

TPL-03

# Checklist de shadow AI em 14 dias

Capítulo 3 | Revisão 3 da editora, p. 124 | Digital v1.0

Plano mínimo de quatorze dias para sair de risco desconhecido para risco mapeado; não substitui um programa completo de governança.

## Como usar

- Execute as etapas no intervalo de dias indicado e registre a conclusão, a data, a evidência e o responsável.
- O objetivo é saber o que existe e onde estão os riscos não governados.
- Use a redução mensurável do uso não sancionado e de dados sensíveis em ferramentas não corporativas como critério de sucesso.

Duplique os blocos conforme o número de registros. Para adaptar livremente, use a versão Word ou planilha.

## Dias 1 a 5: Inventário mínimo

Responsável: CISO. Fontes: telemetria de rede e endpoint (DLP, CASB, proxy); levantamento direto com líderes de área; e revisão de contratos e faturas, inclusive compras departamentais que passam pelo financeiro, mas não por TI.

Ferramenta

Área

Volume estimado de uso

Opções: Alto / Médio / Baixo

Tipo de dado envolvido

Opções: Sensível / Não sensível / Desconhecido

Status

Opções: Homologada / Não homologada / Desconhecida

Concluído?

Opções: Sim / Não

Data

Evidência

Responsável

### Dias 3 a 7: Classificação de risco

Responsáveis: CISO e jurídico. Classificar cada ferramenta por contrato, controles de dados, termos de serviço, residência de dados e compatibilidade com LGPD/GDPR.

Classificação

Opções: Liberada / Restrita / Proibida

Justificativa e evidência

Liberada: contrato avaliado e controles de dados ativos. Restrita: permitida para dados não sensíveis, mediante orientação. Proibida: não atende confidencialidade, retenção ou compliance.

Dados usados para treinamento?

Onde operam os servidores?

Concluído?

Opções: Sim / Não

Data

CISO responsável

Responsável jurídico

## Dias 5 a 10: Política mínima

Responsável: CIO. Diretriz operacional de no máximo duas páginas, com o que é permitido, o que é proibido e como solicitar exceção com resposta em 48 horas.

O que é permitido

Categorias e ferramentas liberadas.

O que é proibido

Inclui inserção de dados confidenciais, pessoais ou proprietários em ferramentas públicas não corporativas.

Como solicitar exceção

Trilha formal com resposta em 48 horas.

Dono da política

CIO.

### Aprovação executiva

CEO ou sponsor.

### Data de revisão

Trimestral.

### Concluído?

Opções: Sim / Não

### Data de publicação

### Evidência

## Dias 7 a 12: Trilha de exceção operacional

Responsável: CIO, com execução pelo Head de IA ou equivalente. Criar canal simples: formulário, e-mail ou ticket ITSM.

### Canal de solicitação

Opções: Formulário / E-mail / Ticket ITSM

### Descrição ou endereço do canal

### Taxa de solicitações

### Taxa de uso não sancionado

Concluído?

Opções: Sim / Não

Data

Evidência de teste

CIO responsável

Executor (Head de IA ou equivalente)

## Dias 10 a 14: Comunicação e monitoramento

Responsável pela comunicação: CEO. Responsável pelo monitoramento: CISO. O CEO comunica a diretriz como regra de negócio, não como restrição técnica; o CISO monitora telemetria e reporta mensalmente ao CIO.

Ferramentas de IA detectadas

Homologadas e não homologadas.

Volume de dados em ferramentas não corporativas

Solicitações de exceção recebidas

Incidentes de dados sensíveis em ferramentas proibidas

Concluído?

Opções: Sim / Não

Data

Evidência da comunicação e relatório baseline

CEO responsável

CISO responsável

## Regras para fechar a decisão

- A entrega da primeira etapa é uma lista com ferramenta, área, volume estimado, tipo de dado e status.
- A entrega da segunda etapa é o inventário classificado.
- A entrega da terceira etapa é a política publicada.
- A entrega da quarta etapa é o canal ativo e testado.
- A entrega da quinta etapa é a comunicação realizada e o relatório baseline gerado.
- Se solicitações são poucas e uso não sancionado é alto, a trilha de exceção não está funcionando.
- A métrica não é zero shadow AI; é redução mensurável do uso não sancionado e do volume de dados sensíveis em ferramentas não corporativas.