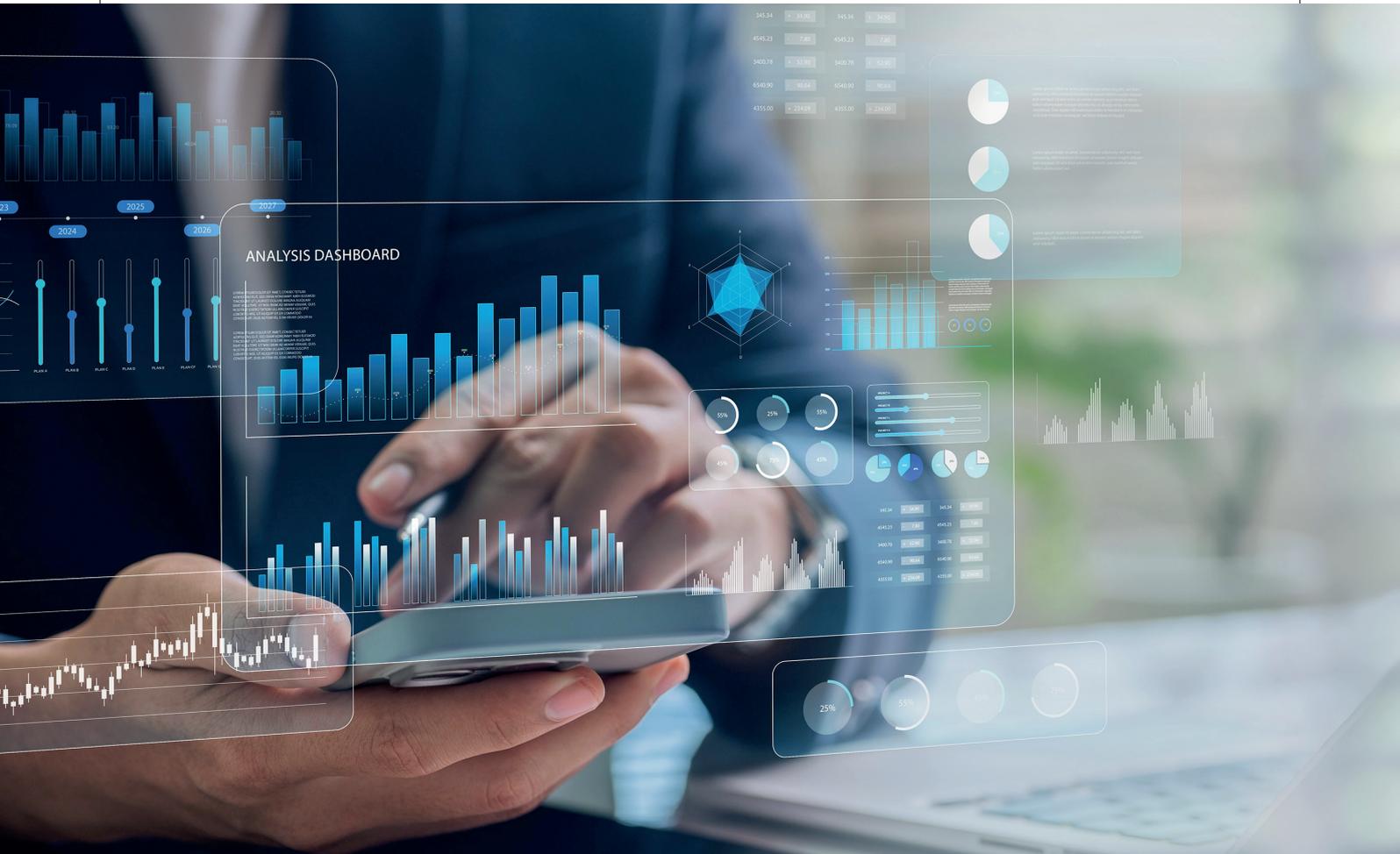


whitepaper



Pesquisa Investimentos em cibersegurança no Brasil

REALIZAÇÃO

tiinside

• w h i t e p a p e r •

Pesquisa: Investimentos em cibersegurança no Brasil



Com o objetivo de identificar os principais desafios enfrentados pelas empresas na área de cibersegurança, suas preocupações, tecnologias adotadas e os investimentos realizados em soluções para a proteção de dados e ativos, conduzimos uma pesquisa para avaliar o nível de maturidade das organizações neste campo.

Os resultados obtidos, além de fornecer uma visão clara sobre o estágio atual das empresas em relação à cibersegurança, servirão como subsídio para aprofundar e enriquecer os debates nos painéis de discussão do **Cybersecurity Forum**, que ocorrerá no dia 11 de março no WTC Events Center, em São Paulo, promovido pela TI Inside.

Conheça a grade do evento com líderes do setor de tecnologia e segurança, trazendo as discussões mais atuais sobre proteção contra ameaças cibernéticas, estratégias de mitigação de riscos e as ferramentas indispensáveis para o futuro das empresas.

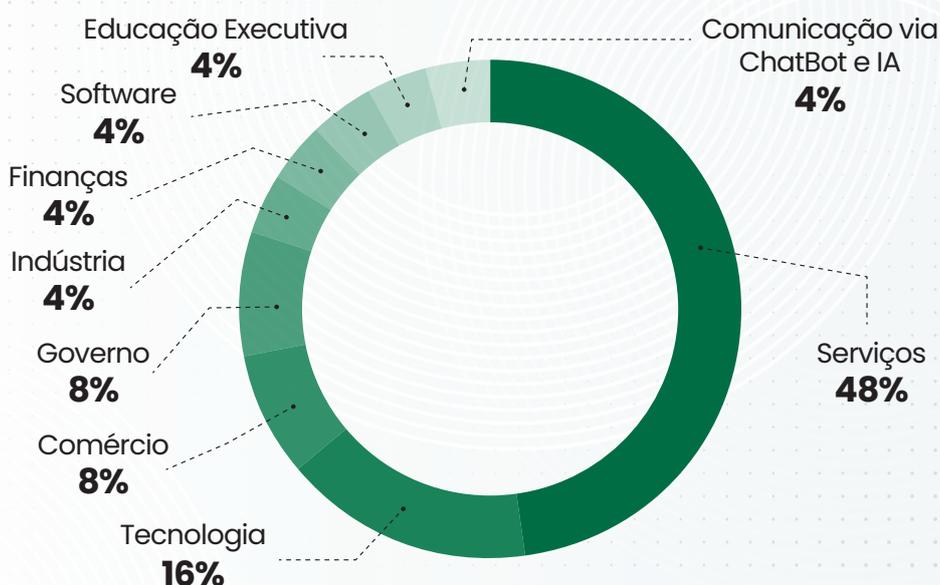
Acesse www.cybersecurityforum.com.br

Boa leitura.

Claudiney Santos
Diretor editorial
TI Inside

Pesquisa: Investimentos em cibersegurança no Brasil

Qual é o setor de atuação da sua empresa?

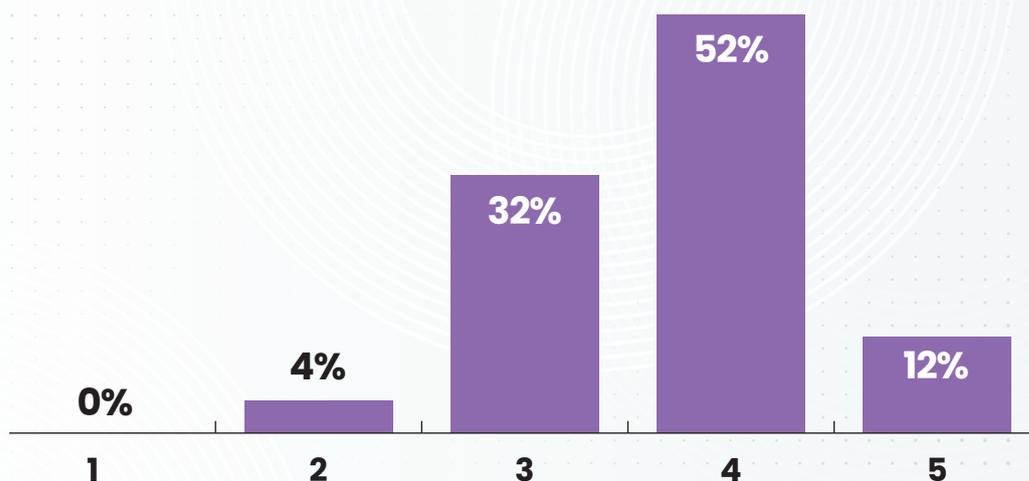


O gráfico destaca que 48% das empresas participantes estão inseridas no setor de serviços, refletindo a crescente necessidade de proteção cibernética em um segmento altamente dependente de dados e interações digitais. Em seguida, 16% das empresas pertencem ao setor de tecnologia, seguido por 8% de empresas nos setores de governo e comércio, ambos com relevância significativa em termos de governança de dados e infraestrutura crítica.

Por outro lado, os setores de indústria e finanças, entre outros, aparecem com 4%, indicando uma possível percepção reduzida dos riscos cibernéticos nesses segmentos ou uma menor priorização de investimentos em soluções de segurança, apesar da exposição crescente a ameaças digitais. Esse panorama sugere que os setores mais orientados ao digital estão mais conscientes e proativos em relação à implementação de medidas de cibersegurança.

Pesquisa: Investimentos em cibersegurança no Brasil

Em uma escala de 1 a 5 (sendo 1 muito baixo e 5 muito alto), como você avalia o nível de maturidade da sua empresa em relação à proteção de dados?



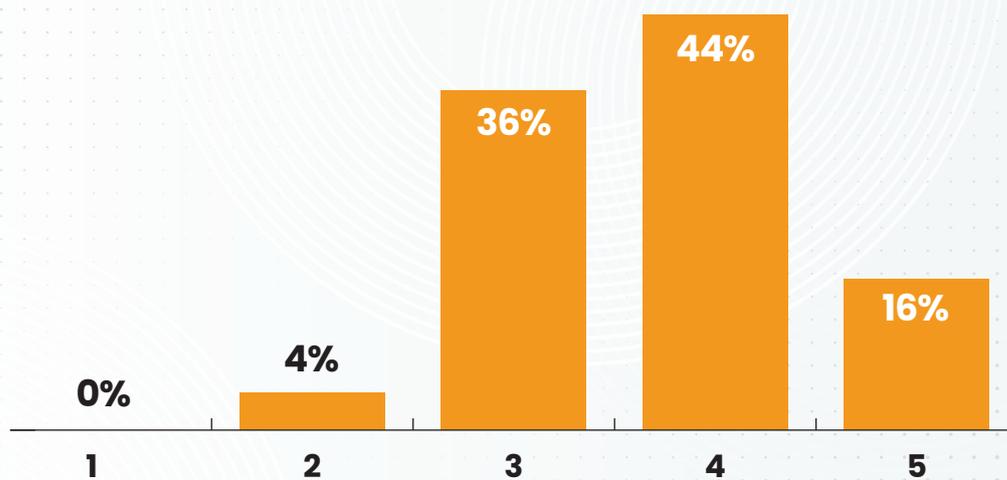
Maturidade em relação à proteção de dados

Os resultados da pesquisa indicam que o nível médio de maturidade das organizações em relação à proteção de dados é de 42%. Contudo, apenas 12% dos respondentes se classificam no nível 5, considerado o mais avançado, refletindo uma avaliação de excelência nos processos de governança de dados e conformidade com regulamentos.

Este panorama é particularmente relevante considerando a vigência da Lei Geral de Proteção de Dados (LGPD), sancionada em agosto de 2018, que impõe requisitos rigorosos de proteção e privacidade de dados pessoais. A discrepância entre a maturidade média e o número reduzido de empresas no nível máximo sugere que, embora haja avanços, muitas organizações ainda enfrentam desafios substanciais para implementar práticas robustas e escaláveis de proteção de dados, alinhadas às exigências legais e melhores práticas do mercado.

Pesquisa: Investimentos em cibersegurança no Brasil

Em uma escala de 1 a 5 (sendo 1 muito baixo e 5 muito alto), como você avalia o nível de maturidade da sua empresa em relação à cibersegurança?



Maturidade em relação à cibersegurança

Ao analisar as respostas dos participantes que atribuíram notas 3 e 4 ao nível de maturidade em cibersegurança, observa-se uma média de 40% das organizações com um nível de segurança considerado razoável, indicando que, embora possuam medidas de proteção em vigor, estas ainda não atendem a padrões elevados de resiliência e governança cibernética. Além disso, apenas 16% dos respondentes se posicionam acima da média, atingindo níveis mais avançados de maturidade, caracterizados por processos e tecnologias sofisticadas para a mitigação de riscos, detecção e resposta a incidentes de segurança.

Este cenário sugere que, apesar de avanços, muitas empresas ainda estão em estágios iniciais de maturação, com lacunas significativas nas suas práticas de cibersegurança que podem comprometer sua capacidade de enfrentar ameaças cibernéticas complexas e em constante evolução.

Pesquisa: Investimentos em cibersegurança no Brasil

Quais são os principais desafios enfrentados pela sua empresa em relação à cibersegurança?

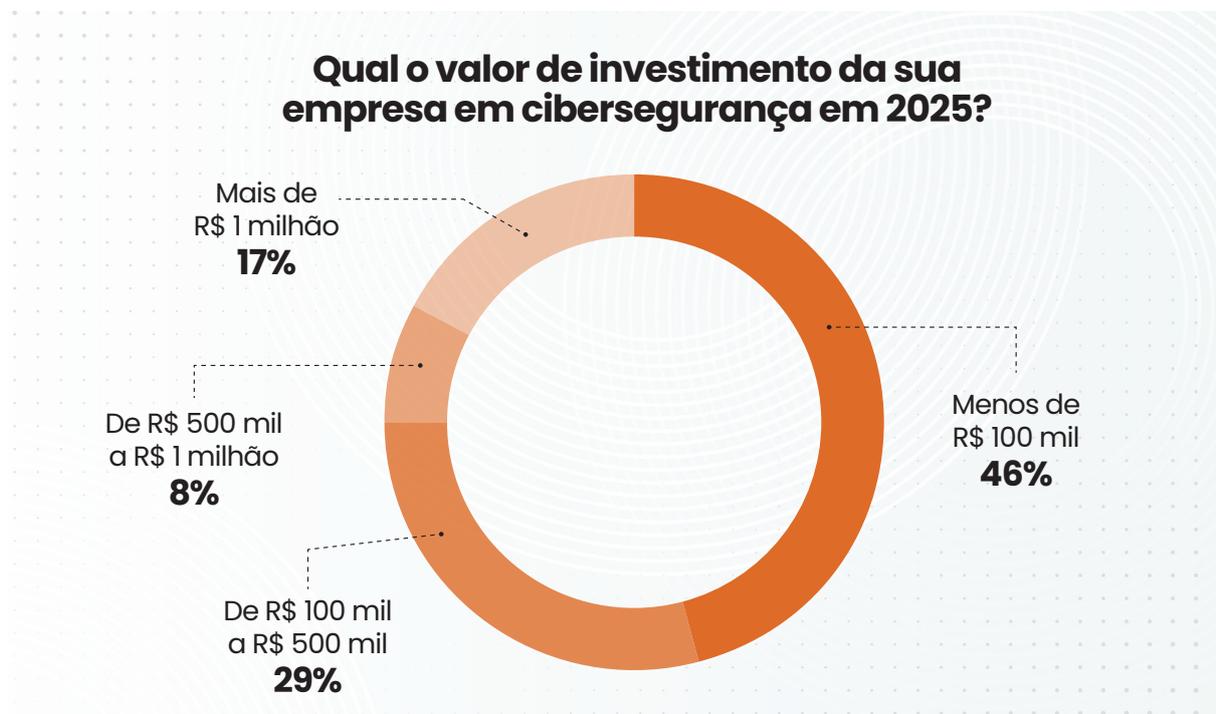


Principais desafios enfrentados pelas empresas

Entre os aspectos mais destacados estão a complexidade crescente na gestão de sistemas de segurança cibernética, a escassez de profissionais qualificados com expertise técnica em segurança da informação e a inadequação dos orçamentos destinados a essa área, que frequentemente não acompanham a escalada dos custos associados à implementação de soluções robustas de proteção e mitigação de riscos.

A complexidade da gestão se refere à necessidade de integrar múltiplas camadas de defesa, coordenar políticas e controles em um ambiente de ameaças dinâmicas, enquanto a falta de recursos humanos especializados compromete a capacidade de monitorar, analisar e responder a incidentes de forma eficaz. Já os orçamentos muitas vezes insuficientes limitam a adoção de tecnologias avançadas e a manutenção de um nível de segurança adequado frente às ameaças sofisticadas e em constante evolução.

Pesquisa: Investimentos em cibersegurança no Brasil



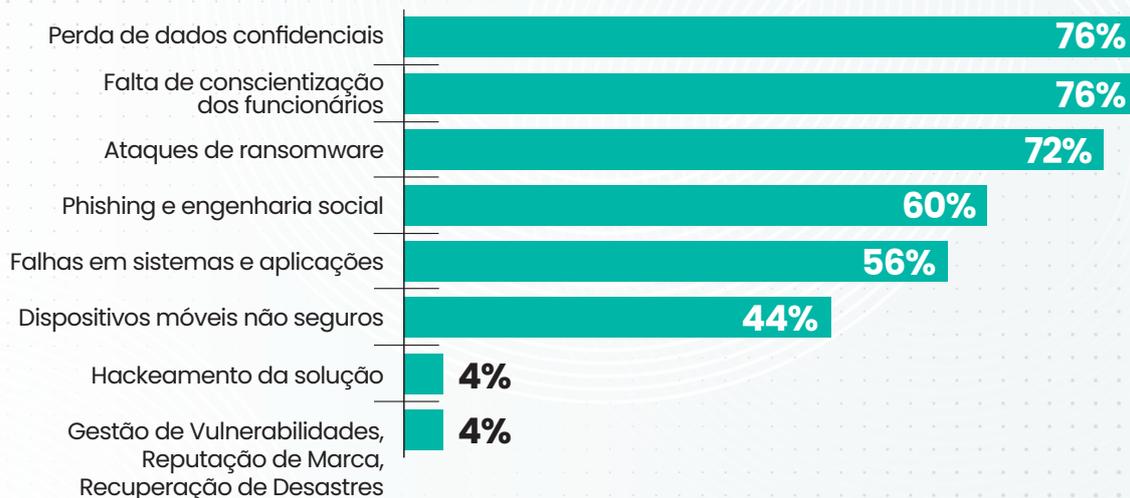
Investimento das empresas em cibersegurança

O gráfico revela que apenas 25% das empresas alocam orçamentos entre R\$ 500 mil e mais de R\$ 1 milhão para cibersegurança, evidenciando uma disparidade significativa no investimento em proteção digital. Esse cenário sugere uma lacuna substancial entre as necessidades de segurança cibernética das organizações e os recursos financeiros destinados a essa área.

Ao mesmo tempo, destaca uma oportunidade considerável para fornecedores de soluções de segurança que buscam atender ao crescente mercado de pequenas e médias empresas (PMEs) no Brasil, muitas das quais ainda apresentam limitações orçamentárias para implementar estratégias de cibersegurança robustas. Esse gap financeiro pode ser explorado por empresas especializadas que ofereçam soluções escaláveis, adaptáveis e com custo-benefício acessível, alinhando-se às realidades econômicas das PMEs enquanto fortalecem sua postura de segurança.

Pesquisa: Investimentos em cibersegurança no Brasil

Quais são as principais preocupações da sua empresa em relação à cibersegurança?



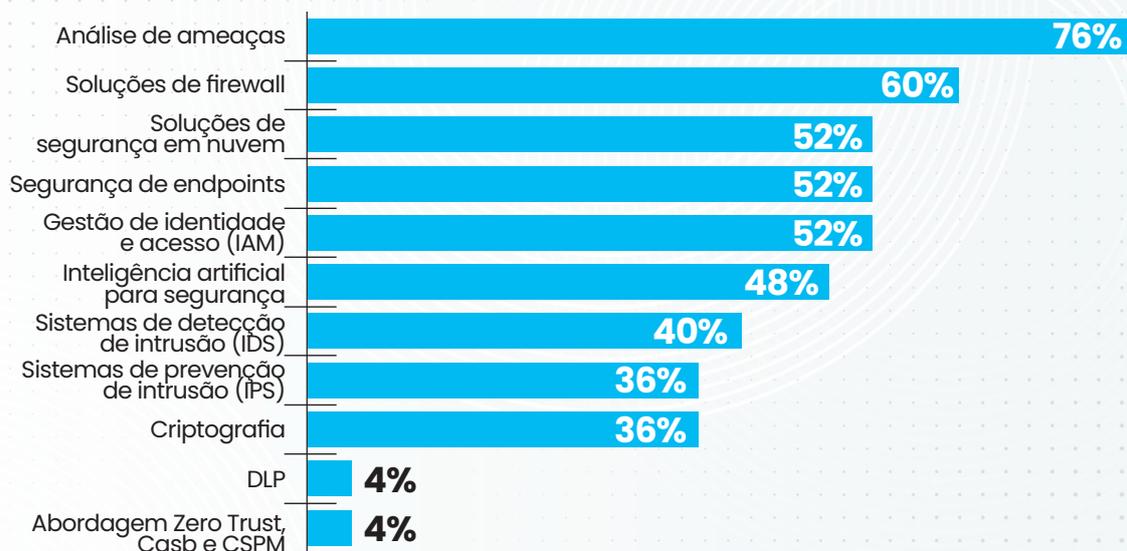
Principais preocupações dos CISOs

O gráfico ilustra as principais preocupações dos CISOs frente às diversas ameaças que podem comprometer a segurança das organizações. A perda de dados confidenciais é a principal para 76% dos respondentes, refletindo a crescente necessidade de proteção e governança de dados sensíveis. 72% dos participantes expressam receio quanto a ataques de ransomware, que têm se tornado uma das ameaças mais disruptivas devido à sua capacidade de paralisar operações e exigir grandes resgates financeiros. Além disso, 60% apontam o phishing e a engenharia social como vulnerabilidades críticas, pois essas técnicas visam manipular usuários para acessar sistemas e dados.

Curiosamente, apenas 4% dos respondentes indicam o hackeamento de soluções como uma preocupação relevante, sugerindo que, embora ainda representem uma ameaça, as organizações talvez estejam investindo mais na proteção contra ataques diretos e de fácil exploração.

Pesquisa: Investimentos em cibersegurança no Brasil

Quais tecnologias de cibersegurança sua empresa está investindo ou planeja investir em 2025?



Tecnologias em que as empresas estão investindo

A diversidade de tecnologias a serem adotadas pelas empresas para garantir a segurança cibernética reflete a complexidade e a evolução das ameaças no ambiente digital. Em 2025, 76% dos respondentes investirão em análise de ameaças para mitigação proativa de riscos; 60% em soluções de firewall para proteção de perímetros; 52% em segurança de endpoints devido ao aumento do trabalho remoto; e 40% em sistemas de detecção de intrusão (IDS) para monitoramento de atividades anômalas.

Além disso, 36% das empresas investirão em criptografia para proteger dados em trânsito e em repouso, assegurando a confidencialidade e integridade das informações sensíveis; outras tecnologias mencionadas incluem abordagens Zero Trust, CASB e CSPM para reforçar a segurança em ambientes híbridos e na nuvem. Essas escolhas refletem uma estratégia de defesa em camadas, visando uma proteção mais abrangente e resiliente.

Quer se aprofundar mais neste assunto e entender como proteger os dados e ativos digitais da sua empresa?

O **Cybersecurity Forum** se consolida como um evento inovador, transformando sua participação em uma experiência única de inspiração e conhecimento.

O que você encontrará no evento:

Conteúdo inovador: temas atuais que transformarão a forma como sua equipe encara a segurança cibernética.

Networking estratégico: conecte-se com empresas e profissionais de destaque no mercado, em um ambiente propício para trocar ideias e fechar parcerias.

Palestrantes de alto nível: conheça líderes do setor de tecnologia e segurança já confirmados.

4ª edição

CYBERSECURITY FORUM



Dia 11 de Março, 2025

EVENTO PRESENCIAL | WTC EVENTS CENTER | SÃO PAULO, SP

Saiba mais em www.cybersecurityforum.com.br

PATROCÍNIO GOLD

EVOLUTIA

Ajuken
Cybersecurity

CLM

AZION

skymail
SOLUÇÕES EM NUVEM

PATROCÍNIO SILVER

GIGA+
EMPRESAS

REALIZAÇÃO

tiinside

PARCEIROS INSTITUCIONAIS

ABEPREST

ABOTTS
Unidos pelo OTT e Streaming