

IA Agêntica: defender com ela e defender-se dela (Os dois lados da moeda)

No cenário tecnológico atual, a cibersegurança não pode mais ser tratada apenas como um jogo de “gato e rato”, focado exclusivamente em defender a infraestrutura tecnológica

Daniel Tupinambá (*)

As organizações precisam dar um passo além do simples combate técnico, pois o desafio reside na capacidade de suportar os negócios de forma compreensiva, com governança de IA, resiliência gerenciada e apoio à recuperação rápida nas hipóteses de ataques, que estão cada vez mais sofisticados. Sofisticação esta, que extrapolou para fraudes digitais e cibernéticas propriamente ditas, nas quais agentes de IA passaram a ser ativamente usados.

Embora mais de 65% das organizações já utilizem a Inteligência Artificial Generativa, a IA agêntica, regularmente em suas operações, assustadores 40% o fazem sem qualquer tipo de framework de cibersegurança estruturado, e meros 21% possuem políticas formais para o tema.

Os hackers mais sofisticados já deixaram de lado os métodos manuais tradicionais e passaram a empregar tecnologias disruptivas que subvertem a segurança corporativa a partir de dentro (insiders), agregando o acesso a megavazamentos, com bilhões de registros expostos. Os cibercriminosos agora utilizam IA avançada para realizar cruzamento e enriquecimento desses dados em massa. O resultado é a criação de identidades sintéticas perfeitas — perfis enriquecidos com documentos de comprovação de vida, amostras de voz e vídeos



Corina Clodrian's Images, CANVA

gerados por IA que são virtualmente indistinguíveis de pessoas reais. Essas identidades dão aos atacantes uma facilidade inédita para aprovar cadastros de crédito, enganar biometrias e aplicar fraudes tão convincentes que mesmo funcionários altamente treinados acabam sendo ludibriados.

A combinação de diferentes técnicas estabelece um novo marco, sem volta, como ocorre nos casos de ransomware baseados em IA, capazes de gerar scripts de criptografia multiplataforma de forma dinâmica e autônoma. Esses ataques utilizam grandes modelos de linguagem (LLMs) executados localmente para evitar a detecção na rede. Mais de 16% das violações corporativas envolvem o uso desse tipo de recurso por cibercriminosos. Esse ecossistema criminoso se apoia majoritariamente em campanhas de phishing com IA, responsáveis por 37% dos casos, e em técnicas

refinadas de falsificação de identidade por meio de deepfakes, presentes em 35%, segundo dados da IBM compilados pela Experian.

Para escalar as funções de seus assistentes virtuais, as empresas começaram a permitir que agentes de IA instalem e usem as chamadas “habilidades” (skills) de terceiros, funcionando de forma muito parecida a aplicativos em um smartphone. No entanto, a pressa em automatizar gerou um ecossistema altamente inseguro, no qual 80% das habilidades têm algum desvio de integridade comportamental (ou seja, faziam coisas que não estavam declaradas em suas especificações e manuais).

Da mesma forma, os 67% dos funcionários das empresas, querendo ser eficientes, alimentam plataformas públicas de IA com dados sensíveis e códigos proprietários corporativos (fenômeno conhecido como Shadow AI), vazando dados sensíveis

e códigos de programação, simplesmente para “agilizar” suas tarefas diárias.

O perigo reside no fato dos atacantes (representados pela fatia de 18,9% com intenção estritamente adversária, segundo pesquisa da Unit 42 da Palo Alto Networks) aprenderam a instrumentalizar este modus operandi. Eles se infiltram em ecossistemas de confiança por meio de engenharia social, usam personas falsas ou sequestram essas conexões “facilitadas” pelos próprios funcionários para roubar credenciais e exfiltrar dados em minutos. Assim, de forma totalmente involuntária, o colaborador brasileiro torna-se um participante ativo — e um facilitador silencioso — de ataques cibernéticos catastróficos.

Combater esse ecossistema exige uma abordagem em duas frentes. De um lado, defender-se da IA adversária por meio de políticas claras de governança, auditoria contínua de modelos e educação corporativa. Do outro, defender-se com IA: integrando agentes autônomos à arquitetura de defesa para antecipar comportamentos anômalos e orquestrar respostas incidentes na mesma escala e velocidade dos atacantes. Em última análise, a cibersegurança moderna não é mais sobre humanos contra máquinas, mas sobre a eficácia das diretrizes e da governança que os humanos estabelecem para as suas próprias máquinas.

(*) - CISO da Elytron, conselheiro OAB-SP.

O maior prejuízo de um ataque cibernético raramente está onde as empresas costumam procurar

Felipe Berneira (*)

Toda empresa sabe exatamente quanto faturou ontem. Poucas sabem quanto perderiam se amanhã não conseguissem faturar nada. Essa é uma conta que quase nunca aparece nas reuniões de planejamento. Até o momento em que um sistema crítico fica indisponível e a discussão deixa de ser tecnológica para se tornar financeira.

Quando isso acontece, o problema deixa de ser o servidor que saiu do ar, o banco de dados inacessível ou os arquivos comprometidos. A preocupação passa a ser outra: pedidos que deixam de ser emitidos, notas fiscais que não são processadas, equipes paradas, entregas atrasadas, contratos descumpridos e clientes sem atendimento. Em poucas horas, a interrupção de um sistema se transforma na interrupção da capacidade de gerar receita.

Esse é um dos maiores equívocos que ainda observo nas empresas. A cibersegurança costuma ser avaliada pelo investimento que exige, quando deveria ser medida pelo prejuízo que ajuda a evitar. Afinal, o ativo mais importante não é apenas a informação armazenada nos sistemas, mas a continuidade da operação que sustenta o negócio.

É comum que as decisões sobre segurança digital fiquem restritas às áreas de tecnologia. No entanto, seus impactos extrapolam qualquer departamento. Eles chegam ao financeiro,

comprometem indicadores comerciais, afetam a experiência do cliente e colocam em risco a reputação construída ao longo de anos. Em muitos casos, o incidente cibernético é apenas o gatilho de uma cadeia de perdas muito mais ampla do que a falha técnica em si.

A questão central para a diretoria precisa mudar de foco. Pergunte ao seu time financeiro: qual é o valor exato de um dia inteiro com a empresa de portas fechadas?

A resposta para essa pergunta determina a prioridade da segurança da informação na estratégia do negócio. Empresas resilientes investem em proteção contínua para garantir a previsibilidade do faturamento e a sobrevivência da operação.

A cibersegurança precisa ser vista como uma espécie de apólice operacional. Não porque elimina todos os riscos — isso simplesmente não existe —, mas porque reduz a probabilidade de que um incidente comprometa a continuidade do negócio.

Empresas resilientes não investem em segurança apenas para proteger servidores ou dados. O objetivo final é manter sua capacidade de operar.

O custo real de um ataque não vem do sistema danificado, mas do faturamento que é interrompido durante a crise.

(*) CEO da Pronnus Tecnologia, uma empresa do Grupo Sancon.

O JORNAL CERTIFICA
AS PUBLICAÇÕES LEGAIS
COM PONTUALIDADE E
TRANSPARÊNCIA, CUMPRINDO
AS NORMAS JURÍDICAS.
AFINAL, O JORNAL É LEGAL.

EAÍ CLUBE AUTOMOBILISTA S.A.

CNPJ nº 34.656.383/0001-72 - NIRE 35300541065

Ata da Assembleia Geral Extraordinária

Data, Hora e Local: 19 de junho de 2026 às 10 horas, na sede social. **Mesa:** Alexandre Mendes Palhares - Presidente; Marina Guimarães Moreira Mascarenhas - Secretária. **Ordem do Dia e Deliberações unânimes:** 1. Aprovam a alteração da redação do caput do Artigo 3 do Estatuto Social, que passará a vigorar com a seguinte redação: **“Artigo 3 - A Companhia tem como objeto social (a) atuar como clube de benefícios automobilísticos, permitindo o aproveitamento de benefícios e serviços por seus usuários, incluindo mas não se limitando a, conceder descontos vinculados ao clube; (b) comercialização, intermediação e prestação de serviços de gestão de relacionamento com geração de pontos e resgate de benefícios aos usuários; (c) gerenciamento de contas para pagamentos digitais; (d) gestão dos valores aportados em carteira digital; (e) captura e liquidação financeira das transações de pagamento em geral em rede de parceiros e entre contas; (f) gestão e oferta de produtos financeiros; (g) licenciamento ou cessão de direito de uso de software; (h) atividades de publicidade; (i) a fabricação ou produção, preparação, mistura, empacotamento, armazenagem, distribuição, transporte e venda de lubrificantes, graxas, líquidos de refrigeração (para resfriar e anticorrosivos), fluidos de freio e outros fluidos, diretamente ou por meio de terceiros; (j) a importação ou exportação de lubrificantes, graxas, líquidos de refrigeração (para resfriar e anticorrosivos), fluidos de freio e outros fluidos, incluindo amostras de aditivos e óleo para análise; (k) a importação, exportação, instalação e venda de produtos e equipamentos relacionados à indústria petrolífera; (l) a importação, exportação, venda e distribuição de equipamentos e produtos, incluindo peças e acessórios para a indústria automotiva; (m) a prestação de serviços de filtragem de óleo para clientes, gerenciamento de estoque, depósito, consultoria técnica, comercial e administrativa; (n) a prestação de serviços aduaneiros e operações portuárias; (o) a comercialização de produtos de marketing ou quaisquer outros produtos relacionados ao objeto da sociedade; (p) a representação de outras sociedades locais ou estrangeiras, diretamente ou por meio de terceiros, mediante comissionamento ou consignação, ou por qualquer outro meio legal; (q) a venda, comercialização e/ou distribuição de óleo básico; (r) a prestação de serviços de armazenagem para terceiros; (s) locação de bens móveis e imóveis; e (t) a distribuição de aditivos para óleos lubrificantes. Parágrafo Único - A Companhia poderá adquirir ações, cotas ou participações em outras empresas.”** 2. Aprovam a consolidação do Estatuto Social, conforme Anexo I da presente ata. Esta ata foi lida, aprovada e assinada pelos presentes. A íntegra da ata está publicada no endereço eletrônico deste jornal nesta data. Registro JUCESP nº 299.881/26-0, em 28/07/2026. Marina Centurion Dardani - Secretária Geral.

EAÍ CLUBE AUTOMOBILISTA S.A.

CNPJ nº 34.656.383/0001-72 - NIRE 35.300.541.065

Ata da Assembleia Geral Extraordinária

Realizada em: 29/12/2025. **Certidão:** Secretaria de Desenvolvimento Econômico - JUCESP. Certifico o Registro sob o número 168.621/26-5 em 30/03/2026. Marina Centurion Dardani - Secretária Geral.

ASSOCIAÇÃO PORTUGUESA DE DESPORTOS

Edital de Convocação
Assembleia Geral Extraordinária

Em conformidade com o Estatuto Social da Associação Portuguesa de Desportos, ficam os senhores associados titulares, em pleno gozo de seus direitos sociais, maiores de 18 anos, com mais de 2 (dois) anos no quadro social e adimplentes com as taxas sociais até o último dia do mês anterior à realização desta Assembleia, convocados para a **ASSEMBLEIA GERAL EXTRAORDINÁRIA**, mediante requerimento do Presidente do Conselho Deliberativo, por meio do Ofício nº 005/2026. A Assembleia será realizada no dia **14 de setembro de 2026**, no Ginásio Rauzão, localizado na Rua Comendador Nestor Pereira, nº 33, Canindé, São Paulo, **com início às 8h**, em primeira chamada, com 2/3 (dois terços) do Conselho Deliberativo, ou, em segunda chamada, uma hora depois, com qualquer número. A Assembleia permanecerá aberta **até às 18h**, quando serão fechados os portões do Ginásio Rauzão. Após esse horário, somente terão direito a voto os associados que estiverem dentro do Ginásio Rauzão. **ORDEM DO DIA:** 1. Homologar ou não o novo Estatuto Social da Associação Portuguesa de Desportos, com a incorporação das três sugestões apresentadas pelo Conselho de Orientação e Fiscalização, conforme aprovado por unanimidade pelos Conselheiros em Reunião Ordinária realizada em 17 de agosto de 2026. **OBS.: O referido documento estará disponível exclusivamente para consulta dos associados titulares, em pleno gozo de seus direitos sociais, junto à Secretaria da Associação, em ambiente fechado. Não será permitida a reprodução ou obtenção de cópias ou fotocópias do documento, em razão da cláusula de confidencialidade.** **ATENÇÃO:** No dia da Assembleia, o clube estará fechado para as demais atividades, não sendo permitida a entrada na sede do clube de pessoas que não sejam associados com direito a voto. São Paulo, 26 de agosto de 2026. **Marcos Rogério Lico** - Presidente da Assembleia Geral





PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Certisign Assinaturas. Para verificar as assinaturas clique no link: <http://assinaturas.certisign.com.br/Verificar/E283-84BB-016E-0D98> ou vá até o site <http://assinaturas.certisign.com.br> e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: E283-84BB-016E-0D98



Hash do Documento

13DD3E659422A75EA8C1FF9619E599EFACF9E8DC794B4D639741A773AB56072F

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 02/09/2026 é(são) :

☒ Lilian Mancuso - 05.687.343/0001-90 em 02/09/2026 20:00 UTC-03:00

Nome no certificado: Jornal Empresas E Negocios Ltda

Tipo: Certificado Digital - JORNAL EMPRESAS E NEGOCIOS LTDA - 05.687.343/0001-90

Evidências

Geolocation: Location not shared by user.

IP: 172.16.4.14

AC: AC Certisign RFB G5

