Jornal
a eletrônica em foco

NOTICIOSO MENSAL DE ELETROELETRÔNICA, TELECOMUNICAÇÃO, INFORMÁTICA, CFTV ETC.
www.aeletronicaemfoco.com.br / aeletronicaemfoco@gmail.com
Abril de 2026
Ano LXV - Nº 789

MANTENHA-SE ATUALIZADO SOBRE AS NOTÍCIAS DO SETOR. ACESSE, DIARIAMENTE, O SITE QUE LHE TRARÁ ESTAS INFORMAÇÕES: WWW.AELETRONICAEMFOCO.COM.BR

Epson lança projetores Smart portáteis para transformar a casa em cinema, palco ou estúdio, com telas de até 150” *Pág. 3*

A LG redefine a instalação de painéis LED com a tela de 136 polegadas pronta para uso - *Pág. 3*

Veja também nesta edição:

Fechaduras inteligentes e câmeras residenciais - *Pág. 3*

Jornal a eletrônica em foco

FUNDADO EM 20-07-60

Um jornal mensal a serviço da Eletroeletrônica,

Informática e Telecomunicação no Brasil.

Redação e Publicidade

R. Cel. Melo Oliveira, 605 - S. Paulo/SP - cep 05011-040

(11) **97166-3344**

e-mail - aeletronicaemfoco@gmail.com / **site -** www.aeletronicaemfoco.com.br

Editor
Desdir Herivelto Amaral

Redação
J. M. Gambi - MTb 7.000
Andréa A. Pastori

Consultor Jurídico
Dr. Neldir Amaral

Assinatura Anual
R$ 75,00 (Físico)
ou R$ 55,00 (Digital)
Números Avulsos R$ 8,00

O futuro quântico vai precisar de mais do que algoritmos

*Por Jamil Mouallem

A computação quântica deixou de ser apenas um conceito teórico restrito a laboratórios para se tornar uma promessa concreta de transformação econômica e tecnológica. O interesse crescente de governos, universidades e empresas sinaliza que essa corrida já começou. De acordo com a Grand View Research, o mercado global de computação quântica foi estimado em US$ 1,42 bilhão em 2024 e deve alcançar US$ 4,24 bilhões até 2030, com taxa média de crescimento anual de 20,5% entre 2025 e 2030. No Brasil, esse movimento também ganha corpo: o mercado nacional gerou cerca de US$ 20 milhões em 2024 e a projeção é que atinja US$ 65 milhões até o fim da década.

Esses números ajudam a dimensionar o tamanho da aposta tecnológica em curso. No entanto, há um ponto menos discutido que tende a se tornar decisivo: a infraestrutura energética capaz de sustentar esse avanço. Computadores quânticos exigem ambientes extremamente controlados, com sistemas de refrigeração criogênica e níveis de estabilidade elétrica muito superiores aos da computação tradicional. Hoje, máquinas quânticas em operação experimental, como as desenvolvidas por IBM e Google, consomem, em média, entre 7 kW e 25 kW de potência, considerando não apenas o processador, mas todo o sistema necessário para manter as condições físicas adequadas ao funcionamento dos qubits.

Esse dado ajuda a deslocar a discussão do plano abstrato para a realidade concreta. Embora a computação quântica ainda esteja longe da adoção massiva, seu modelo de funcionamento já indica um futuro em que o processamento avançado dependerá cada vez mais de energia estável e altamente confiável. O que hoje parece restrito a poucos equipamentos tende a se expandir para centros de pesquisa, ambientes corporativos e aplicações críticas, elevando de forma estrutural a demanda por fornecimento contínuo e de alta qualidade.

O contraste é revelador. De um lado, um mercado que cresce a taxas superiores a 20% ao ano; de outro, uma base energética que precisa evoluir não apenas em volume, mas em consistência e previsibilidade. A computação quântica, assim como a inteligência artificial e os grandes centros de dados, expõe um paradoxo contemporâneo: quanto mais intangível parece a tecnologia, mais concreta se torna sua dependência de infraestrutura física.

Pensar o futuro apenas sob a ótica da inovação digital é, portanto, um exercício incompleto. A verdadeira transformação começa quando se reconhece que não existe salto tecnológico sem base energética sólida. Redes mais resilientes, fontes

diversificadas e modelos de gestão que priorizem continuidade deixam de ser apenas temas do setor elétrico e passam a integrar a estratégia da economia digital.

Antes de ser quântico, o futuro exige outra base energética. Uma base capaz de sustentar não apenas os experimentos do presente, mas as aplicações críticas do amanhã. Ignorar essa equação seria construir castelos tecnológicos sobre fundações frágeis. Encará-la de frente é entender que o avanço real não está apenas nos processadores que ainda virão, mas na capacidade de manter, com solidez, tudo aquilo que eles prometem transformar.

Jamil Mouallem é sócio-diretor da TS Shara indústria nacional fabricante de nobreaks, inversores e estabilizadores de tensão e protetores de rede inteligente.

Imposto de renda 2026: golpes ficam mais sofisticados com uso de IA

Com a abertura do calendário de declarações do Imposto de Renda Pessoa Física (IRPF), o ecossistema digital brasileiro entra em um dos períodos de maior exposição a fraudes. Em 2026, esse cenário ganha uma nova camada de complexidade com o uso crescente de inteligência artificial para sofisticar golpes, aumentar a verossimilhança de comunicações falsas e pressionar a confiança dos cidadãos nos canais digitais oficiais.

Para a TIVIT, multinacional do Grupo Almaviva e provedora de serviços de tecnologia na América Latina, o avanço dessas fraudes exige que a discussão vá além da proteção individual do contribuinte. O tema passa também pela resiliência digital das instituições públicas, pela segurança das jornadas digitais e pela capacidade de preservar a confiança nas infraestruturas críticas do setor público.

Dados da Serasa Experian indicam uma intensificação do problema: no início de 2026, o Brasil registrou uma tentativa de fraude financeira a cada 2,2 segundos. O uso de dados vazados, aliado a táticas de engenharia social hiper-personalizadas, resultou em um salto de quase 30% nas tentativas de fraude no último ciclo. Atualmente, mais de 50% dos brasileiros relatam ter sido alvo de golpes digitais nos últimos 12 meses, desafiando a percepção de segurança dos canais oficiais.

Segundo Thiago Tanaka, Diretor de Cibersegurança da TIVIT, a principal mudança em 2026 está no uso da IA generativa para tornar ataques mais convincentes. "Os golpes ficaram mais sofisticados. A inteligência artificial permite criar comunicações falsas com linguagem, identidade visual e estrutura muito próximas das oficiais, o que aumenta o risco de erro por parte do cidadão e pressiona ainda mais a confiança nos canais digitais", afirma.

No contexto do Imposto de Renda, esse movimento costuma aparecer em páginas falsas, mensagens sobre malha fina, promessas de restituição ou cobranças indevidas. Embora o impacto mais visível recaia sobre o contribuinte, a empresa avalia que o problema também afeta as próprias instituições, ao ampliar a sobrecarga em canais de suporte, dificultar a comunicação oficial e exigir respostas mais rápidas de prevenção e orientação.

O especialista afirma que a proteção nesse cenário depende de uma combinação entre arquitetura digital segura, autenticação robusta, monitoramento contínuo e educação do usuário. O uso de ambientes autenticados, como o portal e-CAC e o aplicativo Meu Imposto de Renda, além de mecanismos como múltiplos fatores de autenticação, segue como uma das principais camadas de defesa para reduzir riscos de acesso indevido e fraude.

"O desafio não é apenas bloquear ataques, mas garantir que a jornada digital do cidadão aconteça de forma segura e confiável do início ao fim. Isso envolve identidade, autenticação, proteção de dados e capacidade de resposta a incidentes", explica Tanaka. "Canais oficiais não utilizam gatilhos de urgência emocional. A resiliência cibernética de uma nação depende tanto de infraestruturas robustas quanto de uma cultura de desconfiança digital por parte do usuário final".

Nesse contexto, ele avalia que fortalecer a resiliência digital do setor público exige uma abordagem integrada, que combine infraestrutura, governança, monitoramento e orientação ao usuário. Em períodos de alta demanda, como o do Imposto de Renda, essa capacidade se torna ainda mais relevante para proteger dados, reduzir vulnerabilidades e preservar a confiança nos serviços digitais.

"Quando a confiança na comunicação oficial é abalada, a eficiência do Governo Digital retrocede. O órgão público é pressionado a atuar em modo de gestão de crise, impactando o planejamento estratégico de arrecadação e fiscalização. A segurança, portanto, deve ser encarada como um pilar de sustentabilidade do negócio público", conclui Tanaka.

A LG redefine a instalação de painéis LED com a tela de 136 polegadas pronta para uso

Com tecnologias inovadoras que superam os mais altos padrões de eficiência, a LG oferece produtos que geram uma redução significativa nos gastos mensais com energia e contribuem para um futuro mais sustentável.

A LG Electronics (LG) reforça sua posição de liderança no mercado de displays profissionais com a sua tela LED All-in-One de 136 polegadas. Consolidado como uma solução de alto impacto para o ambiente corporativo, o modelo LAPA136 se diferencia por desmistificar a instalação de painéis LED, aliando qualidade de imagem superior a um processo de montagem e uso surpreendentemente simples e rápido.

Uma solução completa e inteligente

O grande diferencial da tela All-in-One da LG é a sua concepção. O

produto integra em um único chassi a tela de 136 polegadas, uma controladora de vídeo de alta performance com sistema operacional webOS e um sistema de som. Isso elimina a necessidade de adquirir e configurar múltiplos componentes, o que tradicionalmente eleva a complexidade e o custo de projetos com painéis de LED. A solução chega ao cliente em um único case de transporte, com tudo o que é necessário para a montagem.

Qualidade de imagem profissional

Projetado para ambientes que exigem comunicação visual de excelência, o display possui resolução Full HD (1920x1080), 500 nits de brilho e um pixel pitch de 1.56mm. Essa configuração garante que apresentações, vídeos e outros conteúdos sejam exibidos com clareza, cores vibrantes e ótimo contraste, mesmo em locais com iluminação ambiente. A vida útil de 100.000 horas dos LEDs assegura um investimento duradouro e de baixa manutenção.

"Percebemos que muitas empresas adiavam a modernização de seus espaços pela complexidade que imaginavam em instalar um painel de LED. O nosso display All-in-One LAPA136 foi a resposta da LG a essa dor do mercado e hoje se consolida como a solução ideal", comenta Leonardo Di Clemente, Gerente de Information Displays da LG Brasil. "Ele desmistifica a tecnologia LED, entregando um display de alto impacto visual que é tão simples de montar e usar quanto uma TV. O feedback tem sido fantástico, pois permitiu que projetos de comunicação visual fossem implementados em tempo recorde."

A facilidade de uso se estende ao controle do display, que pode ser feito por um controle remoto intuitivo, e à conectividade, com múltiplas entradas HDMI, DisplayPort e suporte a compartilhamento de tela sem fio, simplificando a vida de apresentadores e equipes de TI.

Fechaduras inteligentes e câmeras residenciais

A evolução das casas inteligentes e a crescente demanda por soluções de segurança conectada impulsionam o lançamento de novas tecnologias no setor de automação residencial.

A EZVIZ, marca global de tecnologia para casas inteligentes e conectadas, apresenta uma nova geração de dispositivos que integram inteligência artificial (IA), monitoramento remoto e controle de acesso em um único ecossistema.

Entre os lançamentos estão soluções voltadas à segurança e à automação residencial, com destaque para fechaduras inteligentes e câmeras conectadas que podem ser gerenciadas por meio de um aplicativo. Esse movimento acompanha a expansão das casas conectadas, com consumidores cada vez mais interessados em soluções integradas, que combinem praticidade, conectividade e proteção no dia a dia.

Um dos destaques é a fechadura DL20FVS Plus, equipada com IA capaz de reconhecer usuários por identificação facial e leitura das veias da palma da mão. Outro lançamento é a fechadura DL50FVS, que conta com reconhecimento facial 3D sem contato, câmera integrada com visão noturna e múltiplos modos de acesso. Já o vídeo-interfone HP7 identifica visitantes e pode ser controlado por app, permitindo visualizar quem está na porta, conversar e liberar o acesso mesmo à distância.

Epson lança projetores Smart portáteis para transformar a casa em cinema, palco ou estúdio, com telas de até 150”

Os novos projetores oferecem projeção de até 150 polegadas e contam com Google TV[1] integrado, permitindo acesso direto a mais de 10 mil aplicativos de streaming, jogos e entretenimento. A tecnologia 3LCD[2] de três chips da Epson garante imagens vibrantes e naturais mesmo em ambientes com iluminação, enquanto o aplicativo exclusivo Epson Projection Studio simplifica o controle do projetor e possibilita criar experiências interativas com fotos e vídeos. Na linha Lifestudio, a experiência é complementada pelo áudio imersivo com tecnologia Sound by Bose e por versões Plus com imagem 4K Pro UHD, elevando o padrão do entretenimento dentro de casa.

“O entretenimento dentro de casa ganhou um novo significado nos últimos anos, com consumidores buscando experiências mais completas, flexíveis e fáceis de usar. Com o lançamento do EF-30 e da linha Lifestudio, a Epson amplia as possibilidades de assistir a filmes, esportes, shows ou jogar videogame em telas grandes, com qualidade de imagem e som, além da praticidade de se adaptar a diferentes ambientes”, afirma Marcelo Madi, Diretor Executivo da Epson Brasil. Conheça os novos projetores

Projetor Smart portátil EF-30

Modelo de entrada da nova geração, ideal para quem busca portabilidade e facilidade de uso no dia a dia, o EF-30 oferece projeção de até 150 polegadas em Full HD. Conta com sistema de alto-falantes com áudio Dolby, Google TV com acesso a mais de 10 mil aplicativos, ajustes automáticos e tecnologia 3LCD de três chips com Triple Core Engine, tudo em um formato compacto, portátil e intuitivo.

Lifestudio Pop (EF-61)

Ideal para quem busca unir estilo e praticidade, o Lifestudio Pop (EF-61) projeta imagens de até 150” em Full HD, com 700 lúmens de brilho e áudio imersivo Sound by Bose. Possui sistema inteligente com Google TV e Android® 14, além de ajustes automáticos como correção de keystone, detecção de obstáculos e enquadramento de tela. Está disponível nas cores Verde Fumê, Bege Rosado e Branco Pérola.

Lifestudio Pop Plus (EF-62)

Mantém o design portátil do Pop e a projeção de até 150”, mas eleva a experiência ao oferecer qualidade de imagem 4K Pro UHD. Também conta com sistema inteligente (Google TV, Android® 14 e Google Assistant™) e ajustes automáticos completos. Está disponível nas cores Azul Marinho e Preto Metálico.

Lifestudio Flex (EF-71)

Desenvolvido para quem busca versatilidade e adaptação a diferentes ambientes, o Lifestudio Flex (EF-71) possui design com inclinação de até 90° e rotação de até 180°, permitindo projeções em diferentes superfícies. Oferece imagem de até 950” em Full HD, 700 lúmens de brilho, áudio Sound by Bose e acesso a mais de 10 mil aplicativos por meio do Google TV, garantindo flexibilidade e facilidade de uso.

Lifestudio Flex Plus (EF-72)

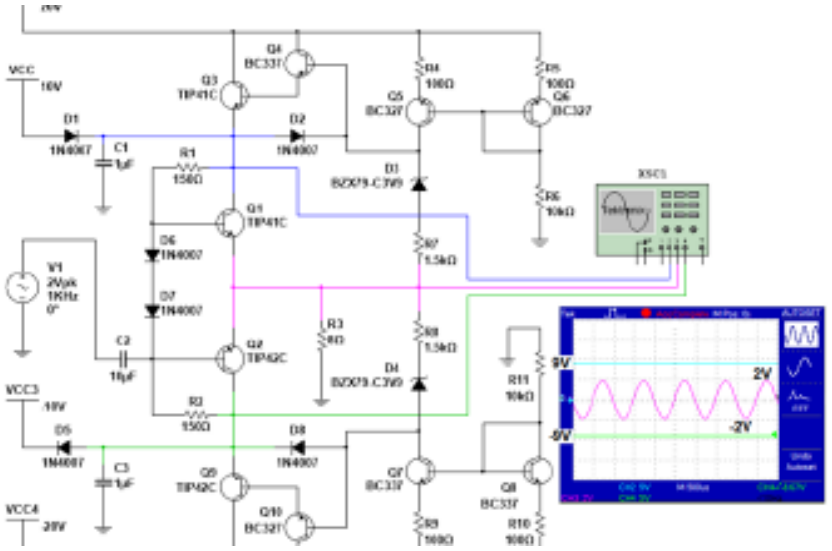
O modelo mais avançado da linha combina projeção de até 150” com qualidade de imagem 4K Pro UHD, brilho de 1.000 lumens e design premium com acabamento que imita madeira. Entre seus diferenciais, destaca-se a função de iluminação integrada, que permite transformar o ambiente mesmo quando o projetor não está em uso. Com um único toque no sensor localizado na parte superior do equipamento, é possível ajustar o brilho e alternar entre diferentes modos de luz, criando o clima ideal para diferentes momentos. Além disso, o Lifestudio Flex Plus é compatível com carregadores portáteis USB-C PD, incluindo os do tipo PowerBank, oferecendo mais liberdade de uso em diferentes ambientes. A inclinação de até 90° e a rotação de até 180°, aliadas ao áudio imersivo Sound by Bose, garantem uma experiência premium de entretenimento doméstico.

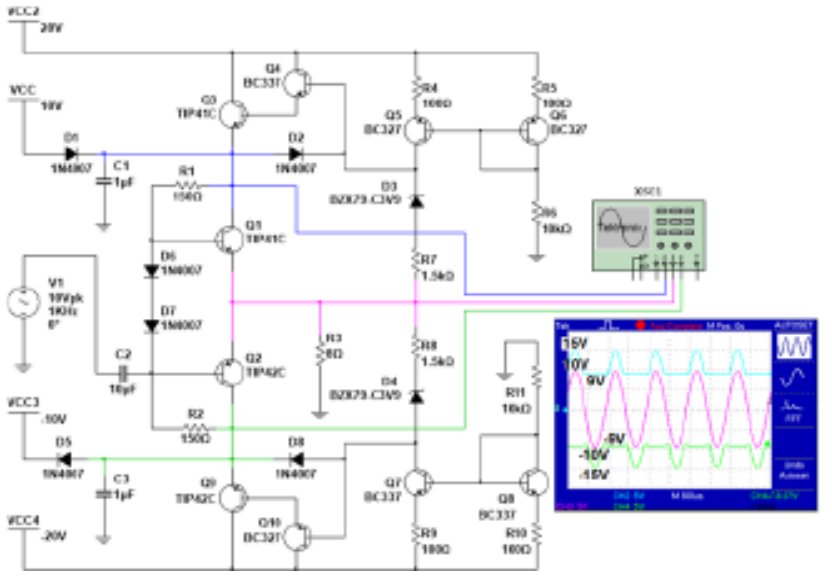
Amplificadores Classes G e H

Por Luis Carlos Burgos

Neste artigo falaremos de tipos especiais de amplificadores classe AB com objetivo de amplificar sinais pequenos com tensões menores de alimentação e sinais grandes com tensões maiores.

Classe G – Veja a seguir o funcionamento:



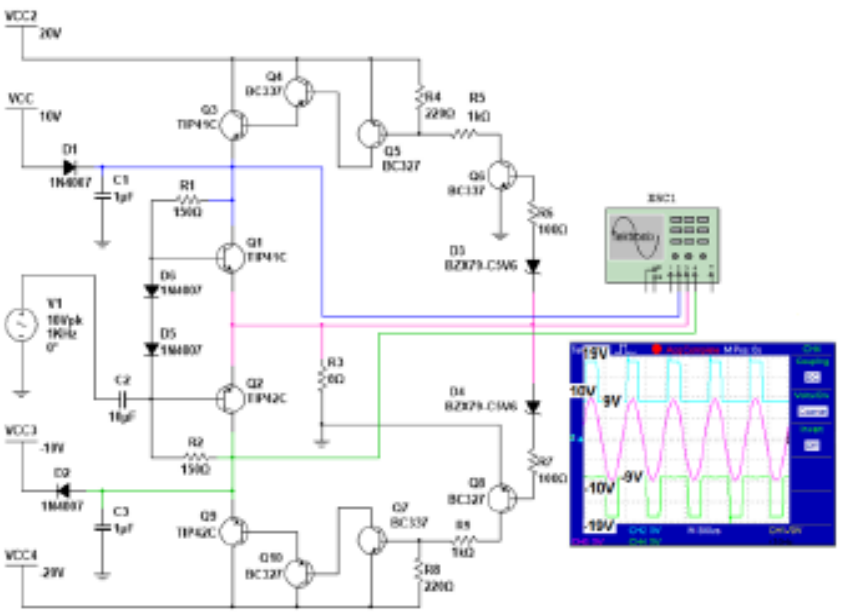


Por que usar classe G – Q1 e Q2 dos circuitos mostrados são os transistores de saída. No primeiro desenho eles recebem 2 Vp de sinal nas bases. Com alimentação de +10 e -10 V (simétrico) a tensão na saída dos transistores oscilará entre +2 e -2 V (lembre-se que eles são amplificadores de corrente e não de tensão). Assim cada transistor terá uma queda de tensão variando de 8 a 10 V. Se a corrente for por exemplo 1 A quando a queda de tensão for 8 V, só em cada transistor teremos uma dissipação de calor de 8 W. Isto com alimentação de +10 e -10 V. Se a alimentação for de +20 e -20 V teremos uma dissipação de 16 W nos transistores. Então a ideia é aumentar a tensão de alimentação à medida que o sinal na base dos transistores aumenta.

Assim evita-se o aumento de temperatura com sinais fracos pois sobraria maiores tensões de queda nos transistores de saída.

Como funciona – Q3, Q4, Q9 e Q10 funcionam como chaveadores e resistores variáveis. Assim dependendo do tamanho do sinal de entrada eles conduzem mais ou menos variando a tensão de alimentação entre 10 e 20 V, -10 e -20 V para os coletores dos transistores de saída. Q5, Q6, Q7 e Q8 são espelhos de corrente. Assim a corrente circulante por eles e pelos diodos zeners fica muito próxima a 1,9 mA. No resistor R7 sempre teremos 1,9 mA x 1.5 K cerca de 3 V. No desenho de cima com sinal de 2 Vp na base dos transistores de saída, no pico máximo positivo teremos 2 + 3 + 3,9 = 8,9 V na base de Q4. Como esta tensão é menor que os 9,3 V do emissor de Q3, estes Darlington (Q3 e Q4) não condizem e o coletor de Q1 será alimentado com 9,3 V (10 menos queda em D1). Por analogia o pico máximo negativo do sinal será -2 V e o transistor Q2 será alimentado por -9,3 V. No desenho de baixo, o pico do sinal será 10 V. Teremos 10 + 3 + 3,9 = 16,9 V na base de Q4. Ele conduz, polariza Q3 e no emissor dele (alimentação do Q1) teremos 15,5 V. Por analogia teremos -15,5 V no coletor de Q2. Podemos observar este efeito pelos osciloscópios desenhados. No superior temos um sinal fraco com as alimentações de 9 V e -9 V.

E no inferior com sinal mais forte quando ultrapassam determinados valores as alimentações sobem e descem proporcionalmente.



Este difere da classe G no fato dos transistores que alimentam as saídas não funcionarem como resistores variáveis e sim apenas como chave liga/desliga. Com sinais fracos os transistores ficam desligados e a saída funciona com a fonte baixa. Com sinais fortes os transistores ligam e alimentam a saída com a tensão alta.

Como funciona – Q1 e Q2 são os transistores de saída. Os transistores Q3 ao Q10 funcionam como interruptores. Com um sinal fraco de por exemplo 2 Vp os diodos zeners D3 e D4 de 5,6 V não conduzem. Desta forma todos os transistores chaveadores Q3 ao Q10 ficam desligados e a saída é alimentada com 9 V e -9 V. Quando sinal fica mais forte, por exemplo 10 Vp, os zeners conduzem e acionam todos os transistores chaveadores. Assim Q3 e Q9 levam a alimentação 0 e – 20 V para os transistores de saída. Podemos ver o funcionamento através dos desenhos de osciloscópio conectados em vários pontos destes circuitos separados por cores diferentes correspondentes às que a aparecem na tela deles.

Temos cursos, kits e livros técnicos em nossa loja virtual:
http://burgoseletronica.com.br
Siga nosso canal no Youtube:
www.youtube.com/c/Burgoseletronica05
Whatsapp (11) 92006-5996
Instagram: @burgoseletronica
Muito obrigado a todos e até nosso próximo artigo.

Baterias integradas à energia solar podem ter payback de dois anos em projetos residenciais e comerciais, aponta Powersafe

Segundo estudos de casos da empresa, consumidores com perfil de aumento de consumo e que buscam redução de picos de demanda e mitigação de prejuízos por quedas de energia têm o retorno do investimento mais rápido

A instalação de sistemas de armazenamento de energia integrados à geração solar já pode apresentar payback de até dois anos no Brasil, tanto em aplicações residenciais quanto em estabelecimentos comerciais. É o que aponta a experiência prática da Powersafe, fabricante brasileira de baterias e sistemas de energia, com base em projetos em operação em diferentes regiões do País.

Segundo os estudos de casos da Powersafe, a combinação entre a queda acelerada dos custos das baterias de íon-lítio, especialmente da tecnologia LFP (lítio-ferro-fosfato), o aumento das tarifas de energia no Brasil e a busca crescente por confiabilidade no fornecimento tem transformado o armazenamento em um ativo estratégico, indo muito além de uma solução complementar aos sistemas de geração própria solar.

Conforme projeções da própria Empresa de Pesquisa Energética (EPE), considerando um custo de R$ 3.000/kWh para baterias, o payback de sistemas de geração solar distribuída com armazenamento pode ser de aproximadamente 6 anos para aplicações residenciais e cerca de 5 anos para aplicações comerciais. “Se considerarmos cenários de custo mais competitivo, por volta de R$ 2.000/kWh, que é o caso agora no mercado brasileiro, esse retorno pode se reduzir significativamente, ficando entre 2 e 4 anos, tanto para residências quanto para estabelecimentos varejistas”, explica André Ribeiro, gerente de operações e renováveis da Powersafe.

“Em determinados perfis de consumo, principalmente quando há foco em aumento de autoconsumo, redução de picos de demanda e mitigação de prejuízos causados por quedas de energia, observamos, de fato, projetos com retorno do investimento em cerca de 24 meses”, acrescenta Ribeiro.

De acordo com o executivo, os consumidores que já possuem geração solar nos telhados e coberturas são os mais propensos a investir em baterias, uma vez que buscam maximizar o retorno do sistema existente e reduzir a dependência da rede elétrica. “Nesse contexto, o armazenamento permite deslocar o consumo para horários mais vantajosos (time shift), elevar o autoconsumo da energia solar e reduzir custos associados a picos de demanda (peak shaving)”, aponta.

Além do ganho econômico, a resiliência energética tem sido um dos principais motivadores para a decisão de investimento. Interrupções no fornecimento, flutuações de tensão e instabilidades da rede impactam diretamente residências, comércios e serviços essenciais, tornando o armazenamento energético um diferencial cada vez mais valorizado.

“Para muitos clientes, especialmente no varejo, serviços e pequenas indústrias, o custo de uma interrupção supera o valor da economia direta na conta de luz. Quando esse fator entra no cálculo, o payback percebido se torna ainda mais rápido”, explica Ribeiro.

Queda de custos acelera viabilidade

A redução global dos preços das baterias tem sido determinante para essa evolução. Dados de mercado indicam que o preço médio de packs de baterias de íon-lítio caiu de forma expressiva na última década, alcançando patamares que viabilizam projetos com retornos mais curtos. Em cenários de custos mais competitivos, combinados com uma gestão energética eficiente, o armazenamento se consolida como parte integrante do desenho energético de residências e estabelecimentos comerciais.

Na prática, a Powersafe observa que aplicações bem dimensionadas, integradas a inversores híbridos e sistemas de gestão de energia (EMS), apresentam ganhos que vão além do ROI tradicional, incluindo melhoria da qualidade da energia, maior previsibilidade de custos e aumento da autonomia do consumidor.

Com a expectativa de avanços regulatórios e maior maturidade do mercado, a Powersafe projeta um crescimento acelerado das soluções de armazenamento até 2026, com destaque para os segmentos comercial, residencial, rural e de serviços críticos. A tendência é que as baterias passem a ser incorporadas desde a concepção dos projetos solares, ampliando o valor entregue ao consumidor final.

“A bateria deixa de ser apenas uma proteção contra apagões e passa a ser uma ferramenta de gestão energética inteligente, com impacto direto na economia e na segurança do fornecimento”, conclui Ribeiro.

A IDADE DO ELÉTRON-100 ANOS DE PROGRESSO NA ELETRÔNICA - VIII

Por Carlos Alberto Fazano *(in memoriam)*

Continuação da edição anterior

3.5.2 - OS RECEPTORES DO PERÍODO 1920 - 1924

Geralmente eram radiorreceptores de construção caseira, onde os seus componentes com resistores, capacitores, soquetes, válvulas eram geralmente montados sobre bases de madeira ou ebonite.

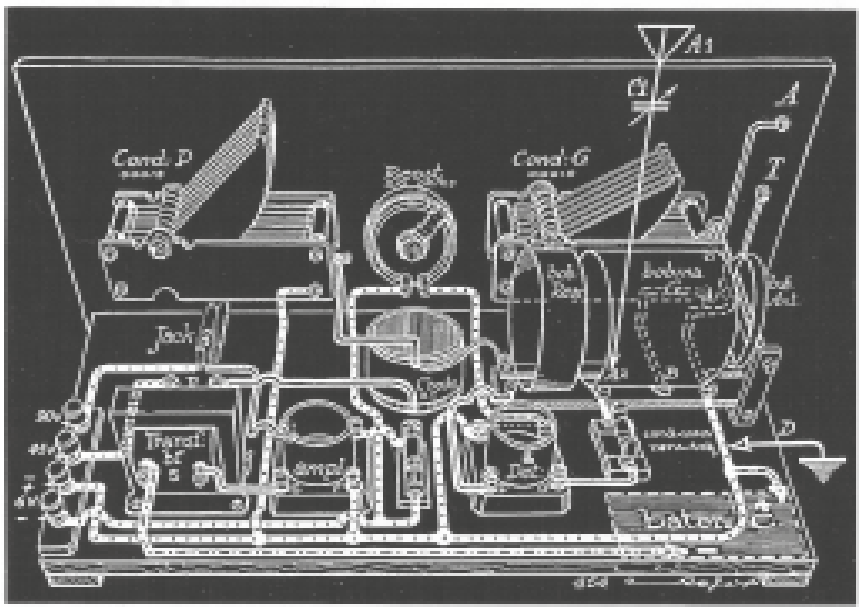


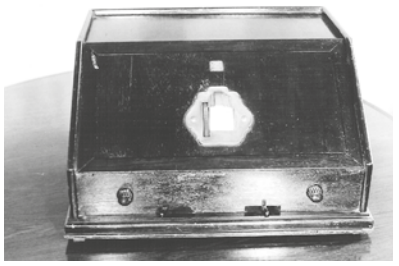
Ilustração mostrando um receptor de construção caseira fabricado por volta de 1923.

Fig. 30 - rádio regenerativo de origem alemã fabricado pela NORA em 1923.

3.5.3 - OS RECEPTORES DO PERÍODO 1924 - 1930

Fig. 31 - receptor modelo OE 333 fabricado em 1926 pela companhia alemã LOEWE operando apenas com 1 válvula tipo 3NF. Esta válvula considerada o primeiro tipo de circuito integrado continha no seu envólucro três triodos, dois resistores de anodo, dois resistores de grade e dois capacitores de acoplamento. Este tipo de receptor usava apenas uma válvula, para diminuir os impostos cobrado pelo governo alemão logo após a primeira guerra mundial. - (vide seção 10.6.1)

Fig. 32 - o receptor modelo 9W fabricado pela Telefunken em 1927 na Alemanha, usando circuito tipo Neutrodino com 6 válvulas operando nas faixas de frequências de 150 - 1500 kHz.
(coleção Maria de Oliveira)



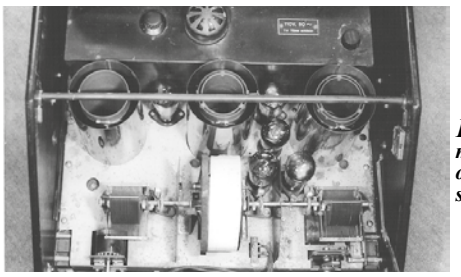


Fig. 33 - detalhe interno do receptor modelo 9W mostrando as suas 4 válvulas tipo REN 1104 para o 1º estágio de rádio frequência, tipo RE 134 como saída de áudio e RGN 1503 como retificadora.

Fig. 34 - receptor modelo 40W fabricado pela Telefunken em 1929; operando em corrente alternada de 115V nas frequências de 140 - 1500 KHz . Usava os seguintes tipos de vá1vulas: RGN 1154, RENS 1204, Ren 1004 e REN 1159.
(coleção Maria de Oliveira)

Fig. 34a - radiorreceptor marca Stromberg-Carlson de origem americana, fabricado por volta de 1926, operando com circuito tipo neutródino.
(coleção Maria de Oliveira)

Continua na próxima edição

PIADINHAS

Se fosses solteiro com quem casarias?

Numa entrevista coletiva com alguns ministros e políticos importantes, estavam muitos jornalistas na sala e, lá no fundo, um bêbado.

Quase no fim da entrevista, um jornalista fez a seguinte pergunta aos três entrevistados:

- Senhores, se Vossas Excelências fossem solteiros, com quem os senhores gostariam de se casar?

O primeiro a responder foi, o presidente do congresso:

- Eu casava-me com a Gabriela Botelho atual miss mundo, a mulher mais bonita do Brasil.

Então o bêbado, lá no fundo, batendo palmas, grita:

- Isso mesmo, muito bom, casou pela beleza! Muito bom mesmo!!!

Logo após, foi a vez do atual Presidente do Senado a responder:

- Eu casava-me com a minha mulher, pois ela me ama!!!

O bêbado, mais uma vez:

- Que bonito, é isso aí, casou por amor! Grande homem!!!

E então, o ministro, querendo ficar bem perante os brasileiros:

- Eu casava-me com o Brasil, o meu coração pertence a este País!!

O bêbado, até saltou da cadeira de tão entusiasmado que ficou:

- Muito bom, muito bom mesmo! Isso é que é homem honrado: F*deu… tem que casar!!

PÍLULAS DE SABEDORIAS

"Diziam que eu tinha 3 mil pares de sapato. Pura mentira. Nunca tive mais do que 1.600".

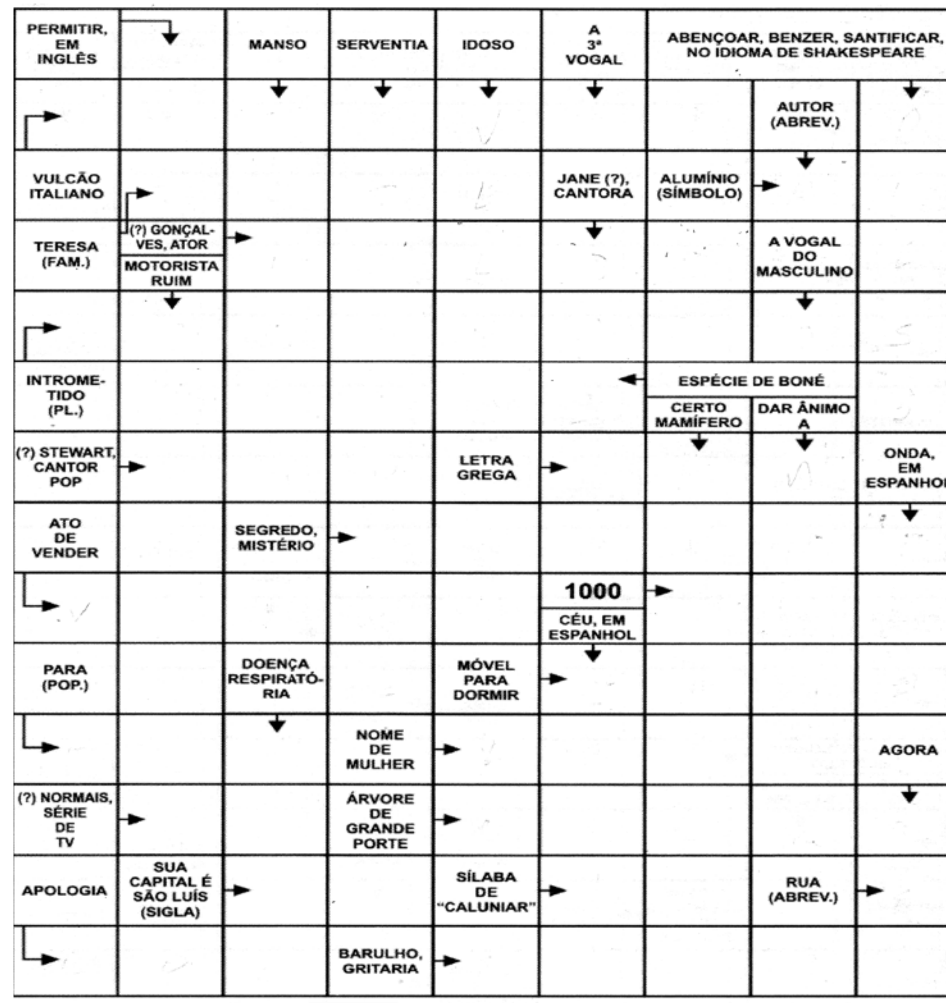
Imelda Marcos, ex-primeira-dama das Filipinas.

"Se eu tivesse só um pouquinho de humildade, eu seria perfeito".

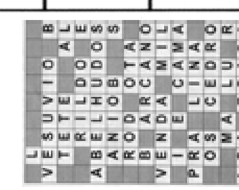
Ted Turner, empresário americano.

"Se você se vestir mal, vão criticar sua roupa. Se vestir-se de forma impecável, aí sim vão notar a mulher que existe por dentro da roupa".

Coco Chanel, estilista francesa.



BLESS / CIELO / RILDO



ADULTERADO
CAPITAL
CONHECIDA
CONSTRUÇÃO
DISSE
ENTREGA
ESCÓRIA

FICAR
GALINHA
GARFO
INTERPOLADO
INTRÉPIDO
SUDÃO
VAREJO

ALTURA
DINHEIRO
INDENIZAÇÃO
LUVA
PRISONEIRO
TAMBÉM
TRAMITAR

G	Y	C	L	I	N	T	R	É	P	I	D	O	A
H	Q	I	W	D	V	P	C	M	W	R	L	C	D
U	W	V	U	I	M	R	O	A	L	U	V	A	U
E	T	U	Y	N	F	I	N	P	D	I	J	U	L
N	S	C	D	H	I	S	S	N	I	D	I	R	T
T	R	D	M	E	C	O	T	U	E	I	N	B	E
R	A	U	V	I	A	N	R	W	S	S	T	Q	R
E	A	M	O	R	R	E	U	X	C	S	E	J	A
G	V	E	B	O	R	I	Ç	H	Ó	E	R	T	D
A	S	R	J	É	O	R	Ã	X	R	G	P	R	O
G	Q	Z	M	Ã	M	O	O	X	I	J	O	A	A
A	M	Z	D	C	A	P	I	T	A	L	L	M	L
R	V	U	D	V	A	R	E	J	O	J	A	I	T
F	S	C	O	N	H	E	C	I	D	A	D	T	U
O	I	N	D	E	N	I	Z	A	Ç	Ã	O	A	R
G	K	F	W	K	G	A	L	I	N	H	A	R	A

Golpe do silêncio: ligações mudas viram arma para clonar sua voz

Criminosos usam chamadas silenciosas para coletar áudio e alimentar ferramentas de clonagem de voz, criando golpes de impostor que pressionam as vítimas a enviar dinheiro e dados

A inteligência artificial mudou o jeito como golpes telefônicos acontecem. Agora, criminosos não precisam insistir em longas conversas para causar dano. Em muitos casos, eles ligam, ficam em silêncio e esperam a vítima falar primeiro. Esse padrão, conhecido como "Silent Call Scam", pode parecer apenas uma chamada estranha ou um telemarketing mal executado.

No entanto, ele pode esconder uma etapa inicial de um golpe maior: coletar pequenos trechos de áudio para alimentar ferramentas de clonagem de voz. Segundo Adrianus Warmenhoven, especialista em cibersegurança da NordVPN, o risco não está só no golpe "final", mas também no que acontece antes dele.

"Uma tecnologia barata e eficiente de clonagem de voz já consegue criar imitações muito convincentes", afirma Warmenhoven. Na prática, criminosos usam essas vozes para se passar por alguém confiável, como um familiar ou um líder da empresa, e assim pressionar as vítimas a enviar dinheiro ou compartilhar informações sensíveis.

Por que o silêncio funciona?

O "Silent Call Scam" aproveita um comportamento comum: atender e dizer "alô" automaticamente. Essa resposta pode virar um ponto de partida para clonagem de voz, especialmente quando o criminoso combina esse áudio com outros trechos encontrados em redes sociais, vídeos, entrevistas, áudios em aplicativos e gravações do dia a dia.

Ferramentas de clonagem costumam precisar de apenas alguns segundos de áudio claro (cerca de 10 a 20 segundos) para criar uma imitação convincente. Um simples "alô" nem sempre basta para uma clonagem de alta qualidade, mas pode iniciar a coleta. Além disso, se a vítima continua falando, por irritação, por curiosidade ou para "pegar o golpista no flagrante", ela pode, sem querer, entregar mais material para aprimorar a voz clonada.

Warmenhoven destaca que mesmo quando você percebe que é um golpe, isso não significa que você está seguro. Se a chamada estiver sendo gravada, o criminoso pode usar o áudio depois, em um ataque direcionado contra seus contatos.

Depois da coleta, os criminosos tendem a atacar onde dói mais, ou seja, em pontos de confiança e urgência. Os roteiros mais comuns envolvem um pedido desesperado supostamente feito por alguém próximo, com histórias que criam pressão emocional como acidentes, problemas com a polícia, emergências financeiras, situações sensíveis e pedidos de transferência imediata.

Os alvos preferidos costumam incluir pais e responsáveis, além de pessoas mais velhas, justamente porque os golpistas apostam em reações rápidas para "resolver o problema" sem checar detalhes. E quando a voz parece real, até pessoas cuidadosas podem ser enganadas.

O que mudar no seu comportamento ao atender o telefone

Para quem quer atender chamadas, mas também quer reduzir risco, a recomendação é deixar o outro lado falar primeiro. Se a chamada for silenciosa, isso já é um sinal para encerrar. Se você precisar responder, use uma frase neutra, sem emoção, e evite entregar um "modelo" fácil da sua voz.

A NordVPN recomenda estas medidas preventivas contra golpes com clonagem de voz:

Deixe o chamador falar primeiro. Evite começar com "alô" e não ofereça amostras desnecessárias da sua voz.

Se precisar responder, prefira algo neutro como "Quem fala?" Por ser menos expressivo e menos "padrão", tende a ser menos útil como amostra.

Desligue imediatamente se a ligação parecer suspeita ou se houver pedido de dinheiro, dados pessoais, senhas, códigos ou qualquer "urgência" incomum.

Não prolongue a conversa. Quanto mais você fala, mais material você fornece para clonagem e melhor pode ficar a imitação.

Verifique antes de agir. Se alguém pedir algo estranho, desligue e retorne pelo número conhecido, ou contate a pessoa por um canal confiável (mensageiro, ligação habitual, etc.).

Tenha cuidado com o que publica em redes sociais. Vídeos e áudios públicos viram um dos maiores bancos de amostras de voz para criminosos.

Reporte números e ligações suspeitas para sua operadora e, quando possível, para as autoridades, ajudando a mapear redes de golpe.

Além disso, vale combinar um hábito familiar simples: criar um "passo de verificação" em casa. Por exemplo, se surgir um pedido urgente por telefone, todos concordam em confirmar por mensagem ou retornar à ligação para um número já salvo. Essa pausa curta pode impedir perdas financeiras e vazamentos de dados.

O que a IA sabe sobre você? Conversas em apps geram perfis detalhados de usuários

Um modelo de Inteligência Artificial (IA) é, por natureza, um devorador de dados. Ele é treinado com bilhões de informações disponíveis na internet e, em muitos casos, também com o conteúdo que os próprios usuários digitam diretamente. Essa interação contínua significa que cada vez que você conversa com a IA, o modelo aprende mais sobre como as pessoas se comunicam e, potencialmente, sobre você em particular. O simples ato de interagir já se configura como um ato de exposição que muitos ignoram.

"As pessoas geralmente não percebem que, ao enviar informações para um LLM (Large Language Model), estão expondo dados a um ambiente que não diferencia conteúdo sensível de conteúdo comum. Muitos usuários copiam códigos, contratos, registros internos ou dados pessoais acreditando estar num espaço privado, mas o modelo apenas processa o que recebe, e os provedores podem manter esses dados para si, para aprendizagem da IA, além de registros técnicos para auditoria e segurança", alerta Pollyne Zunino, Subcoordenadora do SWAT Team na Apura e especialista em Investigação de Crimes Cibernéticos, Fraudes Eletrônicas e Inteligência Digital.

O levantamento feito pela equipe da Apura joga luz sobre uma armadilha que não enxergamos e cada vez mais comum: a entrega inocente de informações sensíveis a sistemas que não foram feitos para guardá-las.

E casos reais que ilustram o risco. Um dos mais frequentes envolve desenvolvedores que enviam trechos de código para otimização, sem notar que deixaram ali embutidos tokens de acesso, URLs internas ou credenciais temporárias. Mesmo que o modelo responda com eficácia, o estrago já está feito — ou seja, aquele dado confidencial foi transmitido, processado e possivelmente registrado em logs da plataforma. E, uma vez que a informação foi usada para aprendizagem de uma IA, ela pode eventualmente fazer parte de uma resposta para outros usuários do mesmo serviço de LLM. Seja um token, um CPF, um pedaço de contrato ou um pipeline estratégico, a lógica é a mesma: o que entra no modelo passa a fazer parte da IA e não volta mais ao controle do usuário.

Nas empresas, o cenário é ainda mais crítico. A facilidade de uso e adoção espontânea e desordenada de ferramentas de IA pelos colaboradores cria um ambiente conhecido como Shadow AI, um ecossistema paralelo e invisível, onde dados corporativos circulam fora das camadas de proteção projetadas para guardá-los.

Informações de clientes, código proprietário, planos estratégicos, contratos confidenciais e ativos críticos: tudo pode ser copiado, colado e enviado a uma plataforma externa sem qualquer avaliação de risco.

Ferramentas não homologadas abrem brechas que passam despercebidas por sistemas tradicionais de defesa cibernética, como DLP, SIEM e EDR, transformando modelos de IA externos em potenciais canais de vazamento.

"Provedores como OpenAI, Google e Anthropic, só para citar alguns, possuem políticas de privacidade que limitam o uso de dados pessoais e diferenciam o tratamento entre API e interface web", explica Zunino. "Normalmente, indicam que não utilizam dados enviados por API para treinar modelos, embora possam reter informações operacionais para segurança".

Já no universo open source — um conjunto de softwares, ferramentas, sistemas e comunidades cujo código-fonte é aberto e pode ser visto, modificado, aprimorado e distribuído por qualquer pessoa — a proteção recai inteiramente sobre quem hospeda e opera o modelo. E, muitas vezes, essa hospedagem não está preparada ou estruturada para garantir segurança adequada.

A Apura ressalta que os cibercriminosos estão bastante atentos à esses fatos. "Hoje, grupos especializados exploram desde falhas de configuração em modelos corporativos até vazamentos involuntários em logs, repositórios e instâncias internas", explica a especialista da Apura Cyber Intelligence.

Técnicas como model inversion, membership inference e prompt injection permitem extrair padrões sensíveis, reidentificar usuários, manipular comportamentos do modelo e reconstruir dados originalmente sigilosos. "Em outras palavras, o criminoso não precisa mais invadir a rede. Ele só precisa acessar o que vazou pelos prompts de IA", reforça Pollyne.

Como se proteger

A especialista reforça: "A IA não é seu diário. Não é sua caixa de e-mail relareporconfidencial. Antes de colar qualquer conteúdo, a pergunta deve ser: 'Se isso vazasse, eu ficaria tranquilo?'".

Entre as principais orientações:

• jamais inserir dados pessoais ou corporativos sensíveis;

• seguir rigidamente as políticas internas de cibersegurança;

• priorizar ferramentas de IA homologadas pelo time de tecnologia e segurança da sua empresa;

• adotar modelos locais e agentes autônomos operados dentro da própria infraestrutura da empresa.

"LLMs locais eliminam o envio de dados para terceiros e facilitam a conformidade com legislações sobre privacidade como LGPD e GDPR. Além disso, permitem automações avançadas, com navegadores autônomos, extração de dados e geração de relatórios, sem comprometer a privacidade", explica.

A Apura, referência em Cyber Threat Intelligence (CTI), tem acompanhado de perto a evolução desse ecossistema de risco e mapeado como criminosos incorporam IA em cada fase do ataque.

"Nós monitoramos fontes abertas, comunidades e infraestruturas onde criminosos compartilham prompts corporativos vazados, artefatos sensíveis e novas técnicas de exploração de modelos", afirma Pollyne Zunino. "Esse trabalho identifica exposições involuntárias e também como grupos maliciosos usam a IA para automatizar engenharia social, varredura de vulnerabilidades, spear phishing e a produção de artefatos maliciosos mais sofisticados".

A especialista finaliza afirmando: "A IA está aprendendo o tempo todo e, se você não prestar atenção, ela pode aprender muito mais do que deveria."