

GUIA PRÁTICO EM CINCO ETAPAS

Como usar IA sem expor dados **de auditoria.**

Para auditores e profissionais de GRC que já usam ChatGPT, Copilot, Claude ou Gemini no trabalho.

ETAPA 1

Entenda o risco

ETAPA 2

Faça e não faça

ETAPA 3

**Ajuste as
configurações**

ETAPA 4

Anonimize

ETAPA 5

Registre e valide

CONTEXTO

O risco começa antes de qualquer política ser aprovada.

A discussão sobre IA em GRC costuma parar no plano da estratégia. A governança de dados fica para a fase de implementação. Enquanto o projeto não sai do papel, o auditor abre uma janela de IA no meio da manhã e cola ali um trecho de papel de trabalho para resumir.

A exposição começa nesse gesto, meses antes de qualquer política ser aprovada. Este guia não pede que você pare de usar IA. Ele mostra onde está a configuração mais permissiva e o que fazer diferente hoje, sem esperar o projeto de governança formal.

3 anos

Tempo que o Google mantém conversas revisadas por humanos, mesmo após o usuário apagar a atividade.

30 dias

Prazo da OpenAI para excluir chats temporários, que não entram na memória da conta.

0

Telas de IA que mostram esses prazos no momento em que você digita.

ENTENDA ANTES DE AGIR

Saiba o que acontece com o que você cola.

Em conta pessoal, o que você envia alimenta o serviço de duas formas: o histórico, consultado depois para personalizar respostas, e a melhoria do próprio modelo, que pode incluir revisão feita por pessoas.



Os prazos estão publicados

O Google informa que conversas analisadas por revisores humanos ficam armazenadas por até três anos, desvinculadas da conta, e que não somem quando o usuário apaga a atividade. A OpenAI informa que chats temporários são excluídos em 30 dias.



A memória devolve o que guardou

Um número de contrato citado em março volta como contexto em julho, porque a memória guardou o que pareceu relevante. Informação de um trabalho reaparece no meio de outro sem que ninguém tenha autorizado.

Na prática: trate qualquer campo de texto de uma IA pública como um canal que guarda o que recebe por padrão. A exceção precisa ser configurada, não assumida.

GUIA RÁPIDO

Faça isto, não isto.

FAÇA

- ✓ Entrar com a conta corporativa contratada pela empresa.
- ✓ Trocar nome de cliente, CNPJ e número de contrato por rótulos antes de colar.
- ✓ Descrever a situação e pedir o raciocínio, em vez de anexar o documento.
- ✓ Abrir conversa temporária quando a consulta for pontual.
- ✓ Revisar as configurações de privacidade a cada trimestre, porque elas mudam.
- ✓ Registrar no GRC a conclusão e a base que sustentou a análise.

NÃO FAÇA

- ⚠ Usar a conta pessoal porque o login já estava aberto.
- ⚠ Colar papel de trabalho, laudo ou evidência bruta em ferramenta pública.
- ⚠ Informar valores, saldos, dados pessoais ou nomes de pessoas sob apuração.
- ⚠ Conectar a IA ao e-mail ou à nuvem corporativa sem aval da TI.
- ⚠ Compartilhar link de conversa com informação de cliente ou processo interno.
- ⚠ Supor que assinatura paga significa dado protegido.

AÇÃO IMEDIATA

Ajuste as configurações **hoje.**

Comece pela conta. No Microsoft 365 Copilot Chat, um selo de proteção de dados empresarial aparece ao lado das respostas quando você está autenticado com a conta de trabalho. Sem o selo, a sessão está com proteção de nível pessoal.



ChatGPT

Configurações → Controles de dados

Desative "Melhorar o modelo para todos". As conversas seguem no histórico e param de alimentar o treinamento.



Claude

Configurações → Privacidade

Desligue a opção de ajudar a melhorar o Claude.



Gemini

Configurações → Atividade

Desative "Manter atividade" ou use a conversa momentânea.



Microsoft 365 Copilot

Login com conta de trabalho

Confirme a presença do selo de proteção de dados empresarial. Sem o selo, acione a TI.

Revise também a memória e os aplicativos conectados: cada integração com e-mail, agenda ou nuvem amplia o que o assistente enxerga sem nova autorização sua.

ANTES DE COLAR

Anonimize em **dois minutos**.

- 1 Troque o nome do cliente por "Fornecedor A" e a unidade por "Unidade 2".
- 2 Substitua CNPJ e número de contrato por rótulos.
- 3 Guarde a correspondência entre rótulo e dado real em uma planilha fora da ferramenta de IA.
- 4 Teste: a resposta mudaria com o dado real ali? Na maior parte das análises de risco, controle e plano de ação, a resposta é não.
- 5 Para valores exatos, use faixas. Saldo, provisão e perda operacional identificam a empresa com precisão maior do que o nome dela.



Por que funciona?

O que você quer da IA é raciocínio sobre a estrutura do problema, e a estrutura sobrevive à troca de nomes.

FECHA O CICLO

Registre e valide.

A LGPD trata dado pessoal onde quer que ele esteja. A ferramenta escolhida para acelerar o trabalho não muda essa condição.



A responsabilidade continua sendo sua

Nenhuma IA assina papel de trabalho nem presta contas ao comitê de auditoria. Ela ajuda a chegar mais rápido a uma hipótese. A validação continua humana, com registro no GRC e rastro de quem decidiu o quê.

CHECKLIST DE FECHAMENTO

- ✓ A conclusão está registrada no GRC.
- ✓ A base que sustentou a análise está documentada.
- ✓ Há rastro de quem validou o resultado antes de ele virar posição da auditoria.



CONTINUE NESSA DIREÇÃO

PRÓXIMO PASSO

A Plataforma Perinity GRC leva a Audara para dentro do seu **ambiente de trabalho**.

Governança de dados, classificação da informação e soberania definidas antes da funcionalidade. Veja como a Audara se aplica à rotina da sua auditoria.

Conhecer a Plataforma Perinity

www.perinity.com.br

Perinity GRC · plataforma corporativa de Governança, Riscos e Compliance · ISO 27001 e SOC 2