

Ferramentas de IA podem trazer riscos para a cibersegurança de empresas

Alberto Jorge, especialista em segurança cibernética e CEO da Trust Control, alerta para uso de IAs generativas não autorizadas. 97% dos vazamentos de dados com IA ocorrem porque não há controles de acesso adequados.

“Todo mundo está falando e usando Inteligência Artificial, mas quase ninguém está se preocupando com os perigos que ela pode trazer para a segurança de dados”. A afirmação de Alberto Jorge, especialista em cibersegurança e CEO da Trust Control, evidencia a necessidade que os usuários em geral precisam ter na utilização das ferramentas de Inteligência Artificial, especialmente as chamadas IAs generativas. Estudos especializados mostram que, em todo o mundo, empresas estão enfrentando em média 223 incidentes mensais relacionados à IA generativa. Cerca de 97% dos vazamentos de dados com IA ocorrem porque não há controles de acesso adequados. “O maior risco imediato é o compartilhamento involuntário de informações confidenciais com a IA. Dados inseridos em chatbots públicos são tratados como informação pública”, alerta Alberto Jorge.

No Brasil

Em nosso país, o cenário é particularmente preocupante. Em 2025, o país registrou 1,4 milhão de ataques por minuto, impulsionados por malwares que cresceram 535% com o uso de IA. Em 2026, os ataques autônomos de IA já são realidade: sistemas de IA estão identificando e explorando vulnerabilidades sem intervenção humana. “A Inteligência Artificial cria uma dualidade perigosa na segurança cibernética. Enquanto equipes de defesa usam IA para reduzir o tempo de detecção de incidentes, os hackers usam IA para criar deepfakes e fazer ataques em massa”, observa o CEO da Trust Control.

Shadow IA

A chamada Shadow IA, ou IA Sombria, ocorre quando usuários utilizam ferramentas de IA sem autorização ou fora das políticas de segurança da organização. Esta é considerada uma das maiores ameaças à segurança. Estimativas apontam que, até 2033, 40% das empresas vão sofrer violações relacionadas ao Shadow AI. Utilizar ferramentas de IA não autorizadas pode acarretar em exposição massiva de dados, com consequências legais, resultando em multas, penalidades e até prisão por violação de LGPD ou segredos comerciais.

“A proteção de dados na era da IA exige governança desde o design, passando pela capacitação de equipes, monitoramento contínuo de uso não autorizado de ferramentas e a integração de segurança cibernética em todos os projetos de IA da organização”, recomenda Alberto Jorge.

Veja orientações para utilizar a IA no dia a dia sem correr riscos cibernéticos:

- Configure a privacidade e segurança: ative autenticação de dois fatores (2FA) e desative o histórico de chats quando disponível.
- Nunca insira dados sensíveis ou pessoais, como CPF, senhas, dados bancários ou documentos corporativos. Todo prompt é informação pública, que pode vaziar publicamente.
- Valide todas as respostas e links gerados: Contraste informações com fontes oficiais antes de usar em decisões.
- Use ferramentas corporativas aprovadas: utilize apenas IA aprovada pela empresa com governança definida. Evite extensões e plugins não verificados de fontes não confiáveis.

Empresas de médio porte serão as grandes beneficiadas pela inteligência artificial

Com estruturas mais complexas que as pequenas empresas e menos burocráticas que as grandes corporações, empresas médias estão em posição privilegiada para capturar ganhos de produtividade, reduzir custos e acelerar o crescimento ao implementar novas tecnologias

Durante muito tempo, a adoção de tecnologias avançadas esteve associada às grandes corporações. A Inteligência Artificial (IA), no entanto, está mudando essa lógica. O time de especialistas da QYON Software - empresa norte-americana especializada no desenvolvimento de softwares de gestão com IA - aponta que as empresas de médio porte devem ser as mais beneficiadas pela nova onda tecnológica, justamente por ocuparem uma posição estratégica entre a agilidade das pequenas empresas e a escala das grandes organizações.

Esse movimento já pode ser observado nos números. Estudo da Deloitte mostra que as empresas médias vêm acelerando seus investimentos em IA e, em muitos casos, avançam mais do que grandes corporações na implementação de soluções baseadas em nuvem, machine learning e automação inteligente. Segundo o levantamento, 80% das empresas médias pretendem aumentar seus investimentos em IA, percentual superior ao registrado entre grandes organizações.

Para Maurício Frizzarin, fundador e CEO da QYON Software, a explicação está na combinação entre necessidade operacional e capacidade de adaptação. “As empresas médias estão em um momento importante de crescimento. Elas já possuem operações relativamente complexas, múltiplos departamentos, volumes significativos de dados e



ainda têm velocidade para implementar mudanças. Isso faz com que consigam capturar valor da IA mais rápido do que muitas das grandes corporações”, analisa.

À medida que crescem, as empresas médias enfrentam um problema comum: o aumento da complexidade operacional. Processos financeiros, fiscais, comerciais, administrativos e de atendimento passam a demandar mais pessoas, mais controle e mais tempo de gestão. Em muitos casos, o crescimento da estrutura ocorre em ritmo semelhante ao crescimento da receita, reduzindo ganhos de eficiência. É justamente nesse ponto que a Inteligência Artificial tem demonstrado maior impacto. Afinal, a automação de processos administrativos, financeiros e operacionais permite eliminar tarefas repetitivas, reduzir retrabalho, integrar informações e aumentar significativamente a produtividade das equipes.

“Empresas que implementam IA em processos administrativos registram reduções de custos que

variam entre 15% e 30%, além de ganhos relevantes de produtividade e velocidade na tomada de decisão”, destaca Frizzarin. Por isso, na avaliação do especialista, o maior benefício da IA para empresas médias não está apenas na economia financeira, mas na possibilidade de que gestores e colaboradores dediquem esforços a iniciativas estratégicas. “A IA não está apenas automatizando tarefas, mas devolvendo tempo para que empresários e gestores foquem em inovação, crescimento, relacionamento com clientes e planejamento estratégico”, afirma o executivo.

O CEO da QYON Software aponta que uma das tendências mais promissoras para os próximos anos é o avanço dos chamados ‘agentes de IA’, sistemas capazes de executar tarefas, interagir com usuários, analisar informações e apoiar decisões de forma contínua. Inclusive, uma pesquisa global feita pela McKinsey mostra que 62% das organizações já avaliam o uso de agentes inteligentes em suas operações e 64% das empresas

afirmam que a IA já contribui diretamente para iniciativas de inovação.

Na prática, esses agentes podem atuar como: assistentes administrativos, analistas financeiros, conciliadores bancários, atendedores digitais, agentes de cobrança, etc. A expectativa é que esse modelo transforme profundamente a forma como empresas organizam suas operações.

A tendência é que a Inteligência Artificial se torne um componente essencial da gestão empresarial nos próximos anos. Para Frizzarin, o cenário aponta para uma mudança estrutural no ambiente corporativo. “As empresas médias têm uma oportunidade única de dar um salto de eficiência. A IA permite crescer sem aumentar proporcionalmente os custos e a estrutura operacional. Quem aproveitar esse momento terá uma vantagem competitiva importante nos próximos anos”, afirma o executivo.

Segundo o especialista, a próxima fase da transformação digital será marcada por organizações híbridas, nas quais profissionais humanos atuarão de forma cada vez mais estratégica, enquanto agentes inteligentes assumirão parte significativa das tarefas operacionais. “O futuro não será das empresas que trabalham mais, mas daquelas que conseguem produzir mais valor com menos esforço operacional”, finaliza Maurício Frizzarin, fundador e CEO da QYON Software.

Proclamas de Casamentos

CARTÓRIO DE REGISTRO CIVIL

33º Subdistrito - Alto da Mooca ILZETE VERDERAMO MARQUES - Oficial

Faço saber que os seguintes pretendentes apresentaram os documentos exigidos pelo Art. 1525, do Código Civil Atual Brasileiro e desejam se casar:

O pretendente: **JOÃO VITOR VIEIRA SANTOS**, estado civil divorciado, filho de Roberval Pereira Santos Filho e de Arleide Pereira Vieira, residente e domiciliado no Alto da Mooca, neste subdistrito - São Paulo - SP. A pretendente: **THAIS DA SILVA RIBEIRO**, estado civil solteira, filha de Anderson Tolentino Ribeiro e de Elisângela Maria da Silva, residente e domiciliada em São Paulo - SP.

O pretendente: **DANIEL HUANCA VILLAZANTE**, estado civil solteiro, filho de Humberto Huanca Cuti e de Elizabeth Villazante Mamani, residente e domiciliado neste Subdistrito, Alto da Mooca - São Paulo - SP. A pretendente: **DANIELA CANAVIRI CHIRINOS**, estado civil solteira, filha de Victor Hugo Chirinos Huchani e de Carmen Canaviri Mamani, residente e domiciliada neste Subdistrito, Alto da Mooca - São Paulo - SP.

O pretendente: **RODRIGO PORTO BARACCHINI**, estado civil solteiro, filho de Eduardo Baracchini e de Rita Maria Porto Baracchini, residente e domiciliado no Butantã, nesta Capital - São Paulo - SP. A pretendente: **LETICIA MARINA ARAUJO MEDEIROS**, estado civil solteira, filha de Wellington de Medeiros e de Maria de Lourdes Araujo Medeiros, residente e domiciliada no Alto da Mooca, neste subdistrito - São Paulo - SP. Obs.: O pretendente e residente a Rua Butantã, nº 550, apto. 1202 B, Butantã - nesta Capital - São Paulo - SP e a pretendente é residente à Rua da Mooca, nº 4396, apto. 25, Alto da Mooca, neste subdistrito - São Paulo - SP. Em razão da revogação do parágrafo 4º do Artigo 67, da Lei 6015/77, pelo Artigo 20, Item III, alínea "b" da Lei 14.382/22, deixo de encaminhar Edital de Proclamas para afixação e publicidade ao Cartório de residência do pretendente.

O pretendente: **PAULO RICARDO DORATHIOTO**, estado civil solteiro, filho de Carlos Augusto Dorathioti e de Bernadete Akico Nishiguti Dorathioti, residente e domiciliado neste Subdistrito, Alto da Mooca - São Paulo - SP. A pretendente: **MARIA CLAUDIA PASCHOALATTO MATEO**, estado civil solteira, filha de Luis Antonio Mateo Suanes e de Rosemary Aparecida Paschoalatto Mateo, residente e domiciliada neste Subdistrito, Alto da Mooca - São Paulo - SP.

O pretendente: **MASSIMILIANO BELLAVIA**, estado civil solteiro, filho de Antonino e de Maria Tesouro, residente e domiciliado no Alto da Mooca, neste subdistrito - São Paulo - SP. A pretendente: **RUTH MARIANA CLAROS VALLEJOS**, estado civil solteira, filha de Mario Claros Flores e de Lucia Vallejos Valdiviezo, residente e domiciliada no Alto da Mooca, neste subdistrito - São Paulo - SP.

Se alguém souber de algum impedimento, oponha-se na forma da lei. Lavro o presente, para ser afixado no Oficial de Registro Civil e publicado na imprensa local
Jornal Empresas & Negócios

CARTÓRIO DE REGISTRO CIVIL DE PESSOAS NATURAIS

15º Subdistrito - Bom Retiro Amanda de Rezende Campos Marinho Couto - Oficial

Faço saber que os seguintes pretendentes apresentaram os documentos exigidos pelo Art. 1525, do Código Civil Atual Brasileiro e desejam se casar:

O pretendente: **JUVENAL INÁCIO DA SILVA**, nascido em Itajubá, MG, no dia 07/11/1997, profissão produtor rural, estado civil viúvo, residente e domiciliado neste Subdistrito, São Paulo, SP, filho de Inacio Ferreira da Silva e de Maria Aparecida Maciel da Silva. A pretendente: **LUANA JESUS DE LIMA**, nascida em Corumbá, MS, no dia 13/12/1990, profissão enfermeira, estado civil solteira, residente e domiciliada neste Subdistrito, São Paulo, SP, filha de Venancio Leme de Lima e de Maria Expedita de Jesus.

O pretendente: **DERLI FRANCISCO JUNIOR**, nascido em São José, SC (registrado no Subdistrito Estreito em Florianópolis, SC), no dia 21/08/1996, profissão músico regente, estado civil solteiro, residente e domiciliado neste Subdistrito, São Paulo, SP, filho de Derli Francisco e de Rosânia de Souza Francisco. A pretendente: **JULIA PEDROTTI**, nascida nesta Capital, Santa Cecília, SP, no dia 17/12/1995, profissão produtora, estado civil solteira, residente e domiciliada neste Subdistrito, São Paulo, SP, filha de Vitor Antonio Pedrotti e de Maria Luiza Santiago de Oliveira Pedrotti.

Se alguém souber de algum impedimento, oponha-se na forma da lei. Lavro o presente, para ser afixado no Oficial de Registro Civil e publicado na imprensa local
Jornal Empresas & Negócios

Quatro dicas para não cair em golpes ao validar documentos

Especialista aponta cuidados essenciais para evitar golpes em um cenário de avanço de deepfakes, phishing e identidades sintéticas. Com o avanço da digitalização, validar documentos online deixou de ser apenas uma etapa operacional e passou a representar um desafio crescente de segurança digital.

Segundo o Relatório de Identidade e Fraude 2025, da Serasa Experian, 51% dos brasileiros sofreram algum tipo de fraude no último ano. Ao mesmo tempo, golpes envolvendo documentos falsos e identidades sintéticas vêm ganhando sofisticação com o uso de inteligência artificial, deepfakes e dados vazados.

O tema ganhou ainda mais relevância após o Conselho Nacional de Justiça (CNJ) anunciar que tornará obrigatória, a partir de maio de 2026, a autenticação em dois fatores nos sistemas da Plataforma Digital do Poder Judiciário (PDPJ-Br), substituindo códigos enviados por e-mail por aplicativos autenticadores como Google Authenticator e FreeOTP.

Para Klaus Riffel, fundador e CEO da doc9, lawtech que desenvolve soluções de automação, gestão operacional e segurança digital para o setor jurídico, o movimento mostra que identidade digital e controle de acessos deixaram de ser uma preocupação restrita à área de tecnologia. “O problema hoje não é apenas um documento falso, mas identidades digitais construídas com dados reais e combinadas com ferramentas de IA. Isso exige processos mais robustos

de autenticação, validação e rastreabilidade”, afirma.

Diante desse cenário, o especialista aponta quatro cuidados essenciais para reduzir o risco de golpes ao validar documentos:

1. Ative autenticação em dois fatores

O uso de aplicativos autenticadores adiciona uma camada extra de segurança e reduz significativamente o risco de acessos indevidos, mesmo em casos de vazamento de senhas. A própria decisão do CNJ de tornar obrigatória a autenticação em dois fatores nos sistemas da PDPJ-Br reforça como identidade digital e validação de acessos passaram a ser temas críticos.

O movimento também aumentou a preocupação de empresas com o controle sobre certificados digitais utilizados para acessar tribunais e sistemas corporativos. Hoje, o Whom.doc9, plataforma de gestão de certificados digitais da doc9, gerencia cerca de 60 mil certificados para mais de 100 mil usuários ativos em todo o país, permitindo rastrear acessos, definir permissões e reduzir riscos relacionados ao uso indevido de credenciais.

2. Confira a origem da plataforma

Antes de enviar documentos pessoais, é importante validar se o link pertence ao domínio oficial da empresa ou instituição. O Brasil registrou mais de 500 milhões de tentativas de phishing em 2025, segundo a Kaspersky.

3. Controle onde e para quem você envia seus documentos

RG, CPF e CNH devem ser enviados apenas por canais confiáveis e, sempre que possível, acompanhados de marca d'água indicando a finalidade do uso. Segundo levantamento da CAF, empresa especializada em verificação documental, as tentativas de fraude com documentos no Brasil mais que dobraram entre 2022 e 2025, chegando a mais de 51 mil casos. Em 84% delas, o documento alvo foi o RG, o mais comum entre os brasileiros e o que circula com maior facilidade em processos digitais. Golpistas montam dossiês combinando dados de diferentes vazamentos para construir identidades sintéticas e fraudar validações em sequência.

4. Não confie apenas na aparência do documento

Deepfakes e documentos gerados por IA tornaram fraudes digitais mais difíceis de identificar visualmente. Em casos sensíveis, a recomendação é validar informações por canais oficiais e utilizar ferramentas adicionais de verificação.

“Quando o Judiciário muda seus protocolos de autenticação e os dados mostram que fraudes documentais digitais já superam as físicas, o recado é claro: o ambiente mudou. Quem ainda valida documentos só na base do olhar crítico ou da assinatura manuscrita está operando com ferramentas do passado para enfrentar ameaças do futuro”, completa Riffel.

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/4526-031E-B6BE-C7BC> 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: 4526-031E-B6BE-C7BC



Hash do Documento

54174806193928579802E25D5E9208A27E8BC09215F3C313BFDC3D11278AFA81

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 22/06/2026 é(são) :

- Lilian Regina Mancuso - 05.687.343/0001-90 em 22/06/2026 19:07 UTC-03:00
Tipo: Certificado Digital - JORNAL EMPRESAS E NEGOCIOS LTDA - 05.687.343/0001-90

Evidências

Geolocation: Location not shared by user.

IP: 172.16.4.22

AC: AC Certisign RFB G5

