TI (NE)

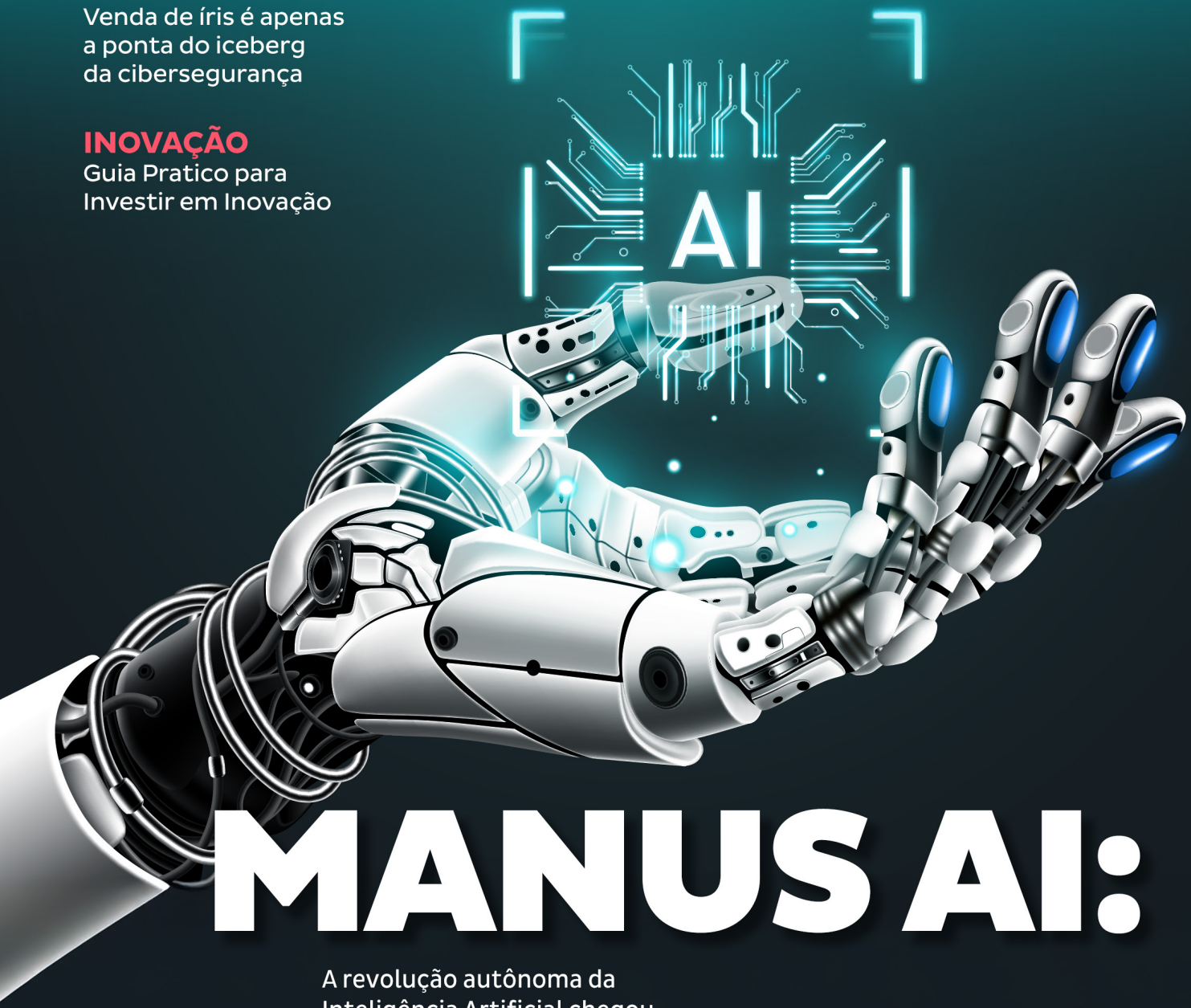
Revista TI Nordeste
Informação a serviço da região

JAN, FEV, MAR E ABR / ANO 13 / Nº68

GTN GRUPO TI NORDESTE

BIOMETRIA
Venda de íris é apenas a ponta do iceberg da cibersegurança

INOVAÇÃO
Guia Pratico para Investir em Inovação



MANUS AI:

A revolução autônoma da Inteligência Artificial chegou

NÓS TEMOS APOIADORES DE PESO

A TI (NE) é uma revista digital e interativa, campeã de audiência na região Nordeste e a mais querida em seu segmento. Em recente pesquisa, o índice de satisfação com o conteúdo da revista atingiu 97% entre os leitores*. Nós sempre apoiamos o desenvolvimento da tecnologia e inovação na região Nordeste.

E AGORA GANHAMOS UM APOIO EXTRA!

O nosso muito obrigado aos nossos apoiadores oficiais

DONE! agência digital

agis

simple

QUITERIO TELECOM

cloud expert xtrategus

A SUA EMPRESA TAMBÉM PODE APOIAR ESSA INICIATIVA. FALE CONOSCO!

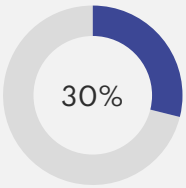
*Pesquisa realizada pela TI Nordeste em sua base de leitores, respondida por 227 leitores. O conteúdo foi avaliado por 50% como ótimo e 47% como bom.

SUMÁRIO

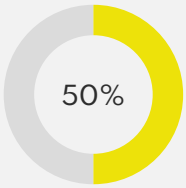
CHEGOU simplo crm

O CRM para a pequena e média empresa

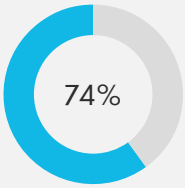
O CRM é mais do que uma ferramenta, ele é **um amplificador de resultados** e possibilita que cada interação se **converta em vendas crescentes.**



O CRM pode **aumentar vendas** em 30%



50% dos empresários dizem que o CRM **aumentou a produtividade**



74% dizem que **aumentou seu relacionamento** com o cliente

*fonte: Finance online

O que o Simplo CRM faz pela sua empresa?

- Integra todo o seu atendimento inclusive Whatsapp e Mídias Sociais (Ominichannel)
- Armazena todas as informações do cliente em uma única plataforma segura em nuvem
- Agendamento automático de tarefas. Nunca mais perca uma oportunidade de venda por omissão
- Funil de Vendas completo. Descubra os gargalos e conduza o cliente na jornada de compra
- Previsibilidade de Vendas
- Facilidade de uso: software 100% brasileiro
- Possibilidade de incluir também o funil de pós-venda
- Suporte para implantação
- Gatilhos Inteligentes

É Simples? **É Simplo!**

Experimente o CRM que vai potencializar as vendas do seu negócio.

Clique aqui e teste gratuitamente por 7 dias.

SUA OPINIÃO É IMPORTANTE!

A Revista TI (NE) quer ouvir você, leitor. Dê a sua opinião, faça sua crítica ou sugestão sobre as nossas matérias.

EMAIL
redacao@tinordeste.com

TELEFONE
71 3480-8130

EXPEDIENTE

Presidente do Grupo TI Nordeste
José Augusto Barretto

Conselho Editorial
Adriele Strada
Diego Caldas
José Augusto Barretto

Redação e Revisão
Niara Araujo

Mídias Sociais
Adriele Strada
Sheyla Limeira

Projeto Gráfico e Diagramação
Tayara Machado

Redação
redacao@tinordeste.com

Para anunciar
comercial@tinordeste.com

Para assinar
www.tinordeste.com/assine

PORTAL
www.tinordeste.com

GTN GRUPO TI NORDESTE

ABNT LANÇA NORMA INOVADORA PARA ACESSIBILIDADE DIGITAL

Nova diretriz visa tornar a web mais inclusiva, garantindo que pessoas com deficiência naveguem com autonomia e equidade

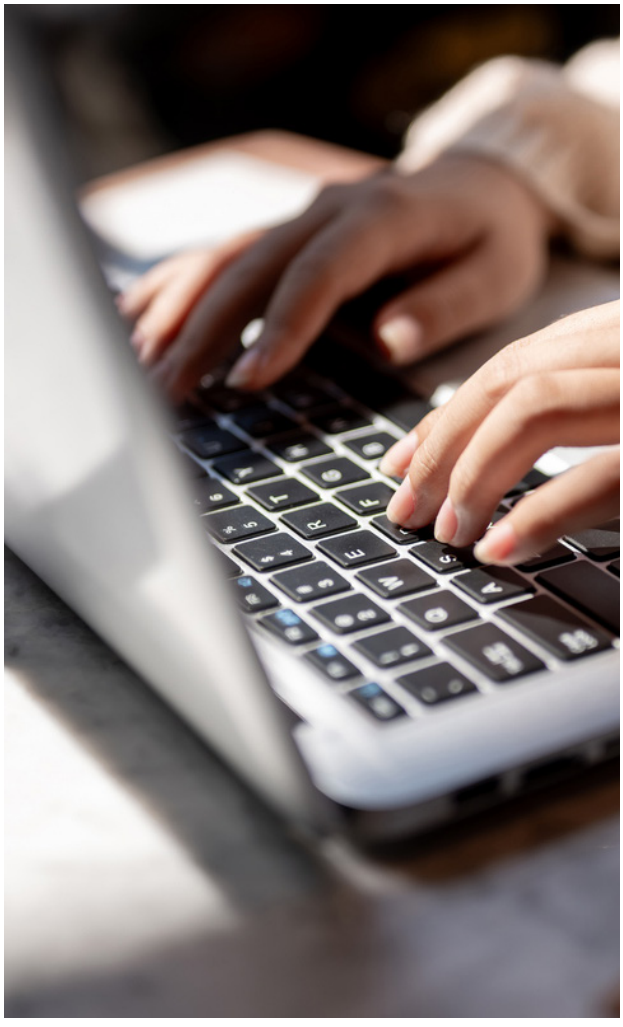
Em um movimento que promete redefinir o cenário da inclusão digital no Brasil, a Associação Brasileira de Normas Técnicas (ABNT) acaba de lançar a ABNT NBR 17225, uma norma técnica abrangente e inovadora, focada na acessibilidade de conteúdo e aplicações de web. O lançamento ocorreu no dia 11 de março de 2025, na sede do Google em São Paulo, reunindo um seleto grupo de especialistas, representantes de diversas entidades e defensores apaixonados pela causa da acessibilidade.

A ABNT NBR 17225, resultado de um trabalho colaborativo desenvolvido no âmbito do Comitê Brasileiro de Acessibilidade (ABNT/CB-040), estabelece critérios técnicos rigorosos e detalhados a fim de garantir que sites e aplicações digitais sejam acessíveis a todas as pessoas, independentemente de suas habilidades ou limitações. A norma se preocupa em garantir o acesso para pessoas com deficiência permanente, mas também para aqueles que enfrentam limitações temporárias ou até mesmo situacionais. Este documento representa um marco fundamental no cumprimento do artigo 63 da Lei Brasileira de Inclusão (LBI), que exige acessibilidade em plataformas digitais de empresas e órgãos públicos, consolidando o compromisso do país com a igualdade de acesso à informação e aos serviços online.

"A ABNT NBR 17225 reforça o compromisso da ABNT com a normalização técnica voltada à inclusão e acessibilidade. Esse trabalho reúne expertise nacional e internacional para estabelecer diretrizes que eliminem barreiras digitais e garantam o acesso equitativo à informação e aos serviços online", declara Mario Esper, presidente da ABNT, enfatizando a importância da norma para a construção de um futuro digital mais inclusivo e acessível a todos os brasileiros.

A criação da ABNT NBR 17225 foi um processo colaborativo, que se estendeu por quase dois anos e envolveu a participação ativa de 178 especialistas de diversas áreas do conhecimento. A iniciativa contou com a coordenação técnica do Centro de Estudos sobre Tecnologias Web (Ceweb.br), do Núcleo de Informação e

IMAGENS: DIVULGAÇÃO



Coordenação do Ponto BR (NIC.br), fortalecendo a sinergia entre a ABNT e outras instituições de referência no campo da acessibilidade digital. Antes de sua publicação oficial, o documento foi submetido a um rigoroso período de Consulta Nacional, garantindo ampla participação da sociedade e da comunidade técnica na definição dos padrões de acessibilidade.

"O Movimento Web para Todos estima que menos de 3% dos sites brasileiros seguem padrões de acessibilidade. Com essa norma, a ABNT coloca o Brasil na vanguarda da acessibilidade digital, reunindo diretrizes alinhadas às melhores práticas internacionais", ressalta Reinaldo Ferraz, gerente de projetos do Ceweb.br|NIC.br, evidenciando a importância da norma para impulsionar a acessibilidade digital no país e torná-lo um exemplo para o mundo.

A norma não apenas estabelece diretrizes técnicas, mas também promove uma mudança de mentalidade em relação à acessibilidade digital, incentivando empresas e organizações a adotarem uma cultura de inclusão e a considerarem a acessibilidade como parte integrante de seus processos de desenvolvimento e design.

O acesso ao conteúdo completo da ABNT NBR 17225 é totalmente gratuito e está disponível para consulta em www.abnt.org.br , permitindo que empresas, organizações, desenvolvedores e designers tenham acesso facilitado às diretrizes e recomendações necessárias para a criação de um ambiente digital mais inclusivo e acessível a todos. A iniciativa da ABNT representa um marco fundamental para a promoção da acessibilidade digital no Brasil e contribui para a construção de uma sociedade mais justa e igualitária, onde todas as pessoas tenham a oportunidade de desfrutar dos benefícios da tecnologia e da informação sem barreiras.

ALERTA VERMELHO: 91% DAS EMPRESAS LANÇAM APPS VULNERÁVEIS

Em um mundo cada vez mais dependente de aplicativos para as mais diversas atividades, desde a simples solicitação de uma refeição até complexas transações bancárias, a segurança dessas ferramentas digitais se tornou uma preocupação crucial e inadiável. No entanto, dados recentes têm acendido um alerta vermelho no mercado: um estudo da Checkmarx revelou que 91% das empresas admitem lançar aplicativos com vulnerabilidades. Essa estatística expõe uma fragilidade preocupante no cenário da segurança digital e exige uma reflexão sobre as práticas de desenvolvimento de software.

Wagner Elias, CEO da Conviso, empresa especializada em segurança de aplicações (AppSec), ressalta a gravidade da situação e a necessidade de evoluir as estratégias de segurança na criação de softwares. "Recentemente, um relatório da Checkmarx me chamou a atenção ao revelar que 91% das empresas admitem lançar aplicativos com vulnerabilidades. Esse dado evidencia o quanto o setor ainda precisa evoluir para garantir a segurança na criação de softwares. Elementos como código, infraestrutura e nuvem demandam uma atenção redobrada. Mesmo diante de prazos apertados, é essencial encontrarmos maneiras mais eficazes de integrar a segurança, de forma mais eficaz, em cada etapa do desenvolvimento", afirma Wagner.

A complexidade inerente aos aplicativos modernos, somada à crescente sofisticação das ameaças cibernéticas, exige uma abordagem proativa e abrangente para garantir a segurança dos sistemas e a proteção dos dados dos usuários. As empresas precisam ir além das medidas tradicionais e adotar estratégias inovadoras que integrem a segurança em todas as fases do ciclo de vida do desenvolvimento de software.

Nesse contexto, Wagner identifica cinco tendências que prometem impactar significativamente a área de segurança de aplicativos até 2025, oferecendo soluções e abordagens promissoras para enfrentar os desafios do cenário digital:

1. **Ferramentas de Automação como Aliadas dos Desenvolvedores:** A automação surge como uma ferramenta indispensável para otimizar os processos de segurança e liberar os desenvolvedores para se concentrarem em tarefas mais estratégicas. O Application Security Posture Management (ASPM), por exemplo, permite a gestão contínua dos riscos associados às aplicações, automatizando a identificação, priorização e correção de vulnerabilidades. O Gartner prevê que até 2026, 60% das empresas vão adotar ASPM para melhorar a gestão da postura de segurança das suas aplicações, demonstrando a crescente importância da automação na segurança de aplicativos.

2. **Integração entre AppSec e CloudSec:** Com a crescente migração das aplicações para a nuvem, a integração entre as áreas de segurança de aplicações (AppSec) e segurança da nuvem (CloudSec) se torna essencial para garantir a proteção dos sistemas e dos dados. A colaboração entre essas áreas permite monitorar e proteger tanto o código quanto a infraestrutura de nuvem, reduzindo os riscos de ataques e falhas de segurança. A segurança deve ser tratada de forma integrada, garantindo que todos os componentes da aplicação estejam protegidos

3. **Inteligência Artificial na Segurança: Potencial e Cuidados:** A inteligência artificial (IA) oferece um enorme potencial para aprimorar a segurança de aplicativos, automatizando tarefas, identificando ameaças e auxiliando os desenvolvedores. Ferramentas como o GitHub Copilot, por exemplo, podem sugerir códigos em tempo real, aumentando a produtividade dos desenvolvedores. No entanto, é preciso ter cautela, pois estudos da Universidade de Stanford apontam que algumas ferramentas podem sugerir bibliotecas de código inseguras, exigindo uma revisão cuidadosa. Apesar desses desafios, a McKinsey prevê que, nos próximos anos, o uso de IA poderá gerar até US$ 340 bilhões no setor financeiro, demonstrando o impacto significativo da IA na segurança.

4. **Mais Autonomia para Desenvolvedores nas Decisões de Segurança:** Uma tendência importante é a crescente autonomia dos desenvolvedores nas decisões de segurança, permitindo que eles implementem soluções mais adequadas às necessidades específicas da aplicação desde o início do desenvolvimento. Essa mudança é positiva, pois os desenvolvedores possuem um conhecimento técnico profundo sobre as necessidades da aplicação e podem tomar decisões mais informadas sobre as ferramentas e práticas de segurança a serem adotadas.

5. **A Segurança de Aplicações será Prioridade em 2025:** A segurança de aplicações se tornará uma prioridade ainda maior para empresas de todos os tamanhos, impulsionada pelo aumento das ameaças cibernéticas e pela crescente dependência de aplicativos para as atividades cotidianas. O setor de segurança de aplicativos deve crescer de US$ 11,62 bilhões em 2024 para US$ 25,92 bilhões até 2029, demonstrando que a segurança se tornou um requisito indispensável.

"A segurança de aplicações será, sem dúvida, uma das principais prioridades para empresas de todos os tamanhos... Para as empresas, investir em segurança não se resume a adotar as ferramentas adequadas; é fundamental integrá-la ao processo de desenvolvimento. Isso exige uma colaboração estreita entre as equipes de desenvolvimento e segurança, assegurando que o software entregue seja não apenas funcional, mas também robusto e protegido contra ameaças", enfatiza o CEO da Conviso.

Diante desse cenário desafiador, as empresas que souberem se adaptar às novas tendências e integrarem a segurança em todas as etapas do ciclo de vida do desenvolvimento de software estarão mais bem preparadas para enfrentar as ameaças cibernéticas e proteger seus sistemas e dados. A segurança de aplicativos não é mais um luxo, mas sim uma necessidade para garantir a continuidade dos negócios e a confiança dos clientes.

CIBERSEGURANÇA 2025: GUIA EM 4 PASSOS FORTALECE A DEFESA DIGITAL

Akamai revela estratégias cruciais para empresas enfrentarem ameaças cibernéticas sofisticadas, com foco em personalização e proatividade.

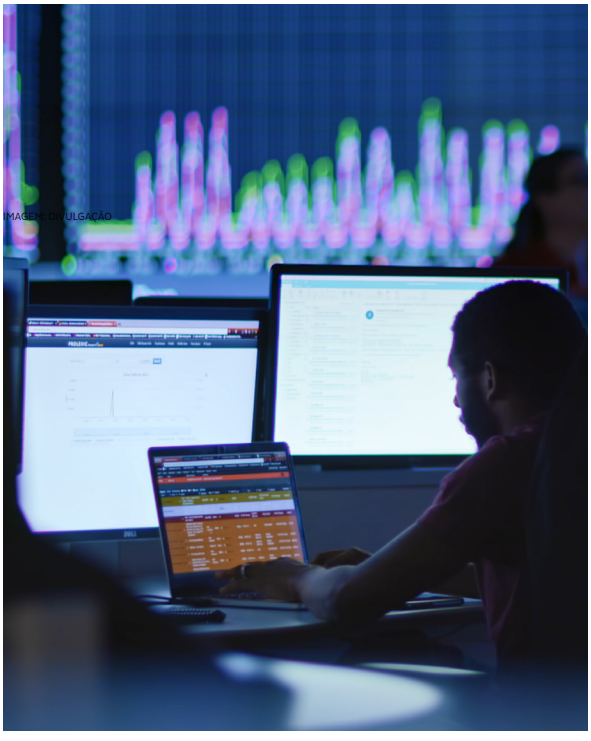


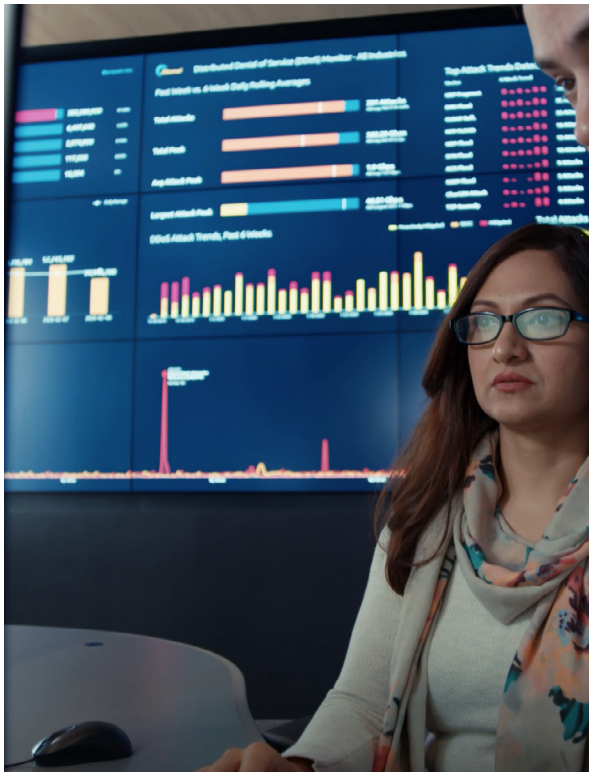
IMAGEM: DIVULGAÇÃO

As medidas digitais e de cibersegurança tradicionais já não são suficientes para proteger as empresas das ameaças cibernéticas atuais, cada vez mais sofisticadas. Para se defender de forma eficaz, é fundamental compreender a fundo o próprio negócio, adotar pesquisas e monitoramentos internos para desenvolver estratégias personalizadas e proativas, e estruturar programas de segurança alinhados aos perigos específicos do setor de atuação. A criação de dinâmicas alinhadas às tendências de ameaça é o diferencial necessário para fortalecer a defesa e minimizar riscos.

Essa é a premissa do relatório "Defender's Guide 2025: Fortify the Future of Your Defense" da Akamai, empresa líder em soluções de cibersegurança e desempenho na nuvem. O estudo reúne anos de pesquisa, insights de segurança e inteligência de mercado para oferecer aos profissionais de segurança as estratégias e técnicas necessárias para combater ataques.

"Ao aplicar análises técnicas e pesquisas à sua estratégia de cibersegurança, as organizações podem mitigar riscos de forma mais efetiva, em um ambiente digital cada vez mais complexo. Essa postura mantém as pessoas informadas e permite melhorar os processos, mitigando riscos, otimizando os investimentos e reduzindo o impacto de eventuais incidentes cibernéticos", explica Claudio Baumann, diretor geral da Akamai Technologies.

"Ao aplicar análises técnicas e pesquisas à sua estratégia de cibersegurança, as organizações podem mitigar riscos de forma mais efetiva, em um ambiente digital cada vez mais complexo. Essa postura mantém as pessoas informadas e permite melhorar os processos, mitigando riscos, otimizando os investimentos e reduzindo o impacto de eventuais incidentes cibernéticos" explica Claudio Baumann, diretor geral da Akamai Technologies.



Um dos levantamentos da Akamai que serve como base do guia para defensores coloca o Brasil na 4ª posição entre os países com mais servidores SSH abertos na internet, com 1,2 milhão de sistemas vulneráveis servindo como possível porta de entrada para ataques. Os Estados Unidos, na liderança, têm 6,2 milhões de servidores, de um total de mais de 22 milhões de infraestruturas em risco identificadas pela Akamai.

"Métricas de quantificação de risco, por exemplo, são amplamente aplicadas e úteis em organizações de todos os tipos, mas são desafiadoras em sua execução", completa Baumann. "É impossível generalizar, enquanto a replicação de um modelo existente é extremamente difícil, pois depende do tamanho, sofisticação e criticidade de cada operação, dentro de estruturas corporativas individuais."

O guia da Akamai elenca falhas comuns em arquitetura e configuração de redes, como brechas na autenticação e segmentação, segredos expostos em repositórios de código e VPNs mal configuradas, como alguns dos principais vetores de ataque a redes corporativas, que exigem atenção em 2025.

O relatório também destaca como os malwares evoluem para se tornarem mais difíceis de combater. Alguns operam sem arquivos (fileless), utilizando o próprio sistema operacional, enquanto outros adotam uma arquitetura descentralizada de controle e comando, tornando a campanha ofensiva mais difícil de combater. Ao mesmo tempo, prevalece a exploração de vulnerabilidades mais "tradicionais", como os equipamentos desatualizados, falhas Zero-Day ou tentativas de roubo de identidade, enquanto seguem como questões importantes a desfiguração de sites e o abuso de Kubernetes, elementos essenciais na gestão de aplicações.

"Os ciberataques podem ser lançados até mesmo por criminosos amadores, enquanto os grupos especializados estão se tornando cada vez mais habilidosos. E ainda temos a inteligência artificial, tornando os riscos ainda mais profundos, enquanto facilita o uso de ferramentas por atacantes de todos os níveis, com o resultado sendo um cenário mais imprevisível e perigoso do que nunca", completa Baumann.

4 Passos Essenciais para a Defesa Digital em 2025:

- Implementação de medidas de higiene digital para garantir a segurança cibernética das organizações.
- Uso de plataformas de segurança e segmentação, com firewalls, sistemas de proteção de APIs e arquitetura distribuída.
- Olhar aprimorado para os serviços mais críticos da empresa, priorizando medidas avançadas de proteção.
- Contar com times internos ou parceiros especializados em resposta a incidentes para mitigar danos e restabelecer as operações rapidamente.

GUIA PRÁTICO PARA INVESTIR EM INOVAÇÃO EM 2025

POR
ANNE TORRES

POR
LAÍS LEONCINI

[Laís Leoncini e Anne Torres são Gerentes de Negócios no FI Group, consultoria especializada na gestão de incentivos fiscais e financiamento à Pesquisa & Desenvolvimento (P&D)]

Mesmo sendo fundamental para alavancar a economia e fortalecer os negócios, a inovação ainda enfrenta desafios no Brasil. O País ocupa a 50ª posição no Índice Global de Inovação 2024, que avalia 133 nações e, embora siga sendo o líder entre as economias da América Latina e do Caribe, esse contexto ainda evidencia os obstáculos enfrentados pelo Brasil no que tange pesquisa, infraestrutura, investimento em novas tecnologias, educação e carência de divulgação e transparência nas políticas públicas que promovem a concepção de projetos inovadores.

Nesse sentido, trazendo à tona o cenário empresarial, é válido ressaltar que as empresas brasileiras assumem um papel fundamental no desenvolvimento da inovação no País, tendo em vista que impulsionam o crescimento socioeconômico, fomentando a geração de novos empregos e rendas. No entanto, ainda há uma longa jornada a ser percorrida para que as companhias ampliem ainda mais seu impacto inovador no mercado.

Desafios

Num cenário em que inovar é o caminho para se manter competitivo no mercado, muitas organizações ainda enfrentam o desafio de encarar a pesquisa e desenvolvimento de inovação (PD&I) como um custo, e não como prioridade. Além disso, é comum que a PD&I seja tratada de forma isolada, quando, na realidade, esse setor deve estar integrado à estratégia central do negócio para gerar resultados efetivos e mensuráveis.

Também é uma verdade que as empresas enfrentam um cenário incerto, caracterizado por volatilidade econômica e desafios regulatórios que exigem flexibilidade e adaptação constante, mas que, em contrapartida, se mostram como uma oportunidade para inovar, principalmente quando a mudança é tecnológica.

Em termos de barreiras burocráticas em inovação, um exemplo prático é o processo de aprovação de patentes no Brasil, que continua moroso. Não pode ser descartada, também, a escassez de mão de obra qualificada em áreas tecnológicas e científicas, dada a demanda e a saída de profissionais especializados para outros países.

Ou seja, todos esses pontos dificultam a implementação de soluções inovadoras, mas é a partir deles que fica clara a importância de repensar processos, investir em capacitação, melhorar a eficiência da desburocratização e, acima de tudo, tratar a inovação como centro estratégico do crescimento empresarial, social e econômico.

Os tipos de inovação

Existem diversos tipos de inovação disponíveis para diferentes empresas, variando conforme suas necessidades e os recursos disponíveis, e é importante compreendê-las para que haja um crescimento sustentável frente ao investimento.

A inovação incremental é a mais viável a curto e médio prazo, pois está associada a melhorias contínuas em produtos, processos e serviços já existentes, com mudanças que representam menor risco, mas que podem agregar ganhos significativos na competitividade, uma vez que é mais fácil de ser aceita pelo mercado em sua sutileza.

Já a inovação disruptiva introduz um novo modelo de negócio ou tecnologia que pode transformar setores inteiros e desestabilizar as empresas tradicionais. Esse modelo apresenta um risco mais elevado, além de exigir investimentos substanciais desde as fases iniciais de desenvolvimento.

Por outro lado, a inovação radical, menos comum, ocorre quando há uma mudança profunda na dinâmica de um mercado, alterando seu funcionamento ou até mesmo criando um segmento. É o tipo de inovação com mais vantagens competitivas no longo prazo.

Não obstante, além dos tipos mencionados, há, também, os modelos de inovação, ou seja, a maneira como as empresas optam por investir em inovação considerando a sua cultura e planejamento.

O mais conhecido, atualmente, é a Inovação Aberta (Open Innovation), que se baseia na colaboração entre empresas e

outros agentes desse ecossistema, como é o caso das startups, centros de pesquisa e universidades. Esse é um modelo significativamente importante para o desenvolvimento socioeconômico do País, pois permite a troca de conhecimento e amplia o acesso aos diferentes momentos tecnológicos que cada um desses agentes vivencia.

Existem segmentos que são mais maduros em relação à inovação, como é o caso das startups, que vêm crescendo ano após ano impulsionadas pelo conceito de Inovação Aberta. Esse modelo as incentiva a desenvolverem tecnologias mais ágeis e disruptivas para o mercado. Além disso, grandes empresas têm investido cada vez mais em startups, seja por meio de aportes financeiros ou fusões e aquisições (M&As).

Há, ainda, outros setores do mercado que se destacam em inovação, sendo eles farmacêutico, químico, informática, produtos eletrônicos, máquinas e equipamentos, bem como agrícola e bancário, impulsionados pelo avanço de tecnologias, como Inteligência Artificial (IA) e Internet das Coisas (IoT).

IMAGEM: ISTOCK

O passo a passo para uma empresa inovar

A implementação de uma estratégia de inovação requer planejamento estruturado e alinhamento dos objetivos da empresa, com definição do impacto esperado em termos de crescimento e competividade e dos indicadores de medição, com a criação de uma governança clara e comprometida.

Uma vez realizada a definição estratégica, a companhia inicia o processo de reunir insights e iniciativas inovadoras para as empresas, compreendendo as necessidades já pré-existentes e identificando as soluções que se destacam tanto em inovação quanto em aplicabilidade.

Na sequência, a organização precisa criar a abertura de um projeto para, então, realizar uma avaliação de viabilidade técnica e financeira da iniciativa. A partir disso, deve-se preparar um plano de projeto, reunindo as documentações necessárias para o termo de abertura da iniciativa.

O próximo passo é elaborar um plano de gestão de projetos, seguido do gerenciamento do escopo, que estrutura os objetivos e define a organização analítica que a iniciativa deve seguir. Vale ressaltar que o plano de gerenciamento é essencial para definir as fases do projeto, atribuir responsáveis e acompanhar o status de execução quando a iniciativa já estiver em prática.

Posteriormente, entra em ação o plano de gerenciamento de trabalho, que controla todas essas vertentes e garante que tudo esteja sendo cumprido conforme o planejamento inicial. Além disso, há o plano de garantia de qualidade, que verifica se os padrões de qualidade estabelecidos no início do projeto estão sendo alcançados.

Por fim, é essencial desenvolver um plano de gerenciamento de riscos. Nessa etapa, devem ser definidas as soluções propostas para superar esses desafios, além da possibilidade de surgirem novas oportunidades que extrapolem a iniciativa original. Também são estabelecidas as ações necessárias para mitigar riscos e dar início às etapas técnicas, incluindo ensaios e testes para comprovação de desempenho, eficiência e qualidade.

Finalizando, são realizadas as etapas de documentação final, com a obtenção das aprovações em todos os testes e aplicações, sejam eles laboratoriais ou em

campo, garantindo a homologação definitiva do projeto.

O que não se pode perder no processo rotineiro da inovação é o acompanhamento dos indicadores e metas estabelecidos, pois serão eles que nortearão as tomadas de decisões na renovação do ciclo de investimento.

A relevância dos incentivos fiscais

Este deve ser o ponto de partida para as empresas que desejam inovar. Dessa forma, logo no início do processo, a empresa deve avaliar se existem mecanismos de fomento à inovação que facilitem a aplicação ou proporcionem ganhos além dos aspectos técnicos e competitivos já previstos na iniciativa. Isso, muitas vezes, facilita o desenvolvimento do projeto e permite que a empresa se organize melhor quanto aos recursos necessários.

Os incentivos fiscais, como a Lei do Bem, a Lei de Informática e o Programa Mover, encorajam as empresas a continuarem inovando, funcionando como mecanismos que fomentam o ciclo do investimento contínuo. Se investir em inovação é o caminho para a competitividade, essa ação é inevitável, então direcionar um projeto ou a área de PD&I a um incentivo permite que as empresas recuperem parcial ou totalmente esse recurso financeiro, podendo realizar cada vez mais aportes em soluções inovadoras no país.

Nesse âmbito, o ideal é que o empreendimento conte com uma consultoria especializada, de forma que a operação seja minimamente impactada, enquanto a companhia obterá respaldo quanto à segurança e qualidade de todo processo, com a rastreabilidade total das documentações acessórias, para a geração e usufruto do potencial máximo do incentivo.

ROI em inovação

O ROI (Retorno sobre Investimento) avalia o lucro ou prejuízo de um investimento, oferecendo previsibilidade sobre os resultados da iniciativa proposta. Embora seja um indicador relevante, as empresas precisam ir além dos ganhos financeiros e considerar outros fatores essenciais dentro de um processo de inovação, como a estrutura de governança e a cultura de inovação.

Ter uma governança sólida e uma cultura de inovação é importante para garantir que os passos práticos da iniciativa funcionem de maneira efetiva. Dessa forma, a companhia deve iniciar o processo de inovação com um propósito estratégico e concluí-lo com resultados mensuráveis, fortalecendo o papel do time de P&D como parte essencial da estratégia da companhia.

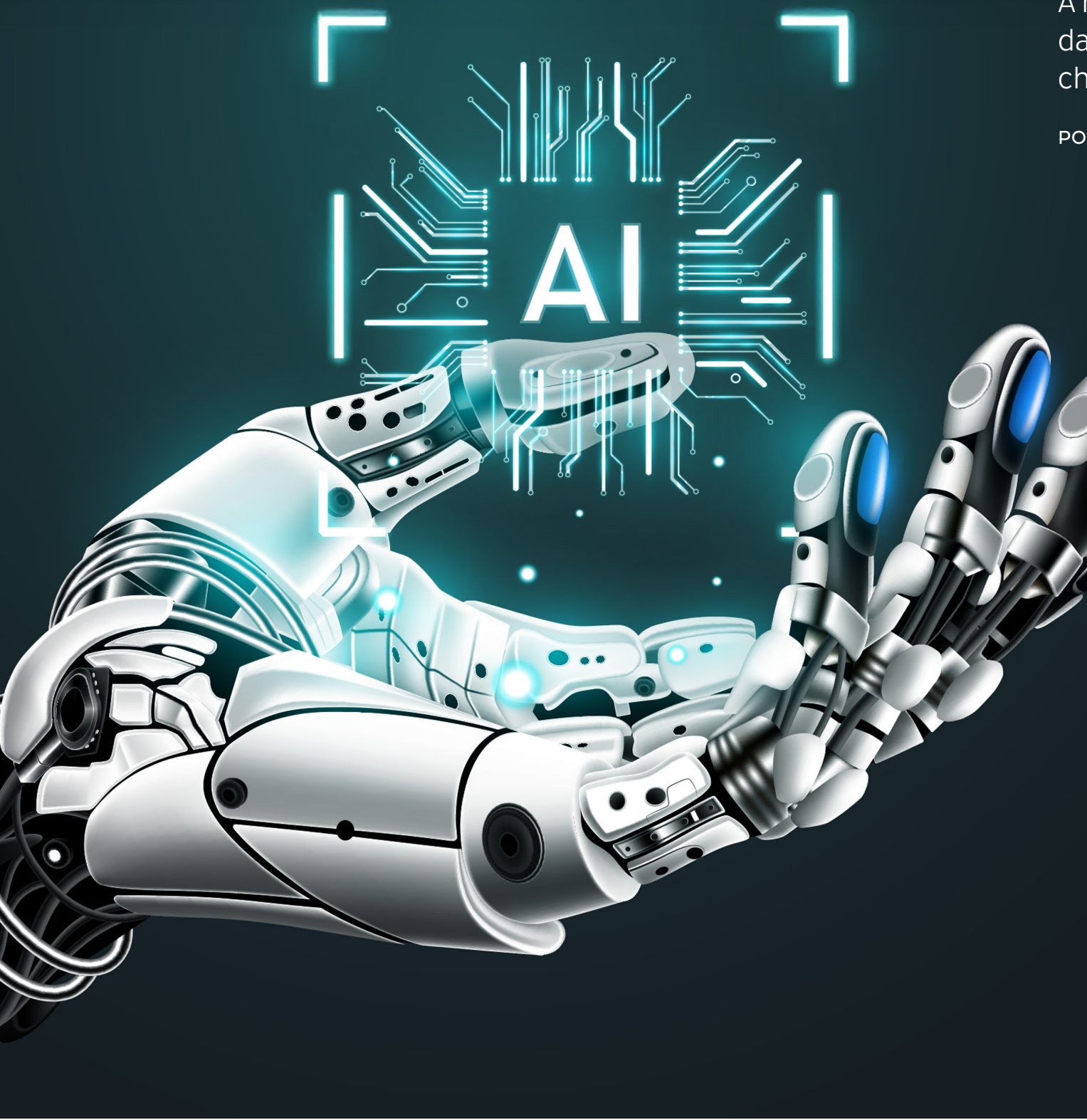
Caso a empresa não demonstre um diferencial competitivo, um valor agregado e se reinvente para acompanhar as tendências, corre o risco de se tornar defasada, perdendo a eficiência no mercado.

Além disso, o investimento em inovação tecnológica não apenas assegura o posicionamento e a estabilidade da empresa, mas também pode permitir a expansão do seu mercado. Isso não se limita à manutenção da posição atual, mas também promove a melhoria da qualidade, produtividade nos produtos, processos e serviços, gerando redução de custos, otimização de tempo e alavancando os negócios e a competitividade.

MANU

A r
da
ch

PO



US AI:

revolução autônoma
inteligência artificial
negou - E agora?

R NIARA XAVIER

O mundo da inteligência artificial (IA) está em constante ebulição, mas raramente vemos um anúncio que realmente balança as estruturas como o da Manus AI. Desenvolvida pela startup chinesa Butterfly Effect, essa IA não é apenas mais um chatbot ou assistente virtual. Ela promete ser um "agente autônomo", capaz de aprender, decidir e executar tarefas complexas sem a necessidade de supervisão humana constante. A Manus AI chegou para desafiar a nossa compreensão do que é possível, e a pergunta que fica é: estamos prontos para essa revolução?

Pense na Manus AI como uma orquestra sinfônica de inteligências artificiais. Ela não é um único programa monolítico, mas sim uma combinação inteligente de múltiplos modelos de IA, cada um especializado em diferentes tarefas. Ao integrar tecnologias como o Claude 3.5 Sonnet e Qwen, a Manus AI se torna versátil e adaptável. Essa arquitetura modular permite que ela aprenda continuamente, evoluindo com base em novas informações e experiências.

Imagine uma IA que não se limita a responder a perguntas com base em um banco de dados pré-definido, ela vai poder navegar na internet, analisar dados em tempo real, criar relatórios complexos, escrever e implementar código de software, e até mesmo tomar decisões estratégicas com base nas informações disponíveis. É como ter um assistente executivo ultra-inteligente que nunca dorme.

As demonstrações iniciais da Manus AI impressionam. Ela pode:

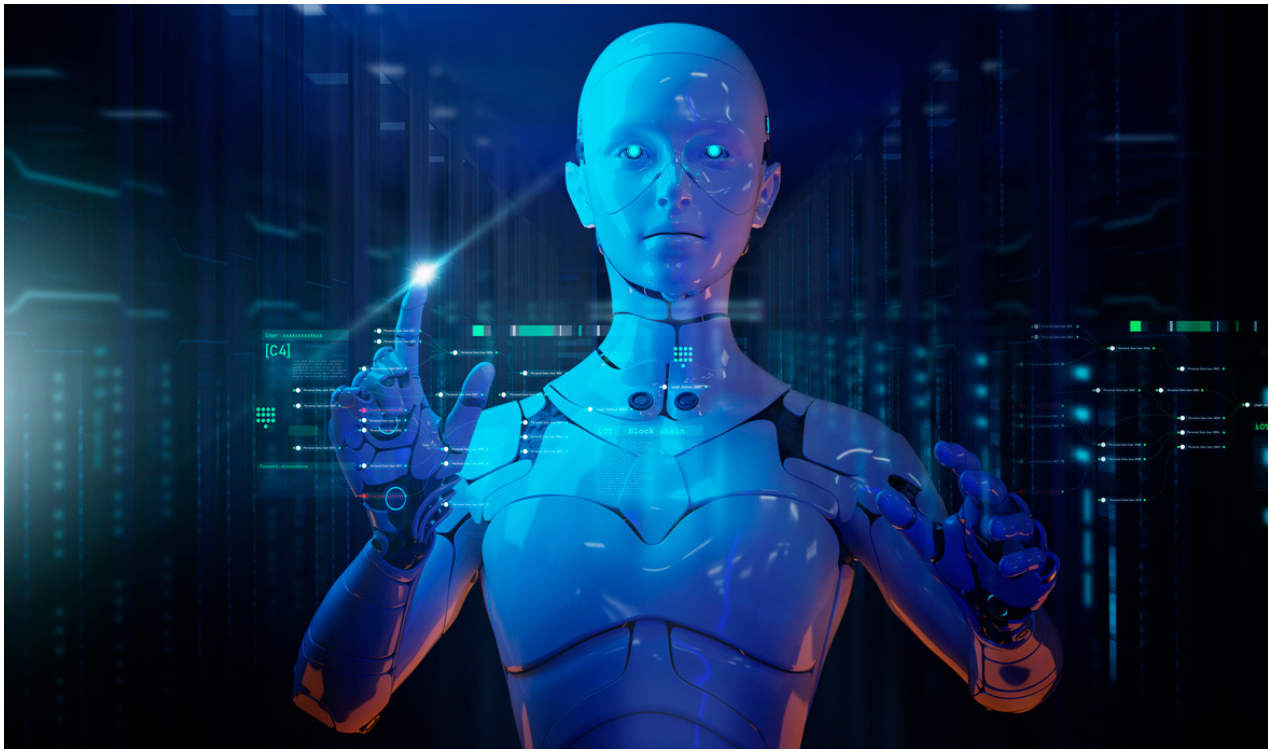
- **Criar e gerenciar websites:** Desde o design até a implementação, a Manus AI pode construir websites completos com precisão milimétrica.
- **Encontrar imóveis perfeitos:** Analise milhares de listagens e encontre o imóvel ideal com base em critérios complexos como localização, preço, tamanho, características e até mesmo o histórico de crimes da região.
- **Desenvolver currículos de estudo personalizados:** Crie um plano de estudos completo sobre qualquer assunto, adaptado ao seu nível de conhecimento e objetivos.
- **Analisar dados e gerar insights:** Identifique tendências, padrões e oportunidades em grandes conjuntos de dados.
- **Automatizar processos empresariais:** Otimize fluxos de trabalho, reduza custos e aumente a eficiência.

O diferencial da plataforma reside em sua capacidade de operar de forma autônoma. Ao contrário de chatbots tradicionais que precisam de instruções explícitas para cada tarefa, ela pode definir seus próprios objetivos, planejar ações e tomar decisões com base em sua própria análise da situação.

Porém a chegada dessa tecnologia levanta questões profundas sobre o futuro do trabalho. Se uma IA pode realizar tantas tarefas de forma autônoma, o que sobrará para os humanos? Será que estamos à beira de uma era de desemprego em massa? Ou será que o avanço das IA's criará novas oportunidades?

Riscos e desafios:

- **Desemprego Tecnológico:** A automação em larga escala pode levar à perda de empregos em diversos setores.
- **Desinformação e Manipulação:** A IA pode ser usada para criar notícias falsas, gerar propaganda enganosa e influenciar a opinião pública.
- **Discriminação Algorítmica:** Se os dados de treinamento da IA forem tendenciosos, ela pode perpetuar e amplificar preconceitos existentes.
- **Falta de Transparência:** É fundamental entender como a IA toma decisões para garantir que ela seja utilizada de forma ética e responsável.
- **Responsabilidade Legal:** Quem é responsável quando a IA comete um erro? A empresa que a desenvolveu? O usuário que a utiliza? A própria IA?



Assim, para aproveitar os benefícios da plataforma e mitigar seus riscos, é preciso que sejam tomadas medidas proativas, como:

- **Regulamentação Inteligente:** Criar leis e regulamentos que incentivem o desenvolvimento responsável da IA e protejam os direitos dos cidadãos.
- **Transparência e Auditabilidade:** Exigir que as empresas tornem seus algoritmos de IA mais transparentes e sujeitos a auditorias independentes.
- **Educação e Requalificação:** Investir em programas de educação e treinamento para ajudar as pessoas a adquirir as habilidades necessárias para trabalhar com a IA.
- **Novas Formas de Trabalho:** Explorar modelos de trabalho alternativos, como renda básica universal e semana de trabalho de quatro dias.
- **Ética e Valores:** Promover um debate público sobre os valores éticos que devem guiar o desenvolvimento e a utilização da IA.

Atualmente, o programa está em fase de testes e disponível apenas para um grupo seleto de convidados. Ainda não há uma data definida para o lançamento público da tecnologia.

A Manus AI representa um ponto de inflexão na história da inteligência artificial. Ela nos força a repensar nossas ideias sobre trabalho, ética e o futuro da sociedade. A pergunta não é se a IA vai mudar o mundo, mas sim como vamos moldar essa mudança.

DONE! A AGÊNCIA DIGITAL QUE FALA TECNOLOGÊS

[Inbound Marketing] [E-books] [Google Ads]
[Produção de Conteúdo] [Mídias Sociais]

Especializada em
Geração de Leads

RD STATION PARTNERS

Top **10 Agência** do Brasil em 2021 com mais de **1.800.000 leads** gerados para seus clientes

DONE!

COM A XTRATEGUS, É IR ALÉM DAS NUVENS!

Uma empresa brasileira que agrega valor aos seus negócios com a segurança Microsoft!

CONHEÇA AGORA!

Soluções Microsoft Office 365 Azure Microsoft Teams

Rua Grã Nicco, 113, CJ 105, Bloco II, Ecoville, CEP 81.200-200,
Curitiba-PR | +55 41 3542-1886 | +55 41 3521-8600

www.xtrategus.com

cloud expert xtrategus

Microsoft Partner
Microsoft

Gold Cloud Platform
Gold Cloud Productivity
Gold Datacenter
Gold Small and Midmarket Cloud Solutions
Gold Enterprise Mobility Management

O seu parceiro de serviços Microsoft

O DESENVOLVEDOR DO FUTURO: COMO A IA ESTÁ REDEFININDO O PAPEL NA TECNOLOGIA

Fabio Seixas
[Especialista em soluções tecnológicas e CEO da Softo]

O papel do desenvolvedor está passando por uma transformação sem precedentes. Se antes sua principal habilidade era a capacidade de escrever códigos complexos, agora ele precisa incorporar uma visão 360º, compreender dinâmicas de negócios e, acima de tudo, colaborar de forma eficiente com a inteligência artificial (IA). Desde os primeiros códigos em linguagem de máquina até as arquiteturas baseadas em nuvem, o desenvolvimento de software sempre foi moldado pelas ferramentas disponíveis. Agora, a IA não apenas redefine a maneira como programamos, mas também altera profundamente o papel dos profissionais de tecnologia. O foco deixa de ser a mera execução técnica e passa a abranger a concepção, a orquestração e a integração de soluções inteligentes.

A ascensão dos assistentes de codificação baseados em IA, como GitHub Copilot, Amazon CodeWhisperer e Cursor, já está automatizando tarefas repetitivas e acelerando processos, liberando os desenvolvedores para atividades mais analíticas e estratégicas. Isso inaugura uma nova era para a profissão, em que o diferencial não está na escrita de código, mas na capacidade de conectar tecnologia e negócios de maneira inovadora. Dessa evolução, nasce um novo perfil profissional: o Software Composer. Assim como no início da internet havia o webmaster — um generalista que combinava design, tecnologia e conteúdo —, o desenvolvedor do futuro será um híbrido, transitando entre engenharia de software, UX, estratégia de produto e visão de mercado.

O setor e tecnologia está se consolidando como uma camada de abstração no desenvolvimento de software, reduzindo barreiras técnicas e tornando a programação acessível a um público mais amplo. Com ferramentas de no-code e low-code evoluindo rapidamente, profissionais sem formação tradicional em tecnologia começam a contribuir para a criação de soluções digitais. Isso pode representar uma disrupção no setor, impulsionando a democratização da tecnologia e ampliando a diversidade de talentos na indústria.

Essa nova era tecnológica já está moldando três grandes perfis de desenvolvedores. O primeiro é o Full Stack de Solução Digital, que vai além do front-end e back-end, integrando IA, cloud computing e DevOps para garantir produtos escaláveis e alinhados às estratégias de negócio. O segundo é o Desenvolvedor de Infraestrutura e Segurança, essencial em um cenário onde a preocupação com segurança cibernética e conformidade regulatória cresce a

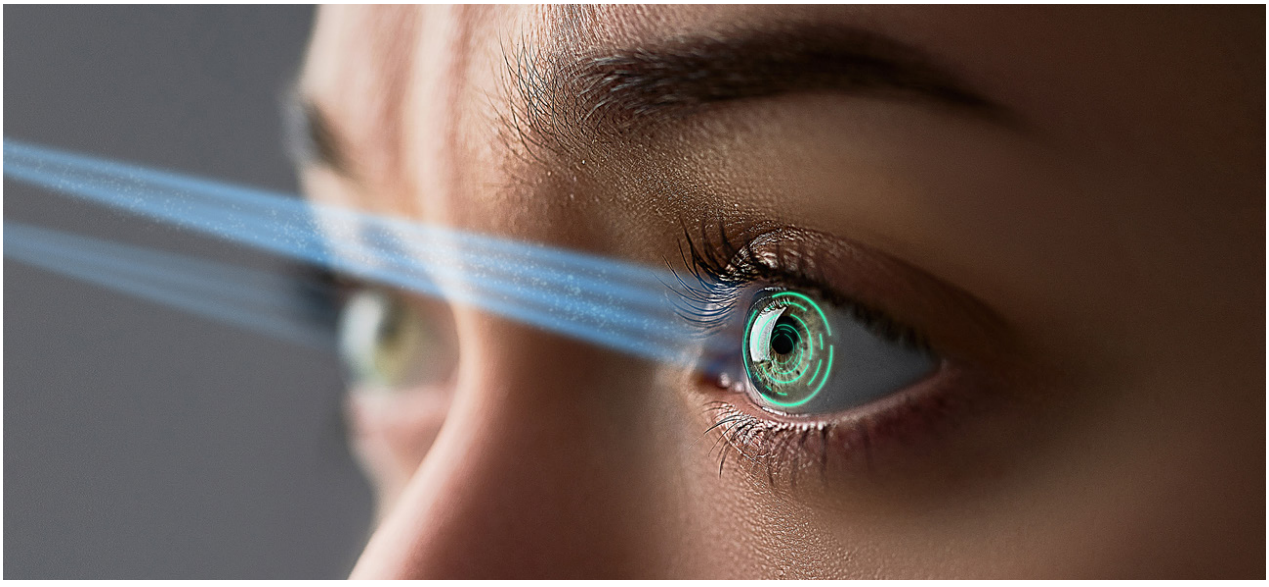
cada dia. Por fim, surge o Desenvolvedor de IA, especializado na criação e aplicação de modelos de machine learning, tornando a inteligência artificial cada vez mais acessível e funcional para o mercado.

A ascensão da inteligência artificial não representa o fim da programação, mas exige uma transformação profunda no papel dos desenvolvedores. Com o código se tornando uma commodity, a diferenciação no mercado dependerá de um conjunto ampliado de habilidades. A colaboração com IA será essencial, exigindo que os profissionais saibam direcionar, corrigir e potencializar o uso dessas ferramentas. Com isso, a visão estratégica ganha protagonismo, já que compreender o impacto das soluções digitais vai muito além da técnica, envolvendo também aspectos de negócios e experiência do usuário.

Em um setor de rápida evolução, o aprendizado contínuo se torna indispensável, garantindo adaptação às novas demandas. Com a automação assumindo tarefas operacionais, a criatividade e a inovação serão diferenciais cruciais, impulsionando os desenvolvedores a focarem na solução de problemas complexos e na construção de produtos disruptivos. As

empresas que compreenderem essa mudança e investirem na capacitação de seus times sairão na frente. O desenvolvedor do futuro não será apenas um programador, mas um arquiteto de soluções, um estrategista digital que integra tecnologia, experiência do usuário e visão de mercado para construir produtos que definirão a nova era da economia digital.

VENDA DE ÍRIS: A PONTA DO ICEBERG DA CIBERSEGURANÇA



O recente escândalo envolvendo a comercialização de íris humanas não é um incidente isolado, mas sim um sintoma alarmante de um problema muito maior: as práticas de cibersegurança arriscadas e a falta de conscientização digital que permeiam a sociedade contemporânea. A venda de dados biométricos, como íris, impressões digitais e reconhecimento facial, representa apenas a ponta do iceberg de uma crise de segurança que ameaça a privacidade, a segurança financeira e até mesmo a liberdade individual de milhões de pessoas.

Os números são estarrecedores: de acordo com um levantamento da Surfshark, o Brasil registrou em 2024 um aumento assombroso de 2.322,3% no número de contas violadas, totalizando 84,6 milhões de registros expostos. Esse salto expressivo, que coloca o país como o sétimo mais afetado globalmente, evidencia a disseminação de práticas arriscadas e a urgência de promover a educação digital em todos os níveis da sociedade.

Bruno Telles, COO da BugHunt, empresa brasileira pioneira em Bug Bounty na América Latina, alerta para os perigos ocultos por trás de atitudes cotidianas que muitas vezes são consideradas inofensivas. "A venda de íris é só um símbolo de um problema maior. Práticas simples, como compartilhar dados em formulários, podem ser exploradas de forma criminosa", afirma Telles. O especialista destaca que o fornecimento de dados pessoais para cadastros online, a criação de perfis em redes sociais sem critérios de privacidade e o uso indiscriminado de biometria são condutas de alto risco que facilitam crimes como roubo de identidade, fraudes financeiras e engenharia social.

A falta de cuidado com dados sensíveis pode gerar impactos de longo prazo, especialmente quando se trata de informações biométricas, que, ao contrário de senhas, não podem ser alteradas. O vazamento de dados biométricos pode viabilizar vigilância em massa, discriminação, acessos não autorizados a serviços críticos e até mesmo a manipulação de sistemas de segurança.

"Os riscos associados a essas práticas vão além de fraudes financeiras. O vazamento de dados biométricos pode viabilizar vigilância em massa, discriminação e acessos não autorizados a serviços críticos. Por serem dados permanentes, uma vez comprometidos, o impacto é irreversível", analisa Telles.

Diante desse cenário alarmante, a adoção de medidas preventivas se torna imprescindível para proteger a identidade

digital e evitar prejuízos irreparáveis. Telles recomenda a adoção de práticas como educação digital, o uso de criptografia e autenticação multifatorial para fortalecer a segurança das contas online. Além disso, o especialista reforça que empresas que coletam dados sensíveis devem garantir a segurança das informações com práticas como auditorias regulares e descarte seguro de dados. A Lei Geral de Proteção de Dados (LGPD) também exige consentimento explícito para o uso de dados biométricos, reforçando a necessidade de transparência e responsabilidade no tratamento de informações pessoais.

Guia Prático para Proteger seus Dados Biométricos:

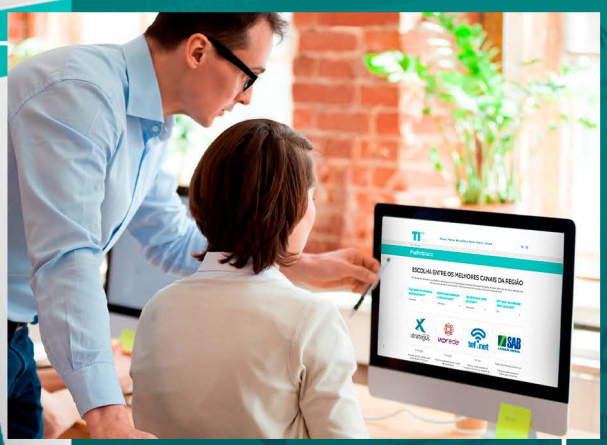
- **Avaliar a necessidade:** Questione se é realmente necessário compartilhar seus dados biométricos e qual será o impacto a longo prazo dessa decisão. Reflita sobre os riscos e benefícios antes de fornecer informações sensíveis.
- **Pesquisar a empresa ou serviço:** Verifique a reputação da companhia ou plataforma que está solicitando as informações, confirmando se há políticas claras de proteção de dados e se a empresa possui um histórico de segurança confiável.
- **Verificar o consentimento explícito:** Certifique-se de que está fornecendo os dados de forma voluntária e com total compreensão dos riscos envolvidos. Leia atentamente os termos de uso e certifique-se de que você concorda com as políticas de privacidade da empresa.
- **Entender os termos de uso:** Leia os termos e condições para saber como seus dados serão utilizados, armazenados e se há possibilidade de venda a terceiros. Fique atento a cláusulas que permitam o compartilhamento de suas informações com parceiros ou anunciantes.
- **Monitorar o uso dos dados:** Após o compartilhamento, acompanhe o uso dos seus dados e esteja atento a sinais de uso indevido. Verifique regularmente seus extratos bancários, contas online e relatórios de crédito para identificar atividades suspeitas.

"As pessoas precisam entender que seus dados têm valor e que compartilhar informações sem critério pode trazer riscos permanentes. A proteção começa pela educação digital", finaliza Telles. A conscientização sobre os riscos e a adoção de medidas preventivas são as principais armas para proteger a identidade digital e evitar se tornar mais uma vítima da crescente onda de crimes cibernéticos. A hora de agir é agora.

> **"As pessoas precisam entender que seus dados têm valor e que compartilhar informações sem critério pode trazer riscos permanentes. A proteção começa pela educação digital"** , finaliza Telles.

MARKETPLACE TI NORDESTE

Escolha entre ***os melhores da região*** em um marketplace exclusivo para o ***Nordeste***!



- **Cloud**
- **Automação**
- **Energia Solar**
- **Agência digital**
- **Ar-condicionado**
- **Cybersegurança**
- **Revenda Gamer**

Entre outras!

QUERO ACESSAR