil millones en daños globales.

¿Qué sectores enfrentan mayor riesgo? Usualmente aquellos donde **la mayor intensidad de automatización se cruza con la menor capacidad de reparación - conocida en inglés como *patchability*,** tales como energía, manufactura industrial e infraestructura de transporte. El problema central es precisamente ese: la limitada capacidad de actualización. JPM estima que, mientras solo alrededor del 20% de los sistemas IT no se pueden reparar, entre el 40% y el 55% de la base instalada de OT no se puede reparar de ninguna forma - en inglés *unpatchable* -, sin importar los esfuerzos que realicen los operadores.

> “A medida que el cuidado de la salud mejoró y creció, también lo hizo la infraestructura necesaria para apoyar esta industria. Creemos que la ciberseguridad evolucionará de manera similar y requerirá grandes cantidades de inversión y gasto.”

Entonces, ¿cuál es la solución? Combatir IA con IA. En un intento por preparar a las organizaciones para las capacidades de Mythos, Anthropic pausó su lanzamiento y creó Project Glasswing, un programa de acceso controlado que involucra a más de 50 organizaciones, incluyendo grandes empresas tecnológicas y financieras, permitiéndoles usar el modelo para poner a prueba sus sistemas y entrenar modelos defensivos de ciberseguridad. En este contexto, algunos analistas estiman que, para mediados de 2027, alrededor del 85% de los protocolos de detección y respuesta podrían generarse dinámicamente, adaptándose continuamente a amenazas en tiempo real. Este proceso requerirá que las empresas automaticen operaciones de seguridad, adopten arquitecturas de confianza de cero centradas en la identidad, mejoren la confiabilidad de detección y fortalezcan la resiliencia mediante recuperación más rápida y preparación criptográfica. **En la práctica, sin embargo, las empresas aún están lejos de esto. La encuesta de ciberseguridad de Bain & Company de 2025 muestra que las empresas planean aumentar el capex en ciberseguridad alrededor de un 10% anual, muy por debajo del ritmo al que avanzan los modelos de IA de frontera. Esta brecha entre la realidad y la burocracia es donde surgen las oportunidades de inversión.**

Parte 2. Donde el riesgo se convierte en oportunidad

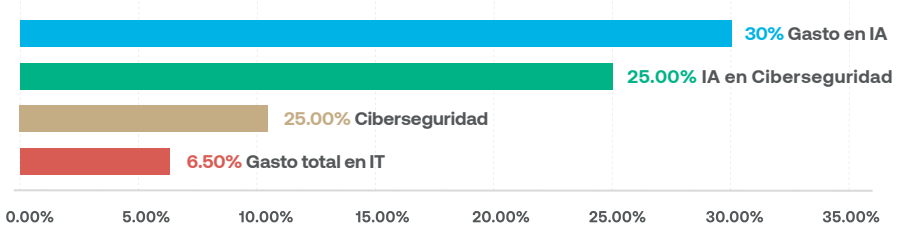
Al igual que en el campo médico, donde la proliferación de enfermedades eventualmente creó un ecosistema complejo de profesionales, maquinaria e infraestructura, lo mismo ocurre en la industria de la ciberseguridad, donde la proliferación de riesgos, especialmente los expuestos por la IA, dará lugar a una industria multifacética. Comparemos el estado actual de la ciberseguridad con el inicio del campo médico estructurado en los siglos XVIII y XIX. En ese entonces, los profesionales eran en su mayoría médicos locales que practicaban medicina general, que trataban desde un resfriado común hasta la amputación de una extremidad. Poco a poco surgieron otras empresas que desarrollaron herramientas y maquinaria para mejorar la eficacia y la eficiencia de la atención médica. A medida que el cuidado de la salud mejoró y creció, también lo hizo la infraestructura necesaria para apoyar esta industria. Creemos que la ciberseguridad evolucionará de manera similar y requerirá grandes cantidades de inversión y gasto. **Entonces, ¿qué empresas se beneficiarán a medida que el sector de la ciberseguridad evolucione de su forma actual? Creemos que tres grupos de la industria serán los principales beneficiarios: software, hardware e infraestructura.**

En 2025, el gasto empresarial anual en ciberseguridad fue de aproximadamente USD 200 mil millones. La firma de análisis Statista estima que para 2030 esta cifra podría alcanzar los USD 265 mil millones anuales. Sin embargo, este número podría resultar conservador. Otros proveedores como Zero-Threat estiman que podría alcanzar los USD 500 mil millones. El Gráfico 2 muestra la tasa de crecimiento anual compuesta del gasto en IT de las empresas globales. Aunque el gasto general en IT continuará creciendo a una tasa de 6.5%, partiendo de una base muy grande de USD 7 billones, una parte significativa del crecimiento del gasto provendrá de la IA y de la ciberseguridad necesaria para proteger esta tecnología.

Los practicantes: las empresas de software de ciberseguridad

El aumento del gasto en ciberseguridad beneficia directamente a los proveedores especializados en software de seguridad que se enfocan en proteger redes, datos e identidades. Empresas como Palo Alto Networks, Fortinet, CrowdStrike y Zscaler podrían beneficiarse a medida que las organizaciones asignen más presupuesto para prevenir brechas y responder a amenazas crecientes como el ransomware y los ataques de estado nacional. Estas compañías ofrecen soluciones críticas, firewalls, protección de *endpoints*,

Gráfico 2: Crecimiento proyectado del gasto empresarial global
(Tasa de crecimiento anual compuesta 2025-2028)



Fuente: Insigneo, Oxford Economics, Grand View Research, SWOT Reports; As of 2025

seguridad en la nube y arquitecturas de confianza cero, que, una vez adoptadas, suelen considerarse no discrecionales. A medida que los riesgos aumentan, los clientes tienden a expandir contratos existentes y añadir más módulos en lugar de cambiar de proveedor, lo que impulsa el crecimiento de los ingresos recurrentes y el poder de fijación de precios.

Las grandes plataformas de software con ofertas de seguridad integradas también podrían beneficiarse significativamente del aumento de la inversión en ciberseguridad. Empresas como Microsoft, Google (Alphabet), Amazon y Oracle incorporan herramientas de seguridad en sus plataformas de nube, productividad, e infraestructura empresarial. A medida que las empresas migran cargas de trabajo a la nube, el gasto en seguridad tiende a concentrarse en los mismos proveedores, favoreciendo a quienes pueden integrar la ciberseguridad dentro de suites más amplias. Esta integración reduce la complejidad para el cliente y convierte la seguridad en un diferenciador estratégico, ayudando a estas compañías a aumentar el ingreso promedio por cliente mientras refuerzan sus ventajas competitivas.

Por último, las empresas de software empresarial y de gestión de identidades pueden ver beneficios indirectos pero significativos a medida que el gasto en ciberseguridad crece. Compañías como Okta, ServiceNow, Splunk y Datadog podrían beneficiarse de la demanda en gobernanza de identidades, monitoreo de seguridad, automatización de cumplimiento y respuesta a incidentes. La ciberseguridad ya no está aislada en el departamento de IT; ahora impacta flujos de trabajo, analítica y gestión de riesgos en toda la empresa. Como resultado, las firmas que ofrecen visibilidad, automatización y acceso seguro se convierten en socios esenciales, posicionándose para capturar crecimiento sostenido a medida que aumentan los presupuestos de ciberseguridad.

Los instrumentos: las empresas de hardware

Así como las empresas de hardware son necesarias para crear las herramientas que hacen posible la IA, también lo son para habilitar la ciberseguridad que protege a la IA y a sus usuarios. En términos generales, el aumento del gasto en ciberseguridad beneficia a las compañías de redes de hardware que proporcionan la infraestructura física necesaria para asegurar los flujos de datos. Empresas como Cisco, Juniper Networks y Arista Networks se benefician a medida que las organizaciones actualizan routers, switches y firewalls de nueva generación para manejar tráfico cifrado, segmentación e inspección avanzada de amenazas. A medida que las amenazas se vuelven más sofisticadas, las organizaciones requieren hardware de mayor rendimiento capaz de realizar inspección profunda de paquetes y analítica en tiempo real, impulsando ciclos de renovación y mayores precios promedio de venta para estos proveedores.

Los fabricantes de herramientas de seguridad también se benefician directamente del aumento en los presupuestos de ciberseguridad. Empresas como Palo Alto Networks, Fortinet, Check Point y Sophos venden dispositivos diseñados específicamente para ubicarse en el perímetro de redes, centros de datos y oficinas. Incluso cuando la seguridad se mueve hacia la nube, muchas industrias reguladas, como finanzas, salud y gobierno, siguen requiriendo soluciones locales o híbridas por razones de cumplimiento y latencia. El aumento del gasto permite desplegar más hardware en distintas ubicaciones y actualizar a modelos de mayor capacidad, lo que respalda la demanda de estos portafolios.

Finalmente, las empresas de semiconductores y hardware especializado se benefician indirectamente a medida que las cargas de trabajo de ciberseguridad se vuelven más intensivas en cómputo.

Compañías como Intel, AMD, NVIDIA y Marvell suministran procesadores, aceleradores, chips de red optimizados para cifrado, detección de amenazas impulsada por IA y redes seguras. A medida que las herramientas de seguridad y los centros de datos requieren mayor capacidad de procesamiento para tareas como autenticación de confianza cero y monitoreo en tiempo real, aumenta la demanda por chips con capacidades de seguridad integradas. Esto convierte el crecimiento de la ciberseguridad en un impulso no solo para los fabricantes de sistemas, sino también para todo el ecosistema de hardware subyacente. Algunas de estas tecnologías ya están en uso; otras deberán evolucionar a medida que la industria avance.

Los hospitales y sistemas de salud: las empresas que proveen la infraestructura de soporte

El aumento del gasto en ciberseguridad no se limita al software y al hardware. Los médicos necesitan hospitales, clínicas y sistemas para ejercer su profesión; lo mismo ocurre con la ciberseguridad. **Este incremento también podría beneficiar a los proveedores de infraestructura digital, particularmente a los operadores de centros de datos, especialistas en infraestructura en la nube y a las empresas de telecomunicaciones.** Compañías como Equinix, Digital Realty, American Tower, Crown Castle y grandes operadores de telecomunicaciones se benefician a medida que las empresas invierten en conectividad segura, resiliente y distribuida geográficamente. Requisitos más estrictos de ciberseguridad impulsan la demanda por interconexiones privadas, redundancia, manejo de tráfico cifrado y centros de datos seguros donde se puedan aislar cargas sensibles. A medida que los clientes priorizan la disponibilidad continua y el cumplimiento regulatorio, tienden a optar por infraestructura premium certificada en seguridad, lo que impulsa mayores tasas de utilización y contratos de largo plazo para estos proveedores.

De manera similar a la medicina administrada, las empresas de servicios de tercerización de IT también son beneficiarias clave a medida que la ciberseguridad se vuelve más compleja e intensiva en recursos. Compañías como Accenture, IBM, Capgemini, DXC Technology y Cognizant ofrecen servicios de seguridad gestionada, monitoreo, respuesta a incidentes y soporte en cumplimiento. Muchas organizaciones carecen de la capacidad interna para operar centros de operaciones de seguridad 24/7 o gestionar entornos de amenazas en constante evolución, lo que las lleva a externalizar estas funciones. El aumento del gasto en ciberseguridad se traduce en contratos recurrentes de mayor tamaño, una integración más profunda con los clientes y un rol como socios estratégicos en transformaciones de seguridad a gran escala.

Por último, los productores y distribuidores de la energía necesaria para alimentar esta industria serán beneficiarios relevantes del incremento de la demanda de ciberseguridad. Uno de los aprendizajes clave del auge de la IA es que la cantidad de energía requerida para operar estas tecnologías es significativa y sigue creciendo. Independientemente de qué empresas provean el software y el hardware en ciberseguridad, la realidad es que estas tecnologías no pueden operar de manera eficiente sin acceso a una infraestructura energética adecuada.

En última instancia, el extraño “príncipe” en nuestro correo nunca fue la verdadera amenaza, sino apenas un anticipo de bajo presupuesto. El riesgo real proviene ahora de máquinas que no ruegan, no improvisan ni cometen errores, sino que prueban de manera sistemática los límites de los sistemas que operan en la sociedad moderna. A medida que la IA transforma

la ciberseguridad de una disciplina reactiva a una carrera armamentista a escala industrial, el gasto deja de ser opcional y pasa a ser un tipo de seguro frente al caos digital. Para los inversionistas, esta transición se asemeja menos a una narrativa especulativa y más a un proceso de construcción de infraestructura. Al igual que el sistema médico evolucionó por etapas para mejorar el bienestar humano, la ciberseguridad seguirá una trayectoria similar: con el software como los médicos, el hardware como los instrumentos, la infraestructura como los hospitales y la energía como el sistema que lo hace todo posible. ■

Haga click o escanee este código para acceder a más perspectivas en

insigneo.com/es/perspectivas/

Análisis por clases de Activo

Asignación Global de Activos	TÁCTICO (HASTA 3 MESES)	CÍCLICO (HASTA 12 MESES)
Renta Variable	NEUTRAL	SOBREPONDERAR
Renta Fija	SOBREPONDERAR	SOBREPONDERAR
Efectivo	SUBPONDERAR	SUBPONDERAR
Renta Variable EE.UU.[1]	SOBREPONDERAR	NEUTRAL
Renta Variable Europea	NEUTRAL	NEUTRAL
Renta Variable Japonesa	NEUTRAL	SOBREPONDERAR
Renta Variable Mercados Emergentes	SUBPONDERAR	NEUTRAL
Renta Variable China	NEUTRAL	SOBREPONDERAR
Bonos del Tesoro EE.UU.[2]	NEUTRAL	NEUTRAL
Grado de Inversión	NEUTRAL	NEUTRAL
Renta Fija *High Yield*	NEUTRAL	NEUTRAL
Renta Fija Soberana Emergente	NEUTRAL	NEUTRAL
Dólar americano	NEUTRAL	SUBPONDERAR
Energía[3]	NEUTRAL	SUBPONDERAR
Metales Preciosos	NEUTRAL	SOBREPONDERAR

[1] *Relativo a acciones globales en USD*
[2] *Relativo a mercados globales de renta fija en USD*
[3] *Relativo al sector de materias primas*

Divulgaciones Importantes

Insigneo Financial Group, LLC comprende una serie de empresas operativas dedicadas a la oferta de productos y servicios de corretaje y asesoría en varias jurisdicciones, principalmente en América Latina. Los productos y servicios de corretaje se ofrecen a través de Insigneo Securities, LLC, con sede en Miami, miembro de la Autoridad Reguladora de la Industria Financiera (conocida por sus siglas en inglés "FINRA") y de la Corporación de Protección de Valores de Inversionistas (conocida por sus siglas en inglés "SIPC") https://www.sipc.org/. Los productos y servicios de asesoría de inversiones se ofrecen a través de Insigneo Advisory Services, LLC, un asesor de inversiones registrado en la Comisión de Bolsa y Valores. En Uruguay, los servicios de asesoría se ofrecen a través de Insigneo Asesor Internacional S.A., Insigneo Gestor Internacional S.A, Insigneo Asesor Latam S.A., SRL e Insigneo Asesores de Inversión de Uruguay, SRL, en Argentina a través de Insigneo Argentina, SAU y en Chile a través de Insigneo Asesorías Financieras, SPA. En conjunto, estos ocho negocios operativos conforman Insigneo Financial Group. Para obtener más información sobre el corredor de bolsa, incluidos sus conflictos de intereses y prácticas de compensación, visite https://insigneo.com/disclosures/ o www.finra.org Para obtener más información sobre Insigneo Advisory Services, LLC y cualquier conflicto relacionado con sus servicios de asesoría, consulte su Formulario ADV y el folleto que se pueden encontrar en el sitio web de Investment Advisor Public Disclosure https://adviserinfo.sec.gov/.

PARA AFILIADOS LOCALIZADOS EN CHILE

Insigneo Asesorías Financieras SPA se encuentra inscrito en Chile, en el Registro de Prestadores de Servicios Financieros de la Comisión para el Mercado Financiero. Este informe fue efectuado por área de Research & Strategy de Insigneo Securities LLC. o sus proveedores, en base a la información disponible a la fecha de emisión de este. Para evitar cualquier conflicto de interés, Insigneo Securities LLC dispone que ningún integrante del equipo de Research & Strategy tenga su remuneración asociada directa o indirectamente con una recomendación o reporte específico o con el resultado de una cartera. Aunque los antecedentes sobre los cuales ha sido elaborado este informe fueron obtenidos de fuentes consideradas confiables, no podemos garantizar la completa exactitud e integridad de estos, no asumiendo responsabilidad alguna al respecto Insigneo Securities LLC, Insigneo Asesorías Financieras SPA ni ninguna de sus empresas relacionadas. Este material está destinado únicamente a facilitar el debate general y no pretende ser fuente de ninguna recomendación específica para una persona concreta. Por favor, consulte con su ejecutivo de cuentas o con su asesor financiero si alguna de las recomendaciones específicas que se hacen en este documento es adecuada para usted. Este documento no constituye una oferta o solicitud de compra o venta de ningún valor en ninguna jurisdicción en la que dicha oferta o solicitud no esté autorizada o a ninguna persona a la que sea ilegal hacer dicha oferta o solicitud. Las inversiones en cuentas de corretaje y de asesoramiento de inversiones están sujetas al riesgo de mercado, incluida la pérdida de capital. La información base del presente informe puede sufrir cambios, no teniendo Insigneo Securities LLC ni Insigneo Asesorías Financieras SPA la obligación de actualizar el presente informe ni de comunicar a sus destinatarios sobre la ocurrencia de tales cambios. Cualquier opinión, expresión, estimación y/o recomendación contenida en este informe constituyen el juicio o visión de área de Research & Strategy de Insigneo Securities LLC. o sus proveedores, a la fecha de su publicación y pueden ser modificadas sin previo aviso.

PARA AFILIADOS LOCALIZADOS EN URUGUAY

En Uruguay, los valores están siendo ofrecidos en forma privada de acuerdo al artículo 2 de la ley 18.627 y sus modificaciones. Los valores no han sido ni serán registrados ante el Banco Central del Uruguay para oferta pública.

PARA AFILIADOS LOCALIZADOS EN ARGENTINA

Insigneo Argentina S.A.U. Agente Asesor Global de Inversión se encuentra registrado bajo el N° 1053 de la Comisión Nacional de Valores (CNV) e inscripto ante la Inspección General de Justicia (IGJ) bajo el N° 12.278 del Libro 90, Tomo –, de Sociedades por Acciones. Este informe fue efectuado por área de Research & Strategy de Insigneo Securities LLC. o sus proveedores, en base a la información disponible a la fecha de su emisión. Para evitar cualquier conflicto de interés, Insigneo Securities LLC dispone que ningún integrante del equipo de Research & Strategy tenga su remuneración asociada directa o indirectamente con una recomendación o reporte específico o con el resultado de una cartera. Aunque los antecedentes sobre los cuales ha sido elaborado este informe fueron obtenidos de fuentes consideradas confiables, no podemos garantizar la completa exactitud e integridad de estos, no asumiendo responsabilidad alguna al respecto Insigneo Securities LLC, Insigneo Argentina S.A.U. ni ninguna de sus empresas relacionadas. La información base del presente informe puede sufrir cambios, no teniendo Insigneo Argentina S.A.U. la obligación de actualizar el presente informe ni de comunicar a sus destinatarios sobre la ocurrencia de tales cambios. Este material está destinado únicamente a facilitar el debate general y no pretende ser fuente de ninguna recomendación específica para una persona concreta. Por favor, consulte con su ejecutivo de cuentas o con su asesor financiero si alguna de las recomendaciones específicas que se hacen en este documento es adecuada para usted. Este documento no constituye una oferta, recomendación o solicitud de compra o venta de ningún valor negociable en ninguna jurisdicción en la que dicha oferta o solicitud no esté autorizada o a ninguna persona a la que sea ilegal hacer dicha oferta o solicitud. Las inversiones en valores negociables están sujetas al riesgo de mercado, incluida la pérdida parcial o total del capital invertido. Cualquier opinión, expresión, estimación y/o recomendación contenida en este informe constituyen el juicio o visión de área de Research & Strategy de Insigneo Securities LLC. o sus proveedores, a la fecha de su publicación y pueden ser modificadas sin previo aviso.

insigneo