IA no trabalho com segurança

Manual de boas práticas para o uso da IA generativa no setor administrativo

Emerson Lopes · Kamila da Silva · Miguel Máximo · Samuel Barbosa

Recife, 2026

PARA QUE SERVE ESTE MANUAL

A inteligência artificial generativa já faz parte da rotina administrativa: ela redige e-mails, resume documentos e ajuda a montar planilhas. Mas, na maioria das ferramentas, tudo o que você digita ou cola é enviado aos servidores da empresa que oferece o serviço.

Este manual mostra como aproveitar a IA sem expor dados de clientes, de colegas e da empresa. Ele responde a três perguntas:

1. O que posso compartilhar com a IA?

2. O que nunca devo compartilhar?

3. Como conferir o que ela me devolve?

Como usar: leia uma vez do início ao fim e volte ao Semáforo dos dados e ao Checklist sempre que tiver dúvida.

Sumário: 1. A IA generativa no trabalho · 2. Principais riscos · 3. Dados que exigem cuidado · Semáforo dos dados · 4. Boas práticas · Errei, e agora? · 5. Situações da rotina · O que diz a lei · Glossário · Para saber mais

1. A IA GENERATIVA NO TRABALHO

Pergunta-chave: o que é a IA generativa e como ela entra na sua rotina?

A IA generativa cria conteúdo novo, como textos, imagens, resumos e códigos, a partir das instruções que você escreve, os chamados prompts.

Ela não "sabe" as respostas: calcula as palavras mais prováveis com base nos dados com que foi treinada. Por isso, pode errar com muita segurança.

Na rotina administrativa, ela ajuda a:

- redigir e revisar e-mails e comunicados;
- resumir documentos e atas;
- criar fórmulas e organizar planilhas;
- preparar apresentações e relatórios.

Em números: 41,9% das indústrias pesquisadas pelo IBGE usaram IA em 2024 (em 2022, eram 16,9%). Entre elas, 87,9% usaram IA na área de administração. **Fonte: IBGE, PINTEC Semestral (2025).**

Lembre-se:

a IA é assistente. O responsável pelo resultado é você (CERT.br).

2. PRINCIPAIS RISCOS

Pergunta-chave: o que pode dar errado?

Vazamento de dados: o que você cola no chat pode ficar armazenado pelo fornecedor e, dependendo da ferramenta e das configurações, ser usado para treinar o modelo.

Alucinações: a IA pode inventar fatos, números, leis e até referências, e apresentar tudo com segurança.

Injeção de comandos: instruções escondidas em arquivos, e-mails ou páginas que você pede para a IA ler podem fazê-la agir contra você, por exemplo, revelando dados.

Golpes com deepfake: criminosos usam IA para imitar a voz e o rosto de chefes e colegas e pedir pagamentos ou senhas.

Vieses: a IA pode repetir preconceitos presentes nos dados de treinamento, o que é grave em tarefas como a triagem de currículos.

Lembre-se: a IA erra, pode ser enganada e pode ser usada por golpistas. Nunca confie nela cegamente.

Fontes: NIST AI 600-1; Barroso e Mello (2024); CERT.br; CGU.

3. DADOS QUE EXIGEM CUIDADO

Pergunta-chave: que informações merecem atenção antes de ir para a IA?

Dado pessoal:

qualquer informação que identifica ou pode identificar uma pessoa, como nome, CPF, RG, endereço, telefone, e-mail ou matrícula (LGPD, art. 5º, I).

Dado pessoal sensível:

dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização religiosa, filosófica ou política, saúde, vida sexual e dados genéticos ou biométricos. Exige proteção redobrada (LGPD, art. 5º, II).

Informação confidencial da empresa:

contratos, propostas comerciais, dados financeiros, planos estratégicos e relatórios internos. Quando não envolve dados de pessoas, fica fora da LGPD, mas é protegida por contratos e políticas de sigilo.

Atenção: no dia a dia, chamamos tudo isso de "dado sensível". Na LGPD, porém, "dado pessoal sensível" é só a segunda categoria.

Lembre-se:

se o dado identifica alguém ou é segredo da empresa, pare e consulte o Semáforo dos dados.

SEMÁFORO DOS DADOS

Antes de colar qualquer informação em uma ferramenta de IA, confira a cor:

VERDE – PODE USAR

Informação pública ou genérica.

Exemplos: textos já publicados no site da empresa, modelos de documento sem dados reais, dúvidas de Excel ou de redação.

AMARELO – CUIDADO

Informação interna não sigilosa ou dados sem identificação das pessoas. Use apenas em ferramenta autorizada pela empresa.

Exemplos: rascunho de comunicado interno, relatório só com totais por setor, sem nomes, CPF ou contatos.

VERMELHO – NÃO USE

Dados pessoais, dados pessoais sensíveis e informações confidenciais. Nunca em ferramentas públicas; só em sistema corporativo autorizado, quando a política da empresa permitir.

Exemplos: nome com CPF ou telefone de clientes, atestados e dados de saúde de funcionários, salários, contratos e planos estratégicos.

Atenção: senhas e credenciais de acesso não devem ser inseridas em nenhuma ferramenta de IA.

Fontes: LGPD; Guia IA Generativa (SGD/Serpro); Guia de uso de IA do Senado Federal; Guia da ANPD.

4. BOAS PRÁTICAS: CHECKLIST DO USO SEGURO

Pergunta-chave: como usar a IA sem expor ninguém?

Antes de enviar:

□ Estou usando uma ferramenta autorizada pela empresa, com a conta de trabalho, e não uma conta pessoal?

□ Retirei nomes, CPF, contatos, valores e tudo o que identifique pessoas ou a empresa?

□ Enviei só o trecho necessário, e não o documento inteiro?

□ Desativei o uso das conversas para treinar o modelo ou usei o chat temporário, quando a ferramenta oferece essas opções?

Ao receber a resposta:

□ Conferi números, datas, nomes e leis em fontes oficiais?

□ Desconfiei de links, pedidos estranhos ou instruções que a IA trouxe de arquivos e e-mails?

Ao usar o resultado:

□ Revisei o texto antes de enviar ou publicar?

□ Informei o uso de IA quando a empresa exige?

□ A decisão final foi tomada por uma pessoa?

Lembre-se: na dúvida, não cole. Pergunte à TI ou ao encarregado de dados.

Fontes: CGU; Guia IA Generativa (SGD/Serpro); Guia do Senado; CERT.br; LGPD.

ERREI, E AGORA?

Colou dados pessoais ou confidenciais em uma ferramenta de IA por engano? Siga estes passos:

---

1. Pare: não envie mais nenhuma informação nessa conversa.

2. Avise imediatamente o setor de TI, seu gestor ou o encarregado de dados.

3. Anote o que foi enviado, em qual ferramenta e quando.

4. Siga as orientações da TI, como apagar a conversa e trocar senhas que tenham sido expostas.

Por que avisar? A LGPD obriga a empresa a comunicar à ANPD e às pessoas afetadas os incidentes de segurança que possam causar risco ou dano relevante (art. 48). Quanto antes a empresa souber, menor o dano.

Prevenção: o guia da ANPD para pequenas empresas recomenda ter uma política de segurança da informação, treinar e conscientizar as equipes e controlar quem acessa os dados pessoais.

Lembre-se: errar acontece. Esconder o erro aumenta o dano.

5. SITUAÇÕES DA ROTINA (1/2)

Pergunta-chave: como fica na prática?

Caso 1 – Resumir a planilha de clientes

Jeito arriscado: colar a planilha com nomes, CPF e telefones no chat e pedir um resumo.

Jeito seguro: apagar as colunas que identificam os clientes ou pedir à IA só a fórmula para fazer o resumo no próprio Excel.

Caso 2 – E-mail de cobrança

Jeito arriscado: informar à IA o nome do cliente, o valor devido e o número do contrato.

Jeito seguro: pedir um modelo genérico ("e-mail cordial de cobrança de fatura em atraso") e preencher os dados reais depois, fora da IA.

Caso 3 – Contrato confidencial

Jeito arriscado: colar o contrato inteiro para a IA revisar.

Jeito seguro: usar só a ferramenta corporativa autorizada ou fazer uma pergunta genérica, como "o que costuma constar em uma cláusula de rescisão?", sem colar o texto. Em caso de dúvida, consulte o jurídico.

5. SITUAÇÕES DA ROTINA (2/2)

Caso 4 – Atestados médicos

Jeito arriscado: enviar fotos de atestados para a IA organizar uma planilha de afastamentos.

Jeito seguro: lançar os dados direto no sistema da empresa. Dados de saúde são dados pessoais sensíveis e não devem ir para ferramentas de IA públicas.

Caso 5 – Áudio do "diretor"

Situação: chega um áudio com a voz do diretor pedindo um pagamento urgente a um novo fornecedor.

Jeito arriscado: pagar porque "a voz é dele".

Jeito seguro: confirmar por outro canal, como uma ligação para o número que você já conhece, antes de qualquer transferência. A voz pode ter sido clonada com IA.

Caso 6 – Lei citada pela IA

Jeito arriscado: copiar para um documento oficial a lei e o artigo que a IA citou.

Jeito seguro: conferir o texto no site oficial (planalto.gov.br) antes de usar. A IA pode inventar leis, artigos e números.

O QUE DIZ A LEI

LGPD – Lei nº 13.709/2018 (em vigor)

- Define dado pessoal e dado pessoal sensível (art. 5º).
- Princípio da necessidade: usar apenas os dados indispensáveis para a finalidade (art. 6º, III).
- As empresas devem adotar medidas de segurança para proteger os dados pessoais (art. 46).
- Incidentes que possam causar risco ou dano relevante devem ser comunicados à ANPD e aos titulares (art. 48).
- O titular pode pedir a revisão de decisões tomadas apenas por meios automatizados (art. 20).

Regulação em andamento

PL nº 2.338/2023 – Marco legal da IA: aprovado pelo Senado em dezembro de 2024, está em análise na Câmara dos Deputados. Ainda não é lei (situação em novembro de 2026). Acompanhe em camara.leg.br.

GLOSSÁRIO

Alucinação: resposta falsa ou inventada que a IA apresenta como verdadeira.

Anonimização: uso de meios técnicos para que um dado não possa mais ser associado a uma pessoa.

Deepfake: áudio, imagem ou vídeo falso criado com IA para imitar uma pessoa real.

Encarregado de dados: pessoa indicada pela empresa para ser o canal de comunicação com os titulares e com a ANPD sobre proteção de dados.

IA generativa: tipo de IA que cria textos, imagens, áudios ou códigos a partir de instruções.

Injeção de comandos: ataque que esconde instruções em textos ou arquivos para manipular a IA.

Prompt: instrução ou pergunta que você escreve para a IA.

Titular: pessoa a quem os dados pessoais se referem.

PARA SABER MAIS

As orientações deste manual se baseiam nestas fontes:

- Lei nº 13.709/2018 – LGPD: planalto.gov.br
- Guia de uso responsável de IA generativa – CGU (2025): repositorio.cgu.gov.br
- IA Generativa no Serviço Público – SGD/MGI e Serpro (2025): gov.br/governodigital
- Guia de uso de IA – Senado Federal: senado.leg.br
- Cartilha de Segurança para Internet, fascículo Inteligência Artificial – CERT.br: cartilha.cert.br
- Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte – ANPD (2021): gov.br/anpd
- NIST AI 600-1: Generative AI Profile (2024): doi.org/10.6028/NIST.AI.600-1
- Barroso e Mello. Inteligência artificial: promessas, riscos e regulação (2024): doi.org/10.1590/2179-8966/2024/84479
- IBGE – PINTEC Semestral (2025): agenciadenoticias.ibge.gov.br
- PL nº 2.338/2023 – Marco legal da IA (em tramitação): camara.leg.br

A IA é assistente. O responsável é você.

Na dúvida, não cole: pergunte à TI ou ao encarregado de dados.

Elaborado por Emerson Lopes, Kamila da Silva, Miguel Máximo e Samuel Barbosa · Recife, 2026 · Versão 1.0