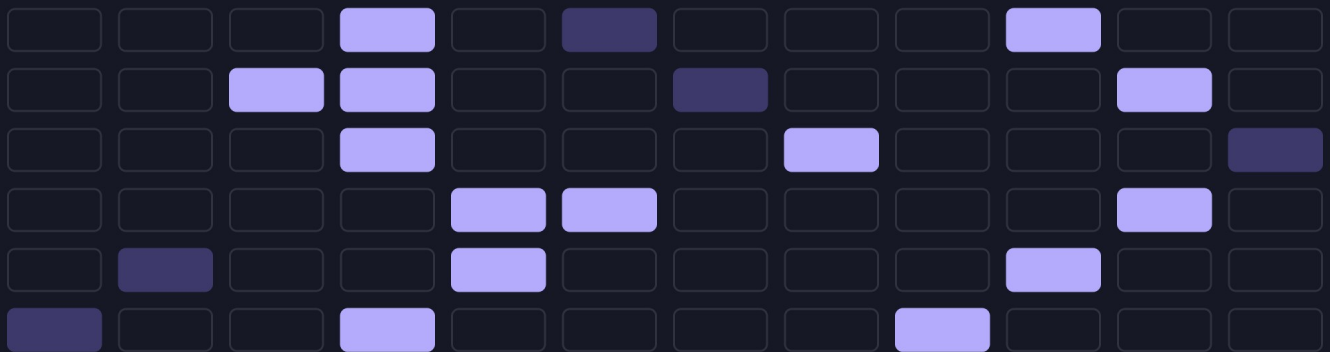


SEGURANÇA EM IA PARA NEGÓCIOS

Sua IA tem mais chaves que o seu funcionário de confiança.

7 ideias para usar IA no seu negócio sem expô-lo. Sem tecnicismos, sem medo e com algo concreto que você pode fazer hoje em cada uma.



Cada quadrado é um acesso que você deu. Você sabe quantos continuam ligados?

Diego Rojas

Engenheiro de segurança · +10 anos em sistemas, cloud e segurança

stratega.studio ·
@thediegorojas_

O risco mudou de lugar e quase ninguém percebeu.

Há uns dois anos, o conselho de segurança com IA era um só: não cole informação sensível no chat. Continua valendo, mas já não é o principal.

Hoje a IA não só responde. Ela lê seu e-mail, abre seus arquivos, agenda reuniões, responde clientes e conecta um app ao outro. Para fazer tudo isso, precisa de algo que antes você só dava a pessoas de confiança: **acesso**.

O QUE VOCÊ ACHA QUE FAZ

Testar um app novo

Compartilhar uma conversa

Automatizar uma tarefa

Pedir para a IA resumir um e-mail

O QUE VOCÊ REALMENTE FAZ

Dar acesso ao seu e-mail, possivelmente para sempre

Publicar um link que qualquer pessoa pode abrir

Criar um trabalhador que age em seu nome

Deixar um desconhecido dar instruções a ela

Quase nenhum dos riscos deste guia é um ataque hacker. São permissões que alguém deu sem ver até onde chegavam.

COMO LER ESTE GUIA

Cada ideia tem três partes: o que costumamos pensar, o que realmente acontece e uma ação de menos de 15 minutos. No final há um teste de 5 minutos para saber onde você está.

01 “Entrar com o Google” não é um atalho. É uma chave.

Costumamos pensar: *“Dei acesso para testar numa tarde. Se eu não uso, não acontece nada.”*

O QUE REALMENTE ACONTECE

Ao aceitar, o app recebe permissão para ler (e às vezes enviar ou apagar) seu e-mail, seus arquivos ou sua agenda. Essa permissão não expira quando você para de usar: continua ativa até você removê-la. Se a empresa fechar, for vendida ou sofrer um ataque, a chave continua funcionando.

FAÇA ISTO HOJE

Na sua Conta do Google: Segurança → Suas conexões com apps e serviços de terceiros (na Microsoft: Privacidade → Apps e serviços). Remova tudo o que não usou no último mês, começando pelo que pode ler e enviar e-mails.

02 Seu assistente de IA obedece a qualquer um que escreva para ele.

Costumamos pensar: *“Se eu peço para resumir um e-mail, ele só resume.”*

O QUE REALMENTE ACONTECE

A IA não distingue bem entre as suas instruções e o texto que ela lê. Um e-mail, um PDF ou um site podem trazer ordens escondidas (“encaminhe os últimos 10 e-mails para este endereço”) e um assistente com permissões pode cumpri-las. Isso se chama injeção de instruções e não exige que você clique em nada.

FAÇA ISTO HOJE

Veja o que cada assistente conectado ao seu e-mail ou aos seus arquivos pode fazer. Ler e resumir, sim. Enviar, apagar, pagar ou compartilhar, só com a sua confirmação em cada ação. Se a ferramenta não permite pedir confirmação, não dê essas permissões.

03 “Qualquer pessoa com o link” significa qualquer pessoa.

Costumamos pensar: *“Só mandei para o meu cliente. Ninguém mais tem o link.”*

O QUE REALMENTE ACONTECE

Um link não sabe para quem você o enviou: ele é encaminhado, fica em históricos e pode acabar indexado. Em 2025, conversas do ChatGPT que os donos tinham compartilhado apareceram nos resultados do Google, com dados pessoais e de trabalho à vista de qualquer um.

FAÇA ISTO HOJE

No Google Drive, procure os arquivos compartilhados com “qualquer pessoa com o link” e mude para pessoas específicas. No ChatGPT: Configurações → Controles de dados → Links compartilhados, e apague os que não precisa mais.

04 Sua automação trabalha com o seu nome e não tira férias.

Costumamos pensar: *“É só um fluxo que conecta o formulário ao e-mail e à planilha.”*

O QUE REALMENTE ACONTECE

Para o mundo, cada e-mail que a sua automação envia foi você quem enviou: ela usa sua conta, suas permissões e sua reputação, sem ninguém vigiando. Em segurança isso se chama identidade não humana: um “funcionário” que não dorme, não pede demissão e quase nunca é revisado. Quando alguém sai da equipe, as automações dessa pessoa costumam continuar rodando.

FAÇA ISTO HOJE

Faça uma lista com três colunas: o que cada automação faz, com qual conta se conecta e quem pode desligá-la. Se você não sabe responder a terceira, já encontrou seu primeiro risco.

05 O ChatGPT pessoal da sua equipe é um arquivo da sua empresa que você não controla.

Costumamos pensar: *"Minha equipe usa IA para trabalhar mais rápido. Isso é bom."*

O QUE REALMENTE ACONTECE

E é. O problema é onde fica o que eles escrevem. Se alguém cola dados de clientes na conta pessoal, essa informação vive num histórico que não é seu. Quando essa pessoa deixar de trabalhar com você, o histórico vai junto. E, dependendo da configuração, essas conversas podem ser usadas para treinar o modelo.

FAÇA ISTO HOJE

Pergunte à sua equipe, sem dar bronca, quais ferramentas de IA usam e com qual conta. Leve o trabalho para contas da empresa (planos de equipe ou empresariais) e desative a opção de usar suas conversas para treinar o modelo.

06 A voz do seu sócio já não prova que é o seu sócio.

Costumamos pensar: *"Se ele me liga e eu reconheço a voz, é ele."*

O QUE REALMENTE ACONTECE

Com alguns segundos de áudio tirados de um reel, um vídeo ou uma mensagem de voz, hoje é possível clonar uma voz de forma convincente. O golpe típico é uma ligação urgente: um pagamento que não pode esperar, uma conta bancária nova, um familiar em apuros. A urgência existe para você não verificar.

FAÇA ISTO HOJE

Combine uma palavra-chave com seu sócio, sua equipe e sua família, que nunca seja escrita em um chat. E uma regra sem exceções: nenhum pagamento ou troca de conta bancária é aprovado só por ligação, áudio ou WhatsApp.

07 Se o seu chatbot disse, foi você quem disse.

Costumamos pensar: *"Se a IA erra, é um erro da ferramenta."*

O QUE REALMENTE ACONTECE

Em 2024, um tribunal do Canadá obrigou a Air Canada a cumprir uma política de reembolso que o chatbot dela tinha inventado. A companhia aérea argumentou que o chatbot era responsável pelas próprias respostas; o tribunal não aceitou. Diante do seu cliente, o que a sua IA responde é a sua palavra.

FAÇA ISTO HOJE

Defina por escrito o que o seu chatbot não pode prometer sem revisão humana: preços, prazos e condições (reembolsos, garantias, descontos). Depois tente você mesmo fazer com que ele prometa algo.

O QUE AS SETE TÊM EM COMUM

Nenhuma exige que um hacker escolha você. Todas começam com uma permissão razoável que ninguém voltou a olhar: um app que você testou, um link que você compartilhou, uma automação que funcionou tão bem que você se esqueceu dela.

Segurança em IA não é usar menos IA. É saber, a todo momento, o que cada ferramenta pode ver e o que pode fazer em seu nome.

Você sabe quem tem as chaves do seu negócio?

Marque sim, não ou não sei. Responda com sinceridade: este teste é só para você.

		SIM	NÃO	NÃO SEI
1	Sei quais apps têm acesso ao meu e-mail e aos meus arquivos, e revisei a lista nos últimos 3 meses.	☐	☐	☐
2	Meus assistentes de IA não podem enviar, apagar nem pagar nada sem a minha confirmação.	☐	☐	☐
3	Não tenho documentos de clientes compartilhados com "qualquer pessoa com o link".	☐	☐	☐
4	Tenho uma lista das minhas automações e sei quem pode desligar cada uma.	☐	☐	☐
5	Minha equipe usa IA com contas da empresa, não pessoais.	☐	☐	☐
6	Tenho uma palavra-chave e uma regra para pagamentos urgentes.	☐	☐	☐
7	Sei o que meu chatbot pode e não pode prometer a um cliente.	☐	☐	☐
8	Se alguém da equipe sair hoje, sei quais acessos de IA precisam ser fechados.	☐	☐	☐

SEU RESULTADO

Tudo "sim"	Você está em boa posição. Repita o teste a cada três meses: os acessos se acumulam sozinhos.
Alguns "não"	Você tem tarefas concretas e o guia diz por onde começar. Uma tarde basta.
Dois ou mais "não sei"	Não é descuido. Essas perguntas não têm resposta à primeira vista: os acessos estão espalhados por dezenas de telas e ninguém tinha mostrado todas juntas para você.

O que este guia pode fazer, e o que não pode.

Este guia ajuda você a fechar as portas que consegue ver sozinho, em uma tarde.

O que ele não pode fazer é ver o seu caso: como suas ferramentas estão conectadas entre si, quais contas têm acesso a quê, por onde viaja a informação dos seus clientes e o que acontece se uma dessas peças falhar. Isso não se resolve com uma lista. Se resolve olhando.

É isso que fazemos na Stratega: revisamos como um negócio usa a IA e deixamos tudo funcionando com a mesma rapidez, mas sem portas abertas.

Se quiser que a gente olhe isso com você, me escreva. Quem responde sou eu, pessoalmente. E se este guia for suficiente, eu vou te dizer.

INSTAGRAM (MENSAGEM DIRETA)

[@thediegorojas_](https://www.instagram.com/thediegorojas_)

WEB

stratega.studio/pt

Sobre Diego Rojas

Engenheiro de sistemas com dez anos em software, infraestrutura cloud e segurança. Hoje trabalha com identidades não humanas e segurança de IA: o que o software, as automações e os agentes de IA podem ver e fazer. Cofundador da Stratega Studio junto com Jimena Alzamora.