Market Commentary
May 2026

English Version

The Mythos Effect: Cybercrime-as-a-service

Get guidance on investments, and the major structural factors behind your clients' portfolios.

insigneo

Mauricio Viaud
Senior Investment Strategist and PM

Andrés Salamanca
Investment Strategist

The Mythos Effect: Cybercrime-as-a-service

> Cybercrime is being transformed into a scalable, automated industry, where AI can identify and exploit vulnerabilities in seconds, putting unprecedented offensive power into the hands of even non-experts.

> The stakes are no longer just digital: modern cyberattacks can shut down factories, disrupt critical infrastructure, and cause real-world damage with massive economic consequences.

> As this threat landscape expands, cybersecurity is evolving into a full ecosystem, where software, hardware, and infrastructure providers all play critical roles in defending the digital economy.

> For investors, this shift extends far beyond pure cybersecurity firms, opening opportunities across the entire value chain, from software and network hardware to data centers, telecom infrastructure, and even the energy systems required to power it all.

Ever had a random “prince” or mysteriously rich stranger slide into your inbox offering you a massive inheritance for almost nothing? Mankind’s development has generally followed a path from *mythos* to logos, from belief to reason. But in cybersecurity, that trajectory now appears to be reversing. In this context, Anthropic, the main competitor of OpenAI (creator of ChatGPT), has recently introduced Claude Mythos, a model that is forcing companies to rethink what they once considered “logical.” Widely regarded as Anthropic’s most powerful model to date, Mythos has demonstrated in testing the ability to identify and ex-

ploit thousands of cybersecurity vulnerabilities within seconds. While cyber damage has traditionally been associated with scams and other non-physical threats, as we will explore in this piece, tools like Mythos could mark a turning point for societies in general.

While AI is pushing us to confront scenarios that would have seemed dystopian only a few years ago, it is also creating meaningful opportunities for investors. With that in mind, this piece is divided into two parts: the first outlines what is happening and why it matters, while the second examines the companies positioning themselves to benefit from this new landscape of modern-day "*mythos*."

Part 1. "It's not if, but when" - A series of questions to understand the current cybersecurity landscape

What is cybersecurity? According to IBM, it is the practice of protecting people, systems, and data from cyberattacks through a combination of technologies, processes, and policies. Although the first computers appeared in the 1940s, cybersecurity as a concept is often traced back to researcher Bob Thomas in 1970. From those early beginnings, the industry has grown into a massive global market. By 2025, spending on professional security services reached approximately USD 61.9 billion, while cybersecurity software revenues climbed to nearly USD 140 billion. Notably, even before the emergence of frontier AI, the industry was already expected to grow at a compound annual rate of 14.3% through 2030.

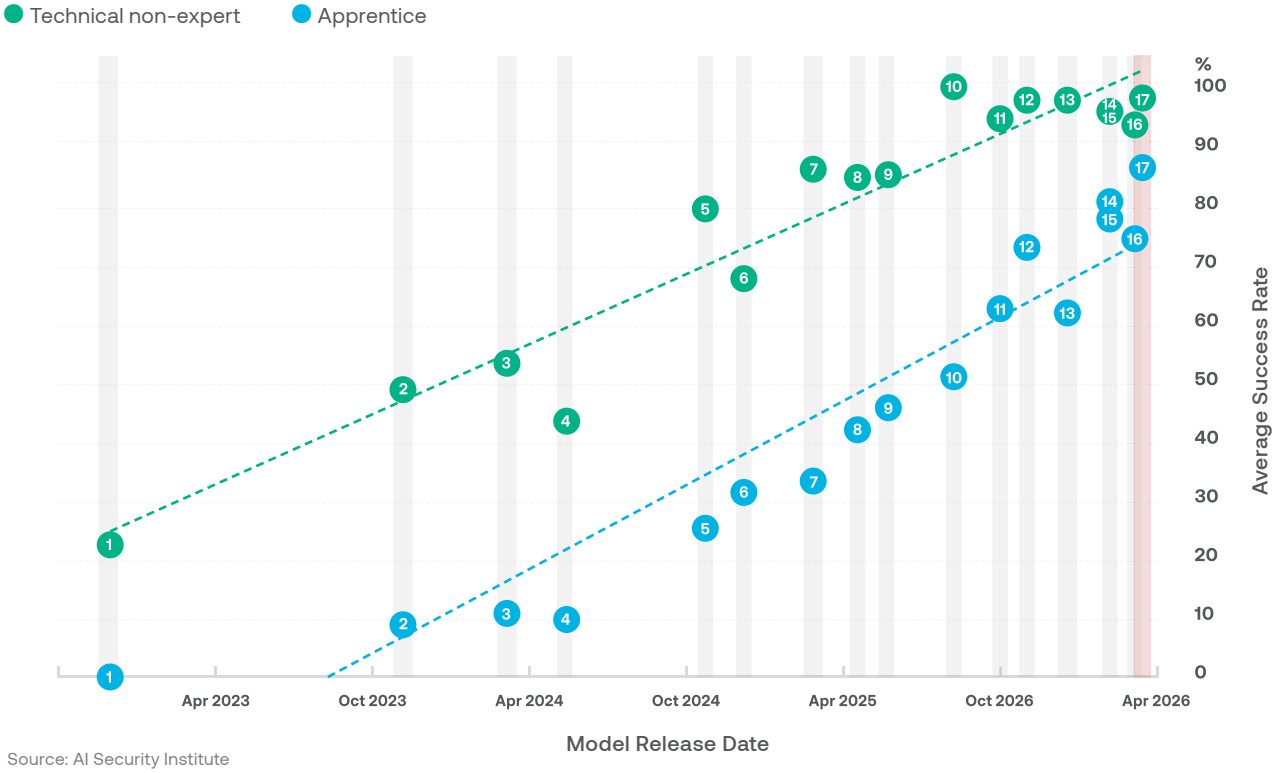
"With the arrival of advanced AI models, cyberattacks are no longer limited to small groups attempting to steal information; they are becoming scalable, automated, and increasingly autonomous operations."

What has changed? With the arrival of advanced AI models, cyberattacks are no longer limited to small groups attempting to steal information; they are becoming scalable, automated, and increasingly autonomous operations. **In practical terms, models like Claude's Mythos can orchestrate global cyberattack campaigns.** The US Federal Bureau of Investigation's IC3 received more than 1 million complaints in 2025, with reported losses reaching USD 21 billion, a 26% year-over-year increase. In addition, according to SoSafe's 2025 cybercrime trend report, 87% of global companies experienced an AI cyberattack in 2025. **It's not if, but when.**

How does it work? AI is no longer just a coding assistant that helps write or debug scripts; it is a system capable of systematically scanning, understanding, and stress-testing entire codebases to uncover exploitable weaknesses at scale. Modern models can identify known vulnerabilities (exploits) to take advantage of flaws or zero-day vulnerabilities, which are bugs that have not yet been patched or disclosed. By combining pattern recognition with reasoning, these systems can map surfaces, chain multiple weaknesses together, and simulate how an attacker might move through a network. **The result is a shift from manual, time-intensive security research to large-scale automated discovery.** In the context of models like Mythos, this represents a fundamental change: what once required highly specialized human expertise can now be accelerated, replicated, and potentially deployed across thousands of targets simultaneously, reshaping both the threat landscape and the defensive strategies needed to contain it.

Graph 1: Beginner CTF Challenge Performance by Model (2.5M Token budget)

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



Source: AI Security Institute

How good is Mythos? As shown in Graph 1, the AI Security Institute (AISI) conducted a Capture the Flag (CTF) test designed to see how effectively models could identify and exploit vulnerabilities in a target system. In the study, Mythos was benchmarked against 16 other models, with tasks executed by both apprentices and technical non-experts to measure performance in realistic, low-specialized conditions. Apprentices achieved an average success rate of nearly 90%, while technical non-experts got close to 100% effectiveness. Taken together, these findings highlight the **unusually high capability of Mythos to enable vulnerability discovery and exploitation even in the hands of non-professional users.**

Are there different levels of risk? Modern systems are broadly divided into Information Technology (IT) and Operational Technology (OT). IT encompasses traditional digital infrastructure, including servers, cloud environments, databases, and corporate networks; while OT refers to systems that control physical processes through devices like Programmable

"OT infrastructure underpins critical sectors across society, including power generation, oil and gas exploration, water treatment facilities, drug manufacturing, and traffic control systems."

Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) platforms. For example, in an automotive assembly plant, IT systems handle inventory tracking, production planning, and resource management, whereas OT systems run the factory floor, controlling robotic arms, welding stations, and painting systems.

The risk profile differs sharply between the two. A cyberattack on IT systems, while disruptive, can often be contained through shutdowns, patches, and system recovery with limited impact on physical output. **An attack on OT systems, however, can halt entire production lines, leading to significant downtime costs and even posing safety risks to operators.** Siemens published a study called The True Cost of Downtime, where reported that unplanned downtime accounted for roughly 11% of Global Fortune 500's revenues in 2024, approximately USD 1.4 trillion in losses. Continuing with the automotive sector, a single hour of unplanned downtime can cost as much as USD 2.3M, equivalent to more than USD 600 per second.

Why is it so hard to patch OT systems? Many of these systems are decades old and were never designed to be updated frequently. In some cases, the original vendors no longer exist or have stopped supporting these legacy platforms, leaving operators with few viable upgrade options. At the same time, **OT infrastructure underpins critical sectors across society, including power generation, oil and gas exploration, water treatment facilities, drug manufacturing, and traffic control systems.** A clear example of a legacy OT is Windows XP: launched in 2001 and unsupported after 2014, it is still used in some industrial environments because many SCADA systems were built to run on it and replacing them often requires a full overhaul of operations rather than a simple patch.

How bad can a cyberattack be? Examples of both OT and IT cyberattacks can be found in recent history. On the OT side, Stuxnet stands out as the first major cyberattack to cause physical damage: a highly sophisticated worm discovered in 2010 that targeted Iran's Natanz nuclear facility in an effort to disrupt uranium enrichment. Stuxnet infiltrated industrial control systems through multiple zero-day vulnerabilities, subtly altering the speed of uranium enrichment centrifuges by intermittently increasing and decreasing their rotation beyond safe operating thresholds. This caused excessive mechanical stress, ultimately leading to the failure of a significant number of centrifuges while simultaneously feeding false normal readings to operators to avoid detection. On the IT side, in 2017, NotPetya disrupted core port infrastructure by disabling the digital systems needed to identify containers, coordinate cranes, and manage logistics flows, effectively forcing terminals to shut down despite the physical equipment remaining operational. The shipping giant Maersk reported losses of approximately USD 250–300M after halting port operations worldwide, and the White House stated in 2018 that the attack caused more than USD 10 billion in global damages.

Which sectors face the greatest security risk? Typically, those where **high automation intensity intersects with low patchability,** such as energy systems, industrial manufacturing, and transportation infrastructure. The core issue is precisely that: limited ability to patch. JPM estimates that while only about 20% of IT systems are effectively unpatchable, between 40% and 55% of the installed OT base cannot be patched at all, regardless of operator efforts.

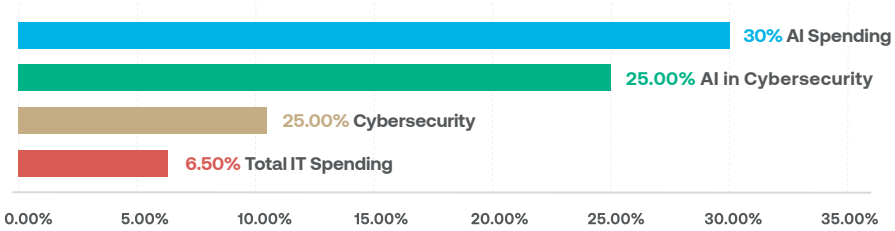
So, what is the solution? Fighting AI with AI. In an effort to prepare organizations for the capabilities of Mythos, Anthropic paused its release and launched Project Glasswing, a controlled-access program involving more than 50 organizations, including major tech and financial companies, allowing them to use the model to stress-test systems and train defensive cybersecurity models. Against this backdrop, some analysts estimate that by mid-2027, around 85% of detection and response playbooks could be dynamically generated, continuously adapting to evolving threats in real time. This process will require companies to automate security operations, adopt identity-centric zero trust architectures, improve detection reliability, and strengthen resilience through faster recovery and cryptographic readiness. **In practice, however, companies are still far from this. According to Bain & Company, its 2025 cybersecurity survey shows that firms plan to increase cybersecurity capex by around 10% annually, well below the pace at which frontier AI models are pushing cybersecurity. This gap between reality and bureaucracy is where investment opportunities emerge.**

> "The cybersecurity industry will evolve in a similar manner, requiring large amounts of investment and spending as risks proliferate and a complex, multifaceted ecosystem emerges."

Part 2. Where Security Risk Becomes Opportunity

Much like in the medical field, where the proliferation of diseases eventually created a complex ecosystem of practitioners, machinery, and infrastructure, so is the case in the cybersecurity industry, where the proliferation of risks, especially those exposed by AI, will create a complex, multifaceted industry. Think of the current state of the cybersecurity industry as being in a similar situation as the onset of the structured medical field in the 18th and 19th century. In those days, the medical professionals operating in the field were mostly local doctors practicing mostly general medicine that treated everything from the common cold to removing a limb. Slowly but surely, other companies emerged, which created tools and machinery to improve the efficacy and efficiency of healthcare. As medical care improved and grew, so did the infrastructure needed to support this industry. We believe that the cybersecurity industry will evolve in a similar manner, and it will require large amounts of investment and spending. **So, which companies will benefit as the cybersecurity sector in its current form transitions? We believe that three industry groups stand to benefit the most: software, hardware, and infrastructure.**

Graph 2: Projected Global Enterprise Spending Growth
(Compound Annual Growth Rate 2025-2028)



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

In 2025, annual enterprise spending on cybersecurity was approximately USD $200 billion. The analytics firm Statista estimates that by 2030, this number could reach USD $265 billion annually. However, this number could prove conservative. Other providers such as Zero-Threat estimate that this number could reach as high as USD 500 billion. Graph 2 shows the compounded annual growth rate of IT spending by global enterprises.

It shows that although general IT spending will continue to grow at 6.5%, albeit from a very large base of USD 7 trillion, a meaningful portion of spending growth will come from AI and the cybersecurity needed to secure this technology.

The Practitioners: The cybersecurity software companies themselves

Increased spending on cybersecurity directly benefits pure play security software vendors that focus on protecting networks, data, and identities. Companies such as Palo Alto Networks, Fortinet, CrowdStrike, and Zscaler could potentially stand to gain as organizations allocate more budget toward preventing breaches and responding to growing threats like ransomware and nation state attacks. These firms offer mission critical solutions—firewalls, endpoint protection, cloud security, and zero trust architectures—that are often considered nondiscretionary once adopted. As cyber risks rise, customers tend to expand existing contracts and add more modules rather than switch vendors, supporting recurring revenue growth and pricing power.

Large platform software companies with integrated security offerings could also benefit meaningfully from higher cybersecurity investment. Firms like Microsoft, Google (Alphabet), Amazon, and Oracle embed security tools across their cloud, productivity, and enterprise infrastructure platforms. As enterprises migrate workloads to the cloud, security spending increasingly follows the same providers, favoring vendors that can bundle cybersecurity into broader software suites. This integration lowers customer complexity and makes security a strategic differentiator, helping these companies grow average revenue per customer while reinforcing their competitive moats.

Finally, enterprise IT and identity management software companies may see indirect but significant gains as cybersecurity spending expands. Companies such as Okta, ServiceNow, Splunk, and Datadog could potentially benefit from demand for identity governance, security monitoring, compliance automation, and incident response. Cybersecurity is no longer isolated to the IT department; it now touches workflows, analytics, and risk management across the enterprise. As a result, firms that provide software enabling visibility,

automation, and secure access become essential partners, positioning them to capture sustained growth as cybersecurity budgets continue to rise.

The Instruments: The hardware companies

Much like hardware companies are needed to create the picks and shovels that give life to AI, hardware companies are also needed to create the tools that enable the cybersecurity needed to protect AI and its users. Largely, increased spending on cybersecurity benefits network hardware companies that provide the physical infrastructure required to secure data flows. Firms such as Cisco, Juniper Networks, and Arista Networks gain as enterprises upgrade routers, switches, and next generation firewalls to handle encrypted traffic, segmentation, and advanced threat inspection. As cyber threats grow more sophisticated, organizations often need higher performance hardware capable of deep packet inspection and real-time analytics, driving refresh cycles and higher average selling prices for networking equipment vendors.

Dedicated security appliance manufacturers also benefit directly from rising cybersecurity budgets. Companies like Palo Alto Networks, Fortinet, Check Point, and Sophos sell purpose built appliances that sit at the periphery of networks, data centers, and branch offices. Even as security software shifts to the cloud, many regulated industries—such as finance, healthcare, and government—still require on premise or mixed hardware solutions for compliance and latency reasons. Increased spending allows customers to deploy more hardware across locations and upgrade to higher capacity models, supporting steady demand for these vendors' hardware portfolios.

Lastly, semiconductors and specialized hardware companies benefit indirectly as cybersecurity workloads become more compute intensive. Firms such as Intel, AMD, NVIDIA, and Marvell supply processors, accelerators, and networking chips optimized for encryption, AI driven threat detection, and secure networking. As security appliances and data centers require faster processing for tasks like zero trust authentication and real time monitoring, demand rises for chips with built in security features and acceleration capabilities. This makes cybersecurity growth a tailwind not only for system manufacturers but also for the underlying hardware ecosystem that powers secure IT infrastructure. Some of these technologies are already in service; others will need to evolve as the industry evolves.

The Hospitals and Healthcare Systems: The companies providing the supporting infrastructure

Increased spending on cybersecurity does not stop with the software and hardware companies. Medical practitioners need hospitals, clinics, and systems to practice medicine. So does cybersecurity. **Increased spending on this industry could also potentially benefit digital infrastructure providers, particularly data center operators, cloud infrastructure specialists, and telecom network owners.** Companies such as Equinix, Digital Realty, American Tower, Crown Castle, and major telecom carriers benefit as enterprises invest in secure, resilient connectivity and geographically distributed infrastructure. Stronger cybersecurity requirements drive demand for private interconnections, redundancy, encrypted traffic handling, and secure colocation facilities where sensitive workloads can be isolated. As customers prioritize uptime and compliance, they are more likely to choose premium, security certified infrastructure, supporting higher utilization rates and long term contracts for these providers.

Much like managed healthcare, managed services and IT outsourcing firms are also key beneficiaries as cybersecurity becomes more complex and resource intensive. Companies like Accenture, IBM, Capgemini, DXC Technology, and Cognizant provide managed security services, monitoring, incident response, and compliance support. Many organizations lack the in house expertise to operate 24/7 security operations centers or manage evolving threat landscapes, leading them to outsource these functions. Rising cybersecurity budgets translate into larger recurring contracts, deeper client integration, and expanded advisory roles for these firms, which often act as strategic partners during major security transformations.

Lastly, the producers and distributors of the vast amount of energy needed to power this industry will be important beneficiaries of increased spending on and demand for cybersecurity. One thing that the AI boom has taught us is that the amount of energy needed to power this technology is massive, and the appetite for increased power is insatiable. Regardless of which companies provide the software and hardware needed in cybersecurity, the undeniable fact is that this technology cannot operate optimally without adequate power.

In the end, the strange "prince" in our inbox was never the real threat—it was merely the low budget preview. The true risk now comes from machines that don't beg, bluff, or misspell, but calmly and systematically test the limits of the systems operating in modern society. As AI pushes cybersecurity from a reactive craft into an industrial scale arms race, spending is no longer a choice but a form of insurance against digital chaos. For investors, this transition looks less like speculative hype and more like infrastructure buildout. Much like the medical field evolved in stages for the betterment of humanity, so should cybersecurity, with software as the physicians, hardware as the instruments, infrastructure as the hospitals, and energy as the lifeblood that powers everything. ■

Click or scan this code to access more insights at insigneo.com/insights

House Views Matrix

Global Asset Allocation	TACTICAL (UP TO 3 MONTHS)	CYCLICAL (UP TO 12 MONTHS)
Equities	NEUTRAL	OVERWEIGHT
Fixed Income	OVERWEIGHT	OVERWEIGHT
Cash	UNDERWEIGHT	UNDERWEIGHT
US Equities[1]	OVERWEIGHT	NEUTRAL
European Equities	NEUTRAL	NEUTRAL
Japanese Equities	NEUTRAL	OVERWEIGHT
Emerging Market Equities	UNDERWEIGHT	NEUTRAL
Chinese Equities	NEUTRAL	OVERWEIGHT
US Treasuries[2]	NEUTRAL	NEUTRAL
Investment Grade Fixed Income	NEUTRAL	NEUTRAL
High Yield Fixed Income	NEUTRAL	NEUTRAL
Emerging Market Sovereign	NEUTRAL	NEUTRAL
US Dollar	NEUTRAL	UNDERWEIGHT
Energy[3]	NEUTRAL	UNDERWEIGHT
Precious Metals	NEUTRAL	OVERWEIGHT

[1] Relative to global equities in USD
[2] Relative to aggregate fixed income markets in USD
[3] Relative to an overall commodity allocation

Important Disclosures

Insigneo Financial Group, LLC comprises a number of operating businesses engaged in the offering of brokerage and advisory products and services in various jurisdictions. Brokerage products and services are offered through Insigneo Securities, LLC, a broker-dealer registered with the U.S. Securities and Exchange Commission ("SEC") and member of FINRA and SIPC. Investment advisory products and services are offered through Insigneo Advisory Services, LLC, an investment adviser registered with the SEC. Insigneo has affiliated companies in different locations, so it is important to understand which entity you are conducting business with. Please visit https://insigneo.com/legalentities/ for more information about the differences between these companies, their locations, and what that means for you.

This material should not be construed as an offer to sell or the solicitation of an offer to buy any security. It is for general information purposes only. To the extent that this material discusses general market activity, industry or sector trends or other broad-based economic or political conditions, it should not be construed as research or investment advice. To the extent that it includes references to securities, those references do not constitute a recommendation to buy, sell or hold such security. It does not constitute a recommendation or a statement of opinion, or a report of either of those things and does not, and is not intended, to consider the particular investment objectives, financial conditions, or needs of individual investors. Any target prices provide reflect our current expectations, are subject to change and may not be achieved due to a variety of risks, including changes in economic conditions, interest rates, geopolitical developments, and issuer-specific factors. The target price does not guarantee future results and should not be relied upon as a sole basis for investment decisions.

Not All Risks Are Disclosed – Past performance is not indicative of futures results. Investments involve significant risks, and it is possible to lose some or all of your principal investments and therefore may not be suitable for everyone. Always consider whether any investment is suitable for your particular circumstances and, if necessary, seek professional advice from your Investment Professional.

This material may contain opinions, expressions, and estimates that represent the analysis and perspective of Insigneo Securities, LLC's Investment Strategy department or its providers at the time of publication. These are subject to change at any time, without notice.

FOR AFFILIATES LOCATED IN 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.

FOR AFFILIATES LOCATED IN URUGUAY

Insigneo Asesor Uruguay S.A. está inscripto en el Registro de Mercado de Valores del Banco Central del Uruguay como Asesor de Inversiones. 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. 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 según su perfil y estrategia de inversión. Este documento no constituye un asesoramiento ni una recomendación u oferta o solicitud de compra o. 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. Rentabilidades históricas de los productos anunciados no aseguran rentabilidades futuras.

FOR AFFILIATES LOCATED IN 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