

OPINIÃO

Como ter a melhor conversa com a inteligência artificial

Henrique Calandra (*)

Você não precisa dar Bom dia! para o Chat GPT ou para o Google Gemini. Entretanto, precisa saber como começar uma conversa com essas ferramentas ou modelos de inteligência artificial (IA) generativa para receber boas respostas.

Quero falar um pouco sobre prompts para quem está começando a utilizar ferramentas e modelos de IA no trabalho, nos estudos ou no dia a dia, falando tanto da criação de conteúdo, como de tarefas com aplicativos e softwares.

Um prompt pode ser uma pergunta, um comando ou um pedido, ou seja, ele é o ponto de partida da sua conversa com a IA. E quanto melhor for o seu prompt, quanto mais claro, específico e contextualizado, maior será a chance de você receber exatamente o que precisa.

E mais: a IA generativa pode funcionar como o seu “desbloqueio” criativo, apontando alguns caminhos que você pode desenvolver posteriormente.

Então, evite dizer apenas “Escreva um e-mail para o meu chefe” ou “Traga um texto sobre marketing digital”.

Seja mais específico e detalhado no seu pedido, apresente o contexto, estabeleça o formato (um texto, uma lista, um e-mail), peça um tom para o texto (formal, criativo, técnico) e indique para quem será aquele conteúdo (alunos, clientes, etc.).

Dois exemplos: “Escreva um texto para o meu blog com cerca de 800 palavras sobre as três melhores estratégias de marketing digital para pequenas empresas, usando um tom otimista e informal”.

E “Escreva um e-mail gentil de dois parágrafos para nossos clientes lembrando que o prazo para confirmar a presença no

nosso evento termina nesta sexta-feira”.

Para criar conteúdos um pouco mais complexos, você pode pedir para a IA resumir dados de artigos científicos ou notícias recentes, para que você consiga construir o seu texto com maior embasamento. Por exemplo, “faça um resumo das principais questões discutidas na COP 29 e que ainda devem ser debatidas na COP 30 em Belém; liste também os países que já confirmaram sua presença no encontro deste ano”.

E não pare na primeira tentativa. A chave para bons resultados é testar variações de prompts e comparar as respostas, às vezes, combinando os diversos retornos da IA.

Gosto de lembrar que a IA é um excelente apoio, mas não um atalho. Pesquisas e respostas elaboradas pela ferramenta serão ótimas para você construir o seu próprio conteúdo, carregado de fontes e informações, que devem ser sempre verificadas e checadas.

Para tarefas do trabalho que consomem muito tempo, como conferência de planilhas e tabelas, triagem de dados, otimizar estoque, etc., você pode compartilhar os arquivos com a ferramenta de IA e criar prompts pedindo para otimizar ou automatizar certas ações, indicando o que você busca como resultado final. O importante é sempre testar e refinar os resultados.

Além disso, tenha em mente as boas práticas do seu trabalho e a segurança dos dados. Se for preciso, consulte as diretrizes da sua organização. Nunca insira informações sensíveis, como dados pessoais ou identificáveis, contratos e senhas, em ferramentas públicas de IA. O ideal é utilizar versões corporativas e com controle de privacidade.

(*) Fundador do WallJobs, empresa de tecnologia brasileira que oferece soluções automatizadas para contratos de estágio, autor do livro “Inteligência Artificial Generativa para Iniciantes”, colunista da ABStartups e palestrante de grandes ecossistemas como InovaBRA e Distrito.

Alemanha abaterá drones

O governo da Alemanha está elaborando uma lei que dará às forças de segurança poder para agir contra drones de operadores desconhecidos.

Vivaldo José Breternitz (*)

O texto ainda precisa passar pelo parlamento, mas analistas acreditam que o processo será tranquilo, já que o uso irregular de drones tem se tornado um problema constante na Alemanha e em outros grandes países europeus – já foi aprovado um projeto que autoriza a polícia a abater drones “fora de controle”, considerados ameaças imediatas à segurança.

O chanceler Friedrich Merz afirmou que os incidentes envolvendo drones representam riscos à segurança pública, razão pela qual o governo está propondo as novas regras, com a intenção de detectar, interceptar e neutralizar drones de forma mais rápida e eficaz.

O episódio mais recente ocorreu recentemente no aeroporto de Munique, quando o controle de tráfego aéreo precisou interromper os voos após detectar objetos não identificados no espaço aéreo. No total, 17 voos foram afetados, impactando as viagens de cerca de 3 mil passageiros.

O chanceler associou a crescente ocorrência desses incidentes à “guerra híbrida” movida pelo governo russo contra alguns países da Europa. Autoridades da Polônia e da Dinamarca compartilham da mesma preocupação, após detectarem drones desconhecidos em seus territórios nos últimos meses.

Diante desse cenário, o ministro do Interior, Alexander Dobrindt, defende cooperação ampla com a Ucrânia e Israel, nações que possuem ampla experiência em tecnologias de drones, tanto ofensivas quanto defensivas.

Segundo Dobrindt, a nova legislação também servirá para definir com clareza qual órgão deve responder a incidentes, de



Im_Zion_de_Pexels_CANVA

acordo com o tipo e a gravidade da ameaça. Enquanto a polícia ficaria responsável por neutralizar drones menores, que voam a baixa altitude, as forças armadas seriam encarregadas de lidar com unidades maiores e potencialmente mais perigosas.

Dados das autoridades de segurança da aviação (Luftfahrt-Bundesamt) mostram que, até setembro deste ano, a Alemanha registrou 172 interrupções no tráfego aéreo causadas por drones não identificados, um aumento em relação aos 129 casos em 2024 e 121 em 2023, no mesmo período de nove meses.

Novas tecnologias, novos problemas...

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.

A responsabilidade individual do profissional na gestão de certificados digitais

Nos últimos anos, vimos a segurança da informação deixar de ser um tema restrito ao time de TI e passar a ocupar um espaço estratégico dentro das empresas. Entre tantas camadas de proteção, os certificados digitais continuam sendo uma peça-chave, pois ajudam a garantir a autenticidade das comunicações e preservam a integridade dos dados dentro das organizações.

O que pouca gente comenta, no entanto, é que a responsabilidade pela gestão desses certificados, incluindo seus dados, não é apenas da empresa, mas também dos profissionais que lidam com eles todos os dias. Nesse sentido, o artigo 42 da Lei Geral de Proteção de Dados (LGPD), deixa claro que “o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”.

Isso reforça que a responsabilidade por falhas de gestão não é apenas um problema institucional, mas também pessoal, já que o fator humano continua sendo um dos principais pontos de vulnerabilidade na segurança digital. Segundo dados da IBM, ataques externos e ameaças internas representaram 55% de todas as violações de segurança ocorridas em 2024. No entanto, quase metade dos incidentes restantes teve origem em falhas de TI (23%) e er-



José Luiz Vendramini

ros humanos (22%), demonstrando que problemas técnicos e comportamentais ainda são determinantes na ocorrência de violações de dados.

Hoje, é inegável que muitas organizações ainda tratam a administração de certificados de forma manual, abrindo espaço para esquecimentos e erros de configuração. E, inevitavelmente, são nesses momentos que os holofotes se voltam para quem estava no “comando”, direta ou indiretamente.

Audidores, gestores e órgãos reguladores não querem saber se a equipe estava - ou não - utilizando ferramentas adequadas.

O que importa é se a empresa manteve controles rigorosos, conforme exigem normas como a ISO 27001, a PCI-DSS e a LGPD. Na prática, isso significa que, quando algo dá errado, o profissional responsável precisa estar pronto para explicar cada decisão que tomou. E é aí que entra um ponto importante: o controle e gerenciamento deixaram de ser apenas uma questão de eficiência, e se tornaram também uma proteção pessoal.

Quando você tem ferramentas que te ajudam no monitoramento e, principalmente, na gestão de dados e certificados, você não está só facilitando o seu trabalho, está criando provas de que fez tudo certo. Em uma auditoria, por exemplo, essa documentação pode ser a diferença entre ser apontado como culpado ou reconhecido por ter agido com responsabilidade.

Em resumo, o que podemos tirar de tudo isso é que adotar ferramentas que monitoram e auditam todo o ciclo dos certificados digitais é um investimento duplo, pois protege a infraestrutura da empresa e, ao mesmo tempo, protege a reputação de quem o opera. Afinal de contas, ninguém quer ver anos de carreira comprometidos por um certificado que expirou sem aviso prévio ou que teve um uso indevido por parte de outra pessoa.

(Fonte: José Luiz Vendramini é Sales Account Manager da Redtrust na América Latina).

E-book gratuito aborda a governança da Inteligência Artificial

O Andrade Maia Advogados, em parceria com a CLA Brasil e o D'Avila, Oliveira & Axt Advogados, lançou o e-book gratuito *“Governança da IA: desafios da liderança na prevenção e gestão de riscos legais e regulatórios”*. A publicação oferece um guia prático para lideranças empresariais sobre como adotar a Inteligência Artificial de forma segura, ética e em conformidade com as legislações atuais e futuras. O material aborda temas como responsabilidade jurídica dos administradores, impactos regulatórios, proteção de dados e riscos decorrentes do uso indevido de algoritmos e sistemas automatizados. Também apresenta um modelo de governança estruturado em quatro dimensões — estratégica, normativa, estrutural e performática — e elenca dez prioridades práticas para promover inovação com segurança e transparência. O e-book está disponível para download gratuito em: <https://materiais.andrademaia.com.br/e-book-governanca-da-ia>.



bankajob_CANVA

News@TI

TeamViewer integra DEX ao Agentforce IT Service da Salesforce

@ O TeamViewer anuncia a integração de sua plataforma DEX, conectividade remota e Inteligência Artificial com o novo serviço de TI Agentforce da Salesforce. Com o uso crescente de apps e dispositivos, interrupções no ambiente digital são inevitáveis. O TeamViewer DEX (sigla em inglês para Experiência Digital do Funcionário) monitora em tempo real todos os terminais e aplicativos, detectando e resolvendo problemas antes que prejudiquem a produtividade (www.teamviewer.com).

TD SYNnex cria soluções de TI para o mercado

@ A TD SYNnex (NYSE: SNX), distribuidora líder global e agregadora de soluções para o ecossistema de TI, realizou a segunda edição brasileira de seu evento para canais de venda, o Power Up, no Vibra São Paulo. Reuniu uma audiência de mais de 1.500 pessoas para uma série de palestras permitindo concluir, ao fim do dia, que o mercado de TI - assim como a economia do país - não deverá sofrer oscilações graves no futuro próximo e que inteligência artificial e cibersegurança serão elementos-chave no consumo de TI pelas empresas (<https://lac.tdsynnex.com/br/pt-br/>).